Horizon 7 架构规划指南

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

Horizon 7 体系结构规划指南

《Horizon 7 体系结构规划指南》主要介绍了 VMware Horizon™ 7 的相关信息，包括主要功能特性和部署选项，同时简要介绍了生产环境中的常见组件设置方式。

本指南回答了以下问题：

- 本产品能否解决您需要解决的问题？
- 在您的企业中实施此解决方案是否是一种可行且经济高效的做法？

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。

为帮助您保护已安装的 VMware Horizon View，本指南还针对一些安全功能进行了讨论。

目标读者

本文档所述信息面向 IT 决策制定者、架构师、管理员和其他需要熟悉本产品组件及功能的人员。通过了解这些信息，架构师和规划人员可确定 Horizon 7 是否能够满足企业向最终用户高效、安全地交付 Windows 桌面和应用程序的要求。规划人员可借助示例体系结构了解进行大规模部署所需达到的硬件要求及需要进行的设置工作。

Horizon 7 简介

1

借助 Horizon 7，IT 部门可在数据中心内运行远程桌面和应用程序，并将这些桌面和应用程序作为受管服务交付给员工。最终用户可以获得熟悉的个性化环境，并可以在企业或家庭中的任何地方访问此环境。通过将桌面数据放在数据中心，管理员可以集中进行控制并提高效率和安全性。

本章讨论了以下主题：

使用 Horizon 7 的优势

使用 Horizon 7 能有效提高企业桌面管理的可靠性、安全性、硬件独立性与便捷性。

可靠性与安全性

通过将桌面和应用程序与 VMware vSphere® 进行集成，并对服务器、存储和网络资源进行虚拟化，可实现对桌面和应用程序的集中式管理。将桌面操作系统和应用程序放置于数据中心的某个服务器上可带来以下优势：

- 轻松限制数据访问。防止敏感数据被复制到远程员工的家用计算机。
- RADIUS 支持为选择双因素身份验证供应商提供了灵活性。支持的供应商包括 RSA SecureID、VASCO DIGIPASS、SMS Passcode 和 SafeNet 等。
- 与 VMware Identity Manager 集成意味着最终用户可通过他们用来访问 SaaS、Web 和 Windows 应用程序的同一个基于 Web 的应用程序目录来按需访问远程桌面。用户还可以在远程桌面内使用此自定义应用程序存储来访问应用程序。
- 通过使用预创建的 Active Directory 帐户置备远程桌面，满足具有只读访问策略的锁定 Active Directory 环境的需求。
- 安排数据备份时无须考虑最终用户的系统是否关闭。

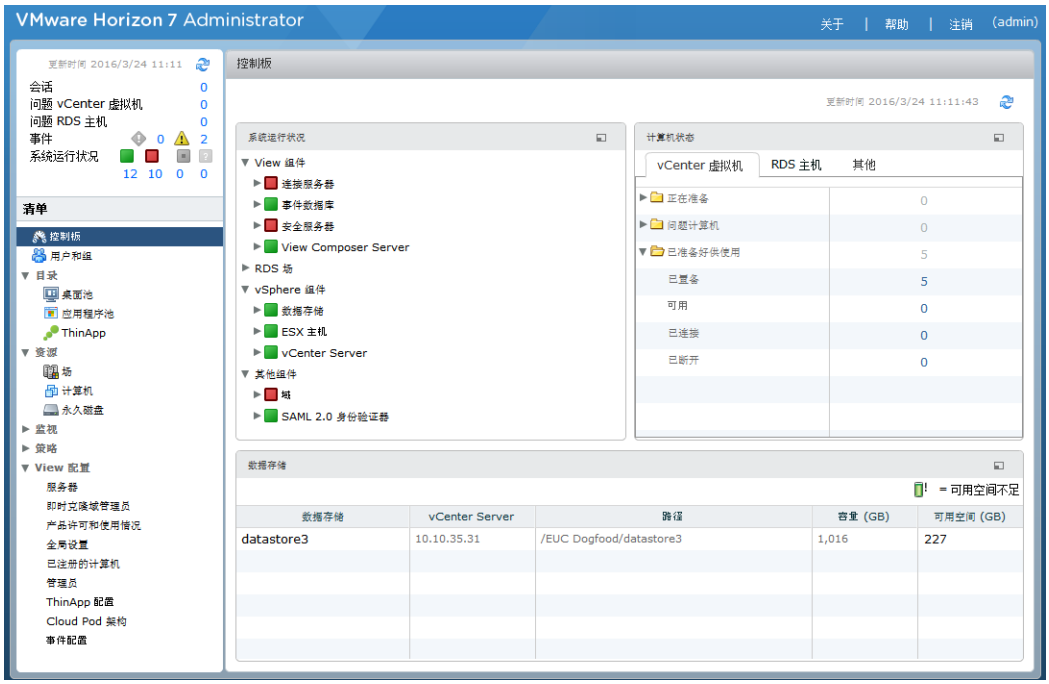
- 数据中心托管的远程桌面和应用程序不会或很少停机。虚拟机可以驻留在具有高可用性的 VMware 服务器群集中。

虚拟桌面还可连接到后端物理系统和 Microsoft 远程桌面服务 (RDS) 主机。

便捷性

统一管理控制台可支持扩展，即使最大规模的 Horizon 7 部署也能通过单个管理界面来有效管理。向导和仪表板可增强工作流，并有助于深入查看详细信息或更改设置。图 1-1. 显示控制板视图的管理控制台 提供了基于浏览器的 Horizon Administrator 用户界面示例。

图 1-1. 显示控制板视图的管理控制台



提高简便性的其他功能包括 VMware 远程显示协议 PCoIP (PC-over-IP) 和 Blast Extreme。这些显示协议提供与使用物理 PC 相同的最终用户体验：

- 在 LAN 中，显示速度较传统远程显示更快，且更流畅。
- 在 WAN 中，这些显示协议还能弥补因延迟增加或带宽减少导致的不便，确保最终用户在任何网络条件下均可保持高效。

可管理性

您能够在很短的时间内置备最终用户的桌面和应用程序。无需在每个最终用户的物理 PC 上逐一安装应用程序。最终用户可连接到已发布的应用程序或应用程序齐备的远程桌面。最终用户可以在不同位置使用各种设备访问同一个远程桌面或应用程序。

使用 VMware vSphere 托管虚拟桌面和 RDS 主机服务器可带来以下优势：

- 简化管理任务和管理工作。管理员无须访问用户的物理 PC 即可修补和升级应用程序和操作系统。

- 与 VMware Identity Manager 集成意味着 IT 管理员能够使用基于 Web 的 VMware Identity Manager 管理界面来监视用户和组的远程桌面授权。
- 通过与 VMware App Volumes（实时应用程序提供系统）集成在一起，企业可以批量提供和管理应用程序。可以使用 App Volumes 将应用程序连接到用户、组或目标计算机，甚至在用户登录到其桌面后。也可以实时置备、提供、更新和停止使用应用程序。
- 通过 Horizon Persona Management，可以集中管理物理桌面和虚拟桌面，包括用户配置文件、应用程序授权、策略、性能及其他设置。转换到虚拟桌面之前，需要为物理桌面用户部署用户配置管理。
- 通过使用 VMware User Environment Manager，最终用户可以获得针对用户情况调整的个性化 Windows 桌面，这意味着，访问所需的 IT 资源基于角色、设备和位置等因素。
- 简化存储管理。借助 VMware vSphere，您可以虚拟化卷和文件系统，从而避免管理单独的存储设备。
- 使用 vSphere 6.0 或更高版本时，可以使用虚拟卷 (VVol)。此功能可将虚拟磁盘及其衍生产品、克隆、快照和副本直接映射到存储系统上名为虚拟卷的对象。此映射允许 vSphere 将密集型存储操作（如拍摄快照、克隆和复制）卸载到存储系统。例如，之前需要一小时的克隆操作现在通过使用虚拟卷只需要几分钟。
- 对于 vSphere 5.5 Update 1 或更高版本，您可以使用 vSAN，它将 ESXi™ 主机上的本地物理固态磁盘和硬盘驱动器虚拟化为一个由群集中的所有主机共享的数据存储。可在创建桌面池时仅指定一个数据存储，各种组件（如虚拟机文件、副本、用户数据和操作系统文件）将根据需要放置在 SSD 磁盘或硬盘上。

  您可以采用默认存储策略配置文件的格式管理虚拟机存储要求（如容量、性能和可用性），这些配置文件会在您创建桌面池时自动创建。
- 利用 Horizon 7 Storage Accelerator，可显著减少 IOPS 存储负载，从而支持更大规模的最终用户登录，无需任何专门的存储阵列技术。
- 如果远程桌面采用 vSphere 5.1 及更高版本所提供的节省空间的磁盘格式，则客户机操作系统中过期或已删除的数据将通过擦除和压缩流程自动回收。

硬件独立性

远程桌面和已发布的应用程序具有硬件独立性。例如，由于远程桌面在数据中心内的某个服务器中运行，且只能从客户端设备访问，因此远程桌面可以使用与客户端设备硬件不兼容的操作系统。

远程桌面可在 PC、Mac、瘦客户端、作为瘦客户端使用的 PC、平板电脑以及手机上运行。已发布的应用程序可在以上部分设备中运行。每个季度将添加一次新的设备支持。

如果您使用 HTML Access 功能，最终用户即可在浏览器中打开远程桌面或应用程序，无需在客户端系统或设备上安装任何客户端应用程序。

Horizon 7 功能

Horizon 7 中包含的功能可支持可用性、安全性、集中式控制和可扩展性。

以下功能提供最终用户所熟悉的体验：

- 在某些客户端设备中，可以在虚拟桌面上使用客户端设备上定义的任何本地或网络打印机进行打印。该虚拟打印机功能可消除兼容性问题，而且您不必在虚拟机上安装额外的打印驱动程序。
- 在大多数客户端设备中，使用基于位置的打印功能映射到物理位置接近客户端系统的打印机。基于位置的打印需要您在虚拟机中安装打印驱动程序。
- 本地打印机重定向专门用于以下用例：
  - 直接连接到客户端上的 USB 或串行端口的打印机
  - 连接到客户端的专用打印机，例如条形码打印机和标签打印机
  - 远程网络上不可从虚拟会话寻址的网络打印机。
- 使用多个显示器。对于 PCoIP 和 Blast Extreme 显示协议，多显示器支持意味着，您可以单独调整每个显示器的显示分辨率和旋转角度。
- 访问连接到可显示虚拟桌面的本地设备的 USB 设备和其他外围设备。

  您可指定最终用户可连接的 USB 设备类型。对于包含多种设备类型的组合设备（例如，包含一个视频输入设备和一个存储设备），可通过分割设备，允许连接其中一个设备（如视频输入设备），而禁止连接另一个（如存储设备）。
- 使用 Horizon Persona Management 在会话间保留用户设置和数据，即使在刷新或重构了桌面后也可这样做。用户配置管理能够按照可配置的时间间隔将用户配置文件复制到远程配置文件存储（CIFS 共享位置）。

  您也可以在不受 Horizon 7 管理的物理机和虚拟机上使用独立版本的用户配置管理。

Horizon 7 还特别提供了以下安全功能：

- 使用 RSA SecurID 或 RADIUS（远程身份验证拨入用户服务）等双因素身份验证或智能卡登录。
- 在针对 Active Directory 提供只读访问策略的环境中配置远程桌面和应用程序时，使用预先创建的 Active Directory 帐户。
- 使用 SSL/TLS 安全加密链路确保对所有连接进行完全加密。
- 使用 VMware High Availability 确保自动进行故障切换。

可扩展性功能需要借助 VMware 虚拟化平台来管理桌面和服务器：

- 与 VMware vSphere 相集成，可以实现远程桌面和应用程序的高性价比密度、高可用性，并提供高级资源分配控制。
- 使用 Horizon 7 Storage Accelerator 功能可以在存储资源相同的情况下支持更大规模的最终用户登录。该 Storage Accelerator 使用 vSphere 5 平台中的功能，为通用数据块读取操作创建主机内存缓存。
- 将 Horizon 连接服务器配置为代理最终用户与授权最终用户访问的远程桌面和应用程序之间的连接。

- 用 View Composer 快速创建与主映像共享虚拟磁盘的桌面映像。采用这种方法使用链接克隆，有助于节省磁盘空间和简化对操作系统的修补程序和更新的管理。
- 使用 Horizon 7 中引入的即时克隆功能快速创建与父映像共享虚拟磁盘和内存的桌面映像。即时克隆不仅具有 View Composer 链接克隆的空间利用效率，而且不再需要刷新、重构和重新平衡，从而进一步简化操作系统修补程序和更新管理。即时克隆完全消除了桌面维护期限问题。

以下功能可用于进行集中式管理：

- 使用 Microsoft Active Directory 管理对远程桌面和应用程序的访问并管理策略。
- 使用用户配置管理简化和优化从物理桌面到虚拟桌面的迁移过程。
- 使用基于 Web 的管理控制台从任意位置管理远程桌面和应用程序。
- 使用 Horizon Administrator 分发和管理 VMware ThinApp™ 附带的应用程序。
- 使用模板或主映像快速创建和置备桌面池。
- 在不影响用户设置、数据或首选项的情况下向虚拟桌面发送更新和修补程序。
- 与 VMware Identity Manager 集成，使最终用户能够通过 Web 上的用户门户访问远程桌面，并在远程桌面内通过浏览器使用 VMware Identity Manager。
- 与 Mirage™ 和 Horizon FLEX™ 集成，可以管理本地安装的虚拟机桌面，并且可以在专用的完整克隆远程桌面上部署和更新应用程序，而不覆盖用户安装的应用程序。

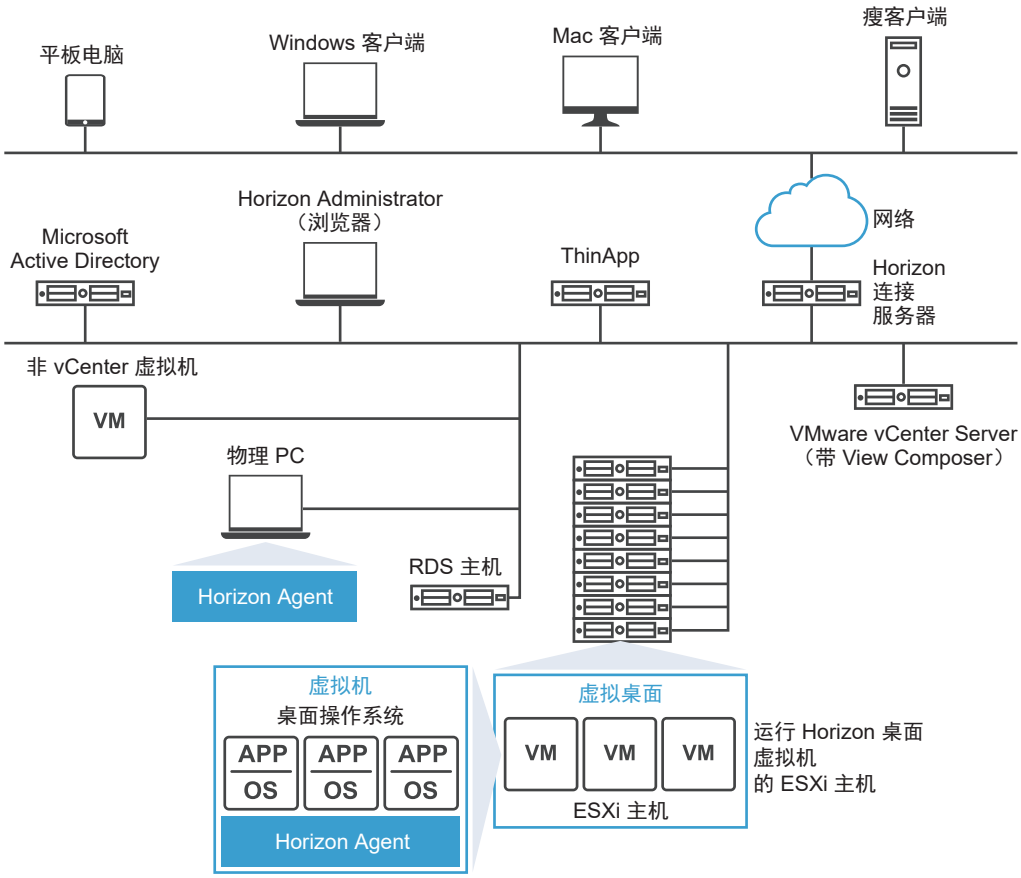
组件如何组成在一起

最终用户启动 Horizon Client 以登录 Horizon 连接服务器。该服务器与 Windows Active Directory 集成，可提供对 VMware vSphere 服务器、物理 PC 或 Microsoft RDS 主机上托管的远程桌面的访问权限。Horizon Client 还提供对 Microsoft RDS 主机上的已发布应用程序的访问权限。

注 Horizon 7 支持多个 Active Directory 域服务 (Active Directory Domain Service, AD DS) 域功能级别。有关支持的 AD DS 域功能级别的更多信息，请参阅 VMware 知识库 (Knowledge Base, KB) 文章 http://kb.vmware.com/kb/2150351。

图 1-2. Horizon 7 环境高级示例 显示了 Horizon 7 部署中各主要组件之间的关系。

图 1-2. Horizon 7 环境高级示例



客户端设备

使用 Horizon 7 的一大优势在于，最终用户可以在任何地点使用任何设备访问远程桌面和应用程序。用户可以通过公司的笔记本电脑、家用 PC、精简客户端设备、Mac、平板电脑或手机访问其个性化虚拟桌面或远程应用程序。

最终用户打开 Horizon Client 可显示其远程桌面和应用程序。瘦客户端设备使用 Horizon 7 瘦客户端软件，您可以对其进行配置，使 Horizon 7 瘦客户端成为用户在设备上唯一能直接启动的应用程序。将传统 PC 作为瘦客户端桌面使用，可以使硬件的使用寿命延长三到五年。例如，通过在瘦客户端桌面中使用 Horizon 7，您可以在较旧的桌面硬件上使用 Windows 8.x 等较新的操作系统。

如果您使用 HTML Access 功能，最终用户即可在浏览器中打开远程桌面，无需在客户端系统或设备上安装任何客户端应用程序。

Horizon 连接服务器

该软件服务充当客户端连接的 Broker。Horizon 连接服务器通过 Windows Active Directory 对用户进行身份验证，并将请求定向到相应的虚拟机、物理 PC 或 Microsoft RDS 主机。

连接服务器提供了以下管理功能：

- 用户身份验证

- 授权用户访问特定的桌面和池
- 将通过 VMware ThinApp 打包的应用程序分配给特定桌面和池
- 管理远程桌面和应用程序会话
- 在用户和远程桌面及应用程序之间建立安全连接
- 支持单点登录
- 设置和应用策略

在企业防火墙内部，您需要安装并配置一个至少包含两个连接服务器实例的组。其配置数据存储在一个嵌入式 LDAP 目录内，并且在组内各成员之间复制。

在企业防火墙外部，您可以在 DMZ 中安装连接服务器并将其配置为安全服务器，也可以安装 Unified Access Gateway 设备。DMZ 中的安全服务器和 Unified Access Gateway 设备与企业防火墙内部的连接服务器进行通信。安全服务器和 Unified Access Gateway 设备可确保唯一能够进入企业数据中心的远程桌面和应用程序流量是经过严格身份验证的用户产生的流量。用户只能访问被授权访问的资源。

安全服务器提供了一个功能子集，且无需包含在 Active Directory 域中。可以将连接服务器安装在 Windows Server 2008 R2 或 Windows Server 2012 R2 服务器中，最好是安装在 VMware 虚拟机上。有关 Unified Access Gateway 设备的更多信息，请参阅《部署和配置 Unified Access Gateway》。

重要事项 可创建不使用连接服务器的 Horizon 7 设置。如果在远程虚拟机桌面上安装 Horizon 7 Agent Direct Connect 插件，客户端可直接连接到虚拟机。所有远程桌面功能（包括 PCoIP、HTML Access、RDP、USB 重定向和会话管理）都以相同方式工作，就像用户已通过连接服务器进行连接一样。有关详细信息，请参见《Horizon 7 Agent Direct-Connection 插件管理》。

Horizon Client

用于访问远程桌面和应用程序的客户端软件可以在平板电脑、电话、Windows、Linux 或 Mac PC 或笔记本电脑、瘦客户端以及更多平台上运行。

登录后，用户可以在授权其使用的远程桌面和应用程序列表中选择。身份验证需要使用 Active Directory 凭据、UPN、智能卡 PIN 或者 RSA SecurID 或其他双因素身份验证令牌。

管理员可以将 Horizon Client 配置为允许最终用户选择显示协议。协议包括用于远程桌面的 PCoIP、Blast Extreme 和 Microsoft RDP。PCoIP 和 Blast Extreme 的速度和显示质量可与物理 PC 媲美。

具体功能因您使用的 Horizon Client 而异。本指南重点介绍适用于 Windows 的 Horizon Client。本指南未详细介绍以下客户端类型：

- 有关适用于平板电脑、Linux 客户端和 Mac 客户端的 Horizon Client 的详细信息。请参阅 Horizon Client 文档，网址为 https://docs.vmware.com/cn/VMware-Horizon-Client/index.html。
- 有关 HTML Access Web client 的详细信息，可通过该客户端在浏览器中打开远程桌面。客户端系统或设备上未安装任何 Horizon Client 应用程序。请参阅 Horizon Client 文档，网址为 https://docs.vmware.com/cn/VMware-Horizon-Client/index.html。
- 各种第三方瘦客户端和零客户端（仅通过认证的合作伙伴提供）。

- View Open Client（支持 VMware 合作伙伴认证计划）。View Open Client 不是正式发布的客户端应用程序，因此不具有同样的支持。

VMware Horizon 用户 Web 门户

通过客户端设备上的 Web 浏览器，最终用户可以连接至远程桌面和应用程序，自动启动 Horizon Client（如果已安装），或下载 Horizon Client 安装程序。

当您打开浏览器并输入一个 Horizon Connection Server 实例的 URL 时，将会显示网页，其中包含 VMware 下载网站链接，用于下载 Horizon Client。但网页上的链接是可配置的。例如，您可将链接配置为指向一个内部 Web 服务器，也可对自己的连接服务器上可用的客户端版本加以限制。

如果您使用 HTML Access 功能，网页还会显示一个用于在支持的浏览器内部访问远程桌面和应用程序的链接。使用此功能，不会在客户端系统或设备上安装 Horizon Client 应用程序。有关更多信息，请参阅 https://docs.vmware.com/cn/VMware-Horizon-Client/index.html 上的 Horizon Client 文档。

Horizon Agent

您可以在所有用作远程桌面和应用程序源的虚拟机、物理系统和 Microsoft RDS 主机上安装 Horizon Agent 服务。在虚拟机上，此代理通过与 Horizon Client 进行通信来提供连接监视、虚拟打印、Horizon Persona Management 和访问本地连接的 USB 设备等功能。

如果桌面源本身是一个虚拟机，您应当首先在该虚拟机上安装 Horizon Agent 服务，然后再将其作为模板或者链接克隆或即时克隆的父虚拟机使用。从该虚拟机创建池时，该代理将自动安装到每个远程桌面上。

您可以在安装代理时选择单点登录选项。使用单点登录后，用户只会在连接 Horizon 连接服务器时收到登录提示，下一次连接远程桌面或应用程序时便不会收到提示。

Horizon Administrator

这款基于 Web 的应用程序允许管理员配置 Horizon 连接服务器、部署并管理远程桌面和应用程序、控制用户身份验证以及排除最终用户遇到的问题。

Horizon Administrator 应用程序会随连接服务器实例一起安装。借助该应用程序，管理员无需在他们的本地计算机上安装应用程序，即可从任何地方管理连接服务器实例。

View Composer

您可将该软件服务安装在管理虚拟机的 vCenter Server 实例上或安装在单独的服务器上。然后，View Composer 将可以从指定的父虚拟机创建链接克隆池。这种策略可节约多达 90% 的存储成本。

每个链接克隆都像一个独立的桌面，带有唯一的主机名和 IP 地址，但不同的是，链接克隆与父虚拟机共享一个基础映像，因此存储需求明显减少。由于链接克隆桌面池共享一个基础映像，因此您可以通过仅更新父虚拟机来快速部署更新和修补程序。最终用户的设置、数据和应用程序均不会受到影响。

也可以使用 View Composer 创建自动链接克隆 Microsoft RDS 主机场，这会为最终用户提供发布的应用程序。

尽管在可以将 View Composer 安装在其自身的服务器主机上，但一项 View Composer 服务只能基于一个 vCenter Server 实例运行。同样地，vCenter Server 实例只能与一个 View Composer 服务相关联。

重要事项 View Composer 是一个可选组件。如果您计划置备即时克隆，您不需要安装 View Composer。

vCenter Server

该服务可充当连接到网络的 VMware ESXi 服务器的中心管理员。vCenter Server 为配置、置备和管理数据中心中的虚拟机提供了中心点。

除了使用这些虚拟机作为虚拟机桌面池的源之外，还可以使用虚拟机托管 Horizon 7 的服务器组件，包括 Horizon Connection Server 实例、Active Directory 服务器、Microsoft RDS 主机和 vCenter Server 实例。

您可以将 View Composer 和 vCenter Server 安装在相同的服务器上或不同的服务器上。vCenter Server 会管理向物理服务器和存储分配虚拟机的情况，以及向虚拟机分配 CPU 和内存资源的情况。

可以将 vCenter Server 作为 VMware 虚拟设备安装，或将 vCenter Server 安装在 Windows Server 2008 R2 服务器或 Windows Server 2012 R2 服务器中，最好是安装在 VMware 虚拟机上。

集成并自定义 Horizon 7

要增强组织中 Horizon 7 的效率，您可以使用多个界面将 Horizon 7 与外部应用程序集成，或是创建可以从命令行或以批处理模式运行的管理脚本。

与其他组件集成

Horizon 7 可与以下这些 VMware 产品集成。

VMware Cloud on AWS

VMware Cloud on AWS 允许您在 Amazon Web Services 上创建 vSphere 数据中心。这些 vSphere 数据中心包括用于管理数据中心的 vCenter Server、用于存储的 vSAN 和用于网络连接的 VMware NSX。您可以将内部部署的数据中心连接到您的云 SDDC，并从单个 vSphere Client 界面同时管理它们。使用已连接的 AWS 帐户，可从 SDDC 中的虚拟机访问 AWS 服务，例如 EC2 和 S3。有关更多信息，请参阅 https://docs.vmware.com/cn/VMware-Cloud-on-AWS/index.html 上的 VMware Cloud on AWS 文档。

从 Horizon 7 7.5 版本开始，您可以在 VMware Cloud on AWS 上部署 Horizon 7 完整克隆。例如，您可以部署一个 VMware Cloud on AWS 环境，该环境在内部部署数据中心和 Horizon 7 实例间使用 Cloud Pod 架构。这使得 Horizon 7 能够轻松地在混合云环境中运行并将 SDDC 基础架构的管理外包给 VMware。

VMware Identity Manager

您可以将 VMware Identity Manager 与 Horizon 7 集成，向 IT 管理员和最终用户提供以下优势：

- 最终用户可通过他们用来访问 SaaS、Web 和 Windows 应用程序的 Web 上的同一个用户门户，使用同样方便的单点登录来按需访问远程桌面和应用程序。

通过使用 True SSO 功能，使用智能卡或双因素身份验证的用户可以访问其远程桌面和应用程序，而无需提供 Active Directory 凭据。

- 最终用户可从远程桌面内访问 Web 上的 VMware Identity Manager，查找所需的应用程序。
- 如果您还使用 HTML Access 功能，最终用户即可在浏览器中打开远程桌面，无需在客户端系统或设备上安装任何客户端应用程序。
- IT 管理员可以使用 VMware Identity Manager 的基于浏览器的管理控制台监视用户和组的远程桌面授权。

VMware Mirage 和 Horizon FLEX

您可以使用 Mirage 和 Horizon FLEX 在专用的完整克隆远程桌面上部署并更新应用程序，而不覆盖用户安装的应用程序或数据。

Mirage 提供的脱机虚拟桌面解决方案比 Horizon 7 之前附带的“本地模式”功能好。Mirage 包含以下用于脱机桌面的安全和管理功能：

- 对本地安装的虚拟机进行加密并阻止用户修改影响安全容器完整性的虚拟机设置。
- 提供各种策略，包括 VMware Fusion™ Professional 和 VMware®Player Plus™ 中可用的过期策略，这些策略与之前“本地模式”功能随附的各种策略相差无几。Fusion Pro 和 Player Plus 均包含在 Mirage 中。
- 使用户不再需要检入或检出桌面即可接收更新。
- 使管理员可以利用 Mirage 分层功能、备份功能和文件门户。

VMware App Volumes

VMware App Volumes 是一个用于 Horizon 7 和其他虚拟环境的集成且统一的应用程序提供和用户管理系统。App Volumes 管理的应用程序和数据保存在专用的 VMDK 或 VHD（称为 AppStack）中，它们将在登录或重新引导时连接到每个 Windows 用户会话。该策略确保为用户提供最新的应用程序和数据。App Volumes 还为用户安装的持久应用程序和设置提供了不同的容器（称为可写卷），在登录或重新引导时还会加载该容器。也可以使用 App Volumes 平台管理用户配置文件和策略设置。

VMware User Environment Manager

您可以使用智能策略功能创建一些策略，用来控制特定远程桌面上 USB 重定向、虚拟打印、剪贴板重定向、客户端驱动器重定向和 PCoIP 显示协议功能的行为。通过使用 User Environment Manager，IT 人员可以控制允许用户个性化的设置以及映射环境设置，例如，网络和位置特定的打印机。使用智能策略，可以创建仅在满足特定条件时才会生效的策略。例如，可以配置这样一个策略：当用户从企业网络外部连接到远程桌面时，禁用客户端驱动器重定向功能。

VMware Unified Access Gateway

对于要从企业防火墙外部访问远程桌面和应用程序的用户，Unified Access Gateway 用作一个安全网关。Unified Access Gateway 是一个安装在隔离区 (Demilitarized Zone, DMZ) 中的设备。使用 Unified Access Gateway 可确保只有经过严格身份验证的远程用户产生的流量才能进入企业数据中心。您可

以使用 Unified Access Gateway 设备替代 Horizon 7 安全服务器。有关更多信息，请参阅 Unified Access Gateway 文档。

与广泛应用的视频会议软件集成

您可以将这些音频和视频会议软件与 Horizon 7 结合使用。

Flash URL 重定向

将 Flash 内容直接从 Adobe Media Server 流式传输到客户端端点可以降低数据中心 ESXi 主机上的负载，无需通过数据中心进行路由，减少将实时视频事件同时流式传输到多个客户端端点所需的带宽。

Flash URL 重定向功能使用由网页管理员嵌入到网页中的 JavaScript。当虚拟桌面用户从网页内部单击指定的 URL 链接时，JavaScript 将从虚拟桌面会话中截获 ShockWave File (SWF) 文件并将其重定向到客户端终端。然后终端将在虚拟桌面会话之外打开本地 VMware Flash Projector，开始在本地播放媒体流。

注 利用 Flash URL 重定向功能，多播或单播流可能被重定向到组织防火墙之外的客户端设备。客户端必须对托管 ShockWave Flash (SWF) 文件的 Adobe Web 服务器具有访问权限，SWF 文件可启动多播或单播流。根据需要配置防火墙，打开相应的端口，以允许客户端设备访问此服务器。

该功能仅适用于某些类型的客户端。为确定某个特定类型的客户端是否支持该功能，请参阅针对特定桌面或移动客户端设备类型的“使用 VMware Horizon Client”文档中提供的功能支持表。请访问 https://docs.vmware.com/cn/VMware-Horizon-Client/index.html。

Microsoft Lync 2013

您可在远程桌面上使用 Microsoft Lync 2013 客户端，以便使用经 Lync 认证的 USB 语音和视频设备来参与统一通信 (UC) VoIP（IP 语音）和视频聊天通话。这样就无需再使用专用 IP 电话。

这种体系结构需要在远程桌面上安装 Microsoft Lync 2013 客户端并在 Windows 7 或 Windows 8 客户端终端安装 Microsoft Lync VDI 插件。客户可使用 Microsoft Lync 2013 客户端获取状态、即时消息、Web 会议和 Microsoft Office 功能。

每次进行 Lync VoIP 或视频聊天通话时，Lync VDI 插件都会将所有媒体处理从数据中心服务器卸载到客户端端点，并将所有媒体编码到经 Lync 优化的音频和视频编解码器中。这种经过优化的体系结构具备较高的可扩展性，这样只需使用较低的网络带宽，并提供点对点的媒体传输，同时支持高品质的实时 VoIP 和视频。有关更多信息，请参阅关于 VMware Horizon 6 和 Microsoft Lync 2013 的白皮书，网址为 http://www.vmware.com/files/pdf/techpaper/vmware-horizon-view-microsoft-lync-install-configure.pdf。

注 目前暂不支持录制音频。只有使用 PCoIP 或 Blast Extreme 显示协议才能支持该项整合。

Skype for Business

最终用户可以使用 Skype for Business 在虚拟桌面中进行优化的音频和视频通话，而不会对虚拟基础架构造成不利影响，也不会导致网络过载。在 Skype 音频和视频通话期间，将在客户端计算机上进行所有媒体处理，而不是在虚拟桌面中进行。

适用于 Skype for Business 的 Virtualization Pack 软件默认作为适用于 Windows 的 Horizon Client（4.6 及更高版本）、适用于 Linux 的 Horizon Client（4.6 及更高版本）以及适用于 Mac 的 Horizon Client（4.7 及更高版本）安装程序的一部分进行安装。Horizon 管理员还必须在 Horizon Agent 安装期间在虚拟桌面上安装适用于 Skype for Business 的 VMware Virtualization Pack 功能。有关更多信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档。要配置 Skype for Business，请参阅《在 Horizon 7 中配置远程桌面功能》文档。

将 Horizon 7 与业务智能软件集成

您可以将 Horizon 连接服务器配置为将事件记录到 Microsoft SQL Server 或 Oracle 数据库。

- 登录和启动桌面会话等最终用户操作。
- 添加授权和创建桌面池等管理员操作。
- 报告系统故障和错误的警告。
- 统计采样，如记录 24 小时内的最大用户数量。

您可以使用 Crystal Reports、IBM Cognos、MicroStrategy 9 和 Oracle Enterprise Performance Management System 等业务智能报告引擎来访问和分析事件数据库。

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，以便分析软件能够访问事件数据。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。如果指定一个文件共享，则这些日志文件会移至该分享。有关更多信息，请参阅《Horizon 7 安装指南》文档。

使用 Horizon PowerCLI Cmdlet 创建管理脚本

可以通过 VMware PowerCLI 使用 Horizon PowerCLI cmdlet。使用 Horizon PowerCLI cmdlet 对 Horizon 组件执行各种管理任务。

有关 Horizon PowerCLI cmdlet 的详细信息，请参阅《VMware PowerCLI cmdlet 参考》。

有关创建高级函数和脚本以用于 Horizon PowerCLI 的 API 规范的信息，请参阅 VMware 开发人员中心的 View API 参考。

有关可用于创建您自己的 Horizon PowerCLI 脚本的示例脚本的更多信息，请访问 GitHub 上的 Horizon PowerCLI 社区。

您可以使用 Horizon PowerCLI cmdlet 在 Horizon 7 组件上执行各种管理任务。

- 创建和更新桌面池。
- 配置多个网络标签，大幅增加分配给池中虚拟机的 IP 地址的数量。
- 将数据中心资源添加到完整虚拟机或链接克隆池。
- 在链接克隆桌面上执行重新平衡、刷新或重构操作。
- 对特定桌面或桌面池的使用情况进行取样。
- 查询事件数据库。
- 查询服务状态。

修改 Horizon 7 中的 LDAP 配置数据

当您使用 Horizon Administrator 修改 Horizon 7 配置时，存储库中相应的 LDAP 数据会随之更新。Horizon 连接服务器将其配置信息存储在与 LDAP 兼容的存储库中。例如，在您添加桌面池时，连接服务器会将与用户、用户组和授权相关的信息存储在 LDAP 中。

您可以使用 VMware 和 Microsoft 命令行工具将 LDAP 配置数据以 LDAP 数据交换格式 (LDIF) 文件导入到 Horizon 7（或者从 Horizon View 导出）。这些命令仅面向希望使用脚本而不使用 Horizon Administrator 或 Horizon PowerCLI 来更新配置数据的高级管理员。

您可以使用 LDIF 文件执行多种任务。

- 在连接服务器实例之间传输配置数据。
- 定义桌面池等各种 Horizon 7 对象，并将其添加到您的连接服务器实例，而无需使用 Horizon Administrator 或 Horizon PowerCLI。
- 备份配置，以便您能够还原连接服务器实例的状态。

有关更多信息，请参阅《Horizon 7 集成指南》文档。

使用 vdmadmin 命令

在连接服务器实例上，您可以使用 `vdmadmin` 命令行界面执行各种管理任务。您可以使用 `vdmadmin` 命令执行那些在 Horizon Administrator 用户界面中无法执行的管理任务，或者执行需要通过脚本自动运行的管理任务。

有关更多信息，请参阅《Horizon 7 管理指南》文档。

规划丰富的用户体验

2

Horizon 7 可为最终用户提供熟悉的个性化桌面环境。例如，在某些客户端系统上，最终用户可以访问与本地计算机连接的 USB 和其他设备、将文档发送至本地计算机能够检测的任意打印机、使用智能卡进行身份验证以及使用多个显示器。

Horizon 7 拥有很多您希望为最终用户提供的功能。在决定使用哪些功能前，您必须了解每项功能的局限和限制。

本章讨论了以下主题：

Horizon Agent 功能支持表

在计划要将哪些显示协议和功能提供给最终用户时，可根据下面的信息来确定哪些代理（远程桌面和应用程序）操作系统支持这些功能。

受支持的客户机操作系统的类型和版本取决于 Windows 版本。有关受支持的 Windows 10 操作系统的列表的更新，请参阅 VMware 知识库 (KB) 文章 http://kb.vmware.com/kb/2149393。对于 Windows 10 以外的 Windows 操作系统，请参阅 VMware 知识库 (KB) 文章 http://kb.vmware.com/kb/2150295。

要查看安装 Horizon Agent 的 Windows 操作系统上支持的特定远程体验功能列表，请参阅 VMware 知识库 (KB) 文章 http://kb.vmware.com/kb/2150305。

注 有关各种类型客户端设备支持的功能的信息，请参阅 Horizon Client 文档，网址为 https://docs.vmware.com/cn/VMware-Horizon-Client/index.html。

此外，还有一些 VMware 合作伙伴提供了面向 Horizon 7 部署的瘦客户端设备和零客户端设备。每个瘦或零客户端设备上提供的功能是由供应商、型号和企业选择使用的配置决定的。有关精简和置零客户端设备的供应商和型号的信息，请参阅 VMware 网站上的《VMware 兼容性指南》。

选择显示协议

显示协议可以图形界面的形式向最终用户显示数据中心内的远程桌面或应用程序。您可以根据所拥有的客户端设备类型，选择 VMware 提供的 Blast Extreme 和 PCoIP (PC-over-IP) 或 Microsoft RDP（远程桌面协议）。

您可以通过设置策略来控制使用哪种协议，也可以让最终用户在登录桌面时选择协议。

注 对于某些类型的客户端来说，既不使用 PCoIP，也不使用 RDP 远程显示协议。例如，如果您使用 HTML Access 功能提供的 HTML Access 客户端，则采用 Blast Extreme 协议，而非 PCoIP 或 RDP。类似地，如果您使用远程 Linux 桌面，则使用 Blast Extreme。

VMware Blast Extreme

针对移动云优化的 VMware Blast Extreme 支持最广泛的启用 H.264 的客户端设备。在众多显示协议中，VMware Blast 具有最低的 CPU 消耗率，从而延长移动设备的电池寿命。VMware Blast Extreme 可对延迟的增加或带宽的减少进行补偿，并且还可同时利用 TCP 和 UDP 网络传输。

VMware Blast 显示协议可用于已发布的应用程序，以及使用 RDS 主机上的虚拟机或共享会话桌面的远程桌面。RDS 主机可以是物理机或虚拟机。VMware Blast 显示协议无法在单用户物理机上运行，但 Windows 10 RS4 企业版和更高版本除外。

注 运行 Windows 10 RS4 的物理机不支持“电影和电视”应用程序。

VMware Blast Extreme 功能

VMware Blast Extreme 的主要功能包括：

- 企业防火墙范围以外的用户可将此协议与企业的虚拟专用网 (Virtual Private Network, VPN) 搭配使用，或者，用户也可通过安全、加密的方式连接到企业 DMZ 中的安全服务器或 Access Point 设备。
- 支持高级加密标准 (Advanced Encryption Standard, AES) 128 位加密，并且默认已启用。但是，您可以将加密密钥密码更改为 AES-256。
- 从各种类型的客户端设备建立连接。
- 用于减少 LAN 和 WAN 的带宽使用的优化控制。

- 在 Windows 代理中，使用 PerfMon 显示以下各项内容的性能计数器，这些计数器准确地显示系统的当前状态，系统也会以恒定的速率更新：
  - Blast 会话
  - 图像处理
  - 音频
  - CDR
  - USB：如果将 USB 流量配置为使用 VMware 虚拟通道 (VMware Virtual Channel, VVC)，则在 Windows 代理上使用 PerfMon 显示的 USB 计数器将有效。
  - Skype for Business：计数器仅用于控制流量。
  - 剪贴板
  - RTAV
  - 串行端口和扫描仪重定向功能
  - 虚拟打印
  - HTML5 MMR
  - Windows Media MMR：仅当将此功能配置为使用 VMware 虚拟通道 (VVC) 时，才会显示这些性能计数器。
- 在 Windows 客户端上出现短暂网络丢失期间保持网络连续性。
- 支持用 32 位色彩进行虚拟显示。
- 支持 ClearType 字体。
- 支持音频重定向，可针对 LAN 和 WAN 动态调整音频质量。
- 支持在某些客户端类型上使用网络摄像头和麦克风的实时音频-视频功能。
- 支持在客户端操作系统与远程桌面或已发布的应用程序之间复制和粘贴文本和图像（在部分客户端上受支持）。对于其他客户端类型，仅支持复制和粘贴纯文本。您无法在系统之间复制和粘贴系统对象，如文件夹和文件。
- 部分客户端类型支持多显示器。在某些客户端上，针对禁用 Aero 的 Windows 7 远程桌面，您最多可以使用 4 个分辨率最高为 2560 x 1600 的显示器或 3 个分辨率为 4K (3840 x 2160) 的显示器。此外还支持旋转显示和自动调整功能。

  启用 3D 功能时，支持最多 2 个分辨率最高为 1920 x 1200 的显示器或最多 1 个分辨率为 4K (3840 x 2160) 的显示器。
- 部分客户端类型支持 USB 重定向。
- 部分 Windows 客户端操作系统和部分远程桌面操作系统（安装了 Horizon Agent）支持 MMR 重定向。
- NVIDIA 显卡支持连接到未接显示器的物理机。为获得最佳性能，请使用支持 H.264 编码的显卡。

如果同时安装附加分离式 GPU 和嵌入式 GPU，操作系统可能默认使用嵌入式 GPU。要修复此问题，您可以在设备管理器中禁用或移除设备。如果问题仍然存在，您可以安装嵌入式 GPU 的 WDDM 图形驱动程序，或在系统 BIOS 中禁用嵌入式 GPU。有关如何禁用嵌入式 GPU 的说明，请参阅系统文档。

小心 禁用嵌入式 GPU 可能导致以后无法访问相关功能，例如通过控制台访问 BIOS 设置或 NT 启动加载程序。

- Blast 编解码器通过提供更清晰的图像和字体改进了桌面使用中的自适应编码器和 H.264 编码器，其运行方式类似于具有运动检测、运动向量和帧间预测宏块的视频编解码器。在以下环境中支持该编解码器，并且在默认情况下已禁用该编解码器：
  - Windows 和 Linux 代理。要启用该编解码器，请执行以下操作：
    - 在 Windows 代理上，设置注册表项：`HKLM\SOFTWARE\VMware, Inc.\VMware Blast\Config\EncoderBlastCodecEnabled = 1`
    - 在 Linux 代理上，在 `\etc\vmware\config` 下设置 `RemoteDisplay.allowBlastCodec=TRUE`
  - 在 Windows、Linux 和 MacOS 客户端设置上禁用 H.264。移动客户端和 Web 客户端不支持此功能。
- 动态编码器切换支持在视频优化编码器（H.264 4:2:0 或 H.264 4:4:4）和文本优化编码器（Blast 编解码器或自适应编码器）之间进行切换。这种切换可帮助保持清晰的文本和视频，并降低使用的带宽。要使用此功能，请启用该编码器开关：
  - 在 Windows 代理上，设置注册表项 `HKLM\SOFTWARE\VMware, Inc.\VMware Blast\Config\EncoderSwitchEnabled = 1`
  - 在 Linux 代理上，在 `\etc\vmware\config` 下设置 `RemoteDisplay.allowSwitchEncoder=TRUE`
  - 启用 Blast 编解码器（默认情况下禁用）。如果未启用 Blast 编解码器，则切换编码器将使用自适应编码器进行文本优化编码。
  - 在 Windows、Linux 和 MacOS 客户端设置上启用 H.264。移动客户端和 Web 客户端不支持此功能。

注 编码器切换仅使用软件 H.264，不支持硬件加速图形。

有关哪些客户端设备支持特定 VMware Blast Extreme 功能的信息，请访问 https://docs.vmware.com/cn/VMware-Horizon-Client/index.html。

LAN 唤醒

使用 Windows 10 RS4 企业版和更高版本的物理机支持 LAN 唤醒。使用此功能，用户可以在与 Horizon Connection Server 建立连接时唤醒物理机。要使用 LAN 唤醒功能，必须满足以下必备条件：

- 仅 IPv4 环境支持 LAN 唤醒 (Wake-on-LAN, WoL) 功能。
- 当在 BIOS 设置及网卡设置中启用 LAN 唤醒功能后，必须将物理机配置为在接收 LAN 唤醒数据包时醒来。
- 目标端口 9 用于接收来自连接服务器的 WoL 数据包。

- WoL 数据包是 IP 定向广播数据包，此类数据包在从 Horizon Connection Server 发送后必须能够到达 Horizon Agent。可在以下场景中使用 LAN 唤醒功能：
  - 连接服务器和物理机上的 Horizon Agent 位于 LAN 环境的同一子网中。
  - 连接服务器和 Horizon Agent 之间的所有路由器均已进行配置，允许 IP 定向广播数据包进入要唤醒的物理机所在的目标子网。

注 LAN 唤醒功能不支持物理 Windows 10 代理的浮动分配池。仅将 WoL 数据包发送到授权给特定用户的专用分配池。

建议的客户机操作系统设置

要以高分辨率全屏模式播放 720p 或更高格式的视频，推荐使用 1 GB 或以上的 RAM 及双 CPU。要对图形密集型应用程序（例如 CAD 应用程序）使用虚拟专用图形加速，建议使用 4GB RAM。

视频质量要求

480p 格式视频	当远程桌面使用单个虚拟 CPU 时，您可以在原始分辨率下播放 480p 或更低格式的视频。如果您希望以高清 Flash 或全屏模式播放视频，此桌面将需要使用双虚拟 CPU。即便使用双虚拟 CPU 桌面，以全屏模式播放 360p 这类格式较低的视频时也会出现落后于音频的情况，特别是在 Windows 客户端上。
720p 格式视频	当远程桌面具有双核虚拟 CPU 时，您可以在原始分辨率下播放 720p 格式的视频。如果您以高清或全屏模式播放 720p 视频，播放性能可能会受到影响。
1080p 格式视频	如果远程桌面使用双虚拟 CPU，您就可以播放 1080p 格式的视频，尽管可能需要将媒体播放器的窗口调小。
3D 呈现	可以将远程桌面配置为使用软件或硬件加速图形功能。这种软件加速图形功能使您能够运行 DirectX 9 和 OpenGL 2.1 应用程序，无需使用物理图形处理单元 (GPU)。这种硬件加速图形功能使虚拟机能够共享 vSphere 主机上的物理 GPU（图形处理单元），或者使物理 GPU 专用于单个虚拟桌面。 对于 3D 应用程序，最多支持 2 台显示器，最高屏幕分辨率为 1920 x 1200。远程桌面上的客户机操作系统必须为 Windows 7 或更高版本。 有关 3D 功能的更多信息，请参阅使用 3D 图形应用程序。

客户端系统的硬件要求

有关特定类型桌面或移动客户端设备的处理器和内容要求信息，请转到 https://docs.vmware.com/cn/VMware-Horizon-Client/index.html。

PCoIP

PCoIP (PC over IP) 针对已发布应用程序的交付或整个远程桌面环境为 LAN 或 WAN 中的广大用户提供了优化的桌面体验，包括应用程序、图像、音频和视频内容。PCoIP 可弥补因延迟增加或带宽减少导致的不便，确保最终用户在任何网络条件下均可保持高效。

PCoIP 显示协议可用于已发布的应用程序以及使用虚拟机、包含 Teradici 主机卡的物理机或 RDS 主机上的共享会话桌面的远程桌面。

PCoIP 功能

PCoIP 的主要功能包括：

- 企业防火墙范围以外的用户可将此协议与公司的虚拟专用网 (Virtual Private Network, VPN) 搭配使用，或者，用户也可通过安全、加密的方式连接到企业 DMZ 中的安全服务器或 Access Point 设备。
- 支持高级加密标准 (Advanced Encryption Standard, AES) 128 位加密，并且默认已启用。但是，您可以将加密密钥密码更改为 AES-256。
- 从各种类型的客户端设备建立连接。
- 用于减少 LAN 和 WAN 的带宽使用的优化控制。
- 支持用 32 位色彩进行虚拟显示。
- 支持 ClearType 字体。
- 支持音频重定向，可针对 LAN 和 WAN 动态调整音频质量。
- 支持在某些客户端类型上使用网络摄像头和麦克风的实时音频-视频功能。
- 支持在客户端操作系统与远程桌面或已发布的应用程序之间复制和粘贴文本和图像（在部分客户端上受支持）。对于其他客户端类型，仅支持复制和粘贴纯文本。您无法在系统之间复制和粘贴系统对象，如文件夹和文件。
- 部分客户端类型支持多显示器。在某些客户端上，针对禁用 Aero 的 Windows 7 远程桌面，您最多可以使用 4 个分辨率最高为 2560 x 1600 的显示器或 3 个分辨率为 4K (3840 x 2160) 的显示器。此外还支持旋转显示和自动调整功能。

  启用 3D 功能时，支持最多 2 个分辨率最高为 1920 x 1200 的显示器或最多 1 个分辨率为 4K (3840 x 2160) 的显示器。
- 部分客户端类型支持 USB 重定向。
- 部分 Windows 客户端操作系统和部分远程桌面操作系统（安装了 Horizon Agent）支持 MMR 重定向。

有关哪些桌面操作系统支持特定 PCoIP 功能的信息，请参阅 Horizon Agent 功能支持表。

有关哪些客户端设备支持特定 PCoIP 功能的信息，请访问 https://docs.vmware.com/cn/VMware-Horizon-Client/index.html。

建议的客户机操作系统设置

要以高分辨率全屏模式播放 720p 或更高格式的视频，推荐使用 1 GB 或以上的 RAM 及双 CPU。要对图形密集型应用程序（例如 CAD 应用程序）使用虚拟专用图形加速，建议使用 4GB RAM。

视频质量要求

480p 格式视频	当远程桌面使用单个虚拟 CPU 时，您可以在原始分辨率下播放 480p 或更低格式的视频。如果您希望以高清 Flash 或全屏模式播放视频，此桌面将需要使用双虚拟 CPU。即便使用双虚拟 CPU 桌面，以全屏模式播放 360p 这类格式较低的视频时也会出现落后于音频的情况，特别是在 Windows 客户端上。
720p 格式视频	当远程桌面具有双核虚拟 CPU 时，您可以在原始分辨率下播放 720p 格式的视频。如果您以高清或全屏模式播放 720p 视频，播放性能可能会受到影响。
1080p 格式视频	如果远程桌面使用双虚拟 CPU，您就可以播放 1080p 格式的视频，尽管可能需要将媒体播放器的窗口调小。
3D 呈现	可以将远程桌面配置为使用软件或硬件加速图形功能。这种软件加速图形功能使您能够运行 DirectX 9 和 OpenGL 2.1 应用程序，无需使用物理图形处理单元 (GPU)。这种硬件加速图形功能使虚拟机能够共享 vSphere 主机上的物理 GPU（图形处理单元），或者使物理 GPU 专用于单个虚拟机桌面。 对于 3D 应用程序，最多支持 2 台显示器，其屏幕分辨率最高为 1920 x 1200。远程桌面上的客户机操作系统必须是 Windows 7 或更高版本。 有关 3D 功能的更多信息，请参阅使用 3D 图形应用程序。

客户端系统的硬件要求

有关处理器和内存要求的信息，请参阅特定桌面或移动客户端设备类型的“使用 VMware Horizon Client”文档。请访问 https://docs.vmware.com/cn/VMware-Horizon-Client/index.html。

Microsoft RDP

远程桌面协议实际上就是人们从家用计算机访问办公计算机时使用的多通道协议。Microsoft 远程桌面连接 (RDC) 使用 RDP 来传输数据。

Microsoft RDP 是远程桌面所支持的显示协议，其使用虚拟机、物理机或 RDS 主机上的共享会话桌面。（已发布的应用程序仅支持 PCoIP 显示协议和 VMware Blast 显示协议。）Microsoft RDP 具有以下功能：

- RDP 7 真正实现了多显示器支持，最多可支持 16 个显示器。
- 您可以在本地系统与远程桌面之间复制和粘贴文本和系统对象（如文件夹和文件）。
- 支持用 32 位色彩进行虚拟显示。
- RDP 支持 128 位加密。

- 企业防火墙范围以外的用户可搭配使用此协议与公司的虚拟专用网 (VPN)，同时，用户也可通过安全、加密的方式连接到企业 DMZ 中的 View 安全服务器。

要支持到 Windows 7 和 Windows Server 2008 R2 的 TLSv1.1 和 TLSv1.2 连接，您必须应用 Microsoft 修补程序 KB3080079。

客户端系统的硬件要求

有关处理器和内存要求的信息，请参阅“使用 VMware Horizon Client”文档，以了解特定类型的客户端系统。请访问 https://docs.vmware.com/cn/VMware-Horizon-Client/index.html。

注 移动客户端 3.x 设备仅使用 PCoIP 显示协议。移动客户端 4.x 客户端仅使用 PCoIP 显示协议或 VMware Blast 显示协议。

使用发布的应用程序

除了远程桌面以外，您还可以使用 Horizon Client 安全地访问发布的基于 Windows 的应用程序。

在启动 Horizon Client 并登录到 Horizon 7 Server 后，除了远程桌面以外，用户还可以通过该功能查看有权使用的所有发布的应用程序。选择某个应用程序将在本地客户端设备上为其打开一个窗口，该应用程序的外观和行为就像是在本地安装的一样。

例如，在 Windows 客户端计算机上，如果最小化应用程序窗口，该应用程序的项将保留在任务栏中，且看起来像是在本地 Windows 计算机上安装的一样。您还可以为将显示在客户端桌面上的应用程序创建快捷方式，就像本地安装的应用程序的快捷方式一样。

在以下情况下，以这种方式部署发布的应用程序可能比部署完整的远程桌面更好：

- 如果使用多层架构设置应用程序（组件可以在地理位置彼此靠近时更好地工作），则使用发布的应用程序是一个很好的解决方案。

  例如，当用户必须远程访问数据库时，如果必须通过 WAN 传输大量数据，则通常会影响性能。对于发布的应用程序，应用程序的所有部分可以位于与数据库相同的数据中心，以便隔离流量并仅通过 WAN 发送屏幕更新。

- 与先打开远程 Windows 桌面，然后再导航至应用程序相比，从移动设备访问单个应用程序更简单一些。

要使用此功能，您可以在 Microsoft RDS 主机上安装应用程序。在这一点上，Horizon 7 发布的应用程序的工作方式类似于其他应用程序远程解决方案。将使用 Blast Extreme 显示协议或 PCoIP 显示协议提供 Horizon 7 发布的应用程序以优化用户体验。

使用 Horizon Persona Management 保留用户数据和设置

可以将 Horizon Persona Management 用于远程桌面以及不受 Horizon 7 管理的物理机和虚拟机。用户配置管理可保留用户对其配置文件所做的更改。用户配置文件中包含各种由用户生成的信息。

- 用户特定的数据和桌面设置，这些信息可以使桌面外观保持一致（无论用户登录到哪个桌面）。
- 应用程序数据和设置。例如，这些设置允许应用程序记住工具栏位置和首选项。

- 由用户应用程序配置的 Windows 注册表条目。

为协助增强这些功能，用户配置管理要求 CIFS 共享位置的存储空间大于或等于用户本地配置文件的大小。

缩短登录和注销时间

用户配置管理最大程度地缩短了登录和注销桌面所需的时间。在登录过程中，默认情况下 Horizon 7 只下载 Windows 需要的文件，如用户注册表文件。Horizon 7 采用远程桌面上的配置文件中的最新更改，并定期将这些更改复制到远程存储库中。

使用用户配置管理，您可以避免通过对 Active Directory 做出任何更改来拥有受管配置文件。要配置用户配置管理，您可以指定一个中心存储库，无需在 Active Directory 中更改用户属性。使用该中心存储库，您可以在一环境中管理用户配置文件，而不会对用户可能登录的物理机产生影响。

使用用户配置管理时，如果您通过 VMware ThinApp 应用程序置备桌面，ThinApp 沙箱数据同样可以存储在用户配置文件中。此数据可随用户漫游，但不会对登录时间产生明显影响。此策略可有效防止数据丢失或损坏。

配置选项

您可以在多个级别配置 Horizon 7 用户配置：单个远程桌面、桌面池、OU 或部署中的所有远程桌面。您也可以在不受 Horizon 7 管理的物理机和虚拟机上使用独立版本的用户配置管理。

通过设置组策略 (GPO)，您可以对用户配置中要包含的文件和文件夹进行粒度控制。您可以指定是否包含本地设置文件夹、登录时加载哪些文件、用户登录后在后台下载哪些文件，以及用户配置中的哪些文件要使用 Windows 漫游配置文件功能（而不是用户配置管理）来管理。

与使用 Windows 漫游配置文件一样，您可以配置文件夹重定向。您可以将下列文件夹重定向到某一网络共享位置。

联系人	我的文档	保存游戏
Cookie	我的音乐	搜索
桌面	我的图片	开始菜单
下载	我的视频	启动项目
收藏夹	网上邻居	模板
历史记录	打印机邻居	Internet 临时文件
链接	最近使用的项目	

限制

用户配置管理存在以下局限和限制：

- 在即时克隆桌面池上不支持该功能。
- 您必须拥有一个包含用户配置管理组件的 Horizon 7 许可证。
- 用户配置管理需要一个 CIFS（公用 Internet 文件系统）共享位置。
- 此功能不适用于 Windows 10 链接克隆桌面池上的永久磁盘。

将 USB 设备与远程桌面和应用程序一起使用

管理员可以配置从虚拟桌面使用各种 USB 设备的能力，如使用拇指闪存盘、摄像头、VoIP（IP 语音）设备和打印机。此功能称为 USB 重定向。虚拟桌面最多可容纳 255 个 USB 设备。

您还可以重定向某些本地连接的 USB 设备，以便在已发布的桌面和应用程序中使用。有关支持的特定设备类型的信息，请参阅《在 Horizon 7 中配置远程桌面功能》文档。

在已在单用户计算机上部署的桌面池中使用该功能时，已附加到本地客户端系统的大多数 USB 设备在远程桌面中变为可用。您甚至可以从远程桌面连接并管理 iPad。例如，可使 iPad 与安装在远程桌面中的 iTunes 同步。在某些客户端设备（如 Windows 和 Mac 计算机）上，将在 Horizon Client 菜单中列出 USB 设备。此菜单可用于连接设备和断开设备的连接。

在大多数情况下，无法同时在客户端系统和远程桌面中使用 USB 设备。只有几种类型的 USB 设备可以在远程桌面和本地计算机之间共享。这些设备包括智能卡读卡器和人机接口设备（如键盘和指针设备）。

管理员可指定最终用户可连接的 USB 设备类型。对于客户端系统上包含多种设备类型（例如，包含一个视频输入设备和一个存储设备）的复合设备，管理员可通过拆分设备，允许连接其中一个设备（如视频输入设备），而禁止连接另一个（如存储设备）。

USB 重定向功能仅适用于特定类型的客户端。要了解某个特定客户端是否支持该功能，请参阅针对该客户端的 Horizon Client 安装和设置文档中提供的功能支持表。

将实时音频-视频功能用于网络摄像头和麦克风

通过使用实时音频-视频功能，您可以在远程桌面或已发布应用程序上使用本地客户端系统的网络摄像头或麦克风。实时音频-视频与标准会议应用程序和基于浏览器的视频应用程序兼容。它支持标准网络摄像头、音频 USB 设备和模拟音频输入。

最终用户可在其远程桌面上运行 Skype、Webex、Google Hangouts 和其他在线会议应用程序。该功能可将视频和音频数据重定向到代理计算机，其占用的带宽要低于 USB 重定向。使用实时音频-视频，网络摄像头图像和音频输入在客户端系统上进行编码，然后被发送到代理计算机。在代理计算机上，虚拟网络摄像头和虚拟麦克风对流进行解码和播放，以便供第三方应用程序使用。

无需进行特殊配置，但是管理员可以设置代理端组策略和注册表项，以配置帧速率和图像分辨率或关闭该功能。默认情况下，帧速率为每秒 15 帧，分辨率为 320 x 240 像素。必要时，管理员还可使用客户端配置设置来设置首选网络摄像头或音频设备。

注　该功能仅适用于某些类型的客户端。要了解某个特定类型的客户端是否支持该功能，请参阅针对该特定类型的桌面或移动客户端设备的安装和设置文档中提供的功能支持表。

使用 3D 图形应用程序

随 Blast Extreme 或 PCoIP 显示协议一起提供的软件加速和硬件加速图形功能支持远程桌面用户运行涵盖 Google Earth 到 CAD 和其他图形密集型应用程序的 3D 应用程序。

NVIDIA GRID vGPU（共享 GPU 硬件加速）	该功能在 vSphere 6.0 和更高版本提供，其允许多个虚拟机共享 ESXi 主机上的物理 GPU（图形处理单元）。如果需要高端硬件加速的工作站图形，可以使用该功能。
采用 vDGA 的 AMD 多用户 GPU	此功能随 vSphere 6.0 及更高版本一起提供，可使一个 AMD GPU 显示为多个 PCI 直通设备，从而允许多个虚拟机共享此 AMD GPU。此功能提供了从轻量级 3D 任务工作者到高端工作站图形超级用户的灵活硬件加速 3D 配置文件。
虚拟专用图形加速 (vDGA)	该功能在 vSphere 5.5 Update 2 和更高版本中提供，其将 ESXi 主机上的单个物理 GPU 专用于单个虚拟机。如果需要高端硬件加速的工作站图形，可以使用该功能。 **注** 某些 Intel vDGA 卡需要特定的 vSphere 6 版本。请参阅位于 http://www.vmware.com/resources/compatibility/search.php 的《VMware 硬件兼容性列表》。此外，对于 Intel vDGA，使用的是 Intel 集成的 GPU 而不是分离式 GPU，其他供应商的情况也是如此。
虚拟共享图形加速 (vSGA)	该功能在 vSphere 5.5 Update 2 和更高版本中提供，其允许多个虚拟机共享 ESXi 主机上的物理 GPU。您可以将 3D 应用程序用于设计、建模和多媒体。
软 3D	软件加速的图形，在 vSphere 5.5 Update 2 和更高版本中提供，允许您在不使用物理 GPU 的情况下运行 DirectX 9 和 OpenGL 2.1 应用程序。对于要求不高的 3D 应用程序（如 Windows Aero 主题、Microsoft Office 2010 和 Google Earth）可以使用该功能。

现在，Microsoft RDS 主机上运行的已发布应用程序中还支持 NVIDIA GRID vGPU 和 vDGA。

重要事项 有关各种 3D 渲染选项和要求的更多信息，请参阅有关图形加速的 VMware 白皮书、《适用于 VMware Horizon 6.1 的 NVIDIA GRID vGPU 部署指南》和《NVIDIA GRID 虚拟 GPU 用户指南》。

将多媒体文件流式传输到远程桌面

适用于 Windows 7 和 Windows 8/8.1 桌面和客户端的 Windows Media MMR（多媒体重定向）功能可支持在将多媒体文件流式传输到远程桌面时在 Windows 客户端计算机上进行全保真播放。

通过 MMR，多媒体流在 Windows 客户端系统上进行解码处理。客户端系统播放媒体内容，从而降低了 ESXi 主机上的负载需求。支持 Windows Media Player 支持的媒体格式，例如：M4V；MOV；MP4；WMP；MPEG-4 Part 2；WMV 7、8 和 9；WMA；AVI；ACE；MP3；WAV。

注 您必须将 MMR 端口作为例外规则添加到防火墙软件中。MMR 的默认端口是 9427。

从远程桌面打印

借助虚拟打印功能，部分客户端系统中的最终用户可从远程桌面使用本地或网络打印机，而不必在远程桌面操作系统中安装额外的打印驱动程序。您可以通过基于位置的打印功能将远程桌面映射到与终端客户端设备距离最近的打印机。

使用虚拟打印时，打印机被添加到某一台本地计算机后，将自动添加到远程桌面的可用打印机列表。无需进行进一步配置。在此功能可以使用的打印机上，您可以设置数据压缩、打印质量、双面打印和色彩等属性的首选项。拥有管理员特权的用户仍然可以在远程桌面上安装打印机驱动程序，且不会与虚拟打印组件发生冲突。

本地打印机重定向专门用于以下用例：

- 直接连接到客户端设备上的 USB 或串行端口的打印机
- 连接到客户端的专用打印机，例如条形码打印机和标签打印机
- 远程网络上不可从虚拟会话寻址的网络打印机。

要将打印作业发送给 USB 打印机，您可以使用 USB 重定向功能或虚拟打印功能。

IT 组织可以通过基于位置的打印将远程桌面映射到与终端客户端设备最近的打印机。以医生为例，无论他在医院的哪个房间打印文档，其打印作业都会发送到最近的一台打印机。使用此功能需要在远程桌面上安装正确的打印机驱动程序。

注　这些打印功能仅在某些类型的客户端中可用。要了解某个特定类型的客户端是否支持打印功能，请参阅针对该特定类型的桌面或移动客户端设备的安装和设置指南中提供的功能支持表。转到 https://docs.vmware.com/cn/VMware-Horizon-Client/index.html。

使用单点登录功能进行登录

单点登录 (SSO) 功能允许最终用户只提供一次 Active Directory 登录凭据。

如果您未使用单点登录功能，最终用户就必须登录两次。系统首先提示他们提供 Active Directory 凭据以登录 Horizon 连接服务器，然后再提示他们登录远程桌面。如果还使用了智能卡，最终用户就必须登录三次，因为用户还必须在智能卡读卡器提示他们输入 PIN 时进行登录。

对于远程桌面，此功能包括凭据提供程序动态链接库。

True SSO

通过 True SSO 功能，用户不再需要提供任何 Active Directory 凭据。在用户使用任何非 AD 方法（例如，RSA SecurID 或 RADIUS 身份验证）登录到 VMware Identity Manager 后，不会提示用户另外输入 Active Directory 凭据以使用远程桌面或应用程序。

如果用户使用智能卡或 Active Directory 凭据进行身份验证，则不需要使用 True SSO 功能，但即使在这种情况下，您也可以配置为使用 True SSO。然后，将忽略用户提供的任何 AD 凭据并使用 True SSO。

True SSO 的工作方式是在 Windows 登录过程中生成唯一的短期证书。您必须设置一个证书颁发机构（如果还没有）和证书注册服务器才能代表用户生成短期证书。您可以通过运行连接服务器安装程序，并选择“注册服务器”选项来安装注册服务器。

True SSO 将身份验证（验证用户身份）与访问（如 Windows 桌面或应用程序）分开。用户凭据是使用数字证书保护的。不会在数据中心存储或传输任何密码。有关更多信息，请参阅《Horizon 7 管理指南》文档。

显示器和屏幕分辨率

您可以将远程桌面扩展到多个显示器。如果具有高分辨率显示器，您可以使用高分辨率查看远程桌面或应用程序。

您可以选择“所有显示器”显示模式以在多个显示器上显示远程桌面。如果使用“所有显示器”模式并单击“最小化”按钮，在最大化窗口时，窗口将恢复为“所有显示器”模式。类似地，如果使用“全屏”模式并最小化窗口，在最大化窗口时，窗口将在一个显示器上恢复为“全屏”模式。

在多显示器设置中使用所有显示器

不管使用何种显示协议，都可以将多个显示器用于远程桌面。如果您让 Horizon Client 使用所有显示器，当您最大化应用程序窗口时，窗口将只在包含它的显示器上扩展为整个屏幕。

Horizon Client 支持下列显示器配置：

- 如果使用两个显示器，它们不需要处于相同的模式。例如，如果您使用连接外接显示器的笔记本电脑，则外接显示器既可以使用纵向模式也可以使用横向模式。
- 只有在使用两个显示器并且总高度低于 4096 像素时，才能并排放置、两两堆叠或垂直堆叠显示器。
- 要使用 3D 呈现功能，您必须使用 VMware Blast 或 PCoIP 显示协议。您最多可以使用两个显示器，最大分辨率为 1920x1200。对于 4K (3840x2160) 分辨率，仅支持一个显示器。
- 使用 VMware Blast 显示协议或 PCoIP 显示协议，可以支持分辨率为 4K (3840x2160) 的远程桌面屏幕。支持的 4K 显示器的数量取决于桌面虚拟机的硬件版本和 Windows 版本。

硬件版本	Windows 版本	支持的 4K 显示器数量
10（兼容 ESXi 5.5.x）	7、8、8.x 和 10	1
11（兼容 ESXi 6.0）	7 （禁用 3D 渲染功能和 Windows Aero）	3
11	7 （启用 3D 渲染功能）	1
11	8、8.x 和 10	1
13 或 14	7、8、8.x 和 10 （启用 3D 渲染功能）	1
13 或 14	7、8、8.x 和 10	4

- 如果使用 Microsoft RDP 7，可用于显示远程桌面的最大显示器数量为 16。
- 如果使用 Microsoft RDP 显示协议，您必须在远程桌面中安装 Microsoft 远程桌面连接 (Remote Desktop Connection, RDC) 6.0 或更高版本。

在多显示器设置中使用一个显示器

如果您具有多个显示器，但希望 Horizon Client 仅使用一个显示器，您可以选择在“所有显示器”以外的任何模式下打开远程桌面窗口。默认情况下，将在主显示器上打开该窗口。有关更多信息，请参阅《适用于 Windows 的 VMware Horizon Client 安装和设置指南》文档。

使用高分辨率模式

在某些类型的客户端上，在使用 VMware Blast 或 PCoIP 显示协议时，Horizon Client 还支持在这些具有高分辨率显示器的客户端系统中使用非常高的分辨率。只有在客户端系统支持高分辨率显示器时，才会显示启用高分辨率模式的选项。

默认情况下，在虚拟机中配置 vGPU 后，将启用硬件编码。将为所有支持的多显示器配置启用硬件编码，但使用小于 1 GB 显存的 vGPU 配置文件使用软件解码器，这是由于 NVENC 内存限制造成的。请参阅 NVENC 需要使用至少 1 GB 帧缓冲区，网址为 https://docs.nvidia.com/grid/4.3/grid-vgpu-release-notes-vmware-vsphere/index.html。

从中心位置管理桌面和应用程序池

3

您可以创建包含一个或成百上千个远程桌面的桌面池。您可以将虚拟机、物理机和 Windows 远程桌面服务 (RDS) 主机作为桌面源使用。创建一个虚拟机并将其用作基础映像后，Horizon 7 便可通过该映像生成大量远程桌面。还可以创建大量应用程序，为用户提供这些应用程序的远程访问权限。

本章讨论了以下主题：

桌面池的优势

借助 Horizon 7，您可以创建桌面池，并将桌面池置备为集中管理的基础。

您可以通过以下来源创建远程桌面池：

- 物理系统，如物理桌面 PC。
- 位于 ESXi 主机上并由 vCenter Server 管理的虚拟机
- 在虚拟化平台上运行的虚拟机，而非支持 Horizon Agent 的 vCenter Server。
- RDS 主机上基于会话的桌面。有关通过 RDS 主机创建桌面池的更多信息，请参阅《在 Horizon 7 中设置已发布的桌面和应用程序》文档。

如果将 vSphere 虚拟机作为桌面源使用，您可以按需要自动生成任意数量的相同虚拟桌面。您可以设置为池生成的虚拟桌面数量的最大值和最小值。设置这些参数可确保您始终能够获得足够的远程桌面来使用，同时又不会生成过多的桌面浪费可用资源。

使用池来管理桌面，您可以对池中的所有远程桌面应用设置或部署应用程序。以下示例介绍了一些可用设置：

- 指定远程桌面默认使用的远程显示协议，以及是否允许最终用户覆盖默认值。

- 对于 View Composer 链接克隆虚拟机或完整克隆虚拟机，指定在不使用时是否关闭虚拟机以及是否将其完全删除。将始终启动即时克隆虚拟机。
- 对于 View Composer 链接克隆虚拟机，您可以指定是使用 Microsoft Sysprep 自定义规范还是 VMware 的 QuickPrep。Sysprep 为池中的每个虚拟机生成唯一的 SID 和 GUID。即时克隆需要使用 VMware 提供的不同自定义规范（称为 ClonePrep）。

也可以指定如何为用户分配池中的桌面。

专用分配池	每个用户都被分配了一个特定的远程桌面，并在每次登录时返回同一个桌面。专用的分配池需要具有一对一的桌面到用户关系。例如，一个具有 100 个用户的组需要使用一个具有 100 个桌面的池。
浮动分配池	利用浮动分配池，您还可以创建可供轮班制用户使用的桌面池。例如，包含 100 个桌面的池可供 300 名轮班制用户（每班 100 个用户）使用。在每次使用远程桌面后可选择性地删除并重新创建远程桌面，从而形成高度可控的环境。

应用程序池的优点

利用应用程序池，您可以授权用户访问在数据中心内的服务器上（而不是在用户的个人计算机或设备上）运行的应用程序。

应用程序池具有多个显著优势：

- 可访问性

  用户可以从网络上的任何位置访问应用程序。您还可以配置安全网络访问。

- 设备独立性

  借助应用程序池，您可以支持多种客户端设备，如智能手机、平板电脑、笔记本电脑、瘦客户端和个人计算机。客户端设备可以运行各种操作系统，如 Windows、iOS、Mac OS 或 Android。

- 访问控制

  您可以轻松、快速地为一个用户或一组用户授予或撤消访问应用程序的权限。

- 加速部署

  使用应用程序池时，由于您仅在数据中心内的服务器上部署应用程序，并且每台服务器可以支持多个用户，因此可以加快应用程序部署。

- 可管理性

  管理部署在客户端计算机和设备上的软件通常需要大量资源。管理任务包括部署、配置、维护、支持和升级。使用应用程序池时，由于软件在数据中心内的服务器上运行，需要的安装副本较少，因此您可以简化企业内的管理。

- 安全性和法规遵从性

  使用应用程序池时，由于应用程序及其关联的数据集中存在于数据中心内，因此可以提高安全性。数据集中可以解决安全问题和法规遵从性问题。

- 降低成本

  根据软件许可协议，在数据中心托管应用程序更节省成本。其他因素（包括加快部署速度和提高可管理性）也可以降低企业内的软件成本。

降低并管理存储要求

在由 vCenter Server 管理的虚拟机上部署桌面，可以实现以前只有虚拟化服务器才能实现的存储效率。将即时克隆或 Composer 链接克隆作为桌面计算机可以节约存储空间，因为池中的所有虚拟机与基础映像共享一个虚拟磁盘。

- 使用 vSphere 管理存储

  vSphere 可以对磁盘卷和文件系统进行虚拟化，这样您在管理和配置存储时，就无需考虑数据的物理存储位置。

- 使用 VMware vSAN 提供高性能存储和基于策略的管理

  VMware VMware vSAN 是一个软件定义的存储层，它是在 vSphere 5.5 Update 2 或更高版本中提供的，用于虚拟化 vSphere 主机群集上提供的本地物理存储磁盘。可以在创建自动桌面池或自动场时仅指定一个数据存储，各种组件（如虚拟机文件、副本、用户数据和操作系统文件）将放在相应的固态磁盘 (SSD) 或直连硬盘 (HDD) 上。

- 使用虚拟卷实现以虚拟机为中心的存储和基于策略的管理

  使用随 vSphere 6.0 或更高版本提供的虚拟卷 (VVol)，单个虚拟机而非数据存储将变为存储管理的单元。存储硬件获得对虚拟磁盘内容、布局和管理的控制。

- 使用 Composer 降低存储要求

  Composer 可创建与基础映像共享虚拟磁盘的桌面映像，因此您可以将存储容量需求降低 50% 到 90%。

- 使用即时克隆减少存储需求

  即时克隆功能利用 vSphere vmFork 技术（在 vSphere 6.0U1 和更高版本中提供）使运行的基础映像或父虚拟机处于静默状态，并快速创建和自定义一个虚拟桌面池。

使用 vSphere 管理存储

vSphere 可以对磁盘卷和文件系统进行虚拟化，这样您在管理和配置存储时，就无需考虑数据的物理存储位置。

vSphere 支持光纤通道 SAN 阵列、iSCSI SAN 阵列和 NAS 阵列等目前广泛应用的存储技术，用以满足各种数据中心存储需求。存储阵列通过存储区域网络与各个服务器组相连，并在各服务器组之间共享存储资源。采用这种结构能够聚合存储资源，还能更加灵活地将这些资源置备给虚拟机。

兼容的 vSphere 5.5 Update 2 或更高版本的功能

对于 vSphere 5.5 Update 2 或更高版本，您可以使用 vSAN，它将 ESXi 主机上的本地物理固态磁盘和硬盘驱动器虚拟化为一个由群集中的所有主机共享的数据存储。vSAN 提供高性能存储以及基于策略的管理，以便在创建桌面池时仅指定一个数据存储，各种组件（如虚拟机文件、副本、用户数据和操作系统文件）将放置在相应的固态磁盘 (SSD) 或直连硬盘 (HDD) 上。

通过使用 vSAN，您还可以使用存储策略配置文件管理虚拟机存储和性能。如果由于主机、磁盘或网络故障或者工作负载发生变化而导致策略不符合要求，vSAN 将重新配置受影响的虚拟机的数据，并优化群集中的资源使用。您可以在最多包含 20 台 ESXi 主机的群集中部署桌面池。

vSAN 支持需要使用共享存储的 VMware 功能（例如 HA、vMotion 和 DRS），同时不再需要使用外部共享存储，并简化了存储配置和虚拟机置备活动。

重要事项 vSphere 6.0 和更高版本中提供的 vSAN 功能包含很多性能改进。对于 vSphere 6.0，此功能还具有更广泛的 HCL（硬件兼容性）支持。有关 vSphere 6 或更高版本中的 vSAN 的详细信息，请参阅《管理 VMware vSAN》文档。

注 vSAN 与 View Storage Accelerator 功能兼容，但与节省空间的磁盘格式功能不兼容，后者擦除并压缩磁盘以回收磁盘空间。

使用 vSphere 5.5 Update 2 或更高版本时，可以使用以下功能：

- 利用 View Storage Accelerator 功能，可以将 ESXi 主机配置为缓存虚拟机磁盘数据。

  如果使用基于内容的读取缓存 (CBRC)，那么，在引导风暴期间，在多台计算机启动的同时运行防病毒扫描的情况下，IOPS 会减少，性能会提高。主机不再从存储系统中一遍遍地读取整个操作系统，而是从缓存中读取常规数据块。
- 如果远程桌面采用 vSphere 5.1 及更高版本所提供的节省空间的磁盘格式，则客户机操作系统中过期或已删除的数据将通过擦除和压缩流程自动回收。
- 副本磁盘必须存储在 VMFS5 或更高版本的数据存储中或 NFS 数据存储中。如果您将副本磁盘存储在 VMFS5 之前的版本中，群集最多可包含 8 台主机。可将操作系统磁盘和永久磁盘存储在 NFS 或 VMFS 数据存储中。

兼容的 vSphere 6.0 或更高版本的功能

使用 vSphere 6.0 或更高版本时，可以使用虚拟卷 (VVol)。此功能可将虚拟磁盘及其衍生产品、克隆、快照和副本直接映射到存储系统上名为虚拟卷的对象。此映射允许 vSphere 将密集型存储操作（如快照、克隆和复制）卸载到存储系统。

通过虚拟卷，还可以使用 vSphere 中的存储策略配置文件来管理虚拟机存储和性能。这些存储策略配置文件基于每个虚拟机规定了存储服务。此类型的粒度置备提高了容量利用率。您可以在最多包含 32 台 ESXi 主机的群集中部署桌面池。

注 虚拟卷与 View Storage Accelerator 功能兼容，但与节省空间的磁盘格式功能不兼容，后者通过擦除和压缩磁盘回收磁盘空间。

注 即时克隆不支持虚拟卷。

使用 VMware vSAN 提供高性能存储和基于策略的管理

VMware VMware vSAN 是一个软件定义的存储层，它是在 vSphere 5.5 Update 2 或更高版本中提供的，用于虚拟化 vSphere 主机群集上提供的本地物理存储磁盘。可以在创建自动桌面池或自动场时仅指定一个

数据存储，各种组件（如虚拟机文件、副本、用户数据和操作系统文件）将放在相应的固态磁盘 (SSD) 或直连硬盘 (HDD) 上。

vSAN 实施基于策略的方法以进行存储管理。在使用 vSAN 时，Horizon 7 以默认存储策略配置文件的形式定义虚拟机存储要求（如容量、性能和可用性），并自动在 vCenter Server 上为虚拟桌面部署这些要求。将自动为每个磁盘单独应用这些策略（vSAN 对象），并在虚拟桌面的整个生命周期中保留这些策略。存储根据分配的策略进行置备和自动配置。您可以在 vCenter 中修改这些策略。Horizon 为每个 Horizon 群集的链接克隆桌面池、即时克隆桌面池、完整克隆桌面池或自动场创建 vSAN 策略。

您可以为 vSAN 群集启用加密，以加密 vSAN 数据存储中的所有静态数据（支持所有 Horizon 7 桌面池类型）。vSAN 加密是在 vSAN 版本 6.6 或更高版本中提供的。有关加密 vSAN 群集的详细信息，请参阅 VMware vSAN 文档。

无论在群集中的物理位置如何，每个虚拟机都会维护各自的策略。如果由于主机、磁盘或网络故障或者工作负载发生变化而导致策略不符合要求，vSAN 将重新配置受影响的虚拟机的数据，并进行负载平衡以符合每个虚拟机的策略。

vSAN 支持需要使用共享存储的 VMware 功能（例如 HA、vMotion 和 DRS），同时不再需要使用外部共享存储基础架构，并简化了存储配置和虚拟机置备活动。

重要事项 与 vSphere 5.5 Update 2 中提供的功能相比，vSphere 6.0 和更高版本中提供的 vSAN 功能包含很多性能改进。对于 vSphere 6.0，此功能还具有更广泛的 HCL（硬件兼容性）支持。此外，VMware vSAN 6.0 还支持使用基于闪存的设备进行缓存和持久存储的全闪存架构。

要求和限制

在 Horizon 7 部署中使用时，vSAN 功能具有以下限制：

- 本版本不支持使用 Horizon 7 节省空间的磁盘格式功能，该功能通过擦除和压缩磁盘回收磁盘空间。
- vSAN 不支持 View Composer Array Integration (VCAI) 功能，因为 vSAN 不使用 NAS 设备。

注 vSAN 与 View Storage Accelerator 功能兼容。vSAN 在 SSD 磁盘上提供一个缓存层，View Storage Accelerator 功能提供基于内容的缓存，以便在发生引导风暴时降低 IOPS 并提高性能。

vSAN 功能具有以下要求：

- vSphere 5.5 Update 2 或更高版本。
- 合适的硬件。例如，VMware 建议为每个对容量有贡献的节点使用 10GB 网卡以及至少一个 SSD 和一个 HDD。有关具体内容，请参阅《VMware 兼容性指南》。
- 至少包含三个 ESXi 主机的群集。您需要具有足够的 ESXi 主机以满足您的设置要求，即使在 vSAN 延伸群集中使用两个 ESXi 主机。有关更多信息，请参阅《vSphere 最高配置》文档。
- SSD 容量至少占 HDD 容量的 10%。
- 需要足够的 HDD 来容纳您的设置。磁盘上的利用率不要超过 75%。

有关 vSAN 要求的详细信息，请参阅《vSphere 5.5 Update 2 存储》文档中的“使用 vSAN”。对于 vSphere 6 或更高版本，请参阅《管理 VMware vSAN》文档。有关为 VMware vSAN 设计 Horizon 7 虚拟桌面基础架构的关键组件以及进行大小调整的指南，请参阅 http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf 中的白皮书。

使用虚拟卷实现以虚拟机为中心的存储和基于策略的管理

使用随 vSphere 6.0 或更高版本提供的虚拟卷 (VVol)，单个虚拟机而非数据存储将变为存储管理的单元。存储硬件获得对虚拟磁盘内容、布局和管理的控制。

使用虚拟卷，抽象存储容器可替代基于 LUN 或 NFS 共享的传统存储卷。虚拟卷可直接将虚拟磁盘及其衍生产品、克隆、快照和副本映射到存储系统上的对象，也称为虚拟卷。通过此映射，vSphere 可以将密集型存储操作（如拍摄快照、克隆和复制）卸载到存储系统。例如，这样之前需要一小时的克隆操作现在通过使用虚拟卷只需要几分钟。

重要事项 虚拟卷的主要优势之一是能够使用基于软件策略的管理 (Software Policy-Based Management, SPBM)。但是，对于该版本，Horizon 7 不会创建 vSAN 所创建的默认粒度存储策略。您而是可以在 vCenter Server 中设置一个全局默认存储策略，该策略将应用于所有虚拟卷数据存储。

虚拟卷具有以下优势：

- 虚拟卷支持将大量操作卸载到存储硬件。这些操作包括快照、克隆和 Storage DRS。
- 使用虚拟卷，您可以使用包括单个虚拟磁盘上的复制、加密、重复数据删除和压缩的高级存储服务。
- 虚拟卷支持此类 vSphere 功能，如 vMotion、Storage vMotion、快照、链接克隆、Flash Read Cache 和 DRS。
- 您可以将虚拟卷与支持 vSphere APIs for Array Integration (VAAI) 的存储阵列结合使用。

要求和限制

虚拟卷功能在 Horizon 7 部署中使用时存在以下限制：

- 本版本不支持使用 Horizon 7 节省空间的磁盘格式功能，该功能通过擦除和压缩磁盘回收磁盘空间。
- 虚拟卷不支持使用 View Composer Array Integration (VCAI)。
- 即时克隆桌面池不支持虚拟卷数据存储。

注 虚拟卷与 View Storage Accelerator 功能兼容。vSAN 在 SSD 磁盘上提供一个缓存层，View Storage Accelerator 功能提供基于内容的缓存，以便在发生引导风暴时降低 IOPS 并提高性能。

虚拟卷功能有以下要求：

- vSphere 6.0 或更高版本。
- 合适的硬件。某些存储供应商负责提供可与 vSphere 集成并提供虚拟卷支持的存储提供程序。每个存储提供程序都必须由 VMware 认证并进行正确部署。
- 您在虚拟数据存储上置备的所有虚拟磁盘都必须为 1 MB 的偶数倍数。

虚拟卷是 vSphere 6.0 功能。有关要求、功能、后台和设置要求的详细信息，请参阅《vSphere 存储》文档中有关虚拟卷的主题。

使用 Composer 降低存储要求

Composer 可创建与基础映像共享虚拟磁盘的桌面映像，因此您可以将存储容量需求降低 50% 到 90%。

Composer 使用基础映像或父虚拟机，可创建最多包含 2,000 个链接克隆虚拟机的池。每个链接克隆都像一个独立的桌面，带有唯一的主机名和 IP 地址，但链接克隆的存储需求明显较少。

副本与链接克隆位于相同数据存储中

在创建链接克隆桌面池或 Microsoft RDS 主机场时，将先从父虚拟机中创建一个完整克隆。完整克隆（或副本）以及与之链接的克隆可存储在相同的数据存储或 LUN（逻辑单元号）上。如有必要，您可以使用重新平衡功能在不同的 LUN 之间移动副本和链接克隆桌面池，或者将链接克隆桌面池从 LUN 移动到 vSAN 数据存储或从 vSAN 数据存储移动到 LUN。

副本与链接克隆位于不同数据存储中

或者，您可以将 Composer 副本和链接克隆分别存放在具有不同性能特征的数据存储中。例如，您可以将副本虚拟机存储在固态磁盘 (SSD) 中。固态磁盘具有低存储容量和高读取性能，通常支持的每秒 I/O 次数 (IOPS) 能达到上万次。您可以将链接克隆存储在基于传统旋转介质的数据存储中。这种磁盘性能较低，但价格相对低廉，并具有较高存储容量，因此适合存储大型池中的大量链接克隆。分层存储配置能够经济高效地处理密集 I/O 负载，如同时重新启动大量虚拟机，或者运行计划内的病毒扫描任务。

有关更多信息，请参阅名为《VMware View 的存储注意事项》的最佳实践指南。

如果您使用 vSAN 数据存储或虚拟卷数据存储，则无法手动为副本和链接克隆选择不同的数据存储。由于 vSAN 和虚拟卷功能自动将对象放在相应类型的磁盘上并缓存所有 I/O 操作，因此，vSAN 和虚拟卷数据存储不需要使用副本分层。

适用于页面文件和临时文件的一次性磁盘

在创建链接克隆池或场时，您还可以选择配置一个单独的一次性虚拟磁盘以存储在用户会话期间生成的客户机操作系统页面文件和临时文件。虚拟机电源关闭后，将删除一次性磁盘。使用一次性磁盘可以减缓链接克隆的增长速度，同时降低已关闭虚拟机所占用的空间，这些都有助于节省存储空间。

适用于专用桌面的永久磁盘

当您创建专用分配桌面池时，Composer 可选择性为每个虚拟桌面创建各自的永久虚拟磁盘。最终用户的 Windows 配置文件和应用程序数据将保存在永久磁盘中。刷新、重构或重新平衡链接克隆时，永久虚拟磁盘中的内容会被保留。VMware 建议您将 Composer 永久磁盘存储在单独的数据存储中。这样便可以备份保存永久磁盘的整个 LUN。

适用于浮动的无状态桌面的本地数据存储

链接克隆桌面可存储在本地数据存储（ESXi 主机上的内部备用磁盘）中。本地存储的优势包括：使用价格低廉的硬件、快速置备虚拟机、实现高效的开关机以及简化管理等。但是，使用本地存储会限制您可使用的 vSphere 基础架构配置选项。本地存储在某些环境中具有优势，但在其他环境中并不合适。

注 本节中所述的限制不适用于 vSAN 数据存储，该数据存储还使用本地存储磁盘，但需要使用特定的硬件，如前面有关 vSAN 的章节中所述。

如果环境中的远程桌面是无状态桌面，则使用本地数据存储将极为可行。例如，您可在部署无状态的 Kiosk 或教室和培训中心时使用本地数据存储。

如果您打算利用本地存储的好处，必须认真考虑以下限制：

- 不能使用 vMotion、VMware High Availability (HA) 或 vSphere Distributed Resource Scheduler (DRS)。
- 不能使用 Composer 的重新平衡操作在资源池中对虚拟机执行负载平衡。
- 不能将 Composer 副本和链接克隆存储在不同的数据存储中，VMware 建议您将二者存储在相同的卷中。

如果您通过控制虚拟机数量及其磁盘增长速度来管理本地磁盘使用情况，且您使用的是浮动分配并定期进行刷新和删除操作，那么您可将链接克隆成功部署至本地数据存储。

有关更多信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档中关于创建桌面池的章节。

使用即时克隆减少存储需求

即时克隆功能利用 vSphere vmFork 技术（在 vSphere 6.0U1 和更高版本中提供）使运行的基础映像或父虚拟机处于静默状态，并快速创建和自定义一个虚拟桌面池。

即时克隆不仅在创建时与父虚拟机共享虚拟磁盘，而且还共享父虚拟机的内存。每个即时克隆都像一个独立的桌面，带有唯一的主机名和 IP 地址，但即时克隆的存储需求明显较少。即时克隆将所需的存储容量减少 50% 到 90%。在创建克隆时，总内存需求也会减少。有关存储需求和大小调整限制的更多信息，请参阅 VMware 知识库 (KB) 文章 https://kb.vmware.com/kb/2150348。

从 Horizon 7 版本 7.8 开始，即时克隆在 vSAN 数据存储中支持 vSphere TRIM 和 UNMAP 功能。

副本与即时克隆位于相同数据存储中

当您创建即时克隆桌面池时，首先需要从主虚拟机创建一个完整克隆。完整克隆（或副本）以及与之链接的克隆可存储在相同的数据存储或 LUN（逻辑单元号）上。

副本与即时克隆位于不同数据存储中

此外，您也可以将即时克隆副本和即时克隆分别存放在具有不同性能特征的数据存储中。例如，您可以将副本虚拟机存储在固态磁盘 (SSD) 中。固态磁盘具有低存储容量和高读取性能，通常支持的每秒 I/O 次数 (IOPS) 能达到上万次。

您可以将即时克隆存储在基于传统旋转介质的数据存储中。这种磁盘性能较低，但价格相对低廉，并具有较高存储容量，因此适合存储大型池中的大量即时克隆。分层存储配置能够经济高效地处理密集 I/O 负载，如同时运行计划内的病毒扫描任务。

如果您使用 vSAN 数据存储，则无法手动为副本和即时克隆选择不同的数据存储。由于 vSAN 自动将对象放在相应类型的磁盘上并缓存所有 I/O 操作，因此，vSAN 数据存储不需要使用副本分层。在 vSAN 数据存储上支持即时克隆池。

在本地数据存储上存储即时克隆

即时克隆虚拟机可以存储在本地数据存储（ESXi 主机上的内部备用磁盘）中。本地存储的优势包括：使用价格低廉的硬件、快速置备虚拟机、实现高效的开关机以及简化管理等。但是，使用本地存储会限制您可使用的 vSphere 基础架构配置选项。本地存储在某些 Horizon 7 环境中具有优势，但在其他环境中并不合适。

注　本主题中所述的限制不适用于 vSAN 数据存储，该数据存储还使用本地存储磁盘，但需要使用特定的硬件。

如果环境中的 Horizon 7 桌面是无状态桌面，使用本地数据存储将是极为可行的。例如，您可在部署无状态的 Kiosk 或教室和培训中心时使用本地数据存储。

如果您的虚拟机具有浮动分配，不是专供单个最终用户使用，并且可以按固定的时间间隔（例如用户注销时）删除或刷新，则可以考虑使用本地数据存储。通过这种方法，您可以控制每个本地数据存储的磁盘使用情况，而无需在各数据存储之间移动虚拟机或对虚拟机执行负载平衡。

但是，您必须考虑使用本地数据存储给 Horizon 7 桌面或场部署带来的限制：

- 您无法使用 VMotion 管理虚拟卷。
- 您无法使用 VMware High Availability。
- 您无法使用 vSphere Distributed Resource Scheduler (DRS)。

  如果您在具有本地数据存储的单个 ESXi 主机上部署即时克隆，则必须配置包含该单个 ESXi 主机的群集。如果您的群集包含两个或更多具有本地数据存储的 ESXi 主机，请从该群集包含的每个主机中选择本地数据存储。否则，即时克隆创建操作会失败。此行为不同于 Composer 链接克隆的本地数据存储行为。
- 您无法在不同的数据存储中存储副本和即时克隆。
- 如果您选择本地旋转磁盘驱动器，其性能可能与商用存储阵列的性能不太一样。本地旋转磁盘驱动器也许具有与存储阵列相似的容量，但达不到与存储阵列相同的吞吐量。吞吐量会随着磁盘转轴数量的增加而增加。如果您选择直连固态磁盘 (SSD)，则性能可能会超出很多存储阵列的性能。
- 如果您打算利用本地存储的优势，那么必须仔细考虑好无法使用 VMotion、高可用性、DRS 及其他功能的后果。如果您通过控制虚拟机数量及其磁盘增长速度来管理本地磁盘使用情况，且您使用的是浮动分配并定期执行刷新和删除操作，那么您就可以将即时克隆成功部署到本地数据存储。
- 即时克隆的本地数据存储支持适用于虚拟桌面和已发布的桌面。

即时克隆和 Composer 链接克隆之间的差异

由于即时克隆的创建速度比链接克隆的创建速度快得多，因此在置备即时克隆池时，不再需要链接克隆的以下功能：

- 即时克隆池不支持配置单独的一次性虚拟磁盘以存储客户机操作系统的页面文件和临时文件。每次用户注销即时克隆桌面时，Horizon 7 将自动删除该克隆，然后根据池的最新可用操作系统映像置备并启动另一个即时克隆。在注销操作期间，将自动删除任何客户机操作系统页面文件和临时文件。
- 即时克隆池不支持为每个虚拟桌面创建单独的永久虚拟磁盘。相反，您可以在 App Volumes 的用户可写磁盘上存储最终用户的 Windows 配置文件和应用程序数据。在最终用户登录时，最终用户的用户可写磁盘将连接到即时克隆桌面上。此外，还可以使用用户可写磁盘永久保存用户安装的应用程序。
- 由于即时克隆桌面具有短期特性，因此，即时克隆不支持空间效率较高的磁盘格式（SE 稀疏）及其擦除和压缩过程。
- 即时克隆桌面池与 Storage vMotion 兼容。Composer 链接克隆桌面池与 Storage vMotion 不兼容。

应用程序置备

通过使用 Horizon 7，您可以使用几个选项置备应用程序：使用传统应用程序置备方法，提供已发布的应用程序而不是远程桌面，分发使用 VMware ThinApp 创建的应用程序包，将应用程序作为 View Composer 或即时克隆基础映像的一部分进行部署，或者使用 App Volumes 连接应用程序。

- 使用 RDS 主机部署单个应用程序

  您可以选择为最终用户提供已发布的应用程序而非远程桌面。在小型移动设备上导航单个已发布的应用程序可能更容易。
- 使用 View Composer 部署应用程序和系统更新

  由于链接克隆桌面池共享一个基础映像，因此您可以通过更新父虚拟机来快速部署更新和修补程序。
- 使用即时克隆部署应用程序和系统更新

  由于即时克隆桌面池共享一个基础映像，因此您可以通过更新父虚拟机来快速部署更新和修补程序。
- 在 Horizon Administrator 中管理 VMware ThinApp 应用程序

  VMware ThinApp™ 能帮您将应用程序封装到可在虚拟化应用程序沙箱中运行的单个文件中。采用这种策略可以灵活地置备应用程序，而且不会产生冲突。
- 使用 App Volumes 部署和管理应用程序

  通过在操作系统上面虚拟化应用程序，VMware App Volumes 提供了一种替代方法以管理应用程序。通过使用该策略，应用程序、数据文件、设置、中间件和配置将作为单独的分层容器使用。
- 使用现有流程或 VMware Mirage 置备应用程序

  利用 Horizon 7，您可以继续沿用贵公司目前采用的应用程序置备技术，并可以使用 Mirage。由此会产生两个新问题，即如何管理服务器 CPU 利用率和存储 I/O，以及确定是否允许用户安装应用程序。

使用 RDS 主机部署单个应用程序

您可以选择为最终用户提供已发布的应用程序而非远程桌面。在小型移动设备上导航单个已发布的应用程序可能更容易。

最终用户可以使用先前用来访问远程桌面的 Horizon Client 并使用相同的 Blast Extreme 或 PCoIP 显示协议来访问基于 Windows 的已发布应用程序。

要提供已发布的应用程序，需要在 Microsoft 远程桌面会话 (RDS) 主机上安装该应用程序。一个或多个 RDS 主机组成场，管理员可以采用与创建桌面池相似的方式从该场创建应用程序池。有关场大小调整的建议，请参阅 VMware 知识库 (KB) 文章 http://kb.vmware.com/kb/2150348。

利用该策略可以简化应用程序的添加、删除和更新，在应用程序中添加或删除用户授权，并可用来从任意设备或网络访问集中式或分布式应用程序场。

使用 View Composer 部署应用程序和系统更新

由于链接克隆桌面池共享一个基础映像，因此您可以通过更新父虚拟机来快速部署更新和修补程序。

借助重构功能，您可以修改父虚拟机、拍摄新状态的快照并向全部或部分用户及桌面提供新版本映像。您可以使用此功能执行以下任务：

- 应用操作系统和软件修补程序及升级
- 应用服务包
- 添加应用程序
- 添加虚拟设备
- 更改其他虚拟机设置，如可用内存

注　由于您还可以使用 View Composer 创建链接克隆 Microsoft RDS 主机场，您可以通过重构功能更新 RDS 主机上的客户机操作系统和应用程序。

创建包含用户设置和其他用户生成数据的 View Composer 永久磁盘。永久磁盘不受重构操作影响。您可以在删除链接克隆时保留用户数据。在员工离开公司后，另一位员工可以访问他的用户数据。拥有多个桌面的用户可以将用户数据整合到单个桌面上。

如果希望禁止用户添加、删除软件或更改设置，您可以使用刷新功能将桌面恢复到默认值。此功能还可以减小链接克隆的大小（链接克隆的大小会不断增长）。

使用即时克隆部署应用程序和系统更新

由于即时克隆桌面池共享一个基础映像，因此您可以通过更新父虚拟机来快速部署更新和修补程序。

借助映像推送功能，您可以更改父虚拟机，拍摄新状态的快照并以滚动方式向全部用户和桌面提供新版本映像。通过滚动更新，可以最大程度地缩短与池维护相关的停机时间。在用户注销即时克隆虚拟桌面时，Horizon 7 会删除即时克隆，通过最新版本的映像创建全新的即时克隆，并准备好新克隆以供下一个用户登录时使用。

您可以使用此功能执行以下任务：

- 应用操作系统和软件修补程序及升级
- 应用服务包
- 添加应用程序
- 添加虚拟设备
- 更改其他虚拟机设置，如可用内存

在 Horizon Administrator 中管理 VMware ThinApp 应用程序

VMware ThinApp™ 能帮您将应用程序封装到可在虚拟化应用程序沙箱中运行的单个文件中。采用这种策略可以灵活地置备应用程序，而且不会产生冲突。

VMware ThinApp 可将应用程序从底层操作系统及其库和框架中分离，并将应用程序捆绑为单个可执行文件（称为应用程序包），从而提供应用程序虚拟化。您可以使用 Horizon Administrator 将 VMware ThinApp 应用程序分发到桌面和池中。

重要事项 如果您更希望将 ThinApp 分配到 Active Directory 用户和组，而不是分布到桌面和池，则可以使用 VMware Identity Manager。

当您使用 VMware ThinApp 创建虚拟化应用程序后，可以选择从共享文件服务器对应用程序进行流式处理，或者选择将应用程序安装到虚拟桌面。如果您要配置虚拟化应用程序以进行流式处理，则必须解决以下架构问题：

- 特定用户组对存储应用程序包的特定应用程序存储库的访问权限
- 应用程序存储库的存储配置
- 流式处理过程中产生的网络流量（很大程度上取决于应用程序的类型）

对于经过流式处理的应用程序，用户可以用桌面快捷方式启动。

如果您要分配 ThinApp 包使其能够安装到虚拟桌面，所需考虑的架构问题与使用基于 MSI 的传统软件置备方法时需要解决的问题类似。对于流式应用程序和远程桌面中安装的 ThinApp 包，均应考虑应用程序存储库的存储配置。

使用 App Volumes 部署和管理应用程序

通过在操作系统上面虚拟化应用程序，VMware App Volumes 提供了一种替代方法以管理应用程序。通过使用该策略，应用程序、数据文件、设置、中间件和配置将作为单独的分层容器使用。

在只读模式下，这些容器称为应用程序堆栈 (AppStack)；在读写模式下，这些容器称为可写卷。管理员可以使用 App Volumes Manager 创建 AppStack 和分配应用程序权限，以及为系统、用户或组提供置备的 AppStack。App Volumes 提供的应用程序看上去就像安装在本地一样，并且它们随用户在会话和设备之间移动。管理员可以实时更新或替换应用程序以及移除分配的任何应用程序：立即移除、在用户仍登录时移除或在下次登录或重新引导时移除。

有关更多信息，请参阅 https://docs.vmware.com/cn/VMware-App-Volumes/index.html 中提供的 VMware App Volumes 文档。

使用现有流程或 VMware Mirage 置备应用程序

利用 Horizon 7，您可以继续沿用贵公司目前采用的应用程序置备技术，并可以使用 Mirage。由此会产生两个新问题，即如何管理服务器 CPU 利用率和存储 I/O，以及确定是否允许用户安装应用程序。

如果您将应用程序同时推送到大量的远程桌面，便会发现 CPU 利用率和存储 I/O 显著增高。这些峰值工作负载会极大影响桌面的性能。因此，最好将应用程序更新安排在非高峰时段进行，如有可能请交错更新桌面。您还必须验证您的存储解决方案是否支持此类工作负载。

如果您的公司允许用户安装应用程序，您可以继续沿用当前策略，但却无法充分利用 View Composer 的功能，如刷新和重构桌面。利用 View Composer，如果某个应用程序未虚拟化或者包含在用户的配置文件或数据设置中，View Composer 执行刷新、重构或重新平衡操作时便会放弃该应用程序。在很多情况下，这种可以严格控制要安装哪些应用程序的功能是一项优势。由于 View Composer 桌面采用与已知可行配置类似的配置，因此您可以轻松支持这些桌面。

如果用户在安装应用程序以及在远程桌面生命周期内永久保存这些应用程序（而不是使用 View Composer 置备应用程序）方面具有严格的要求，您可以将即时克隆与 App Volumes 一起使用。另一个解决方案是创建完整克隆专用桌面，允许用户安装应用程序，然后使用 Mirage 管理和更新桌面，而不覆盖用户安装的应用程序。

重要事项 还要使用 Mirage 管理本地安装的脱机桌面及其应用程序。有关更多信息，请参阅 Mirage 文档页。

使用 Active Directory GPO 管理用户和桌面

Horizon 7 中包含很多组策略管理 ADMX 模板，可用于集中管理和配置 Horizon 7 组件与远程桌面。

将这些模板导入到 Active Directory 后，您就可以用它们来设置应用于以下组和组件的策略：

- 所有系统（无论由哪个用户登录）
- 所有用户（无论登录哪个系统）
- 连接服务器配置
- Horizon Client 配置
- Horizon Agent 配置

应用 GPO 后，属性将存储在特定组件的本地 Windows 注册表中。

您可以使用 GPO 设置 Horizon Administrator 用户界面 (UI) 中提供的所有策略。也可以使用 GPO 设置不能从 UI 中获得的策略。有关通过 ADMX 模板提供的设置的完整列表和说明，请参阅《在 Horizon 7 中配置远程桌面功能》。

使用智能策略

您也可以使用智能策略创建一些策略，用来控制特定远程桌面上 USB 重定向、虚拟打印、剪贴板重定向、客户端驱动器重定向和 PCoIP 显示协议功能的行为。该功能需要使用 User Environment Manager。

使用智能策略，可以创建仅在满足特定条件时才会生效的策略。例如，可以配置这样一个策略：当用户从企业网络外部连接到远程桌面时，禁用客户端驱动器重定向功能。

总之，为 User Environment Manager 中的远程桌面功能配置的 Horizon 策略设置会覆盖任何等效的注册表项和组策略设置。

远程桌面部署的体系结构设计元素与规划指导原则

4

典型的 Horizon 7 体系结构设计采用容器策略。由于硬件配置、所用的 Horizon 7 和 vSphere 软件版本以及其他特定于环境的设计因素的不同，容器的定义可能存在差异。

本文档中的示例说明了可扩展设计足以适应各种企业环境及特定要求。本章详细介绍了有关内存、CPU、存储容量、网络组件和硬件需求的重要细节，为 IT 架构师和规划人员提供了实用的 Horizon 7 解决方案部署指导。

重要事项 本章不涵盖以下主题：

托管应用程序的体系结构设计	一个 Horizon 7 容器可以支持多个 Microsoft RDS 主机场，其中每个场都包含多个 RDS 主机。有关更多信息，请参阅《在 Horizon 7 中设置已发布的桌面和应用程序》。如果您计划使用 RDS 主机的虚拟机，另请参阅 RDS 主机虚拟机配置。
Horizon 7 Agent Direct Connect 插件的体系结构设计	通过在远程虚拟机桌面上运行此插件，客户端可以直接连接到虚拟机。所有远程桌面功能（包括 PCoIP、HTML Access、RDP、USB 重定向和会话管理）都以相同方式工作，就像用户已通过 View 连接服务器进行连接一样。有关详细信息，请参见《Horizon 7 Agent Direct-Connection 插件管理》。

本章讨论了以下主题：

远程桌面的虚拟机要求

在规划远程桌面规格时，您所选择的 RAM、CPU 和磁盘空间配置将对您的服务器、存储硬件和开销情况产生重要影响。

- 基于员工类型的规划

  包括 RAM、CPU 和存储大小在内的很多配置元素的要求，很大程度上取决于使用虚拟桌面的员工类型和必须安装的应用程序。

- 估算虚拟机桌面的内存要求

  服务器 RAM 的成本往往要高于 PC RAM 成本。RAM 成本在整个服务器硬件成本和所需存储总量中占据了很大比例，因此确定合适的内存分配量对规划桌面部署至关重要。

- 估算虚拟机桌面的 CPU 要求

  在估算 CPU 时，您必须收集有关各类企业员工平均 CPU 利用率的信息。

- 选择合适的系统磁盘大小

  在分配磁盘空间时，还要为操作系统、应用程序和用户可能会安装或生成的其他内容提供足够的空间。这个容量通常低于物理 PC 磁盘的容量。

基于员工类型的规划

包括 RAM、CPU 和存储大小在内的很多配置元素的要求，很大程度上取决于使用虚拟桌面的员工类型和必须安装的应用程序。

规划体系结构时，可将员工分为以下几个类型。

任务型员工	任务型员工和管理型员工通常在固定的计算机设备上使用少数应用程序执行重复的任务。与知识型员工使用的应用程序相比，这些应用程序往往不需要消耗大量的 CPU 和内存资源。按特定轮班制度工作的任务型员工可能会在同一时间登录虚拟桌面。任务型员工包括呼叫中心分析人员、零售员工和库房员工等。
知识型员工	知识型员工的日常工作包括访问 Internet、使用电子邮件和创建复杂文档、演示文稿及电子表格。知识型员工包括会计、销售经理和市场调研分析师等。
超级用户	超级用户包括应用程序开发人员和使用图形密集型应用程序的用户。
Kiosk 用户	这些用户需要共享公共位置的桌面。典型的 Kiosk 用户包括：教室内使用共享计算机的学生、护理工作站的护士以及用于工作安排和人员招聘的计算机等。这些桌面需要自动登录。如果需要，可以通过特定的应用程序来进行身份验证。

估算虚拟机桌面的内存要求

服务器 RAM 的成本往往要高于 PC RAM 成本。RAM 成本在整个服务器硬件成本和所需存储总量中占据了很大比例，因此确定合适的内存分配量对规划桌面部署至关重要。

如果分配的 RAM 过低，存储 I/O 将因为频繁的 Windows 分页而受到负面影响。如果分配的 RAM 过高，客户机操作系统的页面文件和每个虚拟机的交换文件和挂起文件将变得非常大，会对存储容量产生不利影响。

RAM 大小对性能的影响

分配 RAM 时，应避免选择过于保守的分配设置。请考虑以下问题：

- 分配的 RAM 不足可导致 Windows 分页过于频繁，由此产生的 I/O 将严重降低性能并增加存储 I/O 负载。
- VMware ESXi 支持透明页面共享和内存膨胀等精密的内存资源管理算法，可显著降低支持给定的客户机 RAM 分配量所需的物理 RAM。例如，即使为虚拟桌面分配了 2 GB 内存，所消耗的物理 RAM 也仅为 2 GB 的一小部分。
- 由于虚拟桌面的性能极易受到响应时间的影响，因此需要在 ESXi 主机上为 RAM 预留设置指定非零值。预留一部分 RAM 可确保空闲但处于使用状态的桌面不会被完全交换到磁盘。此外还可以降低 ESXi 交换文件所消耗的存储空间。但是，较高的预留设置将影响您在 ESXi 主机上过量分配内存的能力，还可能影响 vMotion 维护操作。

RAM 大小对存储的影响

分配到虚拟机的 RAM 容量直接关系到虚拟机使用的某些文件的大小。要访问以下列表中的文件，请使用 Windows 客户机操作系统定位 Windows 页面文件和休眠文件，通过 ESXi 主机的文件系统来定位 ESXi 交换文件和挂起文件。

Windows 页面文件

默认情况下，该文件的大小为客户机 RAM 的 150%。默认情况下，该文件位于 `C:\pagefile.sys`，由于它将被频繁访问，因而会导致精简置备的存储不断增大。View Composer 链接克隆虚拟机上的页面文件和临时文件可被重定向到虚拟机关闭时删除的单独虚拟磁盘中。一次性页面文件重定向可以节约存储容量、减缓链接克隆的增长速度并改善性能。尽管可以从 Windows 中调整该文件的大小，但这样做可能会降低应用程序的性能。

对于即时克隆，将在注销操作期间自动删除任何客户机操作系统页面文件和临时文件，因此，不会随时间的推移变得非常大。每次用户注销即时克隆桌面时，Horizon 将删除该克隆，然后根据池的最新可用操作系统映像置备并启动另一个即时克隆。

笔记本电脑的 Windows 休眠文件

该文件的大小能和客户机 RAM 的大小完全相同。由于 Horizon 部署中不需要该文件，因此您可以安全地将其删除。

ESXi 交换文件

该文件的扩展名为 `.vswp`，如果您预留的 RAM 低于虚拟机的 RAM，则会创建此交换文件。交换文件的大小与未预留的客户机 RAM 的大小相同。例如，如果预留了 50% 的客户机 RAM，且客户机的 RAM 为 2 GB，则 ESXi

	交换文件的大小为 1GB。该文件可以存储在 ESXi 主机或群集的本地数据存储中。
ESXi 挂起文件	该文件的扩展名为 `.vmss`，如果您设置了桌面池注销策略（使虚拟桌面在最终用户注销时挂起），则会创建此文件。该文件的大小与客户机 RAM 的大小相同。

采用 PCoIP 或 Blast Extreme 时适用于特定显示器配置的 RAM 大小

除了系统内存以外，虚拟机还要求在 ESXi 主机上使用少量 RAM 以处理视频开销。该 VRAM 大小要求取决于为最终用户配置的显示器的显示分辨率和数量。表 4-1. PCoIP 或 Blast Extreme 客户端显示开销 中列出了各种配置所需的开销 RAM 量。此表中列条目所显示的内存大小不包括其他 PCoIP 或 Blast Extreme 功能所需的内存。

表 4-1. PCoIP 或 Blast Extreme 客户端显示开销

显示分辨率标准	宽度（像素）	高度（像素）	1 个显示器的开销	2 个显示器的开销	3 个显示器的开销	4 个显示器的开销
VGA	640	480	1.20MB	3.20MB	4.80MB	5.60MB
WXGA	1280	800	4.00MB	12.50MB	18.75MB	25.00MB
1080p	1920	1080	8.00MB	25.40MB	38.00MB	50.60MB
WQXGA	2560	1600	16.00MB	60.00MB	84.80MB	109.60MB
UHD (4K)	3840	2160	32.00MB	78.00MB	124.00MB	不支持

要计算系统要求，除了虚拟机的基本系统 RAM 以外，还需要使用 VRAM 值。在 Horizon Administrator 中指定最大显示器数和选择显示分辨率时，将自动计算和配置开销内存。

如果使用 3D 渲染功能并选择 Soft3D 或 vSGA，您可以在 Horizon Administrator 控件中使用额外的 VRAM 值进行重新计算，以便为 3D 客户机配置 VRAM。或者，对于 Soft3D 和 vSGA 以外的其他类型的图形加速，如果选择使用 vSphere Client 管理 VRAM，您可以指定确切数量的 VRAM。

默认情况下，多显示器配置与主机拓扑相匹配。预先为 2 个以上的显示器计算了额外开销以满足额外拓扑方案的要求。如果在启动远程桌面会话时遇到黑屏，请验证在 Horizon Administrator 中设置的显示器数量值和显示分辨率值与主机系统是否匹配，或者在 Horizon Administrator 中选择**使用 vSphere Client 管理**以手动调整内存量，然后将总显存值设置为最多 128MB。

特定工作负载和操作系统所需的 RAM 大小

由于不同类型员工的 RAM 需求存在很大差异，因此很多企业都通过试运行来确定企业中不同类型员工所需的适当内存设置。

开始时最好分配 1GB（32 位 Windows 7 或更高版本桌面）或 2GB（64 位 Windows 7 或更高版本桌面）的内存。如果要将其中的一个硬件加速图形功能用于 3D 工作负载，VMware 建议使用 2 个虚拟 CPU 和 4GB 的 RAM。在试运行阶段中，需要监视不同类型员工的使用性能和所用磁盘空间，并做出适当调整，最后确定适用于每种类型员工的最佳设置。

估算虚拟机桌面的 CPU 要求

在估算 CPU 时，您必须收集有关各类企业员工平均 CPU 利用率的信息。

对 CPU 的具体要求因员工类型而异。在试运行阶段，请使用性能监测工具（如虚拟机中的 Perfmon、ESXi 中的 `esxtop` 或 vCenter Server 性能监测工具）来了解这些员工组的平均及峰值 CPU 利用率。另外请遵循以下原则：

- 软件开发人员或其他具有高性能需求的超级用户对 CPU 的要求可能高于知识型员工和任务型员工。建议在运行计算密集型任务的 64 位 Windows 7 虚拟机中使用两个或四个虚拟 CPU，例如，使用 CAD 应用程序，播放高清视频或驱动 4K 显示分辨率。
- 至于其他情形，则建议使用单虚拟 CPU。

由于很多虚拟机都运行在一台服务器上，因此当代理程序（如防病毒代理）一起同时检查是否存在更新时，CPU 利用率将达到峰值。请确定有哪些/多少代理可能导致性能问题，并采取适当策略来解决这些问题。例如，以下策略可能会对您的企业有所帮助：

- 使用即时克隆或 View Composer 链接克隆更新映像，而不是由软件管理代理将软件更新下载到每个虚拟桌面。
- 将防病毒程序和软件更新安排在非峰值期间（在登录用户数量较少时）运行。
- 交错或随机执行更新。
- 使用与 VMware vShield API 兼容的防病毒产品。例如，该 API 已集成到 VMware vCloud® Networking and Security 5.1 及更高版本中。

在最初调整大小时，不妨假设每个虚拟机至少需要用到整个 CPU 核心 1/8 到 1/10 的计算资源。也就是在每个核心上试运行 8 到 10 个虚拟机。例如，如果假设在每个核心上运行 8 个虚拟机并使用 2 插槽 8 核 ESXi 主机，您可以在试运行期间在服务器上托管 128 个虚拟机。在此期间监视主机上的 CPU 整体使用情况，确保利用率基本保持在安全值以内（如 80%），从而为满足峰值负载留出足够空间。

选择合适的系统磁盘大小

在分配磁盘空间时，还要为操作系统、应用程序和用户可能会安装或生成的其他内容提供足够的空间。这个容量通常低于物理 PC 磁盘的容量。

由于数据中心磁盘空间每千兆字节的成本通常高于传统 PC 部署中台式机或笔记本电脑的成本，因此需要对操作系统映像大小进行优化。以下建议可用于优化映像大小：

- 删除不需要的文件。例如，减少临时 Internet 文件的配额。
- 关闭 Windows 服务，例如索引器服务、磁盘碎片整理程序服务和还原点。有关详细信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档。
- 选择能满足未来增长需要的虚拟磁盘大小，但不要过大。
- 使用集中的文件共享或 View Composer 永久磁盘或 App Volumes 存储用户生成的内容和安装的应用程序。
- 如果您正在使用 vSphere 5.1 或更高版本，请为 vCenter Server 和链接克隆桌面池启用空间回收功能。

如果虚拟机桌面采用 vSphere 5.1 或更高版本所提供的节省空间的磁盘格式，则客户机操作系统中过期或已删除的数据将通过擦除和压缩流程自动回收。

确定所需的存储空间时，必须考虑每个虚拟桌面的以下文件：

- ESXi 挂起文件的大小与分配给虚拟机的 RAM 容量相同。
- 默认情况下 Windows 页面文件的大小为 RAM 容量的 150%。
- 每台虚拟机的日志文件几乎可占用 100MB。
- 虚拟磁盘或 .vmdk 文件必须能够容纳操作系统、应用程序以及将来的应用程序和软件更新。另外，如果本地用户数据和用户安装的应用程序位于虚拟桌面（而不是文件共享）中，虚拟磁盘还必须能够容纳这些数据和应用程序。

  如果使用 View Composer，.vmdk 文件会不断增大，但您可以为虚拟机桌面池安排 View Composer 刷新操作并设置存储过载策略，并将 Windows 页面文件和临时文件重定向到单独的非永久磁盘，以控制它的增长量。

  如果您使用即时克隆，.vmdk 文件将在登录会话中不断增大。每次用户注销时，将自动删除即时克隆桌面，创建新的即时克隆并做好准备以供下一个用户登录时使用。通过使用该过程，将有效地刷新桌面并恢复为原始大小。

您也可以将这个预估值提高 15%，确保用户的磁盘空间不会耗尽。

Horizon 7 ESXi 节点

节点是指 Horizon 7 部署中托管虚拟机桌面的单个 VMware ESXi 主机。

Horizon 7 能采用最经济高效的方式，最大限度增加整合比率（即 ESXi 主机上托管桌面的数量）。尽管影响服务器选取的因素有很多，但如果您要严格控制采购价格，就必须找到处理能力和内存表现俱佳的服务器配置。

要确定环境和硬件配置的理想整合比率，必须在实际环境下进行性能检测（如试运行）。由于使用模式和环境因素的不同，具体的整合比率可能会有很大差异。请遵循以下原则：

- 作为一般性架构，通常以每个 CPU 核心运行 8 到 10 个虚拟桌面作为考虑计算容量的依据。有关计算每个虚拟机 CPU 要求的信息，请参见估算虚拟机桌面的 CPU 要求。
- 从虚拟桌面 RAM、主机 RAM 和过量分配比率方面思考内存容量问题。尽管可以为每个 CPU 核心部署 8 到 10 个虚拟桌面，但如果虚拟桌面占用 1 GB 或更多的 RAM，就必须仔细衡量物理 RAM 需求。有关计算每个虚拟机所需 RAM 容量的信息，请参阅估算虚拟机桌面的内存要求。

  请注意，物理 RAM 的成本并不符合线性规律，在某些情况下，购买不使用昂贵 DIMM 芯片的小型服务器可能更加划算。在其他情况下，考虑机架密度、存储连接能力、可管理性及其他因素的影响，也有助于最大限度地减少部署中的服务器数量。

- 在 Horizon 7 中，View Storage Accelerator 功能是默认启用的，从而使 ESXi 5.5 Update 2 及更高版本的主机能够缓存常用虚拟机磁盘数据。View Storage Accelerator 可以提高性能并减少用于管理引导风暴和防病毒扫描 I/O 风暴的额外存储 I/O 带宽需求。该功能要求每台 ESXi 主机都具备 1GB 的 RAM。

- 最后，还要考虑群集和故障切换方面的要求。有关更多信息，请参阅确定高可用性的要求。

有关 vSphere 中 ESXi 主机规格的信息，请参阅《VMware vSphere 最高配置》文档。

特定类型员工的桌面池

Horizon 7 提供多种功能来帮助您节约存储空间和降低各种应用情况下所需的处理能力。其中很多功能都是通过池设置来实现。

最基本的问题是衡量特定类型的用户，判定用户需要有状态桌面映像还是无状态桌面映像。需要有状态桌面映像的用户将其数据存放于必须保留、维护和备份的操作系统映像本身中。例如，这些用户会安装一些个人应用程序，或者拥有不能保存在虚拟机本身以外位置（如在文件服务器上或应用程序数据库中）的数据。

无状态桌面映像	无状态体系结构（也称为非持久桌面）具有许多优势，如易于支持和存储成本较低。此外，该体系结构还能限制虚拟机的备份需求，并提供更加简化、廉价的灾难恢复和业务连续性选项。
有状态桌面映像	这些映像（也称为持久桌面）可能需要使用传统映像管理方法。有状态映像与特定存储系统技术一起使用时，可降低存储成本。规划备份、灾难恢复和业务连续性策略时，VMware Site Recovery Manager 等备份和恢复技术都是重要的考量因素。

可以通过两种方法在 Horizon 7 中创建无状态桌面映像：

- 您可以创建即时克隆虚拟机的浮动分配池或专用分配池。可以选择使用文件夹重定向和漫游配置文件存储用户数据。
- 您可以使用 View Composer 创建链接克隆虚拟机的浮动或专用分配池。可以选择使用文件夹重定向和漫游配置文件来存储用户数据，或配置永久磁盘以永久保存用户数据。

可以通过多种方法在 Horizon 7 中创建有状态桌面映像：

- 您可以创建完整克隆或完整虚拟机。一些存储供应商具有经济高效的完整克隆存储解决方案。这些供应商通常拥有自己的最佳实践和置备实用程序。如果使用其中某家供应商的技术，可能需要创建手动的专用分配池。
- 您可以创建即时克隆或链接克隆虚拟机池，并使用 App Volumes 用户可写卷来附加用户数据和用户安装的应用程序。

使用无状态桌面还是有状态桌面取决于具体的员工类型。

- 任务型员工池

  您可以为任务型员工提供标准化无状态桌面映像，让映像随时保有易懂、易于支持的配置，因此员工可以登录到任意可用桌面。

- 知识型员工和超级用户池

  知识型员工必须能够创建复杂的文档并将其保留在桌面上。超级用户则必须能够安装并保留其个人应用程序。根据所保留的个人数据的性质和数量，可以采用有状态或无状态类型的桌面。

- Kiosk 用户池

  Kiosk 用户包括机场登记处的乘客、教室或图书馆内的学生、医疗数据录入工作站的医护人员或自助服务点的顾客。由于用户无需登录即可使用客户端设备或远程桌面，因此与客户端设备（而非用户）关联的帐户才有权使用这些桌面池。但仍可要求用户提供身份验证凭据来访问某些应用程序。

任务型员工池

您可以为任务型员工提供标准化无状态桌面映像，让映像随时保有易懂、易于支持的配置，因此员工可以登录到任意可用桌面。

由于任务型员工需要用一套为数不多的应用程序来执行重复性任务，因此您可以为其创建非固定桌面映像来节省存储空间并降低处理要求。

对于即时克隆桌面池，请使用以下池设置：

- 对于即时克隆池，要优化资源利用率，请使用按需置备以根据使用情况扩大或缩小池。请务必指定足够的备用桌面以满足登录速率要求。
- 对于即时克隆桌面池，每次用户注销时，Horizon 7 都会自动删除即时克隆。将创建新的即时克隆并做好准备以供下一个用户登录时使用，从而在每次注销时有效地刷新桌面。

对于 View Composer 链接克隆桌面池，请使用以下池设置：

- 对于 View Composer 桌面池，请确定在用户注销时执行的操作（如果有）。磁盘容量会不断增长。为节省磁盘空间，您可以在用户注销时将桌面刷新到原始状态。也可以设置计划来定期刷新桌面。例如，安排桌面每天、每周或每月刷新一次。
- 如果适用并且使用 View Composer 链接克隆池，请考虑在本地 ESXi 数据存储上存储桌面。这一策略的优势包括：使用价格低廉的硬件、快速置备虚拟机、实现高效的开关机以及简化管理等。有关限制信息，请参阅适用于浮动的无状态桌面的本地数据存储。在本地数据存储上不支持即时克隆池。

  注 有关其他类型的存储选项的信息，请参见降低并管理存储要求。

- 使用 Persona Management 功能，以便用户始终应用首选的桌面外观和应用程序设置，就像使用 Windows 用户配置文件一样。如果您未将桌面设置为在注销时刷新或删除，您可以配置在注销时移除用户配置。

  重要事项 用户配置管理有助于为希望在会话间保留设置的用户实施浮动分配池。之前，浮动分配桌面的一个限制是：当最终用户注销时，他们会丢失其所有配置设置和存储在远程桌面中的所有数据。

  每当最终用户登录时，其桌面背景即设置为默认壁纸，他们必须重新配置每个应用程序的首选项。使用用户配置管理，浮动分配桌面的最终用户无法区分自身会话与专用分配桌面会话之间的差异。

对于所有桌面池，请使用以下常规池设置：

- 创建一个自动池，以便在创建池时创建桌面，或是根据池的利用率来按需生成桌面。
- 使用浮动分配，以便用户能登录到任意可用桌面。如果所有用户都不需要在同一时间登录，该设置就可以减少所需的桌面数量。
- 创建即时克隆或 View Composer 链接克隆桌面，以使桌面共享相同的基础映像，并减少在数据中心内使用的存储空间（相对于完整虚拟机）。

知识型员工和超级用户池

知识型员工必须能够创建复杂的文档并将其保留在桌面上。超级用户则必须能够安装并保留其个人应用程序。根据所保留的个人数据的性质和数量，可以采用有状态或无状态类型的桌面。

对于不需要使用用户安装的应用程序（临时应用除外）的知识型员工，您可以创建无状态桌面映像，并将其所有个人数据保存在虚拟机以外的位置，如文件服务器或应用程序数据库中。对于其他知识型员工和超级用户，您可以为其创建固定桌面映像。

对于即时克隆桌面池，请使用以下池设置：

- 如果您使用即时克隆桌面，请实施文件共享、漫游配置文件或其他配置文件管理解决方案。

对于 View Composer 链接克隆桌面池，请使用以下池设置：

- 如果将 View Composer 与 vSphere 虚拟桌面一起使用，请为 vCenter Server 和桌面池启用空间回收功能。凭借空间回收功能，客户机操作系统中过期或已删除的数据将通过擦除和压缩流程自动回收。
- 如果您使用 View Composer 链接克隆桌面，请实施用户配置管理、漫游配置文件或其他配置文件管理解决方案。您也可以配置永久磁盘，以便刷新和重构链接克隆操作系统磁盘，并将用户配置文件的副本保存在永久磁盘上。
- 使用 Persona Management 功能，以便用户始终应用首选的桌面外观和应用程序设置，就像使用 Windows 用户配置文件一样。

对于所有桌面池，请使用以下常规池设置：

- 一些超级用户和知识型员工（如会计、销售经理、市场营销研究分析师）可能需要每次登录到相同的桌面。请为他们创建专用的分配池。
- 使用 vStorage Thin Provisioning，以便每一个桌面在最初都能仅使用磁盘在初始操作时所需的存储空间。
- 对于必须安装其个人应用程序（从而在操作系统磁盘中添加数据）的超级用户和知识型员工来说，共有两种选择。一种选择是创建完整虚拟机桌面。

  另一种选择是创建链接克隆或即时克隆池，并使用 App Volumes 在登录之间永久保存用户安装的应用程序和用户数据。
- 如果知识型员工不需要使用用户安装的应用程序（临时使用除外），您可以创建 View Composer 链接克隆桌面或即时克隆桌面。桌面映像可以共享同一个基础映像，所需的存储空间也低于完整虚拟机。

Kiosk 用户池

Kiosk 用户包括机场登记处的乘客、教室或图书馆内的学生、医疗数据录入工作站的医护人员或自助服务点的顾客。由于用户无需登录即可使用客户端设备或远程桌面，因此与客户端设备（而非用户）关联的帐户才有权使用这些桌面池。但仍可要求用户提供身份验证凭据来访问某些应用程序。

由于用户数据无需保留在操作系统磁盘中，因此设置为在 Kiosk 模式中运行的虚拟机桌面使用无状态桌面映像。Kiosk 模式桌面用于在瘦客户端设备或锁定的 PC 中使用。您必须确保：桌面应用程序可通过身份验证机制保证交易安全、物理网络不会被篡改和偷窃，以及连接到网络的所有设备都是受信任的。

最佳做法是使用专用的连接服务器实例处理 Kiosk 模式的客户端，并在 Active Directory 中为这些客户端的帐户创建专用的组织单位和组。这样不仅能防止这些系统遭受意外入侵，还会使客户端的配置和管理变得更加容易。

要设置 kiosk 模式，您必须使用 vdmadmin 命令行界面，并按照《Horizon 7 管理指南》文档中有关 kiosk 模式的主题中所述执行一些步骤。

在此设置过程中，您可以使用以下即时克隆桌面池设置。

- 如果使用即时克隆桌面池，每次用户注销时，Horizon 7 都会自动删除即时克隆。将创建新的即时克隆并做好准备以供下一个用户登录时使用，从而在每次注销时有效地刷新桌面。

在此设置过程中，您可以使用以下 View Composer 链接克隆桌面池设置。

- 如果使用 View Composer 链接克隆桌面，请设置一个刷新策略以经常刷新桌面，例如，每次用户注销时。
- 如果适用，请考虑将桌面存储在本地 ESXi 存储中。这一策略的优势包括：使用价格低廉的硬件、快速置备虚拟机、实现高效的开关机以及简化管理等。有关限制信息，请参阅适用于浮动的无状态桌面的本地数据存储。在本地数据存储上不支持即时克隆池。

  注 有关其他类型的存储选项的信息，请参见降低并管理存储要求。

在此设置过程中，您可以对所有桌面池使用以下常规设置。

- 创建一个自动池，以便在创建池时创建桌面，或是根据池的利用率来按需生成桌面。
- 使用浮动分配，使用户能够访问池中的任何可用桌面。
- 创建即时克隆或 View Composer 链接克隆桌面，以使桌面共享相同的基础映像，并减少在数据中心内使用的存储空间（相对于完整虚拟机）。
- 使用 Active Directory GPO（组策略对象）配置基于位置的打印，以便桌面能够使用位置最近的打印机。有关通过组策略管理 (ADMX) 模板提供的设置的完整列表和说明，请参阅《在 Horizon 7 中配置远程桌面功能》。
- 使用 GPO 或智能策略控制在启动桌面或将本地 USB 设备插入客户端计算机时是否将 USB 设备连接到桌面。

桌面虚拟机配置

示例中的内存、虚拟处理器数量和磁盘空间等项目设置均特定于 Horizon 7。

所需的系统磁盘空间容量取决于基础映像所需的应用程序数量。VMware 曾验证过包含 8 GB 磁盘空间的设置。其应用程序包括：Microsoft Word、Excel、PowerPoint、Adobe Reader、Internet Explorer、McAfee Antivirus 和 PKZIP。

用户数据所需的磁盘空间取决于最终用户的角色和数据存储的组织策略。如果使用 View Composer，此数据将保存在永久磁盘上。

下表中所列的指导原则是针对标准 Windows 7 或更高版本的虚拟机桌面。

表 4-2. Windows 7 或 Windows 8 桌面虚拟机示例

项目	示例
操作系统	32 位或 64 位 Windows 7 或更高版本（具有最新服务包）
RAM	1GB（4GB，如果用户必须具备用于 3D 呈现的硬件加速图形）
虚拟 CPU	1（2，针对 64 位系统或者如果用户必须播放高清或全屏视频）
系统磁盘容量	24GB（比标准值略小）
用户数据容量（作为永久磁盘）	5 GB（起始值）
虚拟 SCSI 适配器类型	LSI Logic SAS（默认类型）
虚拟网络适配器	VMXNET 3

RDS 主机虚拟机配置

可以使用 RDS（远程桌面服务）主机为最终用户提供发布的应用程序和基于会话的远程桌面。

RDS 主机可以是物理计算机或虚拟机。此示例将虚拟机与下表中列出的规格一起使用。该虚拟机的 ESXi 主机可以是 VMware HA 群集的组成部分，以防止物理服务器出现故障。

表 4-3. RDS 主机虚拟机示例

项目	示例
操作系统	64 位 Windows Server 2008 R2 或 Windows Server 2012 R2
RAM	24GB
虚拟 CPU	4
系统磁盘容量	40GB
虚拟 SCSI 适配器类型	LSI Logic SAS（Windows Server 2008 的默认类型）
虚拟网络适配器	VMXNET 3
1 个网卡	1 Gigabit
客户端连接总数最大值（包括基于会话的远程桌面连接和已发布的应用程序连接）	50

注 如果在资源规范的下限配置 RDS 主机，则在使用所有功能（而非默认安装）时可能会遇到资源约束。

有关 RDS 主机配置和已测试工作负载的详细信息，请参阅 http://www.vmware.com/files/pdf/techpaper/VMware-Reference-Architecture-Horizon-6-View-Mirage-Workspace.pdf 上的《VMware Horizon 6 参考架构》白皮书。

vCenter Server 和 View Composer 虚拟机配置

您可以将 vCenter Server 和 View Composer 安装在同一台虚拟机上或不同的服务器上。与桌面虚拟机相比，这些服务器对内存和处理能力的要求更高。

VMware 进行了测试，让 View Composer 通过使用 vSphere 5.1 或更高版本为每个池创建并置备 2,000 个桌面。VMware 还进行了另外一项测试，即让 View Composer 对 2,000 个桌面同时执行重构操作。在这些测试中，vCenter Server 和 View Composer 安装于不同的虚拟机上。

桌面池的大小受以下因素的限制：

- 每个桌面池仅可包含一个 vSphere 群集。
- 在某些设置下，群集最多可以包含 32 个主机。在其他设置下，群集仅限于 8 个主机。有关更多信息，请参阅 vSphere 群集。
- 每个 CPU 内核具有可用于 8 到 10 个虚拟桌面的计算容量。
- 子网可用的 IP 地址数量会限制池中桌面的数量。例如，如果在您的网络设置中，池中子网仅包含 256 个可用 IP 地址，则池的大小将被限制为 256 个桌面。但是，您可以配置多个网络标签，大幅增加分配给池中虚拟机的 IP 地址的数量。

尽管您可以在物理机上安装 vCenter Server 和 View Composer，但是此处选取单独的虚拟机作为示例，这些虚拟机具有下表中所列的规格。这些虚拟机所使用的 ESXi 主机可以是 VMware HA 群集的一部分，以防止物理服务器出现故障。

该示例假设您使用的是 Horizon 7 和 vSphere 5.1 或更高版本及 vCenter Server 5.1 或更高版本。

重要事项 该示例还假设 View Composer 和 vCenter Server 安装在不同的虚拟机上。

表 4-4. vCenter Server 虚拟机示例

项目	管理 10,000 个桌面的 vCenter Server 示例	管理 2,000 个桌面的 vCenter Server 示例
操作系统	64 位 Windows Server 2008 R2 Enterprise	64 位 Windows Server 2008 R2 Enterprise
RAM	48GB	10-24GB，取决于 vSphere 版本
虚拟 CPU	16	2-8，取决于 vSphere 版本
系统磁盘容量	180GB	40GB
虚拟 SCSI 适配器类型	LSI Logic SAS（Windows Server 2008 的默认类型）	LSI Logic SAS（Windows Server 2008 的默认类型）
虚拟网络适配器	E1000（默认）	VMXNET 3（但也可以使用默认的 E1000）
vCenter 最大并发置备操作数量	20	20
最大并发电源操作数量	50	50

表 4-5. View Composer 虚拟机示例

项目	管理 10,000 个桌面的 View Composer 示例	管理 2,000 个桌面的 View Composer 示例
操作系统	64 位 Windows Server 2008 R2 Enterprise	64 位 Windows Server 2008 R2 Enterprise
RAM	10GB 或更多，取决于 vSphere 版本	4-10GB，取决于 vSphere 版本
虚拟 CPU	4 或更多，取决于 vSphere 版本	2-4，取决于 vSphere 版本
系统磁盘容量	50GB	40GB
虚拟 SCSI 适配器类型	LSI Logic SAS（Windows Server 2008 的默认类型）	LSI Logic SAS（Windows Server 2008 的默认类型）
虚拟网络适配器	VMXNET 3	VMXNET 3
View Composer 池的大小上限	2,000 个桌面	1,000 个桌面
View Composer 最大并发维护操作数量	12	12
View Composer 最大并发置备操作数量	8	8

重要事项 VMware 建议您将 vCenter Server 和 View Composer 连接的数据库置于单独的虚拟机上。

Horizon 连接服务器最大连接数和虚拟机配置

Horizon Administrator 用户界面会随 Horizon 连接服务器一起安装。

连接服务器配置

尽管您可以在物理机上安装连接服务器，但此示例使用具有连接服务器虚拟机示例中所列规格的虚拟机。该虚拟机的 ESXi 主机可以是 VMware HA 群集的组成部分，以防止物理服务器出现故障。

表 4-6. 连接服务器虚拟机示例

项目	示例
操作系统	请参阅《Horizon 7 安装指南》文档中的支持的操作系统。
RAM	10GB
虚拟 CPU	4
系统磁盘容量	70GB
虚拟 SCSI 适配器类型	LSI Logic SAS（Windows Server 2008 的默认类型）
虚拟网络适配器	VMXNET 3
网络适配器	1Gbps 网卡

连接服务器群集设计注意事项

您可以在一个组中部署多个连接服务器副本实例来实现负载平衡和高可用性。副本实例组专为支持在连接 LAN 的单数据中心环境内组成群集而设计。

重要事项 要在 WAN、MAN（城域网）或其他非 LAN 中使用连接服务器的一组副本实例，如果 Horizon 部署需要跨多个数据中心，则必须使用 Cloud Pod 架构功能。有关更多信息，请参阅《在 Horizon 7 中管理 Cloud Pod 架构》文档。

连接服务器的最大连接数

“远程桌面连接”中提供了有关 Horizon 7 部署可以承载的并行连接数测定限制的信息。

表 4-7. 远程桌面连接

每个部署中的连接服务器数量	连接类型	最大并行连接数
1 台连接服务器	直接连接、RDP、Blast Extreme 或 PCoIP	4,000（测定配置）
1 台连接服务器	安全加密链路连接、RDP	2,000（默认配置） 4,000（测定配置）
1 台连接服务器	PCoIP 安全网关连接	2,000（默认配置） 4,000（测定配置）
1 台连接服务器	Blast 安全网关连接	2,000（默认配置） 4,000（测定配置）
1 台连接服务器	统一访问物理 PC	2,000（测定配置）
1 台连接服务器	统一访问 RDS 主机	2,000（测定配置）
7 个连接服务器	直接连接、RDP、Blast Extreme 或 PCoIP	RDS 主机 ■ 10,000（默认配置） ■ 20,000（测定配置） 虚拟桌面 ■ 12,000（测定配置）

注 完全支持测定配置。要在单台连接服务器上达到安全加密链路连接、PCoIP 安全网关和 Blast 安全网关最大并行连接数的测定配置 (4,000)，请在装有连接服务器的虚拟机上创建 `locked.properties` 文件：`C:\Program Files\VMware\VMware View\Server\sslgateway\conf`。然后，在 `locked.properties` 文件中设置 `maxConnections=4000`，并重新启动连接服务器。Unified Access Gateway 当前支持 2,000 个会话，因此在测试 20,000 个会话时使用了 14 个 Unified Access Gateway 设备。

如果使用安全服务器或 Unified Access Gateway 设备从企业网络外部建立 PCoIP 连接，则需要使用 PCoIP 安全网关连接。如果使用安全服务器或 Unified Access Gateway 设备从企业网络外部建立 Blast Extreme 或 HTML Access 连接，则需要使用 Blast 安全网关连接。如果使用安全服务器或 Unified Access Gateway 设备从企业网络外部建立 RDP 连接，或者通过 PCoIP 或 Blast 安全网关连接实现 USB 和多媒体重定向 (Multimedia Redirection, MMR) 加速，则需要使用安全加密链路连接。您可以将多个安全服务器与单个连接服务器实例配对。

虽然单个安全服务器或 Unified Access Gateway 设备最多可以支持 2,000 个并行连接，而不是每个连接服务器实例仅使用一个安全服务器（具有 2,000 个会话），但您可以选择使用 2 或 4 个安全服务器或设备。安全服务器监控可能表明 2,000 个用户的活动太多。所需的内存和 CPU 使用量可能表明您应为每个连接服务器实例添加多个安全服务器以分散负载。例如，可以使用 2 个安全服务器，每个处理 1,000 个连接，或者可以使用 4 个安全服务器，每个处理 500 个连接。安全服务器与连接服务器实例的比例取决于特定环境的要求。

每个 Unified Access Gateway 设备的连接数类似于安全服务器的连接数。有关 Unified Access Gateway 设备的更多信息，请参阅《部署和配置 Unified Access Gateway》。

注 在此示例中，尽管 5 个连接服务器实例（已进行适当配置）可以处理 20,000 个连接，但为了实现可用性规划，表中显示数字 7，以容纳来自企业网络内外的连接。

例如，如果您有 20,000 个用户，其中有 16,000 个用户在企业网络内部，则企业网络内部需要有 5 个连接服务器实例。这样，如果其中一个实例不可用，其余 4 个实例还可以处理负载。同样，对于来自企业网络外部的 4,000 个连接，您可以使用 2 个连接服务器实例，这样，当其中一个实例不可用时，您仍有一个实例可以用来处理负载。

这些数字假定外部连接是通过网关提供的。在该示例中，每个处理外部连接的连接服务器实例与 3 个安全服务器配对使用，以便在一个安全服务器变得不可用时，剩下的 2 个安全服务器可以处理负载。如果使用 Unified Access Gateway 设备而不是安全服务器，则总共需要使用 3 个设备在两个连接服务器实例之间进行负载平衡，以便在一个设备变为不可用时，剩下的 2 个设备可以处理负载。

在所有情况下，如果用户使用的连接服务器或网关变得不可用，则需要重新进行连接。

将 Horizon 7 与 Unified Access Gateway 配合使用的硬件要求

与 Horizon 7 配合使用时，VMware 建议在 Unified Access Gateway 设备中使用 2 个 vCPU 和 4GB RAM，以支持最大数量的连接。

表 4-8. Unified Access Gateway 的硬件要求

项目	示例
操作系统	OVA
RAM	4GB
虚拟 CPU	2
系统磁盘容量	20GB（更改默认日志级别需要额外的空间）
虚拟 SCSI 适配器类型	LSI Logic 并行（OVA 的默认设置）
虚拟网络适配器	VMXNET 3
网络适配器	1Gbps 网卡
网络映射	单网卡选项

vSphere 群集

在 Horizon 7 部署中，可使用 VMware HA 群集来防止物理服务器出现故障。群集最多可以包含 32 个节点，具体取决于您的设置。

vSphere 和 vCenter Server 提供了一组丰富的功能，可用于管理托管虚拟机桌面的服务器的群集。由于每个虚拟机桌面池都必须与 vCenter Server 资源池相关联，因此群集配置也很重要。因此，每个池中能容纳的最大桌面数量与您计划在每个群集中运行的服务器和虚拟机的数量有关。

在大型 Horizon 7 部署中，可以通过使每个数据中心对象仅包含一个群集对象（非默认行为）来提高 vCenter Server 的性能和响应能力。默认情况下，vCenter Server 会在同一个数据中心对象内新建群集。

注　有关 Horizon 7 大小调整限制和建议的最新更新，请参阅 VMware 知识库 (KB) 文章 https://kb.vmware.com/s/article/2150348。

在以下条件下，vSphere 群集最多可以包含 32 个 ESXi 主机或节点：

- vSphere 5.1 及更高版本，带有 View Composer 链接克隆池，并且将副本磁盘存储在 NFS 数据存储或 VMFS5 或更高版本的数据存储中
- vSphere 6.0 及更高版本，并且将池存储在虚拟卷数据存储中

如果您具有 vSphere 5.5 Update 1 和更高版本并将池存储在 vSAN 数据存储上，vSphere 群集最多可以包含 20 个 ESXi 主机。

如果您将 View Composer 副本存储在 VMFS5 之前的 VMFS 版本中，群集最多可包含 8 台主机。可将操作系统磁盘和永久磁盘存储在 NFS 或 VMFS 数据存储中。

有关详细信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档中有关创建桌面池的章节。网络要求具体取决于服务器类型、网络适配器数量和 vMotion 的配置方式。

确定高可用性的要求

vSphere 通过强大的效率和资源管理支持，可让您每台服务器支持的虚拟机数量达到业内领先的水平。但增加单台服务器的虚拟机密度后，一台服务器产生的故障也将影响更多的用户。

具体的高可用性要求将因桌面池用途的不同而存在很大差异。例如，无状态桌面映像（浮动分配）池与有状态桌面映像（专用分配）池的恢复点目标 (Recovery Point Objective, RPO) 要求可能会有所不同。对于浮动分配池，如果用户使用的桌面不再可用，可以尝试让他们登录不同的桌面。

如果可用性要求很高，就必须对 VMware HA 进行适当配置。如果您使用了 VMware HA 并计划为每台服务器部署固定数量的桌面，请以较低的容量运行每台服务器。如果服务器出现故障，则在其他主机上重新启动桌面时，每台服务器中桌面的容量不会超出限制。

例如，在一个包含 8 台主机的群集中，每台主机都能够运行 128 个桌面，如果以容许单个服务器出现故障为目标，则需要确保群集中运行的桌面数量不能超过 128 * (8 - 1) = 896 个。您也可以使用 VMware DRS (Distributed Resource Scheduler) 来平衡 8 台主机中的桌面。这样，您可以充分利用额外的服务器容量，而不会闲置任何热备用资源。此外，DRS 还能在故障服务器恢复运行后重新平衡群集。

您还必须确保对存储进行适当配置，使其支持大量虚拟机为响应服务器故障而立即重新启动时产生的 I/O 负载。存储 IOPS 是影响服务器出现故障后桌面恢复速度的最重要因素。

示例： 群集配置示例

下表列出的设置为 Horizon 7 所特有。有关 vSphere 中 HA 群集的限制的信息，请参阅《VMware vSphere 最高配置》文档。

注 以下基础架构示例使用 View 5.2 和 vSphere 5.1 进行了测试。该示例使用 View Composer 链接克隆而不是即时克隆，因为测试是使用 View 5.2 执行的。即时克隆功能是在 Horizon 7 中引入的。View 5.2 中未提供的其他功能包括 vSAN 和虚拟卷。

表 4-9. Horizon 7 基础架构群集示例

项目	示例
虚拟机	vCenter Server 实例、Active Directory、SQL 数据库服务器、View Composer、连接服务器实例、安全服务器、用作桌面池来源的父虚拟机
节点（ESXi 主机）	6 个 Dell PowerEdge R720 服务器（16 核心 * 2 GHz；每个主机具备 192GB RAM）
SSD 存储	vCenter Server 虚拟机、View Composer、SQL 数据库服务器及父虚拟机
非 SSD 存储	Active Directory、连接服务器和安全服务器虚拟机
群集类型	DRS (Distributed Resource Scheduler)/HA

表 4-10. 虚拟机桌面群集示例

项目	示例
群集数量	5
每个群集的桌面和池数量	每个群集具备 1 个包含 2,000 个桌面（虚拟机）的池
节点（ESXi 主机）	以下是每个群集可能会使用的各种服务器示例： ■ 12 Dell PowerEdge R720（16 个内核 * 2 GHz；每个主机上有 192GB 的 RAM） ■ 16 Dell PowerEdge R710（12 个内核 * 2.526 GHz；每个主机上有 144GB 的 RAM） ■ 8 Dell PowerEdge R810（24 个内核 * 2 GHz；每个主机上有 256GB 的 RAM） ■ 6 个 Dell PowerEdge R810 + 3 个 PowerEdge R720
SSD 存储	副本虚拟机
非 SSD 存储	32 个用于克隆的非 SSD 数据存储（每个数据存储为 450 GB）
群集类型	DRS (Distributed Resource Scheduler)/HA

存储和带宽要求

规划虚拟机桌面共享存储、I/O 风暴存储带宽要求和网络带宽需求时，必须考虑几个因素。

VMware 测试设置中所使用的存储和网络组件的详细信息，可参阅以下相关主题。

- 共享存储示例

  在 View 5.2 测试环境下，View Composer 副本虚拟机安置于具备高读取性能的固态磁盘 (SSD) 中，每秒支持数万个 I/O (IOPS)。链接克隆安置在基于传统低性能旋转介质的数据存储中，价格相对低廉，具有较高的存储容量。该示例使用 View Composer 链接克隆而不是即时克隆，因为测试是使用 View 5.2 执行的。即时克隆功能是在 Horizon 7 中引入的。

- 存储带宽问题

  在 Horizon 7 环境中，登录风暴是确定带宽要求时的主要考虑因素。

- 网络带宽问题

  需要使用某些虚拟和物理网络组件来支持典型的工作负载。

- View Composer 性能测试结果

  这些测试结果描述了包含 10,000 个桌面的 View 5.2 设置，在此设置中，由一个 vCenter Server 5.1 实例来管理 5 个池，每个池具备 2,000 个虚拟机桌面。无论是置备一个新的池，还是重构、刷新或重新平衡现有的具备 2,000 台虚拟机的池，都只需要一个维护期。另外还针对 10,000 位用户进行了登录风暴测试。

- WAN 支持

  对于广域网 (Wide-Area Network, WAN)，您必须考虑带宽限制和延迟问题。VMware 提供的 PCoIP 和 Blast Extreme 显示协议适应于不同的延迟和带宽条件。

共享存储示例

在 View 5.2 测试环境下，View Composer 副本虚拟机安置于具备高读取性能的固态磁盘 (SSD) 中，每秒支持数万个 I/O (IOPS)。链接克隆安置在基于传统低性能旋转介质的数据存储中，价格相对低廉，具有较高的存储容量。该示例使用 View Composer 链接克隆而不是即时克隆，因为测试是使用 View 5.2 执行的。即时克隆功能是在 Horizon 7 中引入的。

存储设计注意事项是 Horizon 7 体系结构中的最关键要素之一。是否使用 View Composer 桌面（使用链接克隆技术）将对体系结构产生极大的影响。ESXi 二进制文件、虚拟机交换文件和父虚拟机的 View Composer 副本都存储在共享存储系统上。

vSphere 可以使用的外部存储系统包括光纤通道或 iSCSI SAN（存储区域网络）、NFS（网络文件系统）或 NAS（网络连接存储）。通过使用 vSphere 5.5 Update 1 或更高版本中提供的 vSAN 功能，存储系统还可以是聚合的本地服务器连接存储。

以下示例介绍了在由一个 vCenter Server 管理 10,000 个桌面的 View 5.2 测试设置中所使用的分层存储策略。

注 该示例用于 View 5.2 设置，这是在发布 VMware vSAN 之前执行的。有关为 VMware vSAN 设计 View 虚拟桌面基础架构的关键组件以及进行大小调整的指南，请参阅 http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf 中的白皮书。

与 vSphere 5.5 Update 1 中提供的功能相比，vSphere 6.0 和更高版本中提供的 vSAN 功能包含很多性能改进。对于 vSphere 6.0，此功能还具有更广泛的 HCL（硬件兼容性）支持。有关 vSphere 6 或更高版本中的 vSAN 的详细信息，请参阅《管理 VMware vSAN》文档。

物理存储	■ 仅使用 EMC VNX7500-block ■ 1.8TB 快速缓存 (SSD)

- 8 个 10Gbit FCoE 前端连接（每个控制器各 4 个）。

SSD 存储层

单个 RAID5 存储池：

- 12 * 200GB EFD
- 用于父映像的 250GB LUN
- 用于基础架构的 500GB LUN
- 用于存储副本的 75GB LUN（每个桌面池群集各一个）

虚拟机桌面存储层

两个 RAID 1/0 存储池：

池 1：

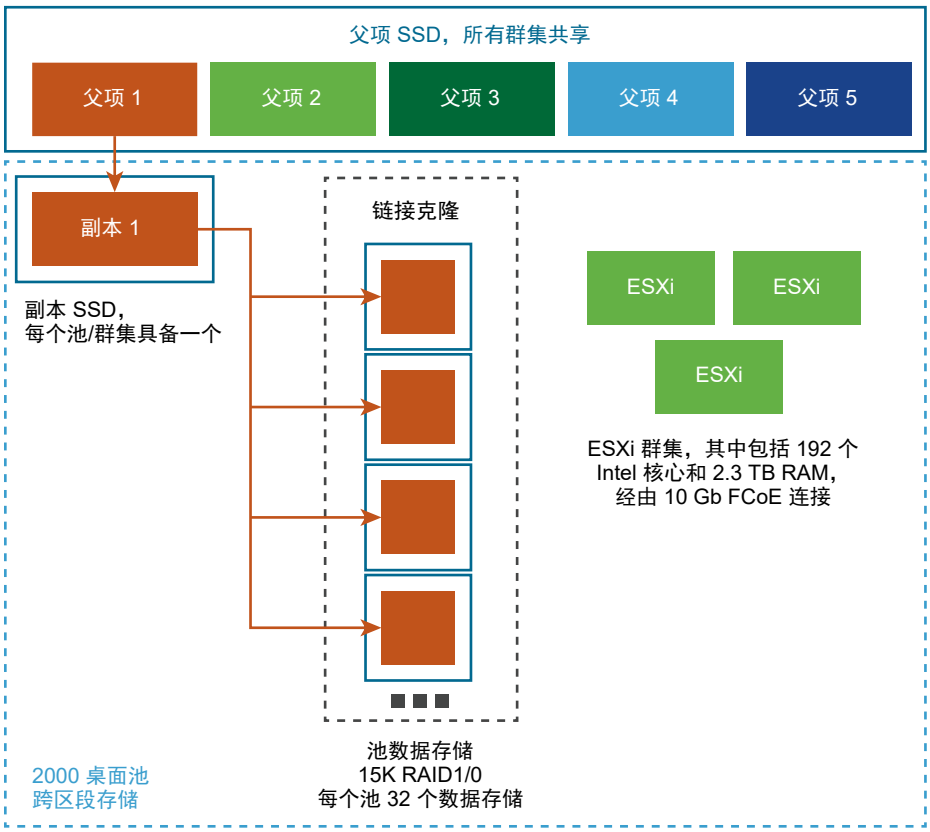
- 360 15K 300GB HDD（47TB 可用）
- 97 个用于桌面的 450GB LUN

池 2：

- 296 15K 300GB HDD（39TB 可用）
- 7 个用于基础架构的 450GB LUN
- 85 个用于桌面的 450GB LUN

该存储策略如下图所示。

图 4-1. 大型桌面池的分层存储示例



从体系结构角度看，View Composer 可以创建共享基础映像的桌面映像，将存储要求降低 50% 甚至更多。通过设置刷新策略使桌面定期返回原始状态，并回收自上一次刷新操作后用于跟踪更改的空间，可以进一步降低存储要求。

如果您使用带 vSphere 5.1 或更高版本虚拟机桌面的 View Composer，那么您可以使用空间回收功能。凭借该功能，当未使用磁盘空间达到一定阈值时，客户机操作系统中过期或已删除的数据将通过擦除和压缩流程自动回收。请注意，如果您使用 vSAN 数据存储，则不支持空间回收功能。

将 View Composer 永久磁盘或共享文件服务器作为用户配置文件和用户文档的主存储库，还可以降低操作系统磁盘空间。View Composer 能帮您将用户数据从操作系统中分开，您只需备份或复制永久磁盘即可，这也会进一步降低存储要求。有关更多信息，请参阅使用 Composer 降低存储要求。

注　您可以在试运行期间作出有关专用存储组件的最佳决策。要考虑的主要问题是每秒的 I/O 次数 (IOPS)。您可以试验分层存储策略或 vSAN 存储，以最大限度提高性能并节约成本。

有关更多信息，请参阅名为《VMware View 的存储注意事项》的最佳实践指南。

存储带宽问题

在 Horizon 7 环境中，登录风暴是确定带宽要求时的主要考虑因素。

尽管很多因素都对支持 Horizon 7 环境的存储系统的设计具有重要的作用，但从服务器配置的角度来看，规划合适的存储带宽才是最重要的问题。另外，您还必须考虑端口整合硬件产生的影响。

Horizon 7 环境中有时会出现 I/O 风暴负载，此时所有虚拟机都会同时执行活动。防病毒软件或软件更新代理等基于客户机的代理可触发 I/O 风暴；人为行为（如所有员工都在早上同一时段登录）也可以触发 I/O 风暴。VMware 已测试了 10,000 个桌面的登录风暴情况。有关更多信息，请参阅 View Composer 性能测试结果。

您可以通过最佳操作实践（如交错更新不同虚拟机）最大程度地减少这些风暴工作负载。另外，您也可以在试运行阶段测试各种注销策略，以确定用户注销时暂停或关闭虚拟机是否会导致 I/O 风暴。将 View Composer 副本存储在单独的高性能数据存储中，可加快大量并发读取操作的速度，从而应对 I/O 风暴负载问题。例如，可以使用以下存储策略之一：

- 手动配置池设置以便在单独的高性能数据存储上存储副本。
- 使用 vSphere 5.5 Update 1 或更高版本中提供的 vSAN，它使用基于软件策略的管理以确定用于副本的磁盘类型。
- 使用随 vSphere 6.0 或更高版本提供的虚拟卷，虚拟卷使用基于软件策略的管理来确定用于副本的磁盘类型。

除确定最佳实践外，VMware 还建议您为每 100 个虚拟机提供 1 Gbps 的带宽，即使平均带宽可能低于这个数值的 1/10。这样的保守规划可确保在峰值负载期间能够获得足够的存储连接。

网络带宽问题

需要使用某些虚拟和物理网络组件来支持典型的工作负载。

在显示流量方面，有很多影响网络带宽的因素，如所用协议、显示器分辨率和配置，以及工作负载中多媒体内容所占的比重。并发启动经过流式处理的应用程序也可能导致出现利用率峰值。

由于这些问题产生的影响有很大差异，因此很多企业都将监视带宽消耗作为试运行项目的一部分。在试运行开始时，为一般知识型员工规划 150 到 200 Kbps 的带宽容量。

使用 PCoIP 或 Blast Extreme 显示协议时，如果您的企业 LAN 带宽是 100 Mb 或 1 Gb 交换网络，那么在以下情况中，您的最终用户可以获得最佳性能：

- 两台显示器 (1920 x 1080)
- 大量使用 Microsoft Office 应用程序
- 大量浏览嵌入 Flash 的 Web 内容
- 经常进行多媒体应用，不常使用全屏模式
- 经常使用基于 USB 的外围设备
- 基于网络的打印

有关更多信息，请参阅名为《PCoIP 显示协议：基于信息和场景的网络大小调整指南》的信息指南。

PCoIP 和 Blast Extreme 中提供的优化控制

如果采用 VMware 的 PCoIP 或 Blast Extreme 显示协议，可以对诸多影响网络带宽使用的因素进行调整。

- 您可以配置网络拥挤时使用的图像质量级别和帧速率。质量级别设置允许您限制显示图像更改区域的初始质量。您还可以调整帧速率。

该项控制对无需进行更新的静态屏幕内容和仅有部分内容需要刷新的情况非常有效。

- 关于会话带宽，您可以配置最大带宽（单位为 kbps）以符合网络连接的类型，如 4 Mbit/s Internet 连接。此带宽包括所有图像、音频、虚拟通道、USB 以及 PCoIP 或 Blast 控制流量。

  您也可以配置为会话预留的带宽下限（单位为 kbps），这样用户无需等待带宽变得可用。您可以指定会话的 UDP 数据包的最大传输单元 (Maximum Transmission Unit, MTU) 大小，范围为 500 至 1500 字节。

有关更多信息，请参阅《在 Horizon 7 中配置远程桌面功能》中的“PCoIP 常规设置”和“VMware Blast 策略设置”部分。

网络配置示例

在每个 vCenter Server 5.1 实例管理 5 个池且每个池包含 2,000 台虚拟机的 View 5.2 测试容器中，每台 ESXi 主机都具备以下硬件和软件，以满足网络要求。

注　该示例用于 View 5.2 设置，这是在发布 VMware vSAN 之前执行的。有关为 VMware vSAN 设计 View 虚拟桌面基础架构的关键组件以及进行大小调整的指南，请参阅 http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf 中的白皮书。另外，该示例使用 View Composer 链接克隆而不是即时克隆，因为测试是使用 View 5.2 执行的。即时克隆功能是在 Horizon 7 中引入的。

供每台主机使用的物理组件	■ Brocade 1860 架构适配器，分别使用 10Gig 以太网和 FCoE 来传送网络和存储流量。 ■ 连接至包含 6 台 VDX6720-60 交换机的 Brocade VCS 以太网架构。交换机向上连接至网络的其他部分，具备两个可连接至 Juniper J6350 路由器的 1 GB 连接端。
vLAN 摘要	■ 每个桌面池（共 5 个）具备 1 个 10Gb vLAN ■ 管理网络具备 1 个 1Gb vLAN ■ vMotion 网络具备 1 个 1Gb vLAN ■ 基础架构网络具备 1 个 10Gb vLAN
虚拟 vMotion-dvswitch（每台主机具备 1 条上行链路）	该交换机供基础架构虚拟机、父虚拟机和桌面虚拟机的 ESXi 主机使用。 ■ 巨型帧 (9000 MTU) ■ 1 个短周期分布式端口组 ■ 专用 VLAN 和 192.168.x.x 地址
Infra-dvswitch（每台主机具备 2 条上行链路）	该交换机供基础架构虚拟机的 ESXi 主机使用。 ■ 巨型帧 (9000 MTU) ■ 1 个短周期分布式端口组

	■ 基础架构 VLAN（24 位网络号，256 个地址）
Desktop-dvswitch（每台主机具备 2 条上行链路）	该交换机供父虚拟机和桌面虚拟机的 ESXi 主机使用。 ■ 巨型帧 (9000 MTU) ■ 6 个短周期分布式端口组 ■ 5 个桌面端口组（每个池各具备 1 个） ■ 每个网络具备含有 2048 个地址的 vlan（21 位网络号）

View Composer 性能测试结果

这些测试结果描述了包含 10,000 个桌面的 View 5.2 设置，在此设置中，由一个 vCenter Server 5.1 实例来管理 5 个池，每个池具备 2,000 个虚拟机桌面。无论是置备一个新的池，还是重构、刷新或重新平衡现有的具备 2,000 台虚拟机的池，都只需要一个维护期。另外还针对 10,000 位用户进行了登录风暴测试。

此处提供的测试结果是通过下述主题所描述的软件、硬件和配置设置而得出的：

- Horizon 连接服务器最大连接数和虚拟机配置中所描述的桌面和池配置
- 共享存储示例中所描述的分层存储组件
- 网络带宽问题中所描述的网络组件

10,000 位用户长达一小时的登录风暴处理能力

注　该示例用于 View 5.2 设置，这是在发布 VMware vSAN 之前执行的。有关为 VMware vSAN 设计 View 虚拟桌面基础架构的关键组件以及进行大小调整的指南，请参阅 http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf 中的白皮书。有关在使用 vSAN 时各种工作负载和 View 操作的测试结果，请参阅参考架构白皮书，网址为 http://www.vmware.com/files/pdf/techpaper/vmware-horizon-view-virtual-san-reference-architecture.pdf。

与 vSphere 5.5 Update 1 中提供的功能相比，vSphere 6.0 和更高版本中提供的 vSAN 功能包含很多性能改进。对于 vSphere 6.0，此功能还具有更广泛的 HCL（硬件兼容性）支持。有关 vSphere 6 或更高版本中的 vSAN 的详细信息，请参阅《管理 VMware vSAN》文档。

在测试设置中，我们使用以下桌面和池设置，测试了 10,000 个桌面的登录风暴情况。桌面的电源策略被设置为始终开启。

对于在 60 分钟内发生的 10,000 个桌面的登录风暴，使用正态分布登录时间。在登录风暴开始前，所有的虚拟机都已开启并可用。登录后，工作负载启动，其中包括以下应用程序：Adobe Reader、Microsoft Outlook、Internet Explorer、Microsoft Word 和 Notepad。

以下为测试过程中所持续的登录风暴的其他详细信息：

- 95% 的登录发生在 +/- 2 标准偏差时间段（40 分钟）。
- 68% 的登录发生在 +/- 1 标准偏差时间段（20 分钟）。
- 登录率峰值为 400 次/分钟（或 6.67 次/秒）。

置备池所需要的时间

池是在您创建池时预先置备或者是在分配用户后按需置备。置备是指创建虚拟机并进行配置，以便使用正确的操作系统映像和网络设置。

在一个已包含 4 个池并且每个池管理 2,000 台虚拟机的测试设置中，继续置备第五个包含 2,000 台虚拟机的池需要花费 4 个小时。所有的虚拟机都是预先置备。

重构池所需要的时间

您可以通过重构操作来提供操作系统修补程序、安装或更新应用程序，或者修改池中虚拟机的桌面硬件设置。在重构池前，你为具备新配置的虚拟机拍摄快照。重构操作使用该快照来更新池中所有的虚拟机。

在一个包含 5 个池并且每个池管理 2,000 台虚拟机的测试设置中，重构一个包含 2,000 台虚拟机的池需要花费 6 小时 40 分钟。在重构操作开始前，所有的虚拟机都已开启并可用。

刷新池所需要的时间

因为磁盘容量会不断增长，因此您可以在用户注销时将桌面刷新到原始状态以节省磁盘空间，或者设置计划来定期刷新桌面。例如，安排桌面每天、每周或每月刷新一次。

在一个包含 5 个池并且每个池管理 2,000 台虚拟机的测试设置中，刷新一个包含 2,000 台虚拟机的池需要花费 2 小时 40 分钟。在刷新操作开始前，所有的虚拟机都已开启并可用。

重新平衡池所需要的时间

重新平衡桌面操作会在可用的逻辑驱动器之间重新平均分配链接克隆桌面。它可以节省过载驱动器上的存储空间，并确保充分利用所有驱动器。您还可以使用重新平衡操作将桌面池中的所有虚拟机迁移到 vSAN 数据存储中，或者从该数据存储中迁移虚拟机。

在一个包含 5 个池并且每个池管理 2,000 台虚拟机的测试容器中，进行一项测试时在容器中添加了 2 个数据存储。 进行另外一项测试时，将 2 个数据存储从容器中移除。当添加或移除数据存储后，对其中的一个池进行重新平衡操作。重新平衡一个包含 2,000 台虚拟机的池需要花费 9 个小时。在重新平衡操作开始前，所有的虚拟机都已开启并可用。

WAN 支持

对于广域网 (Wide-Area Network, WAN)，您必须考虑带宽限制和延迟问题。VMware 提供的 PCoIP 和 Blast Extreme 显示协议适应于不同的延迟和带宽条件。

如果您采用 RDP 显示协议，则必须使用 WAN 优化产品为分支机构或小型企业的用户加速应用程序。采用 PCoIP 和 Blast Extreme 时，许多 WAN 优化技术会内置到基础协议中。

- WAN 优化对基于 TCP 的协议（如 RDP 协议）非常重要，因为这些协议需要在客户端和服务器之间进行多次握手。这些握手可能会产生非常大的延迟。WAN 加速器可以“伪造”握手回复，从而在协议中隐藏网络延迟。由于 PCoIP 和 Blast Extreme 基于 UDP，不需要使用这种形式的 WAN 加速。
- WAN 加速器还能压缩客户端和服务器之间的网络流量，但压缩比率通常只能达到 2:1。PCoIP 和 Blast Extreme 具有高得多的压缩率。

有关可用于调整 PCoIP 和 Blast Extreme 使用带宽的方式的控制的信息，请参阅 PCoIP 和 Blast Extreme 中提供的优化控制。

各类用户的带宽要求

确定适用于 PCoIP 的最小带宽时，请参考以下估值：

- 针对基本办公生产桌面的平均带宽为 100 至 150 Kbps：不包含视频和 3D 图形的典型办公应用程序，使用默认的 Windows 和 Horizon 7 设置。
- 针对优化办公生产桌面的平均带宽为 50 至 100 Kbps：不包含视频和 3D 图形的典型办公应用程序，使用优化的 Windows 桌面设置和优化的 Horizon 7。
- 针对使用了多显示器、3D、Aero 和 Microsoft Office 的虚拟桌面的平均带宽为 400 至 600 Kbps。
- 为突发显示更改提供空间需要 500 Kbps 至 1 Mbps 的最低峰值带宽。一般情况下，可使用平均带宽调整网络带宽，但也要考虑峰值带宽，以适应与大型屏幕更改相关的突发成像流量。
- 每个运行 480p 视频的并发用户为 2 Mbps，具体取决于配置的帧速率限制和视频类型。

注　每个典型用户 50 至 150 Kbps 的平均估值基于以下假设：所有用户每天 8 至 10 小时连续操作并执行相似任务。50 Kbps 带宽使用量这一数值是针对已禁用无损构建功能的 LAN 进行 View Planner 测试得出的结果。该值可能会因情况不同而异，有些用户可能基本不活动，因此几乎不占用带宽，这样每条链路就可用于更多用户。因此，这些指导准则旨在为更详细的带宽规划和测试提供基准。

下例说明了如何计算使用 1.5 Mbps T1 线路的分支机构或远程办公室的并发用户数。

分支机构或远程办公室情景

- 用户拥有基本 Microsoft Office 生产应用程序，无视频，无 3D 图形，具有 USB 键盘和鼠标设备。
- 每个典型办公用户的 Horizon 7 所要求的带宽介于 50-150Kbps 之间。
- T1 网络容量为 1.5 Mbps。
- 带宽利用率为 80%（利用率系数为 0.8）。

确定所支持用户数量的方法：

- 在最坏的情况下，用户需要 150 Kbps：(1.5 Mbps * 0.8)/150 Kbps = (1500 * 0.8)/150 = 8 个用户
- 在最理想的情况下，用户需要 50Kbps：(1.5 Mbps * 0.8)/50 Kbps = (1500 * 0.8)/50 = 24 个用户

结果

每条拥有 1.5 Mbps 容量的 T1 线路可供 8 到 24 个并发用户使用。

重要事项　您可能需要优化 Horizon 7 和 Windows 桌面设置才能实现此用户密度。

Horizon 7 构建基块

构建基块由物理服务器、vSphere 基础架构、Horizon 7 服务器、共享存储和虚拟机桌面组成，供最终用户使用。构建基块是一种逻辑构造，不应针对 2,000 个以上的 Horizon 桌面调整大小。通常情况下，客户在 Horizon 7 容器中包含的构建基块数量不超过五个，尽管从理论上而言，只要此容器中的会话和 Horizon 连接服务器实例分别不超过 10,000 个和 7 个，就能使用更多的构建基块。

表 4-11. 用于 2,000 个虚拟机桌面的基于 LAN 的 Horizon 构建基块示例

项目	示例
vSphere 群集	1 或更多
80 端口网络交换机	1
共享存储系统	1
vCenter Server 与 View Composer 在同一主机上	1（可在基块内运行）
数据库	MS SQL Server 或 Oracle 数据库服务器（可在基块内运行）
VLAN	3（每个分别有 1Gbit 以太网网络：管理网络、存储网络和 VMotion 网络）

每个 vCenter Server 最多可支持 10,000 个虚拟机。这可使您拥有包含 2000 多个虚拟机桌面的构建基块。但基块的实际大小还取决于其他特定于 Horizon 7 的限制。

如果您的容器中只有一个构建基块，请使用两个连接服务器实例来实现冗余。

Horizon 7 容器

容器一个是由 Horizon 7 可扩展性限制决定的组织单元。

使用 5 个构建基块的容器示例

一个传统的 Horizon 7 容器可以将五个包含 2,000 个用户的构建基块进行集成，您可以将其作为一个实体来管理。

表 4-12. 由 5 个构建基块构成的基于 LAN 的 Horizon 7 容器示例

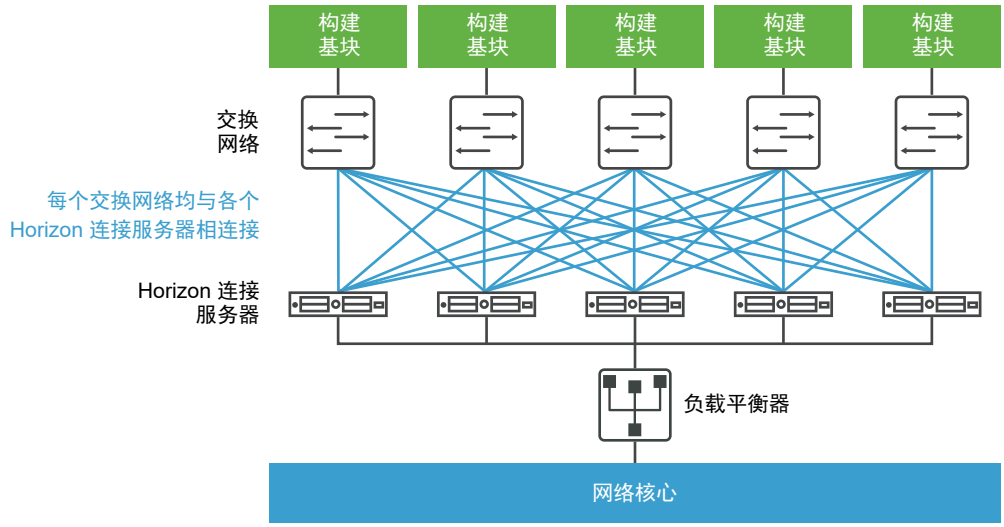
项目	数量/容量
一个 Horizon 7 容器的构建基块数量	5
vCenter Server 和 View Composer	5（每个构建基块具备 1 个虚拟机，用于托管 vCenter Server 和 View Composer）
数据库服务器	5 个（每个构建基块中具备 1 个独立数据库）MS SQL Server 或 Oracle 数据库服务器
连接服务器	7（5 个用于从企业网络内连接，2 个用于从企业网络外连接）
vLAN	请参阅表 4-11. 用于 2,000 个虚拟机桌面的基于 LAN 的 Horizon 构建基块示例。
10 Gb 以太网模块	1
模块化网络交换机	1

每个 vCenter Server 最多可支持 35,000 个注册虚拟机。这可使您拥有包含 2000 多个虚拟机桌面的构建基块。但基块的实际大小还取决于其他特定于 Horizon 7 的限制。

在此处所述的两个示例中，网络核心可跨连接服务器实例对入站请求进行负载平衡。支持冗余和故障切换机制（通常在网络级别）可避免负载平衡程序成为单点故障。例如，虚拟路由器冗余协议 (Virtual Router Redundancy Protocol, VRRP) 可与负载平衡程序进行通信，以添加冗余和故障切换功能。

如果连接服务器实例在活动会话期间出现故障或没有响应，用户不会丢失数据。桌面状态将被保存在虚拟机桌面内，以便用户能够连接其他连接服务器实例，并且其桌面会话可从出现故障时的位置重新开始。

图 4-2. 包含 10,000 个虚拟机桌面的容器图



使用一个 vCenter Server 的容器示例

在上一节中，Horizon 7 容器包含多个构建基块。每个构建模块通过单个 vCenter Server 来支持 2,000 台虚拟机。许多客户及合作伙伴请求 VMware 使用单个 vCenter Server 来管理 Horizon 7 容器。该项请求来源于单个 vCenter Server 能够支持 10,000 台虚拟机这一事实。客户能够使用单个 vCenter Server 来管理包含 10,000 个桌面的环境。本主题介绍了一种使用单个 vCenter Server 管理 10,000 个桌面的架构。

尽管使用一个 vCenter Server 和一个 View Composer 来管理 10,000 个桌面是可行的，但是这样做可能会导致发生单点故障的情况。单个 vCenter Server 的失败会导致整个桌面无法进行电源、置备和维护操作。因此，必须选择能够满足您对组件整体弹性的要求的置备体系结构。

在该例中，一个包含 10,000 个用户的容器由物理服务器、vSphere 基础架构、Horizon 7 服务器、共享存储和 5 个群集（每个群集各包含 2,000 个虚拟桌面）组成。

表 4-13. 包含一个 vCenter Server 的基于 LAN 的 Horizon 7 容器示例

项目	示例
vSphere 群集	6（5 个群集，每个群集各具备一个链接克隆池，及 1 个基础架构群集）
vCenter Server	1
View Composer	1（独立的）
数据库服务器	1 个（独立的）MS SQL Server 或 Oracle 数据库服务器
Active Directory 服务器	1 或 2 个
连接服务器实例	5

表 4-13. 包含一个 vCenter Server 的基于 LAN 的 Horizon 7 容器示例 （续）

项目	示例
安全服务器	5
vLAN	8（5 个用于桌面池群集，管理群集、vMotion 群集和基础架构群集各 1 个）

Cloud Pod 架构 概述

要在 WAN、MAN（城域网）或其他非 LAN 中使用连接服务器的一组副本实例，如果 Horizon 部署需要跨多个数据中心，则必须使用 Cloud Pod 架构功能。

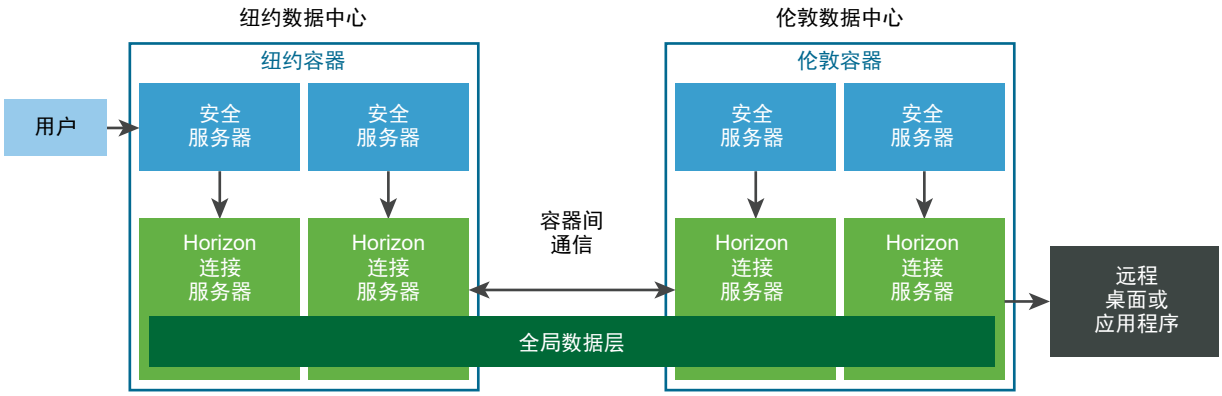
该功能使用标准 Horizon 组件提供跨数据中心管理、全局且灵活的用户到桌面映射、高可用性桌面以及灾难恢复功能。

典型的 Cloud Pod 架构拓扑包含两个或更多容器，这些容器在一个容器联合中链接在一起。容器联合具有特定限制。

表 4-14. 容器联合限制

对象	限制
总会话数	250,000
容器	50
每个容器的会话数	12,000
站点	15
每个容器的连接服务器实例数	7
连接服务器实例总数	350

下图是一个基本 Cloud Pod 架构 拓扑的示例。



在示例拓扑中，不同数据中心内以前独立的两个容器连接到一起，组成了单个容器联合。此环境中的最终用户可以连接到纽约数据中心的连接服务器实例，以及接收伦敦数据中心的桌面或应用程序。

在 IPv6 环境中不支持 Cloud Pod 架构 功能。

有关更多信息，请参阅《在 Horizon 7 中管理 Cloud Pod 架构》文档。

在一个容器中使用多个 vCenter Server 的优势

当您为能够容纳 500 多个桌面的 Horizon 7 生产环境创建设计时，必须考虑几点因素以确定是使用一个还是多个 vCenter Server 实例。

从 View 5.2 开始，VMware 支持在单个 Horizon 7 容器内，通过单个 vCenter Server 5.1 或更高版本管理最多 10,000 个桌面虚拟机。在您尝试通过单个 vCenter Server 实例管理 10,000 个虚拟机前，请考虑以下因素：

- 贵公司的维护时段
- Horizon 7 组件故障承受能力
- 电源、置备和维护操作频率
- 基础架构的简化

维护时段

虚拟机电源、置备和维护操作的并发设置根据 vCenter Server 实例进行确定。

使用一个 vCenter Server 实例的容器设计	并发设置确定整个 Horizon 7 容器可以同时容纳多少个排队等候的操作。 例如，如果您将并发置备操作设置为 20，并且容器中只有一个 vCenter Server 实例，那么当桌面池中超过 20 个操作时，将按顺序排列置备操作。同时将 20 个并发操作进行排队后，只有在完成一个操作后才可继续进行下一操作。进行大规模 Horizon 7 置备时，这种置备操作可能需要很长时间。
使用多个 vCenter Server 实例的容器设计	每个实例可同时置备 20 个虚拟机。

为了确保多个操作在一个维护时段内同时完成，您可以将多个 vCenter Server 实例（最多 5 个）添加至您的容器，并且在由单独的 vCenter Server 实例所管理的 vSphere 群集中部署多个桌面池。在同一时间，一个 vSphere 群集仅可由一个 vCenter Server 实例进行管理。如需跨 vCenter Server 实例实现并发，您必须相应地部署您的桌面池。

组件故障承受能力

Horizon 7 容器中的 vCenter Server 主要是用于提供电源、置备和维护（刷新、重构和重新平衡）操作。当虚拟机桌面已完成部署并且打开电源后，Horizon 7 不依靠 vCenter Server 进行正常操作。

因为每个 vSphere 群集必须由单个 vCenter Server 实例进行管理，该服务器代表了每个 Horizon 7 设计中的单点故障。该风险也适用于每个 View Composer 实例。（每个 View Composer 实例和 vCenter Server 实例之间存在一对一的映射关系。）使用以下任一产品可减轻 vCenter Server 或 View Composer 故障的影响：

- VMware vSphere High Availability (HA)
- 兼容的第三方故障切换产品

重要事项 为了使用这些故障切换策略之一，vCenter Server 实例不得安装在作为由 vCenter Server 实例管理的群集一部分的虚拟机中。

除了这些 vCenter Server 故障切换自动选项，您还可以选择在一台新的虚拟机或物理服务器上重建发生故障的服务器。最关键的信息存储在 vCenter Server 数据库中。

风险承受能力是确定在容器设计中使用一个还是多个 vCenter Server 实例的重要因素。如果您的操作要求您具备执行桌面管理任务的能力，例如所有桌面同时进行电源和维护操作，您应该通过部署多个 vCenter Server 实例，将故障影响缩减到更少的桌面。如果您能够忍受长期无法进行管理或置备操作的桌面环境，或者选择使用手动重建过程，则可以为您的容器置备单个 vCenter Server 实例。

电源、置备和维护操作频率

某些虚拟机桌面电源、置备和维护操作仅能由管理员完成，通常可预见且可控制，同时还能够限定在既定的维护时段内。其他的虚拟机桌面电源和维护操作由用户行为触发（例如使用“注销时刷新”或“注销时挂起”设置），或者由脚本操作触发（例如在用户无操作的时段内使用分布式电源管理 (DPM) 关闭空闲 ESXi 主机）。

如果您的 Horizon 7 设计并不需要由用户触发的电源和维护操作，那么单个 vCenter Server 实例也许就能满足您的需求。如果由用户触发的电源和维护操作频率较低，那么操作就无需排成长队，这样 Horizon 连接服务器就无需长时间等待 vCenter Server 在定义的并发设置限制内完成请求的操作。

很多客户选择部署浮动池并使用“注销时刷新”设置，以始终确保交付的桌面中不再存在以往会话中的过期数据。过期数据包括 `pagefile.sys` 或 Windows 临时文件中的不明存储页。浮动池还能通过频繁地将桌面重新设置为已知的清空状态，将恶意软件的影响降到最低。

有些客户通过配置 Horizon 7 关闭未使用桌面的电源，使 vSphere DRS (Distributed Resources Scheduler) 能够将正在运行的虚拟机合并到最小数量的 ESXi 主机上，从而降低用电量。然后 VMware Distributed Power Management 会关闭空闲主机。在这些情况下，多个 vCenter Server 实例能够更好地适应高频率的电源和维护操作，从而避免操作超时。

基础架构的简化

单个 vCenter Server 实例在用于大规模 Horizon 7 设计时可提供无与伦比的优势，例如在单个位置管理黄金主映像和父虚拟机，单个 vCenter Server 视图匹配 Horizon Administrator 控制台视图，更少的生产后端数据库和数据库服务器。单个 vCenter Server 比多个实例更容易实施灾难恢复计划。切记权衡多个 vCenter Server 实例的优点（例如维护时段及电源和维护操作频率）和缺点（例如额外的父虚拟机映像管理开销及所需基础架构组件数量的增加）。

您也许可通过混合物实现完美设计。您可以选择由一个 vCenter Server 实例管理的相对比较静态的超大型桌面池，及选择几个由多个 vCenter Server 实例管理的较小的更为动态的桌面池。升级现有的大型容器的最佳策略是首先升级您现有容器的 VMware 软件。在更改容器设计前，衡量下改善最新版本的电源、置备和维护操作将带来的影响，然后通过提高桌面池规模进行试验，以便找到更多大型桌面池与更少 vCenter Server 实例之间的平衡点。

安全功能规划

5

Horizon 7 为敏感的企业数据提供了强大的网络安全保障。如果要进一步提高安全性，您可以将 Horizon 7 与特定的第三方用户身份验证解决方案进行集成、使用安全服务器和实施受限制的授权功能。

重要事项 Horizon 6 版本 6.2 和更高版本可以使用 FIPS（联邦信息处理标准）140-2 兼容算法执行加密操作。您可以通过以 FIPS 模式安装 Horizon 7 来启用这些算法。在 FIPS 模式下，并非所有功能都受支持。有关更多信息，请参阅《Horizon 7 安装指南》文档。

本章讨论了以下主题：

了解客户端连接

Horizon Client 和 Horizon Administrator 通过安全 HTTPS 连接与 Horizon 连接服务器主机进行通信。有关连接服务器上的服务器证书的信息将在客户端与服务器之间进行 TLS 握手时传送至客户端。

在用户打开 Horizon Client 并为连接服务器、安全服务器或 Unified Access Gateway 主机提供完全限定域名时，将创建初始 Horizon Client 连接（用于用户身份验证以及选择远程桌面和应用程序）。Horizon Administrator 连接则在管理员在 Web 浏览器中键入 Horizon Administrator URL 时创建。

默认的 TLS 服务器证书是在连接服务器安装期间生成的。默认情况下，当 TLS 客户端访问 Horizon Administrator 等安全页面时，系统会为其提供该证书。

您可以使用默认证书进行测试，但应当尽快将其替换为您自己的证书。默认证书不是由商业证书颁发机构 (CA) 签发的。如果使用未经认证的证书，不受信任方将有可能伪装成您的服务器来截获流量。

- 使用 PCoIP 和 Blast 安全网关的客户端连接

  在客户端使用 VMware 的 PCoIP 或 Blast Extreme 显示协议连接到远程桌面或应用程序时，Horizon Client 可以建立到 Horizon 连接服务器实例、安全服务器或 Unified Access Gateway 设备上的适用安全网关组件的第二个连接。通过 Internet 访问远程桌面和应用程序时，此连接可提供所需的安全级别和连接性能。

- 采用 Microsoft RDP 的安全加密链路客户端连接

  当用户通过 Microsoft RDP 显示协议连接到远程桌面时，Horizon Client 会建立另一个到 Horizon 连接服务器主机的 HTTPS 连接。此连接提供了一条传送 RDP 数据的安全加密链路，因此称作安全加密链路连接。

- 直接客户端连接

  管理员可以配置 Horizon 连接服务器设置，以便绕过连接服务器主机，直接在客户端系统和已发布的应用程序或桌面虚拟机之间建立远程桌面和已发布的应用程序会话。这种连接类型称为直接客户端连接。

使用 PCoIP 和 Blast 安全网关的客户端连接

在客户端使用 VMware 的 PCoIP 或 Blast Extreme 显示协议连接到远程桌面或应用程序时，Horizon Client 可以建立到 Horizon 连接服务器实例、安全服务器或 Unified Access Gateway 设备上的适用安全网关组件的第二个连接。通过 Internet 访问远程桌面和应用程序时，此连接可提供所需的安全级别和连接性能。

安全服务器和 Unified Access Gateway 设备包含 PCoIP 安全网关组件和 Blast 安全网关组件，可提供以下优势：

- 唯一能够访问企业数据中心的远程桌面和应用程序流量是通过严格验证的用户产生的流量。
- 用户只能访问被授权访问的资源。
- PCoIP 安全网关连接支持 PCoIP，Blast 安全网关连接支持 Blast Extreme。两者都是高级远程显示协议，它们在 UDP 而不是 TCP 中封装视频显示数据包以更有效地使用网络。
- 默认情况下，将使用 AES-128 加密保护 PCoIP 和 Blast Extreme。但是您可以将加密密码更改为 AES-256。
- 只要显示协议不被任何网络组件阻止，就不再需要 VPN 连接。例如，试图从宾馆房间访问其远程桌面或应用程序的人员会发现，宾馆所用的代理未被配置为传递 UDP 数据包。

  有关更多信息，请参阅基于 DMZ 的安全服务器的防火墙规则。

安全服务器在 Windows Server 2008 R2 和 Windows Server 2012 R2 操作系统上运行，并可充分利用 64 位体系结构。此安全服务器还可以利用支持 AES 新指令 (AES New Instructions, AESNI) 的 Intel 处理器的功能，从而高度优化加密和解密性能。

有关 Unified Access Gateway 虚拟设备的更多信息，请参阅《部署和配置 Unified Access Gateway》。

采用 Microsoft RDP 的安全加密链路客户端连接

当用户通过 Microsoft RDP 显示协议连接到远程桌面时，Horizon Client 会建立另一个到 Horizon 连接服务器主机的 HTTPS 连接。此连接提供了一条传送 RDP 数据的安全加密链路，因此称作安全加密链路连接。

安全加密链路连接具有以下优势：

- RDP 数据可通过 HTTPS 在安全加密链路中传输，并且使用 SSL 进行加密。这种强大的安全协议与其他安全网站提供的安全性功能（如网上银行和信用卡支付所使用的安全性功能）相同。
- 一个客户端可以通过单个 HTTPS 连接访问多个桌面，降低了整体协议开销。
- 由于 Horizon 7 可管理 HTTPS 连接，因此显著提高了底层协议的可靠性。如果用户临时失去网络连接，HTTP 连接将在网络连接恢复后重新建立，RDP 连接也会自动恢复，用户不必再重新连接并登录。

在连接服务器实例的标准部署中，HTTPS 安全连接的终点为连接服务器。在 DMZ 部署中，HTTPS 安全连接的终点为安全服务器或 Unified Access Gateway 设备。请参阅准备使用安全服务器获取有关 DMZ 部署和安全服务器的信息。

使用 PCoIP 或 Blast Extreme 显示协议的客户端可以使用安全加密链路连接实现 USB 重定向和多媒体重定向 (MMR) 加速，但对于所有其他数据，PCoIP 使用 PCoIP 安全网关，Blast Extreme 使用安全服务器或 Unified Access Gateway 设备上的 Blast 安全网关。有关更多信息，请参阅 使用 PCoIP 和 Blast 安全网关的客户端连接 。

有关 Unified Access Gateway 虚拟设备的更多信息，请参阅《部署和配置 Unified Access Gateway》。

直接客户端连接

管理员可以配置 Horizon 连接服务器设置，以便绕过连接服务器主机，直接在客户端系统和已发布的应用程序或桌面虚拟机之间建立远程桌面和已发布的应用程序会话。这种连接类型称为直接客户端连接。

采用直接客户端连接时，客户端和连接服务器主机之间仍然会建立 HTTPS 连接，以供用户进行身份验证和选择远程桌面及已发布的应用程序，但不会使用第二条 HTTPS 连接（安全加密链路连接）。

直接 PCoIP 和 Blast Extreme 连接具有以下内置安全功能：

- 支持高级加密标准 (Advanced Encryption Standard, AES) 加密（默认启用）和 IP 安全 (IP Security, IPsec)
- 支持第三方 VPN 客户端

对于采用 Microsoft RDP 显示协议的客户端，到远程桌面的直接客户端连接仅适用于企业网络内部的部署环境。采用直接客户端连接时，RDP 流量通过客户端和远程桌面虚拟机之间的连接发送时未加密。

选择用户身份验证方法

Horizon 7 可利用您现有的 Active Directory 基础架构对用户进行身份验证和管理。如想提高安全性，可将 Horizon 7 与双因素身份验证解决方案（如 RSA SecurID 和 RADIUS）和智能卡身份验证解决方案集成。

- Active Directory 身份验证

  每个 Horizon 连接服务器实例都加入到 Active Directory 域，用户可以通过所加入域的 Active Directory 进行身份验证。用户还可以通过与之存在信任协议的其他用户域来进行身份验证。

- 使用双因素身份验证

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

- 智能卡身份验证

  智能卡是一种嵌入计算机芯片的小型塑料卡。很多政府机构和大型企业都利用智能卡来验证其计算机网络来访用户的身份。美国国防部使用的智能卡类型称为通用访问卡 (CAC)。

- 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。

Active Directory 身份验证

每个 Horizon 连接服务器实例都加入到 Active Directory 域，用户可以通过所加入域的 Active Directory 进行身份验证。用户还可以通过与之存在信任协议的其他用户域来进行身份验证。

例如，如果连接服务器实例是域 A 的成员，域 A 和域 B 之间存在信任协议，则域 A 和域 B 的用户均可通过 Horizon Client 连接到此连接服务器实例。

同样，如果某个混合域环境内的域 A 和 MIT Kerberos 领域之间存在信任协议，则 Kerberos 领域中的用户可以在通过 Horizon Client 连接到此连接服务器实例时选择 Kerberos 领域名称。

您可以将用户和组放在以下 Active Directory 域中：

- 连接服务器域
- 与连接服务器域之间具有双向信任关系的其他域
- 与连接服务器域位于不同的林中且与连接服务器域之间存在单向外部或领域信任关系的域
- 与连接服务器域位于不同的林中且与连接服务器域之间存在单向或双向可传递林信任关系的域

连接服务器会从主机所在的域开始遍历信任关系，以确定可以访问哪些域。对于一小组连接良好的域，连接服务器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接性的逐渐降低，确定完整域列表所需的时间也会随之增加。另外，该列表还可能包含您不希望在用户登录其远程桌面和应用程序时为其提供的域。

管理员可以使用 `vdmadmin` 命令行界面来配置域的筛选，从而限制连接服务器实例搜索并向用户显示的域。有关更多信息，请参阅《Horizon 7 管理指南》文档。

限时登录和设置密码有效期这样的策略也是通过现有 Active Directory 操作过程来处理的。

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。

智能卡身份验证

智能卡是一种嵌入计算机芯片的小型塑料卡。很多政府机构和大型企业都利用智能卡来验证其计算机网络来访用户的身份。美国国防部使用的智能卡类型称为通用访问卡 (CAC)。

管理员可以为单个连接服务器实例启用智能卡身份验证。为连接服务器实例启用智能卡身份验证的过程通常包含以下操作：将根证书添加到信任存储区文件，然后修改连接服务器设置。

所有的客户端连接，包括使用智能卡身份验证的客户端连接都可启用 TLS/SSL。

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。有关特定类型的 Horizon Client 是否支持智能卡的信息，请参阅 Horizon Client 文档，网址为 https://docs.vmware.com/cn/VMware-Horizon-Client/index.html。

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。

限制远程桌面访问

您可以使用受限制的授权功能，根据用户连接的 Horizon 连接服务器实例限制远程桌面访问。

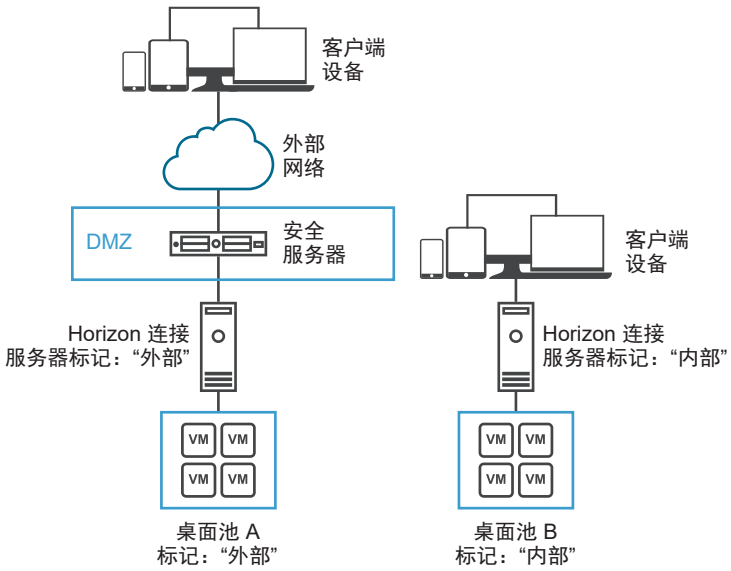
使用受限制的授权功能，您可以为一个连接服务器实例分配一个或多个标记。之后，在配置桌面池时，您可以选择希望能够访问该桌面池的连接服务器实例的标记。当用户通过带标记的连接服务器实例登录时，他们只能访问那些至少有一个匹配标记或没有标记的桌面池。

例如，您的 Horizon 7 部署中可能包含两个连接服务器实例。其中一个实例用于支持内部用户。另一个实例则与安全服务器配对，用于支持您的外部用户。为防止外部用户访问特定桌面，您可以采用以下操作设置受限制的授权：

- 将“内部”标记分配给支持内部用户的连接服务器实例。
- 将“外部”标记分配给与安全服务器配对并支持外部用户的连接服务器实例。
- 将“内部”标记分配给仅供内部用户访问的桌面池。
- 将“外部”标记分配给仅供外部用户访问的桌面池。

外部用户无法看到带“内部”标记的桌面池，因为他们是通过带“外部”标记的连接服务器登录的；而内部用户无法看到带“外部”标记的桌面池，因为他们是通过带“内部”标记的连接服务器登录的。图 5-1. 受限制的授权示例 显示了此配置。

图 5-1. 受限制的授权示例



您也可以使用受限制的授权功能，根据您为特定连接服务器实例配置的用户身份验证方法控制桌面访问。例如，您可以仅允许经过智能卡身份验证的用户使用特定的桌面池。

受限制的授权功能只能强制执行标记匹配。您必须设计网络拓扑结构以强制特定的客户端通过特定的连接服务器实例进行连接。

使用组策略设置保护远程桌面和应用程序

Horizon 7 中包含组策略管理 ADMX 模板，您可以使用这些模板中所含的安全相关组策略设置来保护您的远程桌面和应用程序。

例如，您可以使用组策略设置执行以下任务：

- 指定可接受在用户在适用于 Windows 的 Horizon Client 中选中**以当前用户身份登录**复选框时传送的用户身份和凭据信息的连接服务器实例。
- 为 Horizon Client 中的智能卡身份验证启用单点登录功能。
- 配置 Horizon Client 中的服务器 TLS 证书检查。
- 防止用户通过 Horizon Client 命令行选项提供凭据信息。
- 防止非 Horizon Client 系统使用 RDP 连接到远程桌面。您可以设置此策略，使连接必须由 Horizon Client 管理，这意味着用户必须使用 Horizon 7 连接远程桌面。

有关使用远程桌面和 Horizon Client 组策略设置的信息，请参阅《在 Horizon 7 中配置远程桌面功能》文档。

使用 智能策略

您可以使用智能策略来配置已发布桌面或应用程序中的用户环境设置，以及在计算机引导或会话重新连接期间应用的计算机环境设置。

您可以为用户环境设置创建相应的策略，来控制已发布桌面或应用程序中 USB 重定向、虚拟打印、剪贴板重定向、客户端驱动器重定向行为、Web 和 Chrome 文件传输功能以及带宽配置文件的行为。用于用户环境设置的 Horizon 智能策略在登录期间应用，并且可以在重新连接会话期间刷新。要在用户重新连接到会话时重新应用 Horizon 智能策略，可以配置一个触发任务。

您可以为在最终用户计算机引导时 Dynamic Environment Manager 应用的计算机环境设置创建一些策略。这些 Horizon 智能策略控制 Flash 多媒体重定向、集成打印和 USB 重定向行为。用于计算机环境设置的 Horizon 智能策略在计算机引导期间应用，并且可以在重新连接会话期间刷新。

使用智能策略，可以创建仅在满足特定条件时才会生效的策略。例如，可以配置这样一个策略：当用户从企业网络外部连接到远程桌面时，禁用客户端驱动器重定向功能。

智能策略 功能需要使用 Dynamic Environment Manager。有关更多信息，请参阅《在 Horizon 7 中配置远程桌面功能》中有关智能策略的主题。

实施用于保护客户端系统的最佳做法

请实施这些最佳做法来保护客户端系统。

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

有关 Horizon 7 所提供的所有安全功能的简明参考，请参阅《Horizon 7 安全性》文档。

分配管理员角色

Horizon 7 环境中的一项关键管理任务是确定哪些用户能够使用 Horizon Administrator，以及这些用户有执行哪些任务的权限。

在 Horizon Administrator 中执行任务的授权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。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或更改配置设置的权限。特权还控制管理员可在 Horizon Administrator 中查看的内容。

管理员可以创建文件夹来细分桌面池，然后将特定桌面池的管理权委派给 Horizon Administrator 中不同的管理员。管理员需要针对文件夹为用户分配角色，才能配置对该文件夹中资源的管理员访问权限。管理员只能访问其已经分配角色的文件夹中的资源。管理员在文件夹上的角色决定了其对该文件夹中资源所具有的访问权限级别。

Horizon Administrator 中包含一组预定义角色。管理员还可以组合所选特权来创建自定义角色。

准备使用安全服务器

安全服务器是一个运行部分连接服务器功能的特殊 Horizon 连接服务器实例。您可以使用安全服务器在 Internet 和内部网络之间提供额外的安全保护层。

重要事项 对于 Horizon 6 版本 6.2 和更高版本，您可以使用 Unified Access Gateway 设备替代安全服务器。Unified Access Gateway 设备将部署为强化的虚拟设备，它们基于已自定义以提供安全访问的 Linux 设备，有关 Unified Access Gateway 虚拟设备的更多信息，请参阅《部署和配置 Unified Access Gateway》。

安全服务器位于 DMZ 内，充当受信任网络中的连接代理主机。每个安全服务器均与一个连接服务器实例配对，并将所有流量转发给该实例。您可以将多个安全服务器与单个连接服务器进行配对。这种设计能保护连接服务器实例免受公共 Internet 的威胁，并强制所有无保护的会话请求经过安全服务器传输，从而提供额外的安全保护层。

基于 DMZ 的安全服务器部署要求打开防火墙上的一些端口，以允许客户端与 DMZ 内的安全服务器进行连接。您还必须配置端口，以供安全服务器与内部网络中的连接服务器实例通信使用。有关特定端口的信息，请参阅基于 DMZ 的安全服务器的防火墙规则。

由于用户可以直接连接到内部网络中的任何连接服务器实例，因此您不必在基于 LAN 的部署中实施安全服务器。

注 安全服务器包含一个 PCoIP 安全网关组件和一个 Blast 安全网关组件，这样使用 PCoIP 或 Blast Extreme 显示协议的客户端便可以使用安全服务器而不是 VPN。

有关设置 VPN 以使用 PCoIP 的信息，请参阅 VPN 解决方案概述，可在技术资源中心的技术合作伙伴资源部分找到这些概述，网址为 http://www.vmware.com/products/view/resources.html。

部署安全服务器的最佳实践

在 DMZ 中运行安全服务器时，应遵循以下有关安全策略和步骤的最佳实践。

《DMZ Virtualization with VMware Infrastructure》（在 VMware 基础架构中实施 DMZ 虚拟化）白皮书中介绍了虚拟化 DMZ 方面的最佳实践示例。此白皮书中的许多建议都可应用于物理 DMZ。

要限制帧的广播范围，应在隔离的网络中部署与安全服务器配对的 Horizon 连接服务器实例。该拓扑结构有助于防止内部网络中的恶意用户监视安全服务器与连接服务器实例之间的通信。

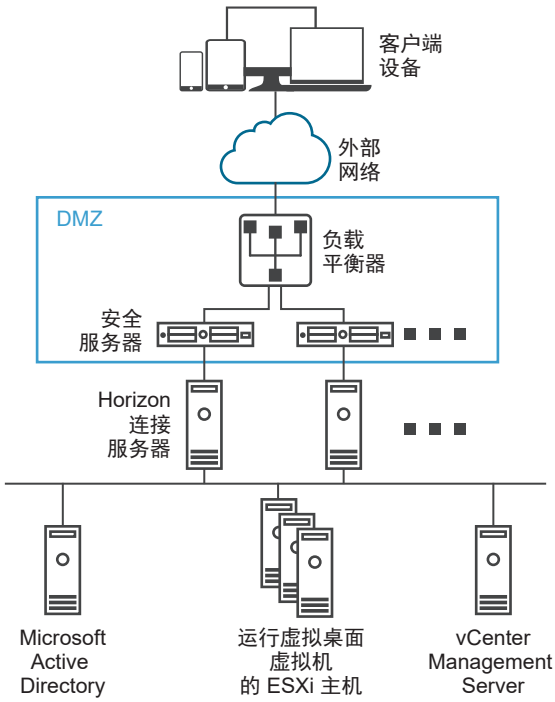
或者，您也可以使用网络交换机的高级安全功能，避免安全服务器和连接服务器的通信受到恶意监视，并抵御 ARP 缓存中毒 (ARP Cache Poisoning) 等监视攻击。有关更多信息，请参见网络设备的管理文档。

安全服务器拓扑结构

您可以实施几种不同的安全服务器拓扑结构。

图 5-2. DMZ 中的负载平衡安全服务器 中展示的拓扑结构显示了一个在 DMZ 中包含两个负载平衡安全服务器的高可用性环境。安全服务器与内部网络中的两个 Horizon 连接服务器实例通信。

图 5-2. DMZ 中的负载平衡安全服务器

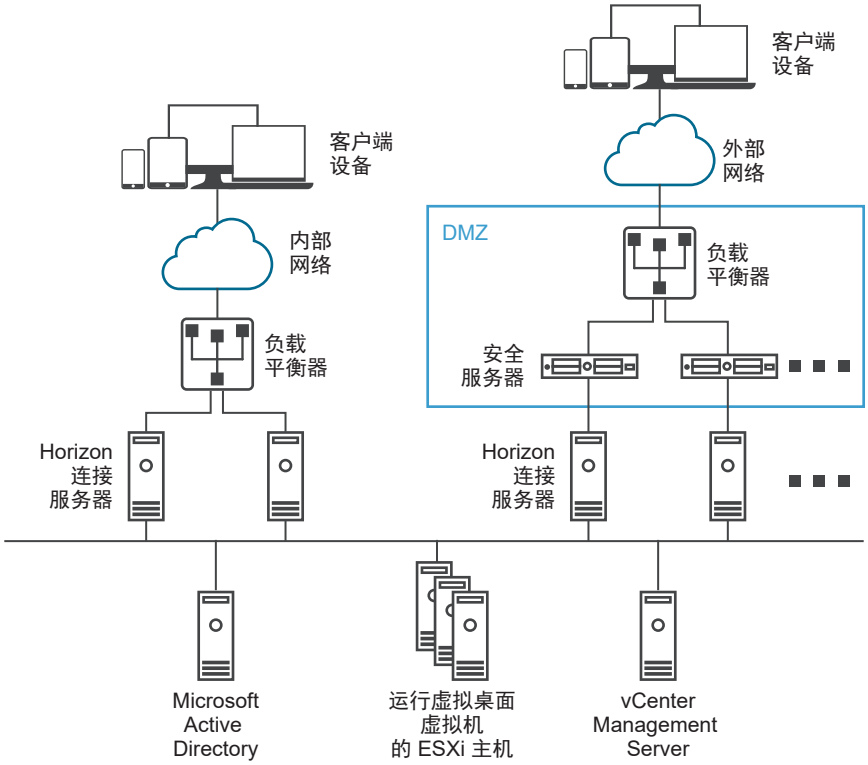


当企业外部的用户连接安全服务器时，他们必须成功通过身份验证，才可以访问远程桌面和应用程序。在这种拓扑结构中，DMZ 两端都实施了合适的防火墙规则，这种结构适用于通过 Internet 上的客户端设备来访问远程桌面和应用程序。

您可以为每个连接服务器实例连接多个安全服务器。您也可以将 DMZ 部署与标准部署结合使用，以便支持内部用户和外部用户访问。

图 5-3. 多个安全服务器 中展示的拓扑结构显示了将四个连接服务器实例作为一个组的环境。内部网络中的实例专供内部网络用户使用，外部网络中的实例则专供外部网络用户使用。如果与安全服务器配对的连接服务器实例启用了 RSA SecurID 身份验证，所有外部网络用户都需要使用 RSA SecurID 令牌进行身份验证。

图 5-3. 多个安全服务器



如果您安装了多个安全服务器，则必须实施硬件或软件负载平衡解决方案。连接服务器本身不提供负载平衡功能。连接服务器可与标准的第三方负载平衡解决方案配合使用。

基于 DMZ 的安全服务器的防火墙

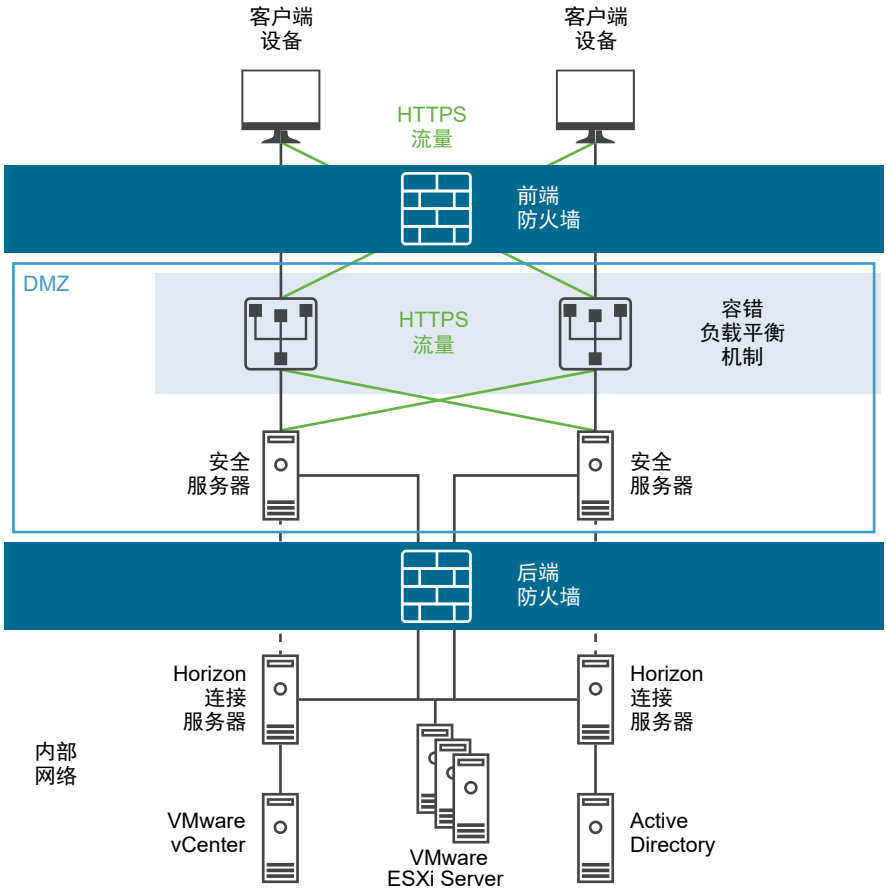
基于 DMZ 的安全服务器部署中必须包含两个防火墙。

- 需要部署一个面向外部网络的前端防火墙，用于保护 DMZ 和内部网络。您需要将该防火墙配置为允许外部网络流量到达 DMZ。
- 需要在 DMZ 和内部网络之间部署一个后端防火墙，用于提供第二层安全保障。您需要将该防火墙配置为仅接受 DMZ 内的服务产生的流量。

防火墙策略可严格控制来自 DMZ 服务的入站通信，这样将大幅降低内部网络泄露的风险。有关配置安全服务器所需的端口的更多信息，请参阅《Horizon 7 安全指南》文档。

下图显示了包含前端和后端防火墙的配置示例。

图 5-4. 双层防火墙拓扑



基于 DMZ 的安全服务器的防火墙规则

您需要为基于 DMZ 的安全服务器配置特定的前端防火墙规则和后端防火墙规则。安装过程中，Horizon 7 服务的默认设置是在特定网络端口进行侦听。必要时，您可以更改使用哪些端口号，以遵循组织策略或避免争用问题。

重要事项 有关其他详细信息及安全性建议，请参见《Horizon 7 安全指南》文档。

前端防火墙规则

要允许外部客户端设备连接到 DMZ 中的安全服务器，前端防火墙必须允许特定 TCP 和 UDP 端口上的流量。表 5-1. 前端防火墙规则中总结了相关的前端防火墙规则。

表 5-1. 前端防火墙规则

源	默认端口	协议	目标	默认端口	说明
Horizon Client	TCP（任意端口）	HTTP	安全服务器	TCP 80	（可选）外部客户端设备通过 TCP 端口 80 连接至 DMZ 中的安全服务器，并且自动定向到 HTTPS。有关让用户连接 HTTP 而非 HTTPS 的安全注意事项相关信息，请参阅《Horizon 7 安全指南》。
Horizon Client	TCP（任意端口）	HTTPS	安全服务器	TCP 443	外部客户端设备通过 TCP 端口 443 连接至 DMZ 中的安全服务器，实现与连接服务器实例和远程桌面及应用程序的通信。

表 5-1. 前端防火墙规则 （续）

源	默认端口	协议	目标	默认端口	说明
Horizon Client	TCP（任意端口） UDP（任意端口）	PCoIP	安全服务器	TCP 4172 UDP 4172	外部客户端设备通过 TCP 端口 4172 和 UDP 端口 4172 连接至 DMZ 中的安全服务器，通过 PCoIP 与远程桌面或应用程序进行通信。
安全服务器	UDP 4172	PCoIP	Horizon Client	UDP（任意端口）	安全服务器通过 UDP 端口 4172 将 PCoIP 数据发送回外部客户端设备。目标 UDP 端口是已接收 UDP 数据包中的源端口。由于这些数据包包含回复数据，通常不需要为此流量添加明确的防火墙规则。
Horizon Client 或 Client Web 浏览器	TCP（任意端口）	HTTPS	安全服务器	TCP 8443 UDP 8443	外部客户端设备和外部 Web 客户端 (HTML Access) 通过 HTTPS 端口 8443 连接到 DMZ 中的安全服务器，以便与远程桌面进行通信。

后端防火墙规则

要允许安全服务器与内部网络中的每个 View 连接服务器实例通信，后端防火墙必须允许特定 TCP 端口上的入站流量。在后端防火墙后面，必须以类似的方式配置内部防火墙，以允许远程桌面应用程序和连接服务器实例相互通信。表 5-2. 后端防火墙规则 中总结了相关的后端防火墙规则。

表 5-2. 后端防火墙规则

源	默认端口	协议	目标	默认端口	说明
安全服务器	UDP 500	IPSec	连接服务器	UDP 500	安全服务器通过 UDP 端口 500 与连接服务器实例协商 IPSec。
连接服务器	UDP 500	IPSec	安全服务器	UDP 500	连接服务器实例通过 UDP 端口 500 响应安全服务器。
安全服务器	UDP 4500	NAT-T ISAKMP	连接服务器	UDP 4500	如果安全服务器与配对的连接服务器实例之间使用 NAT，则需要使用防火墙。安全服务器使用 UDP 端口 4500 遍历 NAT 和协商 IPsec 安全。
连接服务器	UDP 4500	NAT-T ISAKMP	安全服务器	UDP 4500	如果使用 NAT，连接服务器实例通过 UDP 端口 4500 响应安全服务器。
安全服务器	TCP（任意端口）	AJP13	连接服务器	TCP 8009	安全服务器通过 TCP 端口 8009 连接至连接服务器实例以转发来自外部客户端设备的 Web 流量。 如果启用 IPSec，则配对之后 AJP13 流量不会使用 TCP 端口 8009。相反，它将流经 NAT-T（UDP 端口 4500）或 ESP。
安全服务器	TCP（任意端口）	JMS	连接服务器	TCP 4001	安全服务器通过 TCP 端口 4001 连接至连接服务器实例以交换 Java 消息服务 (Java Message Service, JMS) 流量。
安全服务器	TCP（任意端口）	JMS	连接服务器	TCP 4002	安全服务器通过 TCP 端口 4002 连接至连接服务器实例以交换安全 Java 消息服务 (JMS) 流量。
安全服务器	TCP（任意端口）	RDP	远程桌面	TCP 3389	安全服务器通过 TCP 端口 3389 连接至远程桌面以交换 RDP 流量。

表 5-2. 后端防火墙规则 （续）

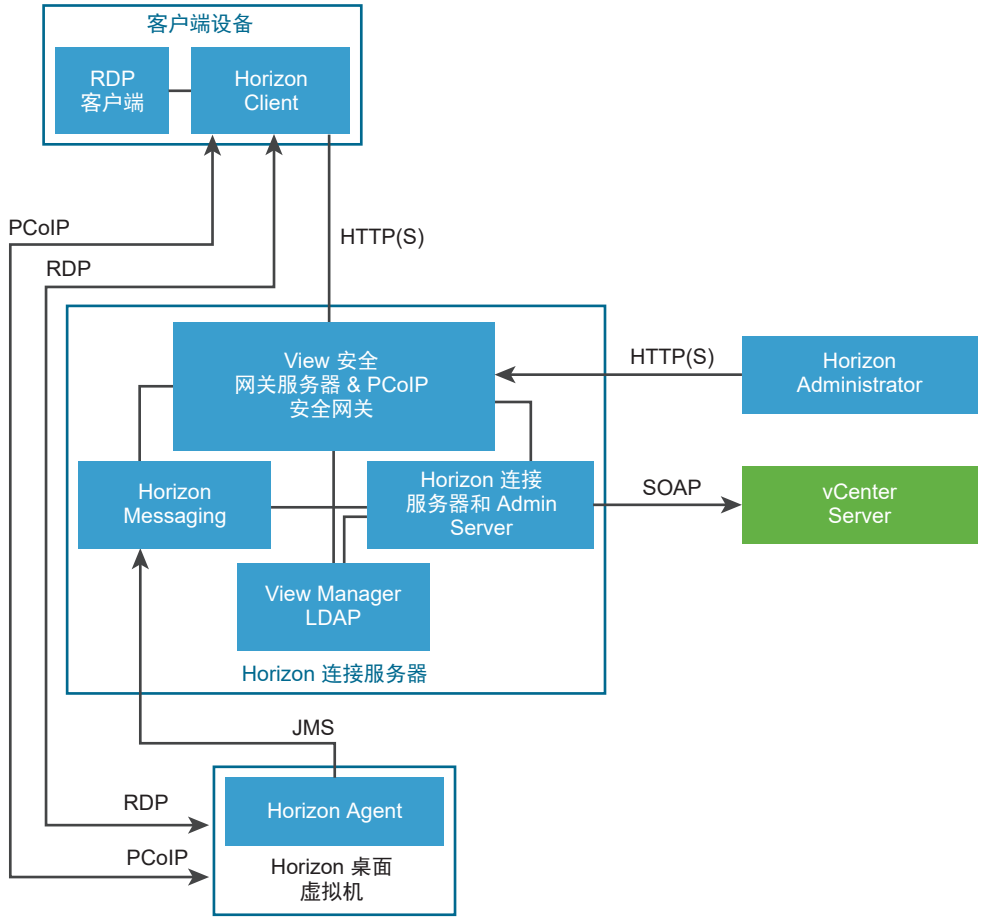
源	默认端口	协议	目标	默认端口	说明
安全服务器	TCP（任意端口）	MMR	远程桌面	TCP 9427	安全服务器使用 TCP 端口 9427 连接到远程桌面以接收与多媒体重定向 (Multimedia Redirection, MMR) 和客户端驱动器重定向有关的流量。
安全服务器	TCP（任意端口） UDP 55000	PCoIP	远程桌面或应用程序	TCP 4172 UDP 4172	安全服务器通过 TCP 端口 4172 和 UDP 端口 4172 连接至远程桌面和应用程序以交换 PCoIP 流量。
远程桌面或应用程序	UDP 4172	PCoIP	安全服务器	UDP 55000	远程桌面和应用程序通过 UDP 端口 4172 将 PCoIP 数据发送回安全服务器。 UDP 目标端口将作为已接收 UDP 数据包的源端口，由于是回复数据，通常不需要为此添加明确的防火墙规则。
安全服务器	TCP（任意端口）	USB-R	远程桌面	TCP 32111	安全服务器通过 TCP 端口 32111 连接至远程桌面，在外部客户端设备和远程桌面之间交换 USB 重定向流量。
安全服务器	TCP 或 UDP（任意端口）	Blast Extreme	远程桌面或应用程序	TCP 或 UDP 22443	安全服务器通过 TCP 和 UDP 端口 22443 连接到远程桌面和应用程序以交换 Blast Extreme 流量。
安全服务器	TCP（任意端口）	HTTPS	远程桌面	TCP 22443	如果您使用 HTML Access，安全服务器会通过 HTTPS 端口 22443 连接至远程桌面，以便与 Blast Extreme 通信。
安全服务器		ESP	连接服务器		不需要 NAT 遍历时封装 AJP13 流量。ESP 是 IP 协议 50。端口号未指定。
连接服务器		ESP	安全服务器		不需要 NAT 遍历时封装 AJP13 流量。ESP 是 IP 协议 50。端口号未指定。

了解通信协议

Horizon 6 和 Horizon 7 组件使用多种不同的协议来交换消息。

图 5-5. 没有配置安全服务器时的 Horizon 6 和 Horizon 7 组件及协议 展示了在没有配置安全服务器时每个组件所使用的通信协议。也就是说，在没有为 RDP、Blast 安全网关和 PCoIP 安全网关启用安全加密链路的情况下。此配置可在典型的 LAN 部署中使用。

图 5-5. 没有配置安全服务器时的 Horizon 6 和 Horizon 7 组件及协议



注　此图展示了使用 PCoIP 或 RDP 协议的客户端的直接连接。然而，默认设置是为 PCoIP 协议采用直接连接，为 RDP 协议采用安全加密链路连接。

请参阅表 5-3. 默认端口 了解每个协议所用的默认端口。

图 5-6. 配置了安全服务器时的 Horizon 6 和 Horizon 7 组件及协议 展示了在配置了安全服务器时，每个组件通信时所采用的协议。此配置可在典型的 WAN 部署中使用。

图 5-6. 配置了安全服务器时的 Horizon 6 和 Horizon 7 组件及协议

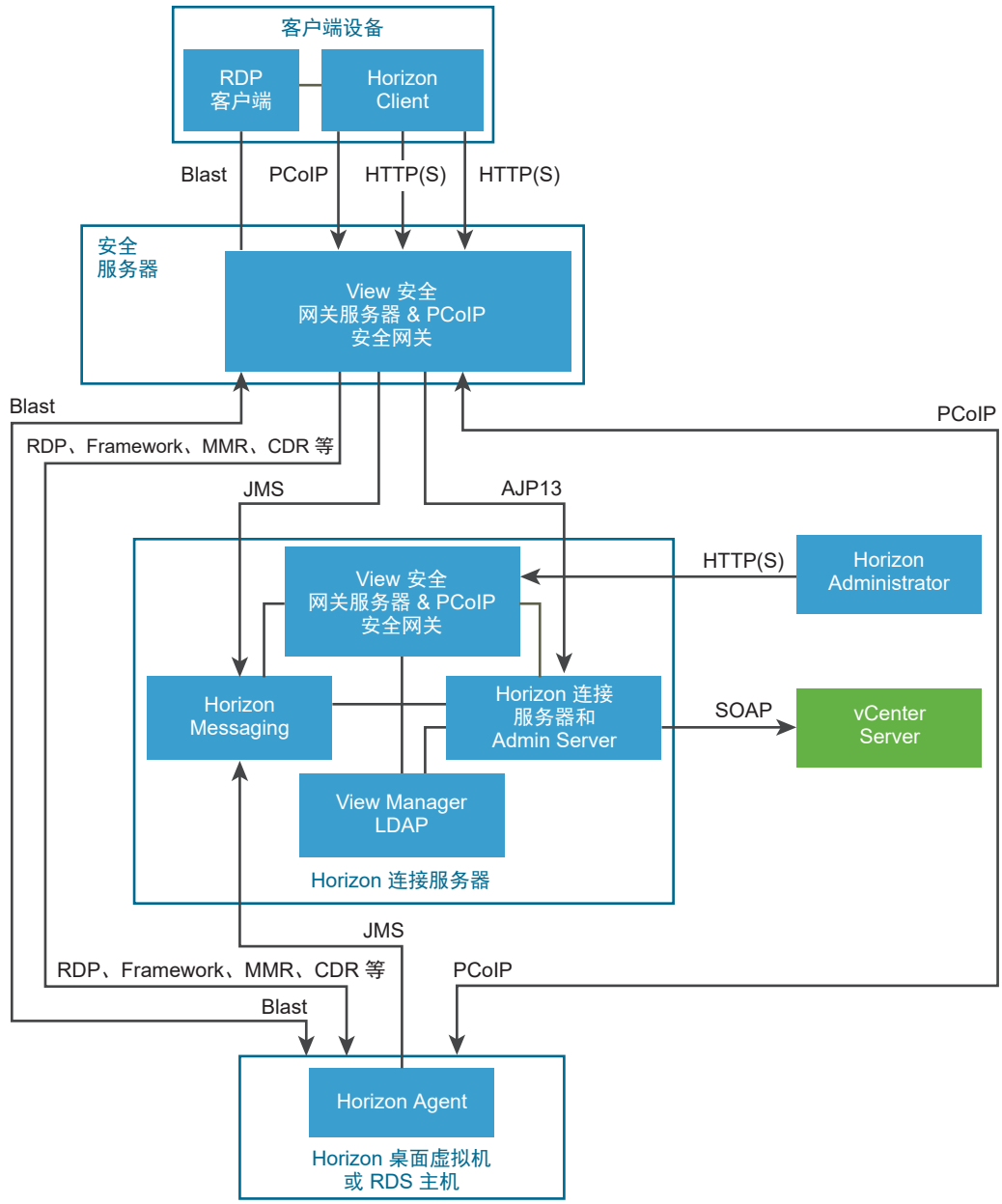


表 5-3. 默认端口 中列出了每个协议所用的默认端口。必要时，您可以更改使用哪些端口号，以遵循组织策略或避免争用问题。

表 5-3. 默认端口

协议	端口
JMS	TCP 端口 4001 TCP 端口 4002
AJP13	TCP 端口 8009 注 AJP13 仅用于安全服务器配置。

表 5-3. 默认端口 （续）

协议	端口
HTTP	TCP 端口 80
HTTPS	TCP 端口 443
MMR/CDR	TCP 端口 9427（用于多媒体重定向和客户端驱动器重定向）
RDP	TCP 端口 3389 注 如果将连接服务器实例配置为采用直接客户端连接，则这些协议将直接从客户端连接到远程桌面，而不会通过 View Secure GW Server 组件使用安全加密链路传送。
SOAP	TCP 端口 80 或 443
PCoIP	TCP 端口 4172 UDP 端口 4172、50002 和 55000
USB 重定向	TCP 端口 32111。此端口还用于时区同步。
VMware Blast Extreme	TCP 端口 8443 和 22443 UDP 端口 443、8443 和 22443
HTML Access	TCP 端口 8443 和 22443

用于连接服务器相互通信的 TCP 端口

组中的连接服务器实例使用其他 TCP 端口来相互通信。例如，连接服务器实例使用端口 4100 或 4101 来相互传输 JMS 路由器之间 (JMS Inter-Router, JMSIR) 的流量。同一组中的连接服务器实例之间通常不使用防火墙。

View Secure Gateway Server

View Secure Gateway Server 是用于客户端系统与安全服务器、Unified Access Gateway 设备或连接服务器实例之间的安全 HTTPS 连接的服务器端组件。

当您为连接服务器配置了安全加密链路连接时，RDP、USB 和多媒体重定向 (MMR) 流量将通过 View Secure Gateway 组件使用安全加密链路传送。当您配置直接客户端连接时，这些协议将直接从客户端连接到远程桌面，不会通过 View Secure Gateway Server 组件使用安全加密链路传送。

注 使用 PCoIP 或 Blast Extreme 显示协议的客户端可以使用安全加密链路连接实现 USB 重定向和多媒体重定向 (MMR) 加速，但对于所有其他数据，PCoIP 使用 PCoIP 安全网关，Blast Extreme 使用安全服务器或 Unified Access Gateway 设备上的 Blast 安全网关。

View Secure Gateway Server 还负责将其他 Web 流量（包括用户身份验证和桌面及应用程序选择流量）从客户端转发到连接服务器。另外，View Secure Gateway Server 还可以将 Horizon Administrator 客户端的 Web 流量传送到 Administration Server 组件。

Blast 安全网关

安全服务器和 Unified Access Gateway 设备包含一个 Blast 安全网关组件。如果启用了 Blast 安全网关，在进行身份验证后，使用 Blast Extreme 或 HTML Access 的客户端可以建立到安全服务器或 Unified Access Gateway 设备的另一个安全连接。此连接允许客户端通过 Internet 访问远程桌面和应用程序。

如果启用了 Blast 安全网关组件，则安全服务器或 Unified Access Gateway 设备将 Blast Extreme 流量转发到远程桌面和应用程序。如果使用 Blast Extreme 的客户端也使用 USB 重定向功能或多媒体重定向 (MMR) 加速功能，您可以启用 View 安全网关组件来转发这些数据。

配置直接客户端连接时，Blast Extreme 流量和其他流量从客户端直接转到远程桌面或应用程序。

最终用户（如家庭用户或移动用户）通过 Internet 访问桌面时，安全服务器或 Unified Access Gateway 设备可提供所需的安全级别和连接性能，因此无需使用 VPN 连接。Blast 安全网关组件可确保唯一能够进入企业数据中心的远程流量是通过严格验证的用户产生的流量。最终用户只能访问被授权访问的资源。

通过 Blast 安全网关操作的 Blast 本机客户端需要使用在 Blast 安全网关上配置的 TLS 证书对其 Blast 会话 TLS 连接进行身份验证。如果客户端的 Blast 连接发现其他一些 TLS 证书，那么连接将会断开，并且客户端会报告证书指纹不匹配。

如果您选择将客户端连接到一个放在该客户端与 Blast 安全网关之间的 TLS 终端代理，则通过安排代理来提供 Blast 安全网关证书（以及私钥）的副本，可以满足客户端的证书要求并避免指纹不匹配错误，从而允许客户端成功进行 Blast 连接。

将 Blast 安全网关的证书复制到代理的一种替代方法是，向代理提供自己的 TLS 证书，然后将 Blast 安全网关配置为建议客户端要求并接受代理的证书，而不是 Blast 安全网关的证书。

您可以在 Unified Access Gateway 中配置 Blast 安全网关，方法是在 Unified Access Gateway“Horizon 设置”的 **Blast 代理证书**中上传代理的证书。请参阅位于 https://docs.vmware.com/cn/Unified-Access-Gateway/index.html 的《部署和配置 VMware Unified Access Gateway》文档。

注 仅上载代理证书。不会将对应的私钥公开到 Unified Access Gateway。

PCoIP 安全网关

安全服务器和 Unified Access Gateway 设备包含一个 PCoIP 安全网关组件。在启用了 PCoIP 安全网关的情况下，通过身份验证后，使用 PCoIP 协议的客户端可与安全服务器或 Unified Access Gateway 设备再建立一条安全连接。此连接允许客户端通过 Internet 访问远程桌面和应用程序。

如果启用了 PCoIP 安全网关组件，则安全服务器或 Unified Access Gateway 设备将 PCoIP 流量转发到远程桌面和应用程序。如果使用 PCoIP 的客户端也使用 USB 重定向功能或多媒体重定向 (MMR) 加速功能，您可以启用 View 安全网关组件来转发这些数据。

配置直接客户端连接时，PCoIP 流量和其他流量从客户端直接转到远程桌面或应用程序。

最终用户（如家庭用户或移动用户）通过 Internet 访问桌面时，安全服务器或 Unified Access Gateway 设备可提供所需的安全级别和连接性能，因此无需使用 VPN 连接。PCoIP 安全网关组件可确保唯一能够访问企业数据中心的远程流量是通过严格验证的用户产生的流量。最终用户只能访问被授权访问的资源。

View LDAP

View LDAP 是 View 连接服务器中的嵌入式 LDAP 目录，也是所有 Horizon 7 配置数据的配置存储库。

View LDAP 中包含代表每个远程桌面和应用程序、每个可访问的远程桌面、集中管理的多个远程桌面和 Horizon 7 组件配置设置的各种条目。

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

Horizon Messaging

Horizon Messaging 组件为 Horizon Connection Server 组件之间以及 Horizon Agent 与连接服务器之间的通信提供消息路由器。

该组件支持 Java 消息服务 (Java Message Service, JMS) API（用于在 Horizon 7 中传送消息）。

组件间消息验证使用 DSA 密钥。默认情况下，密钥大小为 512 位，但 FIPS 模式除外，其密钥大小为 2048 位。

注　消息安全模式设置为**已增强**时，将使用 SSL/TLS 来确保 JMS 连接的安全，而不是使用每消息加密。在增强消息安全模式下，验证仅适用于一种消息类型。对于增强消息模式，VMware 建议将密钥大小增加到 2048 位。如果未使用增强消息安全模式，VMware 建议不要更改默认值（512 位），因为增加密钥大小将会影响性能和可扩展性。

如果您希望所有的密钥均为 1024 位，就必须在安装第一个连接服务器实例后，趁尚未创建更多的服务器和桌面时立即更改 RSA 密钥的长度。有关更多信息，请参阅 VMware 知识库 (KB) 文章 1024431。

Horizon 连接服务器的防火墙规则

必须在防火墙上为连接服务器实例和安全服务器打开某些端口。

安装连接服务器时，安装程序可为您配置所需的 Windows 防火墙规则（可选）。这些规则会打开默认使用的端口。如果在安装后更改了默认端口，则必须手动配置 Windows 防火墙以允许 Horizon Client 设备通过更新的端口连接至 Horizon 7。

下表列出了安装期间可以自动打开的默认端口。如非特别注明，端口均为传入端口。

表 5-4. 在 Horizon 连接服务器安装期间打开的端口

协议	端口	Horizon 连接服务器实例类型
JMS	TCP 4001	标准和副本
JMS	TCP 4002	标准和副本
JMSIR	TCP 4100	标准和副本
JMSIR	TCP 4101	标准和副本
AJP13	TCP 8009	标准和副本
HTTP	TCP 80	标准、副本和安全服务器
HTTPS	TCP 443	标准、副本和安全服务器
PCoIP	TCP 4172 传入； UDP 4172 双向传送	标准、副本和安全服务器
HTTPS	TCP 8443 UDP 8443	标准、副本和安全服务器。 在建立到 Horizon 7 的初始连接后，Web 浏览器或客户端设备通过 TCP 端口 8443 连接到 Blast 安全网关。必须在安全服务器或 View 连接服务器实例上启用 Blast 安全网关以允许建立该第二个连接。

表 5-4. 在 Horizon 连接服务器安装期间打开的端口 （续）

协议	端口	Horizon 连接服务器实例类型
HTTPS	TCP 8472	标准和副本 对于 Cloud Pod 架构 功能：用于容器间通信。
HTTP	TCP 22389	标准和副本 对于 Cloud Pod 架构 功能：用于全局 LDAP 复制。
HTTPS	TCP 22636	标准和副本 对于 Cloud Pod 架构 功能：用于安全的全局 LDAP 复制。

用于 View Agent 或 Horizon Agent 的防火墙规则

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

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

如果您指示 View Agent 或 Horizon Agent 安装程序不启用远程桌面支持，安装程序将不会打开端口 3389 和 32111，您必须手动打开这些端口。

如果在安装后更改了 RDP 端口号，您必须更改关联的防火墙规则。要在安装后更改默认端口，必须手动重新配置 Windows 防火墙规则以允许通过更新后的端口进行访问。请参阅《Horizon 7 安装指南》文档中的“替换 View 服务的默认端口”。

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

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

表 5-5. 在 View Agent 或 Horizon Agent 安装期间打开的 TCP 和 UDP 端口

协议	端口
RDP	TCP 端口 3389
USB 重定向和时区同步	TCP 端口 32111
MMR（多媒体重定向）和 CDR（客户端驱动器重定向）	TCP 端口 9427
PCoIP	对于 RDS 主机，PCoIP 使用以下端口号：TCP 端口 4172 和 UDP 端口 4172（双向）。 对于桌面，PCoIP 使用从可配置范围中选择的端口号。默认情况下使用 TCP 端口 4172 到 4173，UDP 端口 4172 到 4182。针对这些端口的防火墙规则不会指定端口号，而是动态关注由每个 PCoIP Server 打开的端口。系统会将选定的端口号通过连接服务器传达给客户端。

表 5-5. 在 View Agent 或 Horizon Agent 安装期间打开的 TCP 和 UDP 端口 （续）

协议	端口
VMware Blast	TCP 端口 22443 UDP 端口 22443（双向） **注** UDP 不用于 Linux 桌面。
HTML Access	TCP 端口 22443
XDMCP	UDP 177 **注** 仅在运行 Ubuntu 18.04 的 Linux 桌面中打开了该端口以进行 XDMCP 访问。防火墙规则阻止所有外部主机访问该端口。
X11	TCP 6100 **注** 仅在运行 Ubuntu 18.04 的 Linux 桌面中打开了该端口以进行 XServer 访问。防火墙规则阻止所有外部主机访问该端口。

Active Directory 的防火墙规则

如果您在 Horizon 7 环境和 Active Directory 服务器之间部署了防火墙，则必须确保打开了所有必要端口。

例如，View 连接服务器必须能够访问 Active Directory 全局目录和轻型目录访问协议 (Lightweight Directory Access Protocol, LDAP) 服务器。如果全局目录和 LDAP 端口被防火墙软件阻止，管理员将无法正常配置用户授权。

请参见适用于您的 Active Directory 服务器版本的 Microsoft 文档，了解确保 Active Directory 顺利通过防火墙而必须打开的端口。

Horizon 7 环境设置步骤概述

6

请完成以下高级任务以安装 Horizon 7 并配置初始部署。

表 6-1. Horizon 7 安装与设置核对清单

步骤	任务
1	在 Active Directory 中设置所需的管理员用户和组。 说明：《Horizon 7 安装指南》和 vSphere 文档。
2	如果您尚未设置，请安装并设置 ESXi 主机和 vCenter Server。 说明：VMware vSphere 文档。
3	（可选）如果要部署链接克隆桌面，请在 vCenter Server 系统或一个单独的服务器上安装 View Composer。同时还应安装 View Composer 数据库。 说明：《Horizon 7 安装指南》文档。
4	安装并设置 Horizon 连接服务器。同时还应安装事件数据库。 说明：《Horizon 7 安装指南》文档。
5	创建一个或多个可作为完整克隆桌面池模板的虚拟机，或者是可作为链接克隆桌面池或即时克隆桌面池的父虚拟机的虚拟机。 说明：《在 Horizon 7 中设置虚拟桌面》。
6	（可选）设置 RDS 主机并安装最终用户要远程连接的应用程序。 说明：《在 Horizon 7 中设置已发布的桌面和应用程序》。
7	创建桌面池、应用程序池或两者。 说明：《在 Horizon 7 中设置虚拟桌面》和《在 Horizon 7 中设置已发布的桌面和应用程序》。
8	控制用户的桌面访问。 说明：《在 Horizon 7 中配置远程桌面功能》。
9	在最终用户的计算机上安装 Horizon Client，并让他们可访问远程桌面和应用程序。 说明：Horizon Client 文档位于 https://docs.vmware.com/cn/VMware-Horizon-Client/index.html。
10	（可选）创建并配置更多的管理员，允许对特定清单对象和设置进行不同级别的访问。 说明：《Horizon 7 管理指南》文档。
11	（可选）配置策略来控制 Horizon 7 组件、桌面和应用程序池以及最终用户的行为。 说明：《在 Horizon 7 中配置远程桌面功能》。

表 6-1. Horizon 7 安装与设置核对清单 （续）

步骤	任务
12	（可选）配置 Horizon Persona Management，该组件允许用户无论何时登录到桌面均可访问个性化数据和设置。 说明：《在 Horizon 7 中设置虚拟桌面》。
13	（可选）如想提高安全性，请集成智能卡身份验证或 RADIUS 双因素身份验证解决方案。 说明：《Horizon 7 管理指南》文档。