Horizon Console 管理指南

2019 年 12 月
VMware Horizon 7 7.11

vmware®

您可以从 VMware 网站下载最新的技术文档：

https://docs.vmware.com/cn/。

如果您对本文档有任何意见或建议，请将反馈信息发送至：

docfeedback@vmware.com

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

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

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

VMware Horizon Console 管理指南

1

《VMware Horizon Console 管理指南》介绍了如何在 Horizon Console 中配置和管理 VMware Horizon® 7、如何创建管理员、如何设置用户身份验证，以及如何配置策略和执行管理任务。本文档还介绍了如何对 Horizon 7 组件进行维护和故障排除。

有关如何使用 Horizon Console 配置和管理 Cloud Pod 架构环境的信息，请参阅《在 Horizon 7 中管理 Cloud Pod 架构》文档。

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。本文档中的信息专为已熟练掌握虚拟机技术和数据中心操作并且具有丰富经验的 Windows 或 Linux 系统管理员所编写。

使用 VMware Horizon Console

2

VMware Horizon Console 是最新版本的 Web 界面，您可以通过该控制台创建和管理虚拟桌面及已发布的桌面和应用程序。Horizon Console 还集成了用于管理工作区的 VMware Horizon Just-in-Time Management Platform (JMP) 集成工作流功能。

安装并配置 Horizon 连接服务器后，便可以使用 Horizon Console。

有关 JMP 集成工作流功能的更多信息，请参阅第 10 章 JMP Integrated Workflow 入门。

本章讨论了以下主题：

支持的 Horizon 7 功能

Horizon Console 基于 HTML5 技术，可用于管理完整的 Horizon 7 部署。Horizon Console 将取代基于 Flash 的 Horizon Administrator。

有关 Horizon Administrator 支持的 Horizon 7 功能的信息，请参阅《Horizon 7 管理指南》文档。

支持以下功能：

- 服务器
  - Horizon 连接服务器配置
  - 事件数据库
- 授权
  - 用户和组授权
  - 桌面授权
  - 应用程序授权
  - 全局授权

    - 全局策略
- 身份验证
    - 远程访问身份验证
    - 已发布应用程序的未验证访问
    - 智能卡身份验证
    - 基于角色的委托管理
- 虚拟桌面
    - 完整虚拟机的自动专用分配池
    - 自动即时克隆专用分配池和浮动分配池
    - 自动链接克隆桌面池
    - 完整虚拟机的自动浮动分配池
    - 手动桌面池
    - 永久磁盘
- 已发布的桌面
    - 手动场
    - 自动即时克隆场
    - 自动链接克隆场
    - RDS 桌面池
- 已发布的应用程序
    - 手动应用程序池
    - 基于现有应用程序的应用程序池
- 虚拟机
    - vCenter Server 中的可用虚拟机
    - vCenter Server 中的不可用已注册计算机
- Cloud Pod 架构

不支持以下功能：

- ThinApp 应用程序
- 安全服务器
- Mirage 服务器

使用 Horizon Console 的优势

使用 Horizon Console 的优势包括：能够简化桌面和应用程序部署过程，交付 Just-in-Time 桌面，以及提供更安全的 Web 界面以消除安全风险。

Horizon Console Web 界面进行了更新，为部署桌面和应用程序及进行故障排除提供了一些易于使用的工作流。

Horizon Console 中还包含 JMP Integrated Workflow 功能，这些功能将即时克隆、VMware App Volumes 和 VMware Dynamic Environment Manager 技术纳入到一个集成的工作流中，以便交付可快速部署和扩展的按需桌面。有关更多信息，请参阅关于 JMP Integrated Workflow。

Horizon Console 具有基于 HTML5 的 Web 界面，此界面已经更新，消除了许多安全风险和漏洞，因此更加安全。

安装和配置 Horizon Console

在您使用 Horizon 连接服务器安装程序安装并配置连接服务器后，可从 Horizon Administrator Web 界面中访问 Horizon Console URL。使用 JMP Server 安装程序安装并配置 JMP Server 之后，可在 Horizon Console 中使用 JMP Integrated Workflow。

有关安装连接服务器的更多信息，请参阅《Horizon 7 安装指南》文档。

有关安装和配置 JMP Server 的更多信息，请参阅《VMware Horizon JMP Server 安装和设置指南》文档。

登录到 Horizon Console

要执行桌面或应用程序池部署任务、故障排除任务或管理 JMP 工作流，您必须登录到 Horizon Console。您可以通过使用安全 (TLS) 连接访问 Horizon Console。

前提条件

- 确认已在专用计算机上安装 Horizon 连接服务器。
- 必须为用户分配任何预定义的角色或预定义角色的组合才能使其登录到 Horizon Console。在为用户分配自定义角色或预定义角色和自定义角色的组合时，您无法登录到 Horizon Console。有关配置基于角色的访问权限的更多信息，请参阅配置基于角色的委托管理。
- 确认您使用的是 Horizon Console 支持的 Web 浏览器。有关受支持 Web 浏览器的更多信息，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，所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 Console 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
为连接服务器配置一个由 CA 签发的证书。	首次连接时，Web 浏览器会显示**欢迎使用 VMware Horizon 7** 页面。
配置了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 要始终使用 Horizon Console 登录页面，请单击**始终使用此选项**。

注 如果您单击**始终使用此选项**并单击**启动**，则下次在 Web 浏览器中打开标签页并输入 **https://server/admin** 时，您将始终会看到 Horizon Console 登录页面。要再次访问**欢迎使用 VMware Horizon 7** 页面，请转到 **https://server/admin/#home**。

3 单击 Horizon Console 下的**启动**以打开 Horizon Console 登录页面。

4 以具有管理员帐户访问凭据的用户身份登录。

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。

后续步骤

要确定正在使用的连接服务器的 CPA 容器或群集名称，可以在 Horizon Console 标题和 Web 浏览器选项卡中查看此名称。

在 Horizon Console 中配置 Horizon 连接服务器

3

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 Horizon Composer 服务、设置可委派管理员职责的角色以及创建配置数据备份计划。

本章讨论了以下主题：

在 Horizon Console 中配置 vCenter Server 和 Horizon Composer

要将虚拟机用作远程桌面，必须配置 Horizon 7，使其与 vCenter Server 通信。要创建和管理链接克隆桌面池，必须在 Horizon Console 中配置 Horizon 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 Horizon Storage Accelerator。

为 Horizon Composer AD 操作创建用户帐户

如果您使用 Horizon Composer，则必须在 Active Directory 中创建一个用户帐户，以允许 Horizon Composer 在 Active Directory 中执行特定操作。Horizon 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。

为了确保安全，请创建一个单独的用户帐户以用于 Horizon Composer。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，Horizon 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 Console 中执行以下操作时指定该帐户：在**添加 vCenter Server** 向导中配置 Horizon Composer 域，以及配置和部署链接克隆桌面池。

在 Horizon Console 中安装产品许可证密钥

您必须先输入产品许可证密钥，然后才能使用连接服务器。

注 如果您拥有 Horizon 7 订阅许可证，则不需要产品许可证密钥。有关订阅许可证的更多信息，请参阅《Horizon 7 安装指南》文档中的“为订阅许可证启用 Horizon 7”。

首次登录时，Horizon Console 会显示“许可和使用情况”页面。

安装连接服务器副本实例或安全服务器时，不需要配置许可证密钥。副本实例和安全服务器使用存储在 View LDAP 配置中的通用许可证密钥。

注 连接服务器需要有效的许可证密钥。产品许可证密钥是一个包含 25 个字符的密钥。

步骤

1 在 Horizon Console 中，选择**设置 > 产品许可和使用情况**。

2 在**许可设置**面板中，单击**编辑许可证**。

3 输入许可证序列号，然后单击**确定**。

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。

在 Horizon Console 中将 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 (TLS) 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 Horizon 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 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 Horizon Composer 最大操作数限制的设置。

步骤

1 在 Horizon Console 中，导航到**设置 > 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 （可选） 如果 vCenter Server 部署在 VMware Cloud on AWS 上，请选择 **VMware Cloud on AWS**。

有关将 Horizon 7 与 VMware Cloud on AWS 集成的更多信息，请参阅《Horizon 7 集成指南》文档。

9 在“高级设置”下，设置 vCenter Server 和 Horizon Composer 操作的并发操作数限制。

10 单击**下一步**，然后按照提示完成向导。

后续步骤

配置 Horizon Composer 设置。

- 如果为 vCenter Server 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“Horizon 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 Horizon Composer 设置

要使用 Horizon Composer，您必须配置允许 Horizon 7 连接到 Horizon Composer 服务的设置。Horizon 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 Horizon Composer 服务和 vCenter Server 实例之间必须存在一对一的映射关系。每个 Horizon Composer 服务仅适用于一个 vCenter Server 实例。每个 vCenter Server 实例仅能与一个 Horizon Composer 服务相关联。

完成初始 Horizon 7 部署后，您可以将 Horizon Composer 服务迁移到新的主机以支持对 Horizon 7 部署进行扩展或更改。您可以在 Horizon Console 中编辑初始 Horizon Composer 设置，但是必须执行其他一些步骤来确保迁移成功。

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 Horizon 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。请参阅在 Horizon Console 中将 vCenter Server 实例添加到 Horizon 7。
- 确认该 Horizon Composer 服务尚未配置为连接到不同的 vCenter Server 实例。

步骤

1. 在 Horizon Console 中，导航到**设置 > 服务器**。
2. 在 **vCenter Server** 选项卡上，单击**添加**并填写 **vCenter Server 设置**页面上的 vCenter Server 信息，然后单击**下一步**。
3. 在 **Horizon Composer 设置**页面上，如果您未使用 Horizon Composer，请选择**不使用 Horizon Composer**。

   如果选择**不使用 Horizon Composer**，则其他的 Horizon 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。

4 如果您使用 Horizon Composer，请选择 Horizon Composer 主机的位置。

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

5 单击**下一步**以显示 **Horizon Composer 域**页面。

后续步骤

配置 Horizon Composer 域。

- 如果为 Horizon 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“Horizon Composer 域”页面。
- 如果为 Horizon 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。

配置 Horizon Composer 域

您必须配置一个 Active Directory 域，以便 Horizon Composer 在其中部署链接克隆桌面。您可以为 Horizon Composer 配置多个域。首次将 vCenter Server 和 Horizon Composer 设置添加到 Horizon 7 后，您可以通过在 Horizon Console 中编辑 vCenter Server 实例来添加更多 Horizon Composer 域。

前提条件

- 您的 Active Directory 管理员必须为 AD 操作创建 Horizon 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，请参阅为 Horizon Composer AD 操作创建用户帐户。
- 在 Horizon Console 中，确认您已完成**添加 vCenter Server** 向导中的 **vCenter Server 设置**和 **Horizon Composer 设置**页面。

步骤

1 在 Horizon Console 中，导航到**设置 > 服务器**。

2 在 **vCenter Server** 选项卡上，单击**添加**并填写 **vCenter Server 设置**页面上的 vCenter Server 信息，然后单击**下一步**。

3 在 **Horizon Composer 设置**页面上，如果您使用 Horizon Composer，请选择 Horizon Composer 主机的位置，然后单击**下一步**。

有关 Horizon Composer 的更多信息，请参阅配置 Horizon Composer 设置。

4 在 **Horizon Composer 域**页面上，单击**添加**，为 AD 操作帐户信息添加 Horizon Composer 用户。

5 键入 Active Directry 域的域名。

例如：`domain.com`

6 键入 Horizon Composer 用户的域用户名，包括域名。

例如：`domain.com\admin`

7 键入帐户密码。

8 单击**确定**。

9 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。

10 单击**下一步**以显示**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 Horizon Storage Accelerator。

在 Horizon Console 中添加即时克隆域管理员

必须先向 Horizon 7 中添加即时克隆域管理员，然后才能创建即时克隆桌面池。

前提条件

- 确认即时克隆域管理员具有所需的 Active Directory 域特权。有关更多信息，请参阅《Horizon 7 安装指南》文档中的“为即时克隆操作创建用户帐户”。

步骤

1 在 Horizon Console 中，选择**设置 > 即时克隆域帐户**。

2 单击**添加**。

3 选择即时克隆域管理员的域。

4 输入用户名和密码。

后续步骤

在 Horizon Console 中，您可以添加或移除即时克隆域管理员，也可以将即时克隆管理员列表导出到 Microsoft Excel。导航到**设置 > 即时克隆域帐户**，然后选择一个即时克隆域管理员。单击**编辑**可编辑该管理员的域和登录信息。单击**移除**可移除管理员。单击“导出”图标可将即时克隆管理员列表导出到 Microsoft Excel 文件。

允许 vSphere 回收链接克隆虚拟机中的磁盘空间

在 vSphere 版本 5.1 或更高版本中，可以启用 Horizon 7 的磁盘空间回收功能。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 版本 5.1 或更高版本中，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 Console 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。
- 不会影响 Horizon Composer 永久磁盘。
- 仅适用于虚拟硬件版本为 9 或更高版本的虚拟机上的 vSphere 版本 5.1 或更高版本。
- 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 Console 中，导航到**设置 > 服务器**。

2 在 **vCenter Server** 选项卡上，单击**添加**，然后完成**添加 vCenter Server** 向导页面，之后会显示**存储设置**页面。

3 在**存储设置**页面上，选择**回收虚拟机磁盘空间**。

如果是执行 Horizon 7 的全新安装，则默认已选中此选项。如果是升级到 Horizon 7 的更高版本，则必须选择**回收虚拟机磁盘空间**。

后续步骤

在**存储设置**页面上，配置 Horizon 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 Horizon Storage Accelerator

在 vSphere 中，您可以将 ESXi 主机配置为缓存虚拟机磁盘数据。这项称为 Horizon Storage Accelerator 的功能可以使用 ESXi 主机中的 Content Based Read Cache (CBRC) 功能。Horizon 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。

通过在发生引导风暴时减少 IOPS 数量，Horizon Storage Accelerator 可降低对存储阵列的需求，使您能够用更少的存储 I/O 带宽支持 Horizon 7 部署。

您需要按照此过程中所述，在 Horizon Console 的**添加 vCenter Server** 向导中选择 Horizon Storage Accelerator 设置，以启用 ESXi 主机上的缓存功能。

请确保也为各桌面池配置了 Horizon Storage Accelerator。要对某个桌面池进行操作，必须为 vCenter Server 和该桌面池启用 Horizon Storage Accelerator。

默认情况下，会为桌面池启用 Horizon 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池中启用 Horizon Storage Accelerator。

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

Horizon Storage Accelerator 现在可在使用 Horizon 7 副本分层的配置下运行，在此配置下，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 Storage Accelerator 与 Horizon 7 副本分层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。

重要事项 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 Horizon 7 容器，则必须为共享的 ESXi 主机上的所有池启用 Horizon 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》文档中有关介绍 vCenter Server 用户所需的 Horizon 7 和 Horizon Composer 特权的主题。

步骤

1 在 Horizon Console 中，导航到**设置 > 服务器**。

2 在 **vCenter Server** 选项卡上，单击**添加**，然后完成**添加 vCenter Server** 向导页面，完成这些页面后会显示**存储设置**页面。

3 在**存储设置**页面上，选择**启用 Horizon Storage Accelerator**。

默认情况下，此选项处于选定状态。

4 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。

5 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**。

6 在“存储设置”页面上，单击**下一步**。

7 检查**即将完成**页面上的设置后，单击**提交**。

后续步骤

配置客户端会话和连接设置。请参阅《Horizon 7 管理指南》文档中的“配置客户端会话设置”。

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

vCenter Server 和 Horizon 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 Horizon Composer 所执行的并发操作的最大数量。

可以在**添加 vCenter Server** 向导的 **vCenter Server 设置**页面上的“高级设置”面板中配置这些选项。

表 3-1. vCenter Server 和 Horizon Composer 的并发操作数限制

设置	说明
最大并发 vCenter 置备操作数量	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。 默认值为 20。 此设置仅适用于完整的虚拟机。
最大并发电源操作数量	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）。 默认值为 50。 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。 此设置适用于完整的虚拟机和链接克隆。

表 3-1. vCenter Server 和 Horizon Composer 的并发操作数限制 （续）

设置	说明
最大并发 Horizon Composer 维护操作数	确定在此 Horizon Composer 实例所管理的链接克隆上可以发生的最大并发 Horizon Composer 刷新、重构和重新平衡操作数。 默认值为 12。 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。 此设置仅适用于链接克隆。
最大并发 Horizon Composer 置备操作数	确定在此 Horizon 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。 默认值为 8。 此设置仅适用于链接克隆。
最大并发即时克隆引擎操作数	确定在此 vCenter Server 实例所管理的即时克隆上可以发生的最大并发创建和删除操作数。 此设置仅适用于即时克隆。

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 Horizon Composer 实例时，必须确保用于 vCenter Server 和 Horizon Composer 实例的 TLS 证书有效且受连接服务器信任。如果随 vCenter Server 和 Horizon 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 Horizon 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 Horizon 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 Horizon 7 Server 配置 TLS 证书”。

您需要首先在 Horizon Console 中使用**添加 vCenter Server** 向导添加 vCenter Server 和 Horizon 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 vCenter Server。

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 Horizon 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。

步骤

1 当 Horizon Console 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 Horizon Composer 实例配置的证书指纹。

   a 在 vCenter Server 或 Horizon Composer 主机上，启动 MMC 管理单元并打开 Windows 证书存储区。

   b 导航到 vCenter Server 或 Horizon 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 Horizon 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 Horizon 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 Console 中，导航到**设置 > 服务器**。

2 在 **vCenter Server** 选项卡上，选择 vCenter Server 实例。

3 单击**移除**。

此时会显示一条对话框消息，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 Horizon Composer

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

在禁用与 Horizon Composer 的连接之前，您必须从 Horizon 7 中移除由 Horizon Composer 创建的所有链接克隆虚拟机。如果仍存在任何关联的链接克隆，Horizon 7 会阻止您移除 Horizon Composer。禁用与 Horizon 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 Horizon Composer 创建的链接克隆桌面池。

a 在 Horizon Console 中，选择**清单 > 桌面**。

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，还将移除关联的 Horizon Composer 数据库条目以及由 Horizon Composer 创建的副本。

d 对由 Horizon Composer 创建的每个链接克隆桌面池重复执行这些步骤。

2 导航到**设置 > 服务器**。

3 在 **vCenter Server** 选项卡上，选择与 Horizon Composer 关联的 vCenter Server 实例。

4 单击**编辑**。

5 在 **Horizon Composer** 选项卡上的“Horizon Composer Server 设置”下方，选择**不使用 Horizon 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 Horizon Composer 并将 Horizon 7 重新配置为连接到新的 Horizon Composer 服务，则必须执行一些额外的步骤。有关如何在不迁移链接克隆虚拟机的情况下迁移 Horizon Composer 的更多信息，请参阅《Horizon 7 管理指南》文档。

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。

在 Horizon Console 中备份 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 Horizon 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 Horizon 连接服务器和 Horizon Composer 数据。

在 Horizon Console 中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。

Horizon Console 中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 Console 中的状态更新、是否显示登录前提示和警告消息、Horizon Console 是否将 Windows Server 视为支持的远程桌面操作系统，以及其他设置。

在 Horizon Console 中，您可以通过导航到**设置 > 全局设置 > 常规设置**来配置全局设置。

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 3-2. 客户端会话的常规全局设置

设置	说明
View Administrator 会话超时	确定 Horizon Console 会话持续闲置多久后超时。 **重要事项** Horizon Console 会话超时值（以分钟为单位）设置较高会增加未授权使用 Horizon Console 的风险。允许闲置会话持续较长时间时应慎重考虑。 默认情况下，Horizon Console 会话超时为 30 分钟。可将会话超时时间设置为 10 到 4320 分钟（72 小时）间的任何值。 在会话超时之前，会显示一条有 60 秒倒计时的警告消息。如果在倒计时结束前单击会话，会话将继续。60 秒后，将显示一条错误消息，通知您会话已超时，您需要重新登录。
强制断开用户连接	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。 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。 默认值为 **600 分钟之后**。
单点登录 (SSO)	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**。 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。 **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。
启用自动状态更新	确定 Horizon Console 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 Console 的仪表板页面也会每隔几分钟更新一次。 默认情况下不启用此设置。

表 3-2. 客户端会话的常规全局设置 （续）

设置	说明
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:**	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。 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。 **重要事项** 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。 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**。
其他客户端。 **放弃 SSO 凭据:**	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。 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）。 默认值为 **15 分钟之后**。
显示登录前的消息	当 Horizon Client 用户登录时，向其显示免责声明或其他消息。 在“全局设置”对话框的文本框中键入您的信息或说明。 如果不希望显示任何消息，请不要选中该复选框。
强制注销前显示警告	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。 选中该框可显示警告消息。 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。 键入您的警告消息。您可以使用默认的消息： 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。
启用 Windows Server 桌面	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 Console 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。 **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。

表 3-2. 客户端会话的常规全局设置 （续）

设置	说明
关闭 HTML Access 的选项卡时清除凭据	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。 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： ■ 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。 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。 注 此功能在 Horizon 7 版本 7.0.2 及更高版本中可用。
在客户端用户界面中隐藏服务器信息	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。
在客户端用户界面中隐藏域列表	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。 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 `domain\username` 或 `username@domain` 格式输入其用户名。 **重要事项** 如果启用**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。如果具有单个用户域，则该功能不适用于 Horizon Client 5.0 和更高版本。 **重要事项** 有关该设置的安全性和可用性影响的更多信息，请参阅《Horizon 7 安全指南》文档。
发送域列表	如果选中该复选框，则允许连接服务器在验证用户身份之前将域名列表发送到客户端。 **重要事项** 有关该设置的安全性和可用性影响的更多信息，请参阅《Horizon 7 安全指南》文档。

Horizon Console 中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增强安全状态。

在 Horizon Console 中，您可以通过导航到**设置 > 全局设置 > 安全性设置**来配置全局安全设置。

到 Horizon 7 的所有 Horizon Client 连接和 Horizon Console 连接都需要使用 TLS。如果您的 Horizon 7 部署使用负载平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平衡器或中间服务器，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。

表 3-3. 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	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。 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。 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。 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。 不使用安全加密链路时，此设置无效。
消息安全模式	确定用于在各个组件之间发送 JMS 消息的安全机制 ■ 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。 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。
增强安全状态（只读）	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： ■ **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。

Horizon Console 中客户端会话的全局客户端限制设置

全局客户端限制设置可将虚拟桌面、已发布桌面和已发布应用程序的启动限制为特定客户端和版本。

在 Horizon Console 中，通过导航到**设置 > 全局设置 > 客户端限制设置**并输入 Horizon Client 的版本，可以配置全局客户端限制设置。

Horizon Client 必须是版本 4.5.0 或更高版本，但适用于 Chrome 的 Horizon Client 除外，后者必须是版本 4.8.0 或更高版本。配置此功能后，将阻止更低版本的 Horizon Client 连接到远程桌面和已发布的应用程序。

注　客户端限制设置仅阻止最终用户启动远程桌面和已发布的应用程序。此功能不会阻止最终用户登录 Horizon 7。

表 3-4. 客户端会话的全局客户端限制设置

设置	说明
适用于 Windows 的 Horizon Client	输入 Horizon Client 的版本号，此版本号需要为 4.5.0 或更高版本。
适用于 Linux 的 Horizon Client	输入 Horizon Client 的版本号，此版本号需要为 4.5.0 或更高版本。

表 3-4. 客户端会话的全局客户端限制设置 （续）

设置	说明
适用于 Mac 的 Horizon Client	输入 Horizon Client 的版本号，此版本号需要为 4.5.0 或更高版本。
适用于 iOS 的 Horizon Client	输入 Horizon Client 的版本号，此版本号需要为 4.5.0 或更高版本。
适用于 Android 的 Horizon Client	输入 Horizon Client 的版本号，此版本号需要为 4.5.0 或更高版本。
适用于 UWP 的 Horizon Client	输入 Horizon Client 的版本号，此版本号需要为 4.5.0 或更高版本。
适用于 Chrome 的 Horizon Client	输入 Horizon Client 的版本号，此版本号需要为 4.8.0 或更高版本。
适用于 HTML Access 的 Horizon Client	输入 Horizon Client 的版本号，此版本号需要为 4.5.0 或更高版本。
阻止其他客户端	如果选择此选项，将阻止所有其他类型的客户端（加入白名单的 Horizon Client 除外）启动任何桌面或已发布的应用程序。 但是，如果您希望最终用户使用其他类型的客户端来启动桌面和已发布的应用程序，就必须将该客户端类型添加到 `pae-AdditionalClientTypes` LDAP 属性才能绕过该客户端类型的阻止设置。 您可以使用“ADSI 编辑”实用程序来编辑连接服务器上的 LDAP 属性。 在“ADSI 编辑”实用程序中，`pae-AdditionalClientTypes` LDAP 属性在 `CN=Common`、`OU=Global`、`OU=Properties`、`DC=vdi`、`DC=vmware` 和 `DC=int` 下可用。
消息	输入当用户尝试通过未加入白名单的客户端类型或版本启动桌面或已发布的应用程序时要显示的消息。

在 Horizon Console 中禁用或启用 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 Console 中，选择**设置 > 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 Horizon 连接服务器实例的外部 URL

可以使用 Horizon Console 编辑连接服务器实例的外部 URL。

默认情况下，仅位于同一网络的安全加密链路客户端可以连接到连接服务器主机。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 来连接到连接服务器主机。

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到连接服务器主机的 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。

步骤

1 在 Horizon Console 中，选择**设置 > 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 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://horizon.example.com:443

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。

4 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到此连接服务器实例的 IP 地址和端口号。

5 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。

6 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。

7 单击**确定**保存更改。

外部 URL 将立即更新。您无需重新启动连接服务器，所做的更改即可生效。

在 Horizon Console 中注册网关

Horizon Client 会通过您在 Horizon Console 中注册的网关或 Unified Access Gateway 设备进行连接。

您可以在 Horizon Console 中注册或取消注册网关。要取消注册网关，请选择相应的网关或 Unified Access Gateway 设备，然后单击**取消注册**。

步骤

1 在 Horizon Console 中，选择**设置 > 服务器**。

2 在**网关**选项卡上，单击**注册**。

3 输入网关或 Unified Access Gateway 设备的 FQDN。

4 单击**确定**。

设置智能卡身份验证

4

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，以便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

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。如果配置了证书撤消检查，已撤消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 Console 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 Unified Access Gateway 设备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。根据您所在的具体环境，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 Console 中配置智能卡设置

您可以使用 Horizon Console 指定相应设置，以适应不同的智能卡身份验证场景。

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。

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。

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。

  重要事项 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以使所做的更改生效。

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 Console 中配置智能卡身份验证设置。

在 Horizon Console 中配置智能卡设置

您可以使用 Horizon Console 指定相应设置，以适应不同的智能卡身份验证场景。

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 Console 中，选择**设置 > 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“Horizon 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	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。 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。 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。

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 Console 的管理员配置智能卡身份验证，请从 **Horizon Administrator 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 Console。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 Console 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。请参阅在 Horizon Console 中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（如负载平衡器和网关）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，因此其中的一个任务是在 Horizon Console 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 Unified Access Gateway 文档。

步骤

1 为第三方网关或负载平衡器创建一个 SAML 身份验证器。

请参阅在 Horizon Console 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 NTAuth 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 NTAuth 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 NTAuth 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 NTAuth 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 NTAuth 存储区中。

  例如：`certutil –dspublish –f` *`CA 根证书路径`* `NTAuthCA`

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	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	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	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	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	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	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	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	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。

在 Horizon Console 中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时，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 Console 中检查智能卡的身份验证设置。

  a 选择**设置 > 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 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。

使用智能卡证书撤消检查

通过配置证书撤消检查，可以阻止已撤消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，其证书通常会被撤消。

Horizon 7 支持通过证书撤消列表 (Certificate Revocation List, CRL) 和联机证书状态协议 (Online Certificate Status Protocol, OCSP) 进行证书撤消检查。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 证书的撤消状态。

您可以在连接服务器实例或安全服务器上配置证书撤消检查。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消检查。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消检查，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消状态。

- 登录时进行 OCSP 证书撤消检查

  如果您配置了 OCSP 证书撤消检查，Horizon 7 会向 OCSP Responder 发送请求，以确定特定用户证书的撤消状态。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消状态。

- 配置 OCSP 证书撤消检查

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

- 智能卡证书撤消检查属性

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

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消状态。

如果证书已撤消，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 证书撤消检查

如果您配置了 OCSP 证书撤消检查，Horizon 7 会向 OCSP Responder 发送请求，以确定特定用户证书的撤消状态。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。

如果用户证书已撤消，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消状态。

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消检查属性。

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消检查。

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消检查，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-ROOT_CA.crl
```

配置 OCSP 证书撤消检查

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

前提条件

熟悉用于 OCSP 证书撤消检查的 `locked.properties` 文件属性。请参阅智能卡证书撤消检查属性。

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消检查。

b 将 `enableOCSP` 属性设为 **true**，以启用 OCSP 证书撤消检查。

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置。

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消检查，配置 CRL 与 OCSP 证书撤消检查，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
```

智能卡证书撤消检查属性

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

表 4-1. 智能卡证书撤消检查属性 列出了证书撤消检查的 `locked.properties` 文件属性。

表 4-1. 智能卡证书撤消检查属性

属性	说明
`enableRevocationChecking`	将该属性设为 **true** 可启用证书撤消检查。 如果该属性设为 **false**，则禁用证书撤消检查，并忽略其他所有证书撤消检查属性。 默认值为 **false**。
`crlLocation`	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 `allowCertCRLs` 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。
`allowCertCRLs`	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**。
`enableOCSP`	将该属性设为 **true** 可启用 OCSP 证书撤消检查。 默认值为 **false**。
`ocspURL`	指定 OCSP Responder 的 URL。
`ocspResponderCert`	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。
`ocspSendNonce`	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**。
`ocspCRLFailover`	该属性设为 **true** 时，如果 OCSP 证书撤消检查失败，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

5

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

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

  如果用户连接到启用了 RSA SecurID 身份验证或 RADIUS 身份验证的连接服务器实例，则 Horizon Client 中将显示一个特殊登录对话框。

- 在 Horizon Console 中启用双因素身份验证

  通过在 Horizon Console 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。

- RSA SecurID 访问被拒绝故障排除

  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

如果用户连接到启用了 RSA SecurID 身份验证或 RADIUS 身份验证的连接服务器实例，则 Horizon Client 中将显示一个特殊登录对话框。

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 Console 中启用双因素身份验证

通过在 Horizon Console 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。您需在 Horizon Console 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 Console 中，导航到**设置 > 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 在**身份验证**选项卡上，从**高级身份验证**部分的**双因素身份验证**下拉菜单中，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**下拉菜单中，选择**创建新的身份验证器**，并完成此页。

- 要使自定义用户名和通行码标签显示在最终用户的 RADIUS 身份验证对话框中，请在**用户名标签**和**通行码标签**字段中输入自定义标签。
- 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，则会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。

RSA SecurID 访问被拒绝故障排除

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

问题

通过 RSA SecurID 进行验证的 Horizon Client 连接显示 `Access Denied`（访问被拒绝），并且 RSA Authentication Manager 登录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 Console 中，导航到**设置 > 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. 在**身份验证**选项卡上，从**高级身份验证**部分的**双因素身份验证**下拉菜单中，选择 **RSA SecurID**。
4. 选择**清除节点密钥**，然后单击**确定**。
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. 从列表中选择连接服务器，然后取消选中**已创建节点密钥**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 服务器配置为接受连接服务器实例作为 RADIUS 客户端。必须将使用 RADIUS 的每个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。
- 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平衡器或网关相集成。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权限，请确认您在 Horizon Console 中以对根访问组拥有管理员角色的用户身份创建这些桌面和应用程序池。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 Console 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平衡器或网关连接到远程桌面和应用程序，您必须在 Horizon Console 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。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的各个 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 Unified Access Gateway 文档。

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平衡器。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平衡器的 FQDN 或 IP 地址。
- 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 设备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 Console 中，导航到**设置 > 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，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。

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	描述
类型	对于 Unified Access Gateway 设备或第三方设备，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 设备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。
描述	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 `https://<YOUR HORIZON SERVER NAME>/SAAS/API/1.0/GET/metadata/idp.xml` 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平衡器（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 设备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。

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，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。

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**，然后添加 **`pae-SAMLProxyName`** 和 **`pae-SAMLProxyPort`** 条目的值。

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 设备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。

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 Console 禁用无法访问的动态 SAML 身份验证器，以缩短其他动态 SAML 身份验证器上对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 Console 中配置 SAML 身份验证器。

在 Horizon Console 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 Console 中授权用户使用已发布的桌面和应用程序。

步骤

1. 在 Horizon Console 中，导航到**设置 > 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。

对用户和组进行身份验证

6

登录到 Horizon Console 后，您可以通过为用户和组设置身份验证来控制对应用程序和桌面的访问权限。

您可以通过配置远程访问来限制用户和组从网络以外的位置访问桌面。您可以通过设置相应配置来使未通过身份验证的用户无需 AD 凭据即可从 Horizon Client 访问其已发布的应用程序。

本章讨论了以下主题：

限制网络外部的远程桌面访问

您可以允许特定的授权用户和组从外部网络访问远程桌面，而限制其他授权用户和组的访问。所有授权用户都将可以从内部网络访问桌面和应用程序。如果您选择不将访问权限限制给外部网络的特定用户，那么所有授权用户都将可以从外部网络进行访问。

出于安全原因，管理员可能会需要限制网络外部的用户和组访问网络内部的远程桌面和应用程序。当受限的用户从外部网络访问系统时，会显示一条消息，指明此用户无权使用该系统。此用户必须在内部网络中才有权访问桌面和应用程序池。

配置远程访问

您可以允许一些用户和组从网络外部访问连接服务器实例，同时限制其他用户和组的访问。

前提条件

- 必须在网络外部部署 Unified Access Gateway 设备、安全服务器或负载平衡器，作为用户有权访问的连接服务器实例的网关。有关部署 Unified Access Gateway 设备的更多信息，请参阅《部署和配置 Unified Access Gateway》文档。
- 要进行远程访问的用户必须有权访问桌面或应用程序池。

步骤

1 在 Horizon Console 中，选择**用户和组**。

2 单击**远程访问**选项卡。

3 单击**添加**，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用户或组。

注 未验证访问用户将不会显示在搜索结果中。

4 要向某个用户、组或未验证访问用户提供远程访问权限，请选择相应用户或组，然后单击**确定**。

5 要从远程访问中移除用户或组，请选择相应用户或组，单击**删除**，然后单击**确定**。

配置未验证访问

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。

注 桌面池中发布的应用程序不支持未验证访问。

该功能需要设置 Horizon 7 版本 7.1 环境和 Horizon Client 版本 4.4。

有关为用户配置未验证访问的规则和指南的信息，请参阅《Horizon 7 管理指南》文档。

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

- 管理员只能为每个 Active Directory 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。
- 如果选择具有桌面授权的用户，并将该用户设置为未验证访问用户，该用户将无权访问授权的桌面。

步骤

1 在 Horizon Console 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。

4 选择一个用户，然后单击**下一步**。

5 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**提交**。

连接服务器将创建未验证访问用户，并显示用户详细信息，包括用户别名、用户名、名字和姓氏、域、应用程序授权和会话。

后续步骤

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。请参阅《Horizon 7 管理指南》文档中的“启用用户未验证访问”。

在 Horizon Console 中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 Console 中，选择**设置 > 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。有关创建场的更多信息，请参阅《在 Horizon Console 中设置已发布的桌面和应用程序》文档。
- 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。有关创建已发布应用程序的更多信息，请参阅《在 Horizon Console 中设置已发布的桌面和应用程序》。

步骤

1 在 Horizon Console 中，选择**用户和组**。

2 在**授权**选项卡上，从**授权**下拉菜单中选择**添加应用程序授权**。

3 单击**添加**，选择一个或多个搜索条件，选中**未验证用户**复选框，然后单击**查找**以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 选择池中的应用程序，然后单击**提交**。

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。

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。如果删除默认用户，Horizon Console 会显示一个内部错误消息和一个用户成功移除消息。但是，不会从 Horizon Console 中删除默认用户。

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 Console 中，选择**用户和组**。

2 在**未验证访问**选项卡中，选择用户，然后单击**删除**。

3 单击**确定**。

后续步骤

移除用户的应用程序授权。

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。

在 Horizon Console 中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 Console 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。请参阅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 Console 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

对于适用于 Windows 的 Horizon Client，当用户在**选项**菜单中选中**以当前用户身份登录**复选框时，将使用他们在登录到客户端系统时提供的凭据在 Horizon 连接服务器实例和远程桌面中进行身份验证。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。

- 在连接服务器实例上，启用**接受以当前用户身份登录**设置，以允许连接服务器实例接受用户在 Horizon Client 的**选项**菜单中选择**以当前用户身份登录**时传递的用户身份和凭据信息。

  重要事项 在启用该设置之前，您必须了解安全风险。请参阅《Horizon 7 安全指南》文档中的“用户身份验证的安全相关服务器设置”。

- 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**选项**菜单中的**以当前用户身份登录**设置的可用性并指定其默认值。管理员还可以使用组策略指定，哪些连接服务器实例接受用户在 Horizon Client 中选择**以当前用户身份登录**时传递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”功能具有以下限制和要求：

- 如果在连接服务器实例上将智能卡身份验证设置为“必需”，在连接到连接服务器实例时，选择**以当前用户身份登录**的用户的身份验证将会失败。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。如果用户尝试连接到安全服务器或连接服务器实例而没有先建立 VPN 连接，将提示用户提供凭据，并且“以当前用户身份登录”功能无法正常工作。

在 Horizon Console 中配置基于角色的委派管理

7

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 Console，以及这些用户有执行哪些任务的权限。通过基于角色的委派管理，您可以将管理员角色分配给特定 Active Directory 用户和组，从而有选择地分配管理权限。

本章讨论了以下主题：

了解角色和特权

能否在 Horizon Console 中执行任务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 Console 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 Console 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 Console 中包含的预定义角色具有执行常见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。如果角色中包含特定于对象的特权，您可能需要将该角色应用于访问组。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。

在 Horizon Console 中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 Console 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 Console 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。

- 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 7-1. 为不同访问组配置不同管理员 显示了这种配置的示例。

表 7-1. 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 7-2. 为同一访问组配置不同管理员 显示了这种配置的示例。

表 7-2. 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 Console 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。

根据您选择的是管理员用户或组、访问组还是角色，Horizon Console 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，Horizon Console 中是如何显示权限的。管理员用户名为 Admin 1，具有两个权限。

表 7-3. “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 Console 中如何显示同样的权限。

表 7-4. “文件夹”选项卡上显示的 MarketingDesktops 权限

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

第一个权限与 表 7-3. “管理员和组”选项卡上显示的 Admin 1 权限 中显示的第一个权限相同。第二个权限是从 表 7-3. “管理员和组”选项卡上显示的 Admin 1 权限 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“清单管理员”角色时，表 7-3. “管理员和组”选项卡上显示的 Admin 1 权限 中的第一个权限如何在 Horizon Console 中显示。

表 7-5. “角色权限”选项卡上显示的清单管理员权限

Administrator	访问组
horizon-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 Console 来添加和移除管理员用户和组。

管理员角色是 Horizon Console 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。

- 在 Horizon Console 中创建管理员

  要创建管理员，您需要在 Horizon Console 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。

- 在 Horizon Console 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。

在 Horizon Console 中创建管理员

要创建管理员，您需要在 Horizon Console 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。请参阅在 Horizon Console 中添加自定义角色。
- 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 Console 中，导航到**设置 > 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。

已应用于访问组列指示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。

在 Horizon Console 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 Horizon Console 中，导航到**设置 > 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 Console 添加、删除和查看特定管理员用户和组、角色及访问组的权限。

- 在 Horizon Console 中添加权限

  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。

- 在 Horizon Console 中删除权限

  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。

- 在 Horizon Console 中查看权限

  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。

在 Horizon Console 中添加权限

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 Console 中，导航到**设置 > 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。	a 在**管理员和组**选项卡上，选择所需的管理员或组，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。	a 在**角色权限**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。	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。

在 Horizon Console 中删除权限

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 Console 中，导航到**设置 > 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。
删除应用于特定访问组的权限。	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**移除权限**。

在 Horizon Console 中查看权限

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 在 Horizon Console 中，导航到**设置 > 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**角色权限**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 Console 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。

- 在 Horizon Console 中添加访问组

  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。

- 在 Horizon Console 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。

- 在 Horizon Console 中移除访问组

  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。

- 查看访问组中的对象

  您可以在 Horizon Console 中查看特定访问组中的桌面池、应用程序池、场或永久磁盘。

- 查看访问组中的 vCenter 虚拟机

  您可以在 Horizon Console 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。

在 Horizon Console 中添加访问组

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 Console 中，导航到“访问组”对话框。

选项	操作
从桌面中	■ 选择**清单 > 桌面**。 ■ 从**访问组**下拉菜单中，选择**新建访问组**。
从场中	■ 选择**清单 > 场**。 ■ 从**访问组**下拉菜单中，选择**新建访问组**。

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。

在 Horizon Console 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。

步骤

1 在 Horizon Console 中，选择**清单 > 桌面**或**清单 > 场**。

2 选择一个池或场。

3 从**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 Console 会将该池或场移至所选的访问组。

在 Horizon Console 中移除访问组

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。请参阅在 Horizon Console 中将桌面池或场移至不同的访问组。

步骤

1 在 Horizon Console 中，导航到**设置 > 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。

查看访问组中的对象

您可以在 Horizon Console 中查看特定访问组中的桌面池、应用程序池、场或永久磁盘。

步骤

1 在 Horizon Console 中，导航到对象的主页。

对象	操作
桌面池	选择**清单 > 桌面**。
应用程序池	选择**清单 > 应用程序**。
场	选择**清单 > 场**。
永久磁盘	选择**清单 > 永久磁盘**。

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 Console 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 Console 中，导航到**清单 > 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 Console 添加、修改和删除自定义角色。

- 在 Horizon Console 中添加自定义角色

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

- 在 Horizon Console 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。

- 在 Horizon Console 中移除自定义角色
  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。

在 Horizon Console 中添加自定义角色

如果预定义的管理员角色不符合您的要求，您可以在 Horizon Console 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 Console 中，导航到**设置 > 管理员**。

2 在**角色特权**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。

在 Horizon Console 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 Console 中，导航到**设置 > 管理员**。

2 在**角色特权**选项卡上，选择所需的角色。

3 查看角色中的特权，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。

在 Horizon Console 中移除自定义角色

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。请参阅在 Horizon Console 中删除权限。

步骤

1 在 Horizon Console 中，导航到**设置 > 管理员**。

2 在**角色特权**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 Console 中提供了一些预定义角色，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

  对象专用特权用于控制可对特定类型的清单对象执行的操作。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 7-6. Horizon Console 中的预定义角色

角色	用户能力	应用于访问组
管理员	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。 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。 **重要事项** 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： ■ 添加和删除访问组。 ■ 在 Horizon Console 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)	■ 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`）。 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。 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
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	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。 ■ 对 Horizon Help Desk Tool 进行只读访问。 ■ 管理全局会话。 ■ 可以登录到 Horizon Console。 ■ 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)	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。 ■ 对 Horizon Help Desk Tool 进行只读访问。 ■ 可以登录到 Horizon Console。	否

表 7-6. Horizon Console 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	■ 执行所有与计算机、会话和池相关的操作。 ■ 管理永久磁盘。 ■ 对链接克隆池进行重新同步、刷新和重新平衡，以及更改默认池映像。 ■ 管理自动场。 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。 拥有此角色的管理员不能创建手动场或未受管的手动池，也不能在该场或未受管的手动池中添加或移除 RDS 主机。	是
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 7-7. 全局特权

特权	用户能力	预定义角色
控制台交互	登录并使用 Horizon Console。 **注** 从 Horizon 7 版本 7.10 开始，**控制台交互**特权将自动添加到新角色中，并且不会显示在 Horizon Console 的全局特权列表中。	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。 **注** 从 Horizon 7 版本 7.10 开始，**直接交互**特权将自动添加到新角色中，并且不会显示在 Horizon Console 的全局特权列表中。	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
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
管理 vCenter 配置 (只读)	对 vCenter Server 配置进行只读访问。	管理员 管理员 (只读) 清单管理员 清单管理员 (只读) 本地管理员 本地管理员 (只读)

特定于对象的特权

对象专用特权用于控制可对特定类型的清单对象执行的操作。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 7-8. 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
管理对自动桌面和场的维护操作	重构、刷新、重新平衡、调度推送映像、计划维护以及更改桌面池和场的默认映像。	桌面池、场
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 Horizon 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 7-9. 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 Console 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 7-10. 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**
授权或取消授权用户访问池。	**授权桌面和应用程序池**

表 7-10. 池管理任务和特权 （续）

任务	所需特权
添加池。	**管理场以及桌面和应用程序池** **注** 不适用于添加未受管桌面池。管理员还必须具有“全局配置和策略管理员 (只读)”角色，才能执行此任务。
修改或删除池。	**管理场以及桌面和应用程序池** **注** 不适用于删除未受管桌面池。管理员还必须具有“全局配置和策略管理员 (只读)”角色，才能执行此任务。
在池中添加或移除桌面。	**管理场以及桌面和应用程序池** **注** 不适用于在桌面池中添加或移除未受管虚拟桌面。管理员还必须具有“全局配置和策略管理员 (只读)”角色，才能执行此任务。
刷新、重构、重新平衡或更改默认的 Horizon Console 映像。	**管理 Composer 桌面池映像**和**管理 vCenter 配置 (只读)**。
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 Console 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 7-11. 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**或**管理场以及桌面和应用程序池** **注** 不适用于从桌面池或场中移除未受管桌面或 RDS 主机。管理员还必须具有“全局配置和策略管理员 (只读)”角色，才能执行此任务。
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 Console 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 Console 中的“永久磁盘”页面上执行这些任务。

表 7-12. 永久磁盘管理任务和特权

任务	所需特权
分离磁盘。	■ 如果磁盘是辅助磁盘，则需要具有**管理永久磁盘**特权。 ■ 如果磁盘是主磁盘，则需要具有**管理永久磁盘**和**管理计算机**特权。 ■ 要分离不同数据存储上的任何磁盘，管理员还需要具有**管理 vCenter 配置 (只读)** 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**管理计算机**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，对最后一个桌面池拥有**管理场以及桌面和应用程序池**或者**管理计算机**特权。
从 vCenter 导入。	对磁盘拥有**管理永久磁盘**特权，以及**管理 vCenter 配置 (只读)** 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 Console 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 Console 中的**用户和组**页面上对用户进行管理，并在 Horizon Console 中的**全局管理员视图**页面上对管理员进行管理。

表 7-13. 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 Console 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 7-14. 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**

表 7-14. Horizon Help Desk Tool 任务和特权 （续）

任务	所需特权
可以登录到 Horizon Console。	**控制台交互** **注** 从 Horizon 7 版本 7.10 开始，**控制台交互**特权将自动添加到新角色中，并且不会显示在 Horizon Console 的全局特权列表中。
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**
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 7-15. 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本地管理员角色或管理员角色才能删除访问组。 必须在根访问组上具有清单管理员、本地管理员或管理员角色。
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** **注** 从 Horizon 7 版本 7.10 开始，“直接交互”特权将自动添加到新角色中，并且不会显示在 Horizon Console 的特权列表中。
使用 `vdmadmin` 和 `vdmimport` 命令	必须在根访问组上具有管理员角色。

表 7-15. 执行常规管理任务和命令所需的特权 （续）

任务	所需特权
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。
对 vCenter Server 配置进行只读访问。	**管理 vCenter 配置 (只读)**

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 Console 中设置策略

8

您可以使用 Horizon Console 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。

本章讨论了以下主题：

配置全局策略

您可以配置全局策略以控制所有客户端会话用户的行为。

步骤

1　在 Horizon Console 中，选择**设置 > 全局策略**。

全局策略窗格显示了将影响所有客户端会话、桌面池或用户的设置。

表 8-1. Horizon 策略

策略	说明
多媒体重定向 (MMR)	确定是否为客户端系统启用 MMR。 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。 默认值为**拒绝**。 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**。 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。
USB 访问	确定远程桌面是否可以使用 USB 设备连接客户端系统。 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**。
PCoIP 硬件加速	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。 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。 默认值为**允许**，优先级为**中**。

2 单击**编辑策略**以更改设置。

3 单击**确定**保存更改。

维护 Horizon 7 组件

9

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

您可以通过在 Horizon Console 中计划或运行自动备份来备份 Horizon 7 和 Horizon Composer 配置数据。通过手动导入备份的 View LDAP 文件和 Horizon 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 Horizon Composer 数据

完成连接服务器的初始配置后，您应计划对 Horizon 7 和 Horizon Composer 配置数据进行定期备份。您可以通过使用 Horizon Console 来保留 Horizon 7 和 Horizon Composer 数据。

Horizon 7 将连接服务器配置数据存储在 View LDAP 存储库中。Horizon Composer 将链接克隆桌面的配置数据存储在 Horizon Composer 数据库中。

当您使用 Horizon Console 执行备份时，Horizon 7 会备份 View LDAP 配置数据和 Horizon 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《Horizon 7 管理指南》文档中的“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 Console 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 Horizon Console 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 Horizon Composer 服务，那么 Horizon 7 会备份与 vCenter Server 实例关联的所有 Horizon 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 Console 中，选择**设置 > 服务器**。
2. 在**连接服务器**选项卡上，选择要备份的连接服务器实例，然后单击**立即备份**。
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 Horizon Composer 配置数据。您可以在 Horizon Console 中设置备份操作的频率和其他设置。

表 9-1. Horizon 7 配置备份设置

设置	说明
自动备份频率	每小时：每小时整点进行备份。 每 6 小时：在零点、上午 6 点、中午 12 点和下午 6 点进行备份。 每 12 小时：在零点和中午 12 点进行备份。 每天：每天零点进行备份。 每 2 天：在星期六、星期一、星期三和星期五的零点进行备份。 每周：在每周星期六的零点进行备份。 每 2 周：在每隔一周的星期六零点进行备份。 从不：不自动进行备份。
备份时间	计划备份的时间。
备份时间偏移	已计划的备份的时间偏移。
最大备份数量	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。 达到最大数量时，Horizon 7 会删除最早的备份文件。 此设置还适用于您使用**立即备份**功能创建的备份文件。
文件夹位置	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` 当您使用**立即备份**时，Horizon 7 也会将备份文件存储在此位置。

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 Horizon 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 Horizon Composer 配置数据。

还原 Horizon 连接服务器和 Horizon 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 Horizon Composer 数据库文件。

您需要手动运行不同的实用程序来还原连接服务器和 Horizon Composer 配置数据。

还原配置数据前，请确认您在 Horizon Console 中备份了配置数据。请参阅备份 Horizon 连接服务器和 Horizon 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 Horizon Composer 数据从 .svi 备份文件导入到 Horizon 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 Console 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 Horizon 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. 通过停止在其中运行 Horizon Composer 的服务器上的 VMware Horizon Composer Windows 服务，停止 Horizon Composer 的所有实例。
2. 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。
3. 安装连接服务器的一个实例。
4. 通过停止 Windows 服务 VMware Horizon 连接服务器停止连接服务器实例。
5. 单击**开始 > 命令提示符**。
6. 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：

   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。
7. 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：
8. 卸载连接服务器。

   仅卸载 VMware Horizon 连接服务器软件包。

9 重新安装连接服务器。

10 登录到 Horizon Console 并验证配置是否正确。

11 启动 Horizon Composer 实例。

12 重新安装副本服务器实例。

`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 Horizon 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 Horizon Composer 配置。请参阅还原 Horizon Composer 数据库。还原 Horizon Composer 配置后，如果 vCenter Server 中的虚拟机自备份 Horizon Composer 配置以来发生过更改，则您可能需要手动解决此不一致问题。

还原 Horizon Composer 数据库

您可以将 Horizon Composer 配置的备份文件导入存储链接克隆信息的 Horizon Composer 数据库中。

使用 `SviConfig restoredata` 命令，您可以在系统出现故障后还原 Horizon Composer 数据库数据，或是将 Horizon Composer 配置恢复到某个早期状态。

重要事项 只能由经验丰富的 Horizon Composer 管理员使用 `SviConfig` 实用程序。该实用程序旨在解决与 Horizon Composer 服务相关的问题。

前提条件

确认 Horizon 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`。

Horizon Composer 备份文件采用带日期戳和 `.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` - Horizon 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 Horizon Composer 备份文件从连接服务器计算机复制到可从安装了 VMware Horizon Composer 服务的计算机访问的位置。

2 在安装了 Horizon Composer 的计算机上，停止 VMware Horizon 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 Horizon 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 –dsnname=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 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 Horizon Console 数据库时显示的结果代码。

还原 Horizon Console 数据库时显示的结果代码

还原 Horizon Console 数据库时，`SviConfig restoredata` 命令会显示一个结果代码。

表 9-2. Restoredata 结果代码

代码	说明
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。
4	出现异常问题，命令无法完成。
14	其他应用程序正在使用 VMware Horizon Console 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 Horizon Composer 数据库中的数据

您可以将 Horizon Composer 数据库中的数据导出到文件。

重要事项 只有经验丰富的 Horizon Composer 管理员才能使用 SviConfig 实用程序。

前提条件

默认情况下，Horizon 7 将备份文件存储在连接服务器计算机的 C: 驱动器上，路径为 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 Horizon Composer 的计算机上，停止 VMware Horizon 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 Horizon Composer 应用程序位于同一位置。

   Horizon-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_Horizon_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 Horizon Composer 数据库时显示的结果代码。

导出 Horizon Composer 数据库时显示的结果代码

导出 Horizon Composer 数据库时，`SviConfig exportdata` 命令会显示一个退出代码。

表 9-3. Exportdata ExitStatus 代码

代码	说明
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 Console 仪表板，可以快速查看 Horizon 7 部署中的 Horizon 7 和 vSphere 组件的状态。

Horizon Console 将显示有关连接服务器实例、事件数据库、网关、Horizon Composer 服务、数据存储、vCenter Server 实例和域的监控信息。

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 Console 也会将 Kerberos 域的状态显示为未知。

步骤

1 在 Horizon Console 中，导航到**监控 > 仪表板**。

2 在**系统运行状况**窗格中，单击**查看**。

“详细信息”窗格将显示与每个问题相关的名称、版本和其他信息。

- 绿色复选标记表示组件没有问题。
- 红色感叹号表示组件不可用或未运行。
- 黄色感叹号表示组件处于警告状态。
- 问号表明组件状态未知。

3 选择一项以查看有关问题的更多信息。

选项	描述
组件	显示有关服务组件的信息。 单击**连接服务器**、**网关服务器**、**事件数据库**、**View Composer Server** 或 **True SSO** 选项卡，以查看有关服务组件的信息并执行故障排除任务。 选择一个组件以执行以下任务： ■ 查看状态、名称、版本和其他详细信息。 ■ 如果选择连接服务器，请单击**查看服务状态**选项卡，以查看有关网关服务的信息。 ■ 如果选择连接服务器，请单击**查看会话详细信息**选项卡，以查看有关连接服务器会话的信息。
RDS 场	显示有关场的信息。单击场 ID 以查看有关场的更多信息，包括属于该场的 RDS 主机。
vSphere	显示与 vSphere 相关的组件信息。 单击**数据存储**、**ESX 主机**和 **vCenter Server** 选项卡，以查看有关每个组件的信息。
其他组件	单击**域**、**SAML 2.0** 和**许可服务**选项卡，以查看有关每个组件的更多信息。本部分还适用于 Horizon Composer。 **注** 如果 SAML 2.0 身份验证器因为证书不受信任而发出警告，则可以单击证书链接以接受证书并对其进行验证。
远程容器	显示有关远程 Horizon 7 容器的信息。 **注** 仅当启用 Cloud Pod 架构功能时，才会显示此部分。

4 在**会话**窗格中，您可以查看用于显示虚拟桌面、已发布桌面和已发布应用程序的活动会话数、已断开连接的会话数或空闲会话数的条形图。

5 在**会话**窗格中，单击**查看**以查看会话。

“会话”页面显示有关会话的信息。

6 在**工作负载**窗格中，单击**查看**以查看数据存储。

您可以选择一个数据存储以查看其他详细信息，例如该数据存储的当前使用情况。如果数据存储的可用空间缩减至阈值以下，则 Horizon Console 将显示一条警告。如果存在与所选数据存储相关的桌面池，则可以在选择数据存储时查看桌面池的信息。**其他数据存储**列显示有关跨多个数据存储的桌面池或场的信息。

监控 Horizon 连接服务器的负载状态

您可以在 Horizon Console 仪表板中监控连接服务器的负载。对于每个连接服务器，您都可以查看使用的 CPU 和内存的百分比，显示协议会话数、连接服务器连接会话数，或者可连接到连接服务器的最大会话数阈值。您还可以查看 RDS 主机已连接的会话数。

步骤

1 在 Horizon Console 中，导航到**监控 > 仪表板**。

2 在**系统运行状况**窗格中，单击**查看**。

在**组件**窗格的**连接服务器**选项卡上，**会话**列将显示每个连接服务器的连接服务器会话的百分比。**CPU 消耗**列显示了每个连接服务器消耗的 CPU 百分比。**内存消耗**列显示了每个连接服务器消耗的内存百分比。

注 如果没有为连接服务器配置通过 HTTP(s) 安全加密链路、PCoIP 安全网关和 Blast 安全网关连接建立的安全网关连接，则 Horizon Console 不会显示连接服务器会话的百分比，但会列出连接服务器会话的数量。

3 选择一个连接服务器，然后单击**查看会话详细信息**以查看连接服务器会话数、最大连接服务器会话数和显示协议会话数。

注 如果没有为连接服务器配置通过 HTTP(s) 安全加密链路、PCoIP 安全网关和 Blast 安全网关连接建立的安全网关连接，则 Horizon Console 不会显示最大会话数阈值，因为可连接到连接服务器的会话数量并没有阈值。

4 要查看 RDS 主机上的会话数，请在**组件**窗格中，单击 **RDS 场**，然后单击场 ID。

“会话”列将显示 RDS 主机上的会话数。

监控 Horizon 连接服务器上的服务

您可以在 Horizon Console 仪表板中监控连接服务器上运行的网关服务组件。网关服务组件包括配置了 HTTP(s) 安全加密链路、PCoIP 网关和 Blast 安全网关连接的安全网关连接。

步骤

1 在 Horizon Console 中，导航到**监控 > 仪表板**。

2 在**系统运行状况**窗格中，单击**查看**。

3 选择一个连接服务器，然后选择**查看服务状态**。

网关服务状态对话框将显示网关服务组件及正在使用的网关服务组件的状态。

注 未启用的服务组件呈灰显状态。

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 9-4. Horizon 连接服务器主机服务

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

表 9-4. Horizon 连接服务器主机服务 （续）

服务名称	启动类型	说明
VMware Horizon View 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 9-5. 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。

在 Horizon Console 中更改产品许可证密钥或许可证模式

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 Console 更改产品许可证密钥。根据 VMware Horizon Cloud Service 上的 Horizon 7 部署，您可以获取适用于 Horizon 7 的永久许可证或订阅许可证。您可以使用 Horizon Console 将容器的许可证模式从订阅许可证更改为永久许可证，反之亦然。

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 Horizon Composer 和已发布的应用程序），请获取有效的产品许可证密钥。

- 要使用订阅许可证，请确认为订阅许可证启用 Horizon 7。请参阅《Horizon 7 安装指南》文档。**许可**面板会显示有关 Horizon 7 容器订阅许可证的信息。

步骤

1 在 Horizon Console 中，选择**设置 > 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 要编辑许可证密钥，请单击**编辑许可证**，输入许可证序列号，然后单击**确定**。

许可设置面板将显示更新的许可信息。

3 （可选） 要将 Horizon 7 容器从订阅许可证更改为永久许可证，请单击**使用永久许可证**，然后单击**确定**。

许可设置面板将显示更新的许可信息。

4 （可选） 要将 Horizon 7 容器从永久许可证更改为订阅许可证，请单击**使用订阅许可证**，然后单击**确定**。然后，VMware Horizon Cloud Service 管理员可以为订阅许可证启用 Horizon 7 容器。

许可设置面板将显示更新的许可信息。

5 验证许可证的过期日期。

6 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 Horizon 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。

7 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。

监控许可证使用情况

在 Horizon Console 中，您可以监控同时连接到 Horizon 7 的活动用户。**使用情况设置**面板会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 7 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 7 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 7 计算已访问 Horizon 7 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，**使用情况设置**面板上的**当前**列会显示在首次配置 Horizon 7 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 7 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，**使用情况设置**面板上的**最高**列会显示在首次配置 Horizon 7 部署或上次重置最大计数后的最高并发桌面会话数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 邀请了两个人加入他的会话，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 邀请了两个人，但只有一个人加入了会话。Mary 邀请了一个人，但该人没有加入会话。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。

重置许可证使用情况数据

在 Horizon Console 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。请参阅监控许可证使用情况。

步骤

1 在 Horizon Console 中，选择**设置 > 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**。

加入客户体验提升计划

您可以配置 Horizon 7 以加入 VMware 客户体验提升计划 (CEIP)。

有关 VMware 通过 CEIP 收集的数据类型以及 VMware 如何使用这些数据的信息，请参阅“信任与保证中心”，网址为 http://www.vmware.com/trustvmware/ceip.html。

要在 Horizon Client 中配置数据共享，请参阅相应的 Horizon Client 安装和设置指南。例如，对于 Windows 客户端，请参阅《适用于 Windows 的 VMware Horizon Client 安装和设置指南》文档。要在 HTML Access 中配置数据共享，请参阅《VMware Horizon HTML Access 安装和设置指南》文档。

步骤

1 在 Horizon Console 中，选择**设置 > 产品许可和使用情况**。

2 选择**客户体验计划**选项卡，然后单击**编辑设置**。

3 要加入 CEIP，请选择**加入 VMware 客户体验提升计划**。

如果不选择此选项，您就不能加入 CEIP。

4 （可选） 选择您所在的地理位置、您的纵向业务或贵组织中的员工数量。

5 单击**确定**。

Horizon 连接服务器与 Skyline Collector 设备集成

您可以将 Horizon 连接服务器配置为与 Skyline Collector 设备相集成，VMware 技术支持部门将使用此集成来诊断并解决 Horizon 7 存在的问题。Skyline Collector 设备会为配置来进行日志收集的 Horizon 7 管理员用户提取连接服务器日志。

步骤

1 在 Horizon Console 中，创建一个具有收集操作日志特权的自定义角色，并将其命名为“日志收集器管理员”。请参阅在 Horizon Console 中添加自定义角色。

2 为自定义角色添加描述。

3 添加一个新管理员用户，并为该用户选择“清单管理员 (只读)”角色和“日志收集器管理员”自定义角色。

Skyline Collector 设备可以为此管理员用户提取连接服务器日志，以诊断并解决 Horizon 7 问题。

JMP Integrated Workflow 入门

10

熟悉高级 JMP Integrated Workflow 概念并完成开始使用 JMP Integrated Workflow 功能所需的任务。

本章讨论了以下主题：

关于 JMP Integrated Workflow

通过 VMware HorizonJMP (Just-in-Time Management Platform) 集成工作流功能，您可以使用一个控制台来定义和管理用户或用户组的桌面工作区。

桌面工作区可通过定义一个包含 VMware Horizon 桌面池、VMware App Volumes AppStack 和 VMware Dynamic Environment Manager 设置相关信息的 JMP 分配来创建。提交 JMP 分配后，JMP 自动化引擎会与 Horizon 7、App Volumes 和 Dynamic Environment Manager 系统进行通信，以授权用户访问桌面。

您可以使用 Horizon Console 中的**分配 (JMP)** 选项卡来管理现有的 JMP 分配。还可以使用每个组件分配各自的 JMP 组件控制台修改每个组件分配。例如，还可以通过在 Horizon Console 中选择**清单 > 桌面**，对在 JMP 分配中定义的桌面池进行的更改进行修改。

在 Horizon Console 中打开 JMP 分配时，将验证 JMP 分配中每个组件的当前状态，以确保组件处于所预期的状态。发现差异后，会在控制台中突出显示受影响的区域，您可以接受当前状态，也可以修改分配以达到所需的状态并重新为用户授权。

您安装并配置 VMware HorizonJMP Server 后，即可在 Horizon Console 中使用 JMP Integrated Workflow 功能。请参阅 开始使用 JMP 集成工作流和《VMware Horizon JMP Server 安装和设置指南》以了解相关信息。

注　由于 App Volumes 不支持 VMware Cloud，因此在 AWS 上 JMP Integrated Workflow 功能不支持 VMware Cloud®

开始使用 JMP 集成工作流

要开始使用 JMP Integrated Workflow 功能，必须安装和设置 JMP Server，并配置 JMP 设置。

前提条件

查看您计划安装的所有技术组件所需要的必备条件和系统要求。

步骤

1 如有必要，在 Active Directory 中设置所需的管理员用户和组。

请参阅《Horizon 7 安装指南》文档中的“准备 Active Directory”。在配置 JMP 设置时，需要提供 Active Directory 信息。

2 设置 Microsoft SQL Server，并确保已创建您计划在 JMP Server 安装过程中使用的登录凭据。有关更多信息，请参阅《VMware Horizon JMP Server 安装和设置指南》文档中的“JMP Server 的数据库要求”。

3 安装并设置 VMware Horizon 7 版本 7.5 或更高版本。

请参阅《Horizon 7 安装指南》文档。

4 （可选）安装并设置 VMware App Volumes 2.14 或更高版本，该版本可提供用于实时应用程序交付的功能。

有关详细信息，请参阅《VMware App Volumes 安装指南》文档。

5 （可选）要提供上下文策略管理，请安装并设置 VMware Dynamic Environment Manager 9.2.1 或更高版本。

请参阅《安装和配置 VMware Dynamic Environment Manager》文档。

6 获取 JMP Server 与组织网络内其他服务器进行安全通信所需使用的 CA 签名的 SSL 证书。

7 安装 JMP Server 并配置 SSL 证书，以便 JMP Server 能够与 JMP Integrated Workflow 功能所需的其他服务器进行通信。

请参阅《VMware Horizon JMP Server 安装和设置指南》了解更多信息。

8 首次配置 JMP 设置。有关详细信息，请参阅首次配置 JMP 设置。

后续步骤

成功完成前面的任务之后，您现在可以创建一个 JMP 分配。有关信息，请参阅创建 JMP 分配。

管理 JMP 设置

11

安装 JMP Server 后，必须先使用必要的凭据配置 JMP 设置，然后才能创建任何 JMP 分配并开始使用 JMP Integrated Workflow 功能。可以先编辑初始 JMP 设置，然后在适用时添加新的设置信息。

本章讨论了以下主题：

首次配置 JMP 设置

在创建任何 JMP 分配之前，都必须先使用 Horizon Console 配置 JMP 设置。对于用来为用户或用户组分配桌面工作区的 Active Directory 域，必须为其提供凭据。您可以选择包含凭据信息，以在创建 JMP 分配时使用 App Volumes AppStack 和 Dynamic Environment Manager 配置共享。

前提条件

- 确认已成功安装 VMware HorizonJMP Server，并且您有其 URL。请参阅《VMware Horizon JMP Server 安装和设置指南》了解更多信息。
- 获取您计划与 JMP Server 一起使用的 Horizon 7 版本 7.5 或更高版本的管理员帐户凭据。
- 获取必须在 JMP Server 上使用的 Active Directory 凭据。
- 如果要向 JMP 分配中分配应用程序，请确保您具有要使用的 VMware App Volumes Manager 实例的 URL 和管理员帐户凭据。如果由负载平衡器管理计划使用的 App Volumes Manager 实例，请获取负载平衡器的 URL，并在配置 App Volumes Manager 信息时使用此 URL。
- 如果选择使用 VMware Dynamic Environment Manager 配置共享，请获取其 UNC 路径和对其进行访问所需的管理员帐户凭据。

步骤

1 在 Horizon Console 中，单击 **JMP 配置**。

2 输入 JMP Server 信息。

   a 在 **JMP Server** 选项卡中，单击**添加 JMP Server**。

   b 以 `https://jmp.yourcompany.com` 的格式输入 JMP Server URL。

   c 单击**保存**。

将对 JMP Server URL 进行验证。如果收到消息 `JMP Server 无法访问 (JMP Server is unreachable)`，请确认输入的 URL 正确无误、JMP Server 已正确配置，以及 JMP Server 可以访问。

3 输入计划用于 JMP Server 的 Horizon 7 连接服务器版本 7.5 或更高版本的帐户信息。

a 单击 **Horizon 7** 选项卡。

b 如果**连接服务器 URL** 值未自动填充，请输入该值。此 URL 与 Horizon Console 连接到的 Horizon 7 连接服务器的 URL 相同。

c 输入 Horizon 7 服务帐户用户名和密码。

d 在**服务帐户域**文本框中，输入有效的名称以用于要创建的 JMP 分配，然后按 **Enter**。

e 单击**保存**。

4 输入要用于 JMP 分配的 Active Directory 的信息。

a 单击 **Active Directory** 选项卡。

b 单击**新建**。

c 在 **NETBIOS 名称**文本框中，从可用 NetBIOS 域名列表中选择域名。

将使用默认值更新“DNS 域名”和“上下文”文本框。

d 确认 **DNS 域名**文本框中添加的默认值是要使用的正确值。还可以选择输入其他 Active Directory 完全限定域名。例如，`mycompany.com`。

e 在**协议**部分中，选择 Active Directory 使用的协议。

f 在**绑定用户名**和**绑定密码**文本框中，输入绑定标识名 (Distinguished Name, DN) 用户帐户的凭据。例如，`administrator`。

g 如果要使用默认值之外的其他值，可以修改**上下文**文本框中的值。

此值用作 Active Directory 数据搜索的根目录。

h （可选）单击**高级属性**并修改默认端口号值。

默认端口值取决于先前选择的协议。您可以修改端口值或将文本框留空。

i 在**域控制器**文本框中，可以选择输入一个或多个主机名或 IP 地址，用于处理 Active Directory 流量。

例如，`adserver.mycompany.com, 10.111.XXX.XXX`。如果将此文本框留空，将使用 **DNS 域名**文本框中的值。

j 单击**保存**。

5 如果计划在创建 JMP 分配时使用 App Volumes AppStack，请配置想要使用的 App Volumes Manager。

a 单击 **App Volumes** 选项卡。

b 单击**新建**。

c 在**名称**文本框中，输入要分配给 App Volumes 实例的名称。如果将此文本框留空，将使用在 **App Volumes Server URL** 文本框中输入的值。

d 输入希望与 JMP Server 容器关联的 App Volumes Manager 的有效 URL。

重要事项 如果由负载平衡器来管理计划使用的 App Volumes Manager，请输入该负载平衡器的 URL。

e 输入 JMP Server 可用来访问 App Volumes Manager 的 App Volumes Manager 或负载平衡器管理员帐户凭据。

f 输入将用于 JMP 分配的 App Volumes Manager 服务帐户的域名。

g （可选）如果要注册多个 App Volumes Manager，可以使用切换按钮来指示要添加的 App Volumes Manager 是否为创建 JMP 分配时要使用的默认服务器。可以更改要在创建 JMP 分配时使用的实例。

h 单击**保存**。

6 如果要在创建 JMP 分配时使用 Dynamic Environment Manager 配置共享，请在 JMP 设置中添加该共享的信息。

a 单击 **UEM** 选项卡。

b 单击**新建**。

c 在**文件共享 UNC 路径**文本框中以 `\\fileserver-name\UEM-configuration-share-pathname` 格式输入一个值。例如，`\\FileServer\UEMConfig`。

重要事项 请不要在您输入的文件共享 UNC 路径中包含 `General`。

d 输入用来连接到 Dynamic Environment Manager 配置共享的 Dynamic Environment Manager 管理员帐户凭据。

e 从 **Active Directory** 列表中，选择要用于 Dynamic Environment Manager 配置共享的域名。

注 一个 Active Directory 只能与一个 Dynamic Environment Manager 配置共享关联。

f 单击**保存**。

后续步骤

成功配置初始 JMP 设置后，您现在可以创建 JMP 分配。请参阅创建 JMP 分配了解更多信息。

管理 JMP 设置

您可以使用 Horizon Console 修改、添加或删除 JMP 设置的信息。

- 具有修改特定 JMP 设置所需的必要信息。
- 要修改 JMP 设置，请确保您具有相应的管理特权。

编辑 JMP Server 设置

可以使用 Horizon Console 对现有 JMP Server 设置进行更改。

前提条件

- 具有修改特定 JMP Server 设置所需的必要信息。
- 确保具有登录 Horizon Console 和修改 JMP Server 设置所需的适当管理特权。

步骤

1 在 Horizon Console 中，选择 **JMP 配置**。

2 在“JMP 设置”窗格中，单击 **JMP Server** 选项卡。

3 单击**编辑**。

4 输入一个新的 **JMP Server URL**。

5 单击**保存**。

将验证新的 JMP Server URL，如果无效，将显示一条错误消息。

编辑 Horizon 7 凭据

可以使用 Horizon Console 对现有 Horizon 7 连接服务器凭据进行更改。

步骤

1 在 Horizon Console 中，单击 **JMP 配置**。

2 单击 **Horizon 7** 选项卡。

3 单击**编辑凭据**。

4 根据需要在**服务帐户用户名**中输入新用户名。

5 根据需要在**服务帐户密码**中输入新密码。

6 根据需要更改**服务帐户域**中的值。

7 单击**保存**。

编辑 Horizon 连接服务器 URL

如果要将现有 JMP 分配关联到其他 Horizon Connection Server，您必须修改通过 JMP Server 设置进行注册并与这些 JMP 分配相关联的 Horizon Connection Server URL。

Horizon Connection Server 中没有可用于修改 Horizon Console 信息的用户界面。要修改 JMP 设置中的现有 Horizon Connection Server 主机 URL，您必须使用 SQL Server Management Studio。

前提条件

- 确保您具备登录到 SQL Server Management Studio 会话的相应系统管理员特权，以及对为 JMP Server 创建的 SQL Server 数据库的访问权限。

- 在对数据库进行修改之前，备份 SQL Server 数据库。

步骤

1 如果您当前已登录到 Horizon Console 会话，请注销。

2 以 sysadmin (SA) 身份或使用具有 SA 特权的用户帐户登录 SQL Server Management Studio 会话。

3 确认您打算使用的替换 Horizon Connection Server 主机 URL 尚未在其他 JMP Server 实例中注册。

例如，如果替换 Horizon Connection Server 主机 URL 是 `new-horizon-host.com`，请使用以下 SQL 语句来确认该 URL 尚未注册。

```
SELECT * from  xms_services
WHERE xms_services.host = "new-horizon-host.com"
```

4 如果上面的 SQL 语句未返回任何结果，请继续执行下一步。否则，请使用以下语句删除现有 Horizon Connection Server 主机的信息。

```
DELETE from xms_services
WHERE xms_services.host = "new-horizon-host.com"
```

5 使用以下语句更新现有 JMP Server 设置，其中 `new-horizon-server-host.com` 是替换 Horizon Connection Server 主机的 URL，`old-horizon-host.com` 是当前已注册 Horizon Connection Server 主机的 URL。

```
UPDATE xms_service_endpoints
SET host = 'new-horizon-host.com', is_available = 1
WHERE service_id = (SELECT id FROM xms_services WHERE service_type = 'horizon'
    AND host = 'old-horizon-host.com')
AND host = 'old-horizon-host.com'

UPDATE xms_services
SET [name] = 'horizon-https://new-horizon-host.com', host = 'new-horizon-host.com'
WHERE service_type = 'horizon'
AND host = 'old-horizon-host.com'
```

6 使用新的 Horizon Connection Server URL 登录到 Horizon Console，并确认新 Horizon Connection Server 主机现在关联的现有 JMP 分配之前与旧的 Horizon Connection Server 主机相关联。

添加 Active Directory 域

如果您在设置初始 Active Directory 域后需要再添加一个这样的域，可以使用 Horizon Console。

步骤

1 在 Horizon Console 中，单击 **JMP 配置**。

2 单击 **Active Directory** 选项卡，然后单击**添加**。

3 在 **NETBIOS 名称**文本框中，从可用 NetBIOS 域名列表中选择域名。

将使用默认值更新“DNS 域名”和“上下文”文本框。

4 在 **DNS 域名**文本字段中，确认 NETBIOS 名称更新后添加了默认值。还可以选择输入其他 Active Directory 完全限定域名。例如，`mycompany.com`。

5 在**协议**部分中，选择 Active Directory 使用的协议。

6 在**绑定用户名**和**绑定密码**文本字段中，输入绑定标识名 (DN) 用户帐户的凭据，如 Administrator。

7 如果要使用默认值之外的其他值，可以修改**上下文**文本字段中的值。

8 （可选）单击**高级属性**并修改默认端口号值。

默认端口值取决于先前选择的协议。您可以修改端口值或将文本字段留空。

9 在**域控制器**文本字段中，可以选择输入一个或多个主机名或 IP 地址，用于处理 Active Directory 流量。

10 单击**保存**。

有关新添加的 Active Directory 域的信息会显示在 Active Directory 表中。

编辑 Active Directory 域信息

如果在初始配置 JMP 设置后更改了某些信息，可以使用 Horizon Console 来修改 Active Directory 域设置信息。

步骤

1 在 Horizon Console 中，单击 **JMP 配置**。

2 单击 **Active Directory** 选项卡。

3 在 Active Directory 域表中选择一行，然后单击**编辑**。

4 修改需要更新的 Active Directory 信息。

5 单击**保存**。

删除 Active Directory 域信息

如果必须删除现有的 Active Directory (AD) 域设置信息，请使用 Horizon Console。

仅当所有现有 JMP 分配都未在使用已注册的 Active Directory 域时，才能从 JMP 设置中删除有关该域的信息。

步骤

1 在 Horizon Console 中，单击 **JMP 配置**。

2 单击 **Active Directory** 选项卡。

3 选择要从 JMP 设置中删除的 Active Directory 域所在的表行。

4 在出现的删除确认对话框中，阅读消息，然后单击**删除**以确认您要删除此 Active Directory 域信息。

如果没有 JMP 分配使用该 Active Directory 域，该域将被移除。

如果 Active Directory 域被任何 JMP 分配使用，会显示一个警告对话框。警告消息中包含使用该 Active Directory 域的 JMP 分配列表。仅当从 JMP 分配中移除此域，或删除使用此域的那些 JMP 分配后，才能删除域信息。

添加 App Volumes 信息

可以使用 Horizon Console 添加可在创建 JMP 分配时使用的任何其他 App Volumes Manager 的信息。

步骤

1 在 Horizon Console 中，单击 **JMP 配置**。

2 单击 **App Volumes** 选项卡，然后单击**添加**。

将显示**添加 App Volumes 实例**对话框。

3 在**名称**文本框中，输入要分配给 App Volumes 实例的唯一名称。如果将此文本框留空，将使用在 **App Volumes Server URL** 文本框中输入的值。

4 在 **App Volumes Server URL** 文本框中，为要与 JMP Server 关联的 App Volumes Manager 输入一个有效的 URL。如果由负载平衡器来管理所添加的 App Volumes Manager，请输入该负载平衡器的 URL。

注 如果所添加的 App Volumes Manager 连接到不同的 SQL 数据库，则 App Volumes 选项卡中将显示有关所添加 App Volumes Manager 的信息。如果 App Volumes Manager 连接到同一个 SQL 数据库，则 App Volumes 选项卡中将仅显示有关之前已注册的 App Volumes Manager 的信息。

5 输入 JMP Server 可用于访问 App Volumes Manager 的 App Volumes 管理员用户名和密码。

6 为用于 JMP 分配的 App Volumes 服务帐户输入域名。

7 要将当前添加的 App Volumes Manager 设为创建 JMP 分配时使用的默认 App Volumes Manager 服务器，请单击切换按钮。可以更改要在创建 JMP 分配时使用的服务器。

切换按钮会变成蓝色，并带有**是**标签。

8 单击**保存**。

编辑 App Volumes 实例信息

如果必须修改有关由 JMP 分配使用的 App Volumes 实例的现有信息，可以使用 Horizon Console。

步骤

1 在 Horizon Console 中，单击 **JMP 配置**。

2 单击 **App Volumes** 选项卡，然后选择要修改的 App Volumes 实例所在的表行。

3 单击**编辑**。

将显示**添加 App Volumes 实例**对话框。

4 修改要更新的 App Volumes 实例信息。

5 单击**保存**。

删除 App Volumes 实例信息

如果必须删除有关 App Volumes 实例的现有设置信息，请使用 Horizon Console。

仅当已注册的 App Volumes 实例未被任何 JMP 分配使用时，才能从 JMP 设置中删除有关该实例的信息。

步骤

1 在 Horizon Console 中，单击 **JMP 配置**。

2 单击 **App Volumes** 选项卡。

3 选择要从 JMP 设置中删除的 App Volumes 实例信息所在的行。

4 单击**删除**以确认您要删除此 App Volumes 实例信息。

如果没有 JMP 分配使用此 App Volumes 实例，将移除该实例。

如果此 App Volumes 实例被任何 JMP 分配使用，会显示一个警告对话框。警告消息中包含使用 App Volumes 实例的 JMP 分配的列表。仅当从 JMP 分配中移除此 App Volumes 实例，或删除使用此实例的那些 JMP 分配后，才能删除此实例的信息。

添加 Dynamic Environment Manager 配置共享信息

如果在设置初始 Dynamic Environment Manager 配置共享后必须添加另一个配置共享，则可以使用 Horizon Console。

每个 AD 域只能添加一个 Dynamic Environment Manager 配置共享。因此，您要添加的配置共享的 IP 或 DNS 地址不能与 JMP Server 设置中已有的配置共享的 IP 或 DNS 相同。

步骤

1 在 Horizon Console 中，单击 **JMP 配置**。

2 单击 **UEM** 选项卡，然后单击**添加**。

将显示**添加 UEM 文件共享**对话框。

3 在**文件共享 UNC 路径**文本框中以 `\\server-name\UEM-configuration-share-pathname` 格式输入一个值。

例如，如果配置共享位置为 `\\<IP-address>\uemshare\config\general\FlexRepository\..`，那么您需要在**文件共享 UNC 路径**文本框中输入的路径为 **`\\<IP-address>\uemshare\config`**。

4 输入连接 Dynamic Environment Manager 配置文件共享时必须使用的 Dynamic Environment Manager 用户名和密码。

5 从 **Active Directory** 列表中，选择要用于 Dynamic Environment Manager 配置文件共享的域名。

注 一个 Active Directory 只能与一个 Dynamic Environment Manager 配置文件共享关联。

6 单击**保存**。

有关 Dynamic Environment Manager 配置文件共享的信息将添加到 JMP 设置中，并会在 **UEM** 选项卡上的表中添加一个新行。

编辑 Dynamic Environment Manager 配置文件共享信息

如果必须修改有关 JMP 分配所使用的 Dynamic Environment Manager 配置文件共享的现有信息，可以使用 Horizon Console。

步骤

1 在 Horizon Console 中，单击 **JMP 配置**。

2 单击 **UEM** 选项卡，然后从现有信息表中选择要修改的 Dynamic Environment Manager 配置文件共享所在的行。

3 单击**编辑**。

将显示**编辑 UEM 文件共享**对话框。

4 修改需要更新的 Dynamic Environment Manager 配置文件共享信息。

5 单击**保存**。

删除 Dynamic Environment Manager 配置共享信息

如果必须删除有关 Dynamic Environment Manager 配置共享的现有设置信息，请使用 Horizon Console。

仅当已注册的 Dynamic Environment Manager 配置共享未被任何 JMP 分配使用时，才能从 JMP 设置中删除有关该配置共享的信息。

步骤

1 在 Horizon Console 中，单击 **JMP 配置**。

2 单击 **UEM** 选项卡。

3 选择要从 JMP 设置中删除的 Dynamic Environment Manager 配置共享信息所在的行。

4 单击**删除**以确认您要删除此 Dynamic Environment Manager 配置共享信息。

如果没有 JMP 分配使用此 Dynamic Environment Manager 配置共享，将移除此配置共享。

如果此 Dynamic Environment Manager 配置共享被任何 JMP 分配使用，会显示一个警告对话框。警告消息中包含使用该 Dynamic Environment Manager 配置共享的 JMP 分配的列表。仅当将 Dynamic Environment Manager 配置共享从 JMP 分配中移除，或删除使用该配置共享的那些 JMP 分配之后，才能删除此配置共享信息。

管理 JMP 分配

12

安装 JMP Server 并配置 JMP 设置后，可以开始使用 JMP Integrated Workflow 功能来创建、修改、复制或删除 JMP 分配。

必须先安装 JMP Server 并配置 JMP 设置，然后才能开始创建 JMP 分配。有关更多信息，请参阅《VMware Horizon JMP Server 安装和设置指南》和首次配置 JMP 设置。

在创建、编辑、复制或删除 JMP 分配前，请确保满足以下必备条件。

- 确认使用 JMP 设置注册的 Horizon 7 实例已启动且正在运行。
- 确保至少有一个 Active Directory 域使用 JMP 设置进行了注册。
- 确认使用 JMP 设置注册的 App Volumes 实例已启动且正在运行。
- 确认在 JMP 设置中定义的 Dynamic Environment Manager 配置共享已启动且正在运行。

注 不支持全局授权。

尝试创建、编辑、复制或删除 JMP 分配时，可能会收到一条消息，指出所尝试的操作未成功完成。例如，尝试访问其中一个底层 JMP 技术组件时可能会遇到某些问题，从而分配验证无法成功完成。可以在 JMP 分配摘要屏幕上，尝试通过执行以下操作之一来更正此问题。

- 单击**编辑**手动更正这些问题。
- 单击**修复**让 JMP Server 尝试修复当前 JMP 分配上发现的问题。
- 单击**强制删除**移除整个 JMP 分配。

本章讨论了以下主题：

创建 JMP 分配

使用 Horizon Console，您可以创建 JMP 分配，然后使用它们来为用户或用户组创建桌面工作区。

您可以选择 Horizon 桌面池、App Volumes AppStack 和 User Environment Manager 设置以定义 JMP 分配。

前提条件

确保已满足第 12 章 管理 JMP 分配中列出的必备条件。

步骤

1 在 Horizon Console，单击**分配 (JMP)**。

2 单击**新建**。

3 在“新建分配”向导的**用户**选项卡中，输入 Active Directory 下拉列表旁边的几个字符，然后选择要包含在新 JMP 分配中的用户或用户组。

所选的用户或用户组将添加到“已选择的用户/组”部分中。

4 单击**下一步**。

5 在**桌面**选项卡中，选择要包含在 JMP 分配中的桌面池，然后单击**下一步**。

6 在**应用程序**选项卡中，单击想要包含在 JMP 分配中的应用程序名称旁边的复选框。选择完成后，单击**下一步**。

7 在**用户环境**选项卡中，确定是否要使用任何可用的用户环境设置来配置 JMP 分配。

- 将**是否禁用 UEM 设置?** 设置为**否**时，单击**跳过**意味着 User Environment Manager 分配文件将不会保存到 User Environment Manager 配置共享中。所有 User Environment Manager 设置都将应用于使用当前所创建的 JMP 分配为用户创建的虚拟桌面工作区。
- 将**是否禁用 UEM 设置?** 设置为**否**时，选择要应用于所创建的 JMP 分配的用户环境设置。单击**下一步**将使用选定的用户环境设置创建 User Environment Manager 分配文件。所选的设置将应用于使用当前所创建的 JMP 分配为用户创建的虚拟桌面工作区。
- 将**是否禁用 UEM 设置?** 设置为**是**时，将从视图中移除可用用户环境设置列表。当您单击**下一步**时，会将空分配文件写入 User Environment Manager 配置共享。通过禁用 User Environment Manager 设置，可确保不会对使用当前所创建的 JMP 分配为用户创建的虚拟桌面工作区，应用任何用户环境设置。

8 在**定义**选项卡中，接受 JMP 分配的默认名称，或替换为其他名称，并添加描述（可选）。

9 在 **AppStack 连接**下拉列表中，选择何时将 AppStack 附加到 JMP 分配，然后单击**下一步**。

10 在**摘要**选项卡，查看新分配的详细信息。如果可以接受，请单击**提交**。如果必须进行更改，请单击**上一步**以进行调整。

新 JMP 分配将会排入队列，等待存储到 JMP 数据库，并添加到“JMP 分配”窗格中的分配列表中。将 JMP 分配成功添加到 JMP 数据库后，其状态会从“等待处理”发生更改。JMP 分配将变为可从 JMP 分配列表中进行选择，以便您能够对其执行编辑、复制或删除操作。

您还可以使用以下信息验证为新 JMP 分配创建的分配或授权。

- 要验证为 JMP 分配创建的有关 Horizon 桌面池的信息，请使用 Horizon Console。选择**清单 > 桌面**，然后找到 JMP Server 创建的桌面池。
- 要查看 JMP Server 为新 JMP 分配创建的 AppStack 信息，请使用 App Volumes Manager 控制台。选择**卷 > AppStack**，然后找到 JMP Server 创建的 AppStack。
- 要验证您为 JMP 分配配置的用户环境设置，请使用 Dynamic Environment Manager 管理控制台并单击**用户环境**选项卡。从左侧窗格中，选择 JMP 分配所使用的用户环境设置，然后在出现的对话框中单击**分配**选项卡，以查看该用户环境设置的 JMP 分配信息。

编辑 JMP 分配

您可能会由于定义现有 JMP 分配时所使用的组件发生了更改而需要修改该分配。您可以使用 Horizon Console 对 JMP 分配做出必要的更改。

前提条件

- 确保已满足第 12 章 管理 JMP 分配中列出的必备条件。
- 您计划编辑的 JMP 分配不能处于“等待处理”状态。

步骤

1. 在 Horizon Console 中，单击**分配 (JMP)**。
2. 通过单击复选框或列表中的 JMP 分配名称，选择要编辑的 JMP 分配。
3. 单击**编辑**。
4. 在“编辑分配”向导中，修改当前设置。

   如果要在编辑过程中的任何时候停止操作，请单击**取消**。

   a. 如果您要移除当前选定的任何用户或组，请单击删除图标 (**X**)。

   b. 单击**下一步**。

   c. 在**桌面**选项卡中，选择要包括在 JMP 分配中的桌面池。单击**下一步**。

   d. 在**应用程序**选项卡中，选择要添加到 JMP 分配的可用应用程序，或取消选择之前选择的可用应用程序。单击**下一步**。

e 在**用户环境**选项卡中，确定是否要使用任何可用的用户环境设置来配置 JMP 分配。

- 将**是否禁用 UEM 设置?** 设置为**否**时，单击**跳过**意味着 User Environment Manager 分配文件将不会保存到 User Environment Manager 配置共享中。所有 User Environment Manager 设置都将应用于使用当前所编辑的 JMP 分配为用户创建的虚拟桌面工作区。
- 将**是否禁用 UEM 设置?** 设置为**否**时，选择要应用于所创建的 JMP 分配的用户环境设置。单击**下一步**将使用选定的用户环境设置创建 User Environment Manager 分配文件。选定的设置将应用于使用当前所编辑的 JMP 分配为用户创建的虚拟桌面工作区。
- 将**是否禁用 UEM 设置?** 设置为**是**时，将从视图中移除可用用户环境设置列表。当您单击**下一步**时，会将空分配文件写入 User Environment Manager 配置共享。通过禁用 User Environment Manager 设置，可确保不会对使用当前所编辑的 JMP 分配为用户创建的虚拟桌面工作区，应用任何用户环境设置。

f 在**定义**选项卡中，（如果适用）修改**名称**和**描述**的当前值或将 AppStack 附加到 JMP 分配的时间。

g 单击**下一步**。

h 查看所做更改的摘要，然后单击**提交**以保存修改。

如果提交成功，会保存所做的更改。如果遇到任何问题，会提供进一步信息，同时显示您可以执行的可行操作。

复制 JMP 分配

可以通过复制与想要创建的 JMP 分配相似的现有 JMP 分配，更快速地创建 JMP 分配。

前提条件

- 确保已满足第 12 章 管理 JMP 分配中列出的必备条件。
- 计划复制的 JMP 分配不能为“等待处理”或“错误”状态。

步骤

1 从 Horizon Console 中，选择**分配 (JMP)**。

2 选择要复制的 JMP 分配，然后单击**复制**。

3 在“新建分配”向导中，根据需要修改复制的 JMP 分配。

a 选择新用户或组，或者移除所有当前选定的用户或组。单击**下一步**。

b 在“桌面”窗格中，选择一个新的桌面池，或移除所复制的 JMP 分配中包含的任何桌面池。单击**下一步**。

c 选择要包含在新 JMP 分配中的其他应用程序，并取消选择当前选定的应用程序。单击**下一步**。

d 在“用户环境”窗格中，选择要应用于新 JMP 分配的 User Environment Manager 设置。单击**下一步**。

e 在“定义名称”中，可以根据需要替换所创建的默认名称。添加描述，然后指定希望将 AppStack 附加到新 JMP 分配的时间。

f 单击**下一步**，然后查看新 JMP 分配的详细信息摘要。

g 如果对这些信息满意，请单击**提交**。否则，请单击**上一步**进行任何更正。

将验证新 JMP 分配，这可能需要一些时间。验证成功后，会将新创建的 JMP 分配添加到“JMP 分配”窗格上的列表中。将指针放到该分配的名称上时，可以看到它处于等待处理状态，直至成功保存到 JMP 数据库为止。JMP 分配不再处于等待处理状态后，可以对该分配执行任何其他操作。

删除 JMP 分配

可以使用 Horizon Console 删除 JMP 分配。

删除 JMP 分配后，将删除与 JMP 分配关联的 Horizon 池授权、AppStack 分配和 UEM 授权。但是，如果 JMP 分配使用的 Horizon 池授权或 AppStack 分配在创建 JMP 分配之前就存在，将不会被删除。删除 JMP 分配后，它将不再应用于用户或桌面。

前提条件

- 确认已满足第 12 章 管理 JMP 分配中列出的必备条件。
- 计划删除的 JMP 分配不能为“等待处理”状态。

步骤

1 在 Horizon Console 中，单击**分配 (JMP)**。

2 在“JMP 分配”窗格中，选择一个或多个 JMP 分配，然后单击**删除**。

3 在确认对话框中，单击**删除**以确认您要永久删除此分配。

如果删除成功，将从 JMP 数据库以及“JMP 分配”窗格的列表中移除 Horizon 池授权。

如果删除操作未完全成功，将不会删除 JMP 分配。单击状态指示器可提供有关删除操作失败原因的更多信息。

在 Horizon Console 中配置事件报告

13

您可以创建事件数据库来记录有关 Horizon 7 事件的信息。此外，如果您使用 Syslog 服务器，则可以对连接服务器进行配置，使其向 Syslog 服务器发送事件或创建以 Syslog 格式编写的事件平面文件。

本章讨论了以下主题：

在 Horizon Console 中为 Horizon 7 事件添加数据库和数据库用户

您可以通过将事件数据库添加到现有数据库服务器，从而创建一个事件数据库。之后，便可以使用报告软件来分析数据库中的事件。

在专用服务器上部署事件数据库的数据库服务器，以便事件日志记录活动不会影响置备和对 Horizon 7 部署比较重要的其他活动。

注　您无需为此数据库创建 ODBC 数据源。

前提条件

- 确认在连接服务器实例可访问的系统上具有支持的 Microsoft SQL Server 或 Oracle 数据库服务器。

  有关受支持的数据库的最新信息，请参阅 http://www.vmware.com/resources/compatibility/sim/interop_matrix.php 上的“VMware 产品互操作性列表”。有关**解决方案/数据库互操作性**，选择产品和版本后，在“添加数据库”步骤中选择**任意**，然后单击**添加**可查看所有受支持的数据库的列表。
- 确认您拥有在数据库服务器上创建数据库和用户所需的数据库特权。
- 如果您不熟悉在 Microsoft SQL Server 数据库服务器上创建数据库的过程，请参阅《Horizon 7 安装指南》文档中的“将 View Composer 数据库添加到 SQL Server”。

- 如果您不熟悉在 Oracle 数据库服务器上创建数据库的过程，请参阅《Horizon 7 安装指南》文档中的“将 View Composer 数据库添加到 Oracle 12c 或 11g”。

步骤

1 向服务器中添加一个数据库，并为其提供一个描述性名称，如 HorizonEvents。

对于 Oracle 12c 或 Oracle 11g 数据库，还需要提供 Oracle 系统标识符 (System Identifier, SID)，当您在 Horizon Console 中配置事件数据库时将使用该标识符。

2 为该数据库添加一个用户，该用户应具有创建表、视图、Oracle 触发器和序列的权限，以及读写这些对象的权限。

对于 Microsoft SQL Server 数据库，不要使用集成 Windows 身份验证 (Integrated Windows Authentication) 安全模式方法进行身份验证。请确认您使用的是 SQL Server 身份验证方法进行身份验证。

随即会创建数据库，但模式将在 Horizon Console 中配置数据库之后才会安装。

后续步骤

按照在 Horizon Console 中配置事件数据库中的说明操作。

在 Horizon Console 中为事件报告准备 SQL Server 数据库

您必须先配置正确的 TCP/IP 属性并确认 Microsoft SQL Server 使用了 SQL Server 身份验证，然后才能使用 Horizon Console 在该服务器上配置事件数据库。

前提条件

- 为事件报告创建一个 SQL Server 数据库。请参阅在 Horizon Console 中为 Horizon 7 事件添加数据库和数据库用户。
- 确认您拥有配置数据库所需的数据库特权。
- 确认数据库服务器使用 SQL Server 身份验证方法。不要使用 Windows 身份验证。

步骤

1 打开 SQL Server Configuration Manager 并展开 **SQL Server *YYYY* 网络配置**。

2 选择 ***server_name* 使用的协议**。

3 在协议列表中，右键单击 **TCP/IP** 并选择**属性**。

4 将**已启用**属性设置为**是**。

5 确认已分配了一个端口，或者在必要时分配一个端口。

有关静态和动态端口以及如何分配端口的信息，请参阅 SQL Server Configuration Manager 的联机帮助。

6 确认该端口未被防火墙阻止。

后续步骤

使用 Horizon Console 将数据库连接到连接服务器。按照在 Horizon Console 中配置事件数据库中的说明操作。

在 Horizon Console 中配置事件数据库

事件数据库会将有关 Horizon 7 事件的信息存储为数据库记录，而不是日志文件记录。

安装连接服务器实例后，您便可以配置事件数据库。您只需要在连接服务器组中配置一个主机。组中剩余的主机会自动进行配置。

注　确保连接服务器实例与外部数据库之间的数据库连接安全是管理员的职责，但事件流量仅限于有关 Horizon 7 环境运行状况的信息。如果想采取额外的预防措施，可以通过 IPSec 或其他途径保护此通道的安全，也可以在连接服务器计算机本地部署数据库。

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。

您还可以生成 Syslog 格式的 Horizon 7 事件，以便第三方分析软件能够访问事件数据。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。请参阅《Horizon 7 管理指南》文档中的“使用 -I 选项生成 Syslog 格式的 Horizon 7 事件日志消息”。

前提条件

配置事件数据库时需要以下信息：

- 数据库服务器的 DNS 名称或 IP 地址。
- 数据库服务器的类型：Microsoft SQL Server 或 Oracle。
- 用来访问数据库服务器的端口号。适用于 Oracle 的默认端口号是 1521；适用于 SQL Server 的默认端口号是 1433。对于 SQL Server，如果数据库服务器是已经命名的实例，或者您使用的是 SQL Server Express，您可能需要确定端口号。有关连接到已命名的 SQL Server 实例的信息，请参阅 http://support.microsoft.com/kb/265808 上的 Microsoft 知识库文章。
- 您在数据库服务器上创建的事件数据库名称。请参阅在 Horizon Console 中为 Horizon 7 事件添加数据库和数据库用户。

  对于 Oracle 12c 或 11g 数据库，在 Horizon Console 中配置事件数据库时，必须使用 Oracle 系统标识符 (SID) 作为数据库名称。
- 为该数据库创建的用户的用户名和密码。请参阅在 Horizon Console 中为 Horizon 7 事件添加数据库和数据库用户。

  为该用户使用 SQL Server 身份验证 (SQL Server Authentication)。不要使用集成 Windows 身份验证 (Integrated Windows Authentication) 安全模式方法进行身份验证。

- 事件数据库中表的前缀，如 VE_。通过添加前缀，可在安装的 Horizon 7 之间共享数据库。

  注 您必须输入对当前使用的数据库软件有效的字符。填写完对话框时不会对前缀语法进行检查。如果输入的字符对当前使用的数据库软件无效，则当连接服务器尝试连接数据库服务器时将会出现错误。日志文件会提示所有错误，其中包括该错误和数据库名称无效时从数据库服务器返回的任何其他错误。

步骤

1 在 Horizon Console 中，选择**设置 > 事件配置**。

2 在**事件数据库**区域中，单击**编辑**，然后在提供的字段中输入信息，最后单击**确定**。

  要清除事件数据库信息，请单击**清除**。

3 （可选） 在”事件设置“窗口中，单击**编辑**，分别更改事件的显示时间长度以及将事件归为新事件的天数，然后单击**确定**。

  这些设置可控制事件在 Horizon Console 界面中显示的时间长度。在此之后，事件仅在历史数据库表中可见。

4 选择**监视 > 事件**，确认已成功连接到事件数据库。

  如果连接失败，则会显示错误消息。如果您使用 SQL Express 或命名的 SQL Server 实例，您可能需要确定正确的端口号，如前提条件中提到的端口号。

在 Horizon Console 中配置指向文件或 Syslog 服务器的事件日志记录

您可以生成 Syslog 格式的 Horizon 7 事件，以便分析软件能够访问事件数据。

您只需要在连接服务器组中配置一个主机。组中剩余的主机会自动进行配置。

如果启用基于文件的事件日志记录，则事件会在本地日志文件中累积。如果指定文件共享，这些日志文件将移至该共享中。

- 在删除最早的文件之前，本地事件日志目录的最大大小（包含已关闭的日志文件）为 300MB。Syslog 输出的默认目标位置为 `%PROGRAMDATA%\VMware\VDM\events\`。
- 如果是时间很长的事件记录，或者您没有 Syslog 服务器或事件数据库，或者当前的 Syslog 服务器无法满足您的要求，请使用 UNC 路径来保存日志文件。

您也可以使用 `vdmadmin` 命令以 Syslog 格式配置基于文件的事件日志记录。请参阅《Horizon 7 管理指南》文档中有关使用 `vdmadmin` 命令的 `-I` 选项生成 Syslog 格式的 Horizon 7 事件日志消息的主题。

重要事项 在向 Syslog 服务器发送 Syslog 数据时，将在不使用软件加密的情况下跨网络发送这些数据，其中可能包含敏感数据（如用户名）。VMware 建议使用链路层安全机制（例如 IPSEC）来避免这类数据在网络上受到监视。

前提条件

配置连接服务器时需要使用以下信息，以便能以 Syslog 格式记录事件和/或将事件发送到 Syslog 服务器：

- 如果您计划使用 Syslog 服务器侦听 UDP 端口上的 Horizon 7 事件，您必须具有 Syslog 服务器的 DNS 名称或 IP 地址以及 UDP 端口号。默认 UDP 端口号为 514。
- 如果您计划以平面文件格式收集日志，则必须拥有指向存有日志文件的文件共享和文件夹的 UNC 路径，同时还必须具备有权对文件共享执行写入操作的帐户的用户名、域名和密码。

步骤

1 在 Horizon Console 中，选择**设置 > 事件配置**。

2 （可选） 在 **Syslog** 区域，要将连接服务器配置为向 Syslog 服务器发送事件，请单击**发送到 Syslog 服务器**下方的**添加**，然后提供服务器名称或 IP 地址以及 UDP 端口号。

3 （可选） 在**事件到文件系统**区域中，选择是否允许以 Syslog 格式生成事件日志消息并存储在日志文件中。

选项	说明
始终	始终以 Syslog 格式生成事件日志消息并存储在日志文件中。
出现错误时记录到文件（默认）	如果在将事件写入事件数据库或 Syslog 服务器时出现问题，则将审核事件记录到日志文件中。默认情况下，将启用此选项。
从不	从不以 Syslog 格式生成事件日志消息并存储在日志文件中。

如果不指定文件共享的 UNC 路径，日志文件会保留在本地。

4 （可选） 要将 Horizon 7 事件日志消息存储在文件共享中，请单击**复制到位置**下方的**添加**，然后提供文件共享的 UNC 路径和用于存储日志文件的文件夹，以及具有文件共享写入权限的帐户的用户名、域名和密码。

以下是 UNC 路径示例：

```
\\syslog-server\folder\file
```

在 Horizon 7 中监控事件

事件数据库存储了连接服务器主机或组、Horizon Agent 以及 Horizon Console 中所发生事件的相关信息，并会在仪表板中显示事件数量。您可以在**事件**页面上查看事件的详细信息。

注 事件会在 Horizon Console 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 Console 界面中查看这些事件。

除了监控 Horizon Console 中的事件外，还可以生成 Syslog 格式的 Horizon 7 事件，从而允许分析软件访问事件数据。请参阅《Horizon 7 安装指南》文档中的在 Horizon Console 中配置指向文件或 Syslog 服务器的事件日志记录和“使用 -l 选项以 Syslog 格式生成 Horizon 7 事件日志消息”。

如果为多个连接服务器配置了事件数据库，则 Horizon Console 将在**事件**页面上显示与所有连接服务器相关的事件。Horizon Console 会根据您执行的任务筛选事件，并在相关页面上显示这些事件，例如**桌面池**页面或**应用程序池**页面。

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 Console 中，选择**监控 > 事件**。

2 （可选） 在**事件**页面上，您可以选择事件的时间范围，对事件应用筛选器，并在一个或多个列中对列出的事件进行排序。

后续步骤

在 Horizon Console 中，导航到桌面或应用程序池、虚拟机、永久磁盘、用户或组，然后单击**事件**选项卡以查看特定事件。

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 13-1. 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。

在 Horizon Console 中使用 Horizon Help Desk Tool

14

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《Horizon 7 管理指南》文档。
- 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 管理指南》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《Horizon 7 管理指南》文档。
- 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 vdmadmin 命令可在每个连接服务器实例上启用时间安排分析器：

  ```
  vdmadmin -I -timingProfiler -enable
  ```

  使用以下 vdmadmin 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：

  ```
  vdmadmin -I -timingProfiler -enable -server {ip/server}
  ```

本章讨论了以下主题：

在 Horizon Console 中启动 Horizon Help Desk Tool

Horizon Help Desk Tool 已集成到 Horizon Console 中。您可以搜索要在 Horizon Help Desk Tool 中为其排除故障的用户。

步骤

1 您可以在“用户搜索”文本框中搜索用户名或直接导航到 Horizon Help Desk Tool 工具。

- 在 Horizon Console 的“用户搜索”文本框中输入用户名。
- 选择**监控 > 技术支持**，然后在“用户搜索”文本框中输入用户名。

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。

2 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。

您可以单击电子邮件地址来向用户发送消息。

您还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。

注 对于 Linux 桌面用户，不会显示 Skype for Business 信息。

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 14-1. “会话”选项卡

选项	说明
状态	显示有关桌面或应用程序会话状态的信息。 ■ 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。
计算机名称	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。 您可以单击会话信息卡中的选项卡以查看其他信息： ■ **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。 ■ **进程**选项卡显示有关 CPU 和内存相关进程的信息。 ■ **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。 注　对于 Linux 桌面会话，您无法访问**应用程序**选项卡。
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

桌面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 14-2. 桌面

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。对于 Linux 桌面会话，Linux 显示为桌面池。
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”。

表 14-2. 桌面 （续）

选项	说明
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

应用程序选项卡显示有关用户有权使用的已发布应用程序的信息。

注 对于 Linux 桌面会话，您无法访问**应用程序**选项卡。

表 14-3. 应用程序

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** 如果存在全局应用程序授权，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”。
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 Cloud Pod 架构环境中，不会显示用户的事件日志信息。

表 14-4. 活动

选项	说明
时间	选择时间范围。默认值为过去 12 小时。 ■ **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。

表 14-4. 活动 （续）

选项	说明
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 14-5. 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。
操作系统版本	操作系统版本。
连接服务器	会话连接到的连接服务器。
池	桌面或应用程序池的名称。对于 Linux 桌面池，显示 Linux。
vCenter	vCenter Server 的 IP 地址。
会话状态	桌面或应用程序会话的状态。会话状态可能是空闲、活动或已断开。如果用户处于不活动状态的时间达到一分钟，则会话状态会变为空闲。状态图标显示绿色轮廓时表示空闲，显示纯绿色时表示活动，显示灰色时表示已断开连接。 注　Linux 桌面会话不显示空闲状态。
会话持续时间	会话保持连接到连接服务器的时间。
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。
网关/代理名称	安全服务器、Unified Access Gateway 设备或负载平衡器的名称。此信息在连接到会话之后可能需要 30 到 60 秒才能显示。

表 14-5. 虚拟机详细信息 （续）

选项	说明
网关/代理 IP	安全服务器、Unified Access Gateway 设备或负载平衡器的 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。
场	已发布的桌面或应用程序会话的 RDS 主机的场。

用户体验衡量指标

显示使用 PCoIP 或 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**更多**。要刷新这些详细信息，请单击刷新图标。

表 14-6. PCoIP 显示协议详细信息

选项	说明
TX 带宽	PCoIP 会话中的传输带宽（单位为 kbps）。
帧速率	PCoIP 会话中的帧速率（帧/秒）。
数据包丢失	PCoIP 会话中的数据包丢失百分比。
Skype 状态	PCoIP 会话中的 Skype for Business 状态。 ■ 已优化 ■ 回退 ■ 已优化 (版本不匹配) ■ 回退 (版本不匹配) ■ 正在连接 ■ 已断开连接 ■ 未定义 对于 Linux 桌面会话，此选项显示为“不适用”。

表 14-7. Blast 显示协议详细信息

选项	说明
帧速率	Blast 会话中的帧速率（帧/秒）。
Skype 状态	Blast 会话中的 Skype for Business 状态。 ■ 已优化 ■ 回退 ■ 已优化 (版本不匹配) ■ 回退 (版本不匹配) ■ 正在连接 ■ 已断开连接 ■ 未定义 对于 Linux 桌面会话，此选项显示为“不适用”。
BLAST 会话计数器	■ **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。

表 14-7. Blast 显示协议详细信息 （续）

选项	说明
BLAST 图像处理计数器	■ **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	■ **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	■ **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 和内存使用情况及网络和磁盘性能

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 显示协议的网络或磁盘性能图表。

注 在桌面上启动或重新启动 Horizon Agent 后，性能图表可能不会立即显示时间轴。时间轴会在几分钟后显示。

表 14-8. CPU 使用情况

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。

表 14-9. 内存使用情况

选项	说明
会话内存	当前会话的内存使用情况。
主机内存	向其分配会话的虚拟机的内存使用情况。

表 14-10. 网络性能

选项	说明
延迟	显示 PCoIP 或 Blast 会话的延迟图表。 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**。 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**。

表 14-11. 磁盘性能

选项	说明
读取	每秒读取输入/输出 (Input/Output, I/O) 操作的次数。
写入	每秒写入 I/O 操作的数量。
磁盘延迟	显示磁盘延迟的图表。磁盘延迟是从 Windows 性能计数器中检索每秒输入/输出操作 (Input/Output Operations Per Second, IOPS) 数据的时间（以毫秒为单位）。
平均读取速率	每秒随机读取 I/O 操作的平均次数。
平均写入速率	每秒随机写入 I/O 操作的平均次数。
平均延迟	从 Windows 性能计数器中检索 IOPS 数据的平均延迟时间（以毫秒为单位）。

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 14-12. 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。
登录分段	显示在登录过程中创建的分段。 ■ **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。 ■ **协议连接**。在登录过程中完成 PCoIP 或 Blast 协议连接所用的总时间。 ■ **登录脚本**。登录脚本从开始执行到完成所用的总时间。 ■ **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。如果未配置任何全局策略，则 **GPO 加载**登录分段的时间为 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。新会话将显示**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。
- 如果会话是 Linux 桌面会话，则不会显示 **GPO 加载**和**配置文件加载**分段。
- 在连接桌面会话时不会立即显示登录数据。登录数据会在几分钟后显示。

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。

对于 RDS 主机会话，**进程**选项卡会显示由当前用户或当前系统进程启动的当前 RDS 主机会话进程。

表 14-13. 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。 您无法结束**进程**选项卡中可能会列出的关键进程，例如 Windows 核心进程。如果要结束某个关键进程，则 Horizon Help Desk Tool 会显示一条消息，指示其无法结束此系统进程。

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。对于 Linux 桌面会话，您无法访问**应用程序**选项卡。

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。

您可以为最终用户结束应用程序进程。要结束应用程序进程，请单击**结束应用程序**，然后单击**确定**以确认更改。

注　如果应用程序正在等待用户交互（例如存在未保存的数据），或者由于出现其他异常，结束应用程序进程的操作可能会失败。但是，在您结束应用程序时，Horizon Help Desk Tool 不会显示任何成功或失败消息。

表 14-14. 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。
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	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。 **注** 此功能不适用于 Linux 桌面用户。 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。 **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。
重新启动	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。 单击**重新启动 VDI**。
断开连接	断开桌面或应用程序会话连接。 单击**更多 > 断开连接**。
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 vdmadmin 命令

15

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。

- 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#unique_9。

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 15-1. 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。
-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 15-2. 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#unique_186。
-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] -getlogfilelogfile-outfile local_file-d desktop-mmachine
```

```
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 [-mmachine]
```

```
vdmadmin
-A [-b authentication_arguments] -list [-xml] [-w | -n] -d desktop-m machine
```

```
vdmadmin
-A [-b authentication_arguments] -setloglevel level -ddesktop [-mmachine]
```

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 15-3. 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。
`-outfile` *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。
`-setloglevel` *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。

```
vdmadmin -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。

```
vdmadmin -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。

```
vdmadmin -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`。

```
vdmadmin -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。

```
vdmadmin -A -d dtpool2 -m machine1 -getversion
```

显示桌面池 dtpool2 中虚拟机 machine1 的 Horizon Agent 状态。

```
vdmadmin -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。

```
vdmadmin -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 vdmadmin 命令覆盖 Horizon Agent 报告的 IP 地址。

语法

```
vdmadmin
-A [-bauthentication_arguments] -override-iip_or_dns-ddesktop-mmachine
```

```
vdmadmin
-A [-bauthentication_arguments] -override-list-ddesktop-mmachine
```

```
vdmadmin
-A [-bauthentication_arguments] -override-r-ddesktop [-mmachine]
```

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地址不符，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 15-4. 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 [–bauthentication_arguments] [–udomain\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] -monitoridmonitor_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 15-5. 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 15-6. 列出并显示运行状况监视器的选项

选项	说明
-instanceid *instance_id*	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 *monitor_id*	显示指定运行状况监视器 ID 的监视器实例。
-monitorid *monitor_id*	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 15-7. 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。

表 15-7. 列出并显示报告和视图的选项 （续）

选项	说明
`-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 15-8. 以 Syslog 格式生成 Horizon 7 事件日志消息的选项

选项	说明
-disable	禁用 Syslog 日志记录。
-e|-enable	启用 Syslog 日志记录。
-eventSyslog	指定 Horizon 7 事件以 Syslog 格式生成。
-localOnly	仅在本地系统中存储 Syslog 输出。使用 -localOnly 选项时，Syslog 输出的默认目标位置为 %PROGRAMDATA%\VMware\VDM\events\。
-password *密码*	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。
-path	确定 Syslog 输出的目标 UNC 路径。
-u|-user *域名\用户名*	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。

```
vdmadmin -I -eventSyslog -disable
```

将 Horizon 7 事件的 Syslog 输出仅定向到本地系统。

```
vdmadmin -I -eventSyslog -enable -localOnly
```

将 Horizon 7 事件的 Syslog 输出定向到指定路径。

```
vdmadmin -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。

```
vdmadmin -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 vdmadmin 选项的 -L 命令从一个专用池中向用户分配计算机。

语法

```
vdmadmin
-L [-bauthentication_arguments] -ddesktop-m machine-udomain\user
```

```
vdmadmin
-L [-bauthentication_arguments] -ddesktop [-mmachine | -udomain\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，您可能需要在他们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 15-9. 分配专用桌面的选项

选项	说明
-d *桌面*	指定桌面池名称。
-m *计算机*	指定托管远程桌面的虚拟机名称。
-r	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。
-u *域\用户*	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。

- 被分配的用户的 SID。
- 被分配的用户的帐户名。
- 被分配的用户的域名。
- 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 15-10. 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。

```
vdmadmin -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。

```
vdmadmin -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 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。

语法

```
vdmadmin
-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 vdmadmin 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 #unique_203。
- 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 15-11. 回收虚拟机上磁盘空间的选项

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。
-MarkForSpaceReclamation	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} -domaindomain-add [-s
connsvr]
```

```
        vdmadmin
        -N [-b authentication_arguments] -domains-list [-w | -n] [-xml]
```

```
        vdmadmin
        -N [-bauthentication_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 15-12. 配置域过滤器的选项

选项	说明
-add	将域添加到列表中。
-domain *域*	指定要过滤的域。 必须用域的 NetBIOS 名称而非 DNS 名称来指定域。
-domains	指定一个域过滤操作。
-exclude	在排除列表中指定操作。
-include	在包含列表中指定操作。
-list	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。
-list -active	显示运行该命令的连接服务器实例上可用的域。
-remove	从列表中移除域。

表 15-12. 配置域过滤器的选项 （续）

选项	说明
-removeall	从列表中移除所有域。
-s *connsvr*	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。
-search	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在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 15-13. 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，而该域的控制器当前无法访问，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指定 Horizon 7 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 15-14. 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。
–noxslt	指定输出的 XML 文件不应用默认样式表。
–xsltpath *path*	指定用于转换 XML 输出的样式表的路径。

表 15-15. XSL 样式表 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 15-15. XSL 样式表

样式表文件名	说明
unentitled-machines.xsl	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。
unentitled-policies.xsl	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] [-groupgroup_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 15-16. 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` *client_id*	指定客户端的名称或 MAC 地址。
`-description` "*description_text*"	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` *domain_name*	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。

表 15-16. 配置 kiosk 模式客户端的选项 （续）

选项	说明
`-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` *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。
`-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。
`-ou` *DN*	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 `-setdefaults` 选项更改组织单位的配置。
`-password` "*password*"	为客户端帐户指定显式密码。
`-remove`	移除处于 kiosk 模式的客户端帐户。
`-removeall`	移除所有处于 kiosk 模式的客户端的帐户。
`-requirepassword`	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。
`-s` *connection_server*	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。
`-setdefaults`	设置添加客户端帐户使用的默认值。
`-update`	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
```

将按其 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
```

将按其 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 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。

注 带有 -R 选项的 vdmadmin 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

```
vdmadmin
-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。

```
vdmadmin -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 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。

语法

```
vdmadmin
-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 vdmadmin 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 VMwareVDMDS 程序。

3 在另一个连接服务器实例上，使用 vdmadmin 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。

```
vdmadmin -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 vdmadmin 命令为管理员用户提供 Active Directory 辅助凭据。

语法

```
          vdmadmin
          -T [-b authentication_arguments] -domainauth
{-add | -update | -remove | -removeall | -list} -ownerdomain\user-userdomain\user [-passwordpassword]
```

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 vdmadmin 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 15-17. 用于提供辅助凭据的选项

选项	说明
-add	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)。
-update	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。
-list	显示所有者帐户的安全凭据。不会显示密码。
-remove	移除所有者帐户的安全凭据。
-removeall	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 [-bauthentication_arguments] -e-ddesktop-mmachine [-m machine] ...
```

```
vdmadmin
-V [-bauthentication_arguments] -e-vcdnvCenter_dn-vmpath inventory_path
```

```
vdmadmin
-V [-b authentication_arguments] -p-d desktop -m machine [-mmachine] ...
```

```
vdmadmin
-V [-b authentication_arguments] -p-vcdnvCenter_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 15-18. 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 `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。

语法

```
        vdmadmin
        -X [-bauthentication_arguments] -collisions [-resolve]
vdmadmin-X [-bauthentication_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 `vdmadmin` 命令，以手动检测和解决 LDAP 条目冲突。

当 LDAP 复制无效时，升级期间也可能会发生 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 `vdmadmin` 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 15-19. 用于检测和解决 LDAP 条目冲突的选项

选项	说明
`-collisions`	指定一个用于检测连接服务器组中的 LDAP 条目冲突的操作。
`-resolve`	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 15-20. 用于检测和解决 LDAP 模式冲突的选项

选项	说明
`-schemacollisions`	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。
`-resolve`	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。
`-global`	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
```