VMware View 安装指南

View 5.0
View Manager 5.0
View Composer 2.7

在本文档被更新的版本替代之前，本文档支持列出的每个产品的版本和所有后续版本。要查看本文档的更新版本，请访问 http://www.vmware.com/cn/support/pubs。

ZH_CN-000504-00

vmware®

最新的技术文档可以从 VMware 网站下载：

http://www.vmware.com/cn/support/pubs/

VMware 网站还提供最近的产品更新信息。

您如果对本文档有任何意见或建议，请把反馈信息提交至：

docfeedback@vmware.com

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

北京办公室
北京市海淀区科学院南路 2 号
融科资讯中心 C 座南 8 层
www.vmware.com/cn

上海办公室
上海市浦东新区浦东南路 999 号
新梅联合广场 23 楼
www.vmware.com/cn

广州办公室
广州市天河北路 233 号
中信广场 7401 室
www.vmware.com/cn

目录

VMware View 安装

《VMware View 安装指南》文档介绍了如何安装 VMware View™ 服务器和客户端组件。

目标读者

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

1 服务器组件的系统要求

运行 VMware View 服务器组件的主机必须满足特定的硬件和软件要求。

本章讨论了以下主题：

View Connection Server 的要求

View Connection Server 充当客户端连接代理，负责执行身份验证并将传入的用户请求定向到相应的 View 桌面。View Connection Server 具有特定的硬件、操作系统、安装和支持软件要求。

- View Connection Server 的硬件要求第 7 页，
  必须在满足特定硬件要求的专用物理机或虚拟机上安装 View Connection Server。
- View Connection Server 支持的操作系统第 8 页，
  您必须在支持的操作系统上安装 View Connection Server。
- View Connection Server 的虚拟化软件要求第 8 页，
  View Connection Server 需要安装 VMware 虚拟化软件才能正常运行。
- View Connection Server 副本实例的网络要求第 9 页，
  安装 View Connection Server 副本实例时，应在相同位置配置实例并通过高性能 LAN 进行连接。

View Connection Server 的硬件要求

必须在满足特定硬件要求的专用物理机或虚拟机上安装 View Connection Server。

表 1–1 View Connection Server 的硬件要求

硬件组件	需要	建议
处理器	Pentium IV 2.0 GHz 处理器或更高版本	4 个 CPU
网络连接	一个或多个 10/100 Mbps 网络接口卡 (NIC)	1 Gbps NIC

表 1–1 View Connection Server 的硬件要求 （续）

硬件组件	需要	建议
内存 Windows Server 2008 64 位	4GB RAM 或更高	需要至少 10GB RAM 才能部署 50 个或更多的 View 桌面
内存 Windows Server 2003 32 位 R2	2 GB RAM 或更高	如果要部署 50 个或更多 View 桌面并启用物理地址扩展 (Physical Address Extension, PAE)，则需要 6 GB RAM。 请参见 http://support.microsoft.com/kb/283037 上的 Microsoft 知识库文章。

这些要求也适用于您为了实现高可用性或外部访问安装的其他 View Connection Server 副本和安全服务器实例。

重要事项 托管 View Connection Server 的物理机或虚拟机必须使用静态 IP 地址。

View Connection Server 支持的操作系统

您必须在支持的操作系统上安装 View Connection Server。

表 1–2 列出了 View Connection Server 支持的操作系统。

这些操作系统支持所有 View Connection Server 安装类型，包括标准、副本和安全服务器安装。

表 1–2 View Connection Server 支持的操作系统

操作系统	位数版本	版本	服务包
Windows Server 2008 R2	64 位	Standard Enterprise	无或 SP1
Windows Server 2003 R2	32 位	Standard Enterprise	SP2

PCoIP 安全网关的操作系统要求

尽管可以在 Windows Server 2003 物理机或虚拟机上安装安全服务器，但是如果希望使用 PCoIP 安全网关组件，操作系统必须为 64 位 Windows Server 2008 R2。通过使用 PCoIP 安全网关组件，采用 PCoIP 显示协议的 View Client 可以在企业防火墙外部使用安全服务器而不是 VPN 连接。

您可以将在 64 位 Windows Server 2008 R2 主机上运行的安全服务器与在 Windows Server 2003 或 2003 R2 上运行的 Connection Server 实例进行配对。配对后，客户端仍可使用 PCoIP 安全网关。

重要事项 如果在多个安全服务器之间应用负载平衡程序，请确保所有安全服务器使用相同的操作系统。

View Connection Server 的虚拟化软件要求

View Connection Server 需要安装 VMware 虚拟化软件才能正常运行。

- 如果要使用 vSphere，则必须使用以下受支持的版本之一：
  - vSphere 4.0 Update 3 或更高版本
  - vSphere 4.1 Update 1 或更高版本
  - vSphere 5.0 或更高版本
- 支持 ESX 和 ESXi 主机。

View Connection Server 副本实例的网络要求

安装 View Connection Server 副本实例时，应在相同位置配置实例并通过高性能 LAN 进行连接。

请勿使用 WAN 连接 View Connection Server 副本实例。

即使是平均延迟较低且吐量量较高的高性能 WAN，网络也可能会出现无法提供 View Connection Server 实例保持一致性所需性能特性的情况。

如果 View Connection Server 实例上的 View LDAP 配置变得不一致，则用户可能无法访问桌面。用户在连接配置过时的 View Connection Server 实例时，可能会被拒绝访问。

View Administrator 的要求

管理员可使用 View Administrator 配置 View Connection Server、部署和管理桌面、控制用户身份验证、启动并检查系统事件以及执行分析活动。运行 View Administrator 的客户端系统必须满足特定要求。

View Administrator 是您在安装 View Connection Server 时安装的一个基于 Web 的应用程序。您可以通过以下 Web 浏览器访问和使用 View Administrator：

- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9
- Firefox 3.0
- Firefox 3.5

要通过 Web 浏览器使用 View Administrator，您必须安装 Adobe Flash Player 10 或更高版本。客户端系统必须具有访问 Internet 的权限，才能安装 Adobe Flash Player。

要正确显示文本，View Administrator 要求安装 Microsoft 专用字体。如果您的 Web 浏览器在非 Windows 操作系统（例如 Linux、UNIX 或 Mac OS）上运行，请确保您的计算机上已安装 Microsoft 专用字体。

目前 Microsoft 网站尚未提供 Microsoft 字体，但您可以从其他独立网站下载这些字体。

View Composer 的要求

View Manager 使用 View Composer 从一个集中式基础映像中部署多个链接克隆桌面。View Composer 具有特定的安装和存储要求。

- View Composer 支持的操作系统第 9 页，

  View Composer 支持 64 位操作系统，但具有特定要求和限制。必须将 View Composer 安装在 vCenter Server 所在的同一物理计算机或虚拟机上。

- View Composer 的数据库要求第 10 页，

  View Composer 需要使用 SQL 数据库来存储数据。View Composer 数据库必须驻留在 vCenter Server 计算机上或可供 vCenter Server 计算机使用。

View Composer 支持的操作系统

View Composer 支持 64 位操作系统，但具有特定要求和限制。必须将 View Composer 安装在 vCenter Server 所在的同一物理计算机或虚拟机上。

表 1–3 中列出了 View Composer 支持的操作系统。

表 1–3 64 位操作系统对 View Composer 的支持情况

vCenter Server 版本	操作系统	版本	服务包
4.0 Update 3 及更高版本	Windows Server 2008 R2	Standard 或 Enterprise	无或 SP1
4.1 Update 1 及更高版本	Windows Server 2008 R2	Standard 或 Enterprise	无或 SP1
5.0 及更高版本	Windows Server 2008 R2	Standard 或 Enterprise	无或 SP1

View Composer 的数据库要求

View Composer 需要使用 SQL 数据库来存储数据。View Composer 数据库必须驻留在 vCenter Server 计算机上或可供 vCenter Server 计算机使用。

如果当前已存在适用于 vCenter Server 的数据库服务器，且它的版本是表 1–4 中所列的版本，那么 View Composer 可以使用现有数据库服务器。 例如，View Composer 可以使用 vCenter Server 附带的 Microsoft SQL Server 2005 或 2008 Express 实例。如果当前没有数据库服务器，则必须安装一个。

View Composer 支持 vCenter Server 所支持的部分数据库服务器。如果您已将 vCenter Server 与不受 View Composer 支持的数据库服务器一起使用，请继续将该数据库服务器用于 vCenter Server，并单独安装一个数据库服务器以供 View Composer 和 View Manager 数据库事件使用。

重要事项 如果您在 vCenter Server 所在的 SQL Server 实例上创建 View Composer 数据库，请勿覆盖 vCenter Server 数据库。

表 1–4 中列出了支持的数据库服务器和版本。有关 vCenter Server 支持的数据库版本的完整列表，请参阅 VMware vSphere 文档网站上的《VMware vSphere Compatibility Matrixes》（VMware vSphere 兼容性表）。

表 1–4 View Composer 支持的数据库服务器

数据库	vCenter Server 5.0 及更高版本	vCenter Server 4.1 U1 及更高版本	vCenter Server 4.0 U3 及更高版本
Microsoft SQL Server 2005 Express	否	是	是
Microsoft SQL Server 2005 SP3 及更高版本，Standard 和 Enterprise（32 位和 64 位）	是	是	是
Microsoft SQL Server 2008 R2 Express	是	否	否
Microsoft SQL Server 2008 SP1 及更高版本，Standard 和 Enterprise（32 位和 64 位）	是	是	是

表 1–4 View Composer 支持的数据库服务器 （续）

数据库	vCenter Server 5.0 及更高版本	vCenter Server 4.1 U1 及更高版本	vCenter Server 4.0 U3 及更高版本
Oracle 10g Release 2	是	是	是
Oracle 11g Release 2 （装有 Oracle 11.2.0.1 Patch 5 ）	是	是	是

注意 如果使用 Oracle 11g R2 数据库，必须安装 Oracle 11.2.0.1 Patch 5。此修补程序要求适用于 32 位和 64 位版本。

View Transfer Server 的要求

View Transfer Server 是一个可选 View Manager 组件，它支持检入、检出和复制以本地模式运行的桌面。View Transfer Server 具有特定的安装、操作系统和存储要求。

- View Transfer Server 的安装要求第 11 页，

  您必须在满足特定要求的虚拟机中把 View Transfer Server 作为一个 Windows 应用程序来进行安装。

- View Transfer Server 支持的操作系统第 12 页，

  您必须在具有所需最小 RAM 容量的受支持操作系统上安装 View Transfer Server。

- View Transfer Server 的存储要求第 12 页，

  View Transfer Server 可向/从 Transfer Server 存储库传输静态内容，并在本地桌面和在数据中心内的远程桌面间传输动态内容。View Transfer Server 具有特定的存储要求。

View Transfer Server 的安装要求

您必须在满足特定要求的虚拟机中把 View Transfer Server 作为一个 Windows 应用程序来进行安装。

托管 View Transfer Server 的虚拟机必须满足有关网络连接性的若干要求：

- 必须由要管理本地桌面的同一 vCenter Server 实例进行管理。
- 不必是域的一部分。
- 必须使用静态 IP 地址。

小心 必须为托管 View Transfer Server 的虚拟机配置一个 Logic Parallel SCSI 控制器。不能使用 SAS 或 VMware 准虚拟控制器。

在 Windows Server 2008 虚拟机上，LSI Logic SAS 控制器为默认选中。在安装操作系统之前，必须先将此选项更改为 LSI Logic Parallel 控制器。

View Transfer Server 软件无法在相同的虚拟机上与任何其他 View Manager 软件组件（包括 View Connection Server ）共存。

您可以安装多个 View Transfer Server 实例，以实现高可用性和可扩展性。

View Transfer Server 支持的操作系统

您必须在具有所需最小 RAM 容量的受支持操作系统上安装 View Transfer Server。

表 1–5 View Transfer Server 支持的操作系统

操作系统	位数版本	版本	服务包	最低 RAM
Windows Server 2008 R2	64 位	Standard Enterprise	无或 SP1	4GB
Windows Server 2003 R2	32 位	Standard Enterprise	SP2	2 GB

重要事项 为托管 View Transfer Server 的虚拟机配置两个虚拟 CPU。

View Transfer Server 的存储要求

View Transfer Server 可向/从 Transfer Server 存储库传输静态内容，并在本地桌面和在数据中心内的远程桌面间传输动态内容。View Transfer Server 具有特定的存储要求。

- 您配置 Transfer Server 存储库的磁盘驱动器必须具有足够的空间来存储静态映像文件。映像文件为 View Composer 基础映像。
- View Transfer Server 必须可以访问存储要传输的桌面磁盘的数据存储。数据存储必须能从正在运行 View Transfer Serve 虚拟机的 ESX/ESXi 主机进行访问。
- View Transfer Server 能够支持的最大并发磁盘传输数量为 20 个。

  在传输操作过程中，本地桌面的虚拟磁盘会装载到 View Transfer Server 上。View Transfer Server 虚拟机拥有四个 SCSI 控制器。这个配置每次可以将多个磁盘连接到虚拟机。
- 由于本地桌面中可能包含敏感的用户数据，因此需确保在通过网络传输时已对数据进行加密。

  在 View Administrator 中，您可以在每个 View Connection Server 实例上配置数据传输安全选项。要在 View Administrator 中配置这些选项，请单击 **[View Configuration（View 配置）] > [Servers（服务器）]**，选择一个 View Connection Server 实例，然后单击 **[Edit（编辑）]**。
- 将 View Transfer Server 添加到 View Manager 之后，其 Distributed Resource Scheduler (DRS) 自动化策略将设置为 [Manual（手动）]，这样可有效禁用 DRS。

  要将一个 View Transfer Server 实例迁移到另一个 ESX 主机或数据库，您必须在开始迁移前将该实例置于维护模式。

  将 View Transfer Server 从 View Manager 中移除之后，DRS 自动化策略将被重置为未将 View Transfer Server 添加到 View Manager 时的值。

客户端组件的系统要求 2

运行 View Client 组件的系统必须满足特定的硬件和软件要求。

在连接 View Connection Server 时，Windows 系统中的 View Client 会使用 Microsoft Internet Explorer 的 Internet 设置（包括代理设置）。请确保 Internet Explorer 设置准确无误，而且您可以通过 Internet Explorer 访问 View Connection Server URL。您可以使用 Internet Explorer 7、8 或 9。

本章讨论了以下主题：

View Agent 支持的操作系统

View Agent 组件用于协助实现会话管理、单点登录和设备重定向。您必须在将由 View Manager 管理的所有虚拟机、物理系统和终端服务器上安装 View Agent。

表 2–1 中列出了 View Agent 支持的操作系统。

表 2–1 View Agent 操作系统支持

Guest Operating System（客户操作系统）	位数版本	版本	服务包
Windows 7	64 位和 32 位	Enterprise 和 Professional	无和 SP1
Windows Vista	32 位	Business 和 Enterprise	SP1 和 SP2
Windows XP	32 位	Professional	SP3
Windows 2008 R2 Terminal Server	64 位	Standard	无和 SP1
Windows 2008 Terminal Server	64 位	Standard	SP2

表 2–1 View Agent 操作系统支持（续）

Guest Operating System（客户操作系统）	位数版本	版本	服务包
Windows 2003 R2 Terminal Server	32 位	Standard	SP2
Windows 2003 Terminal Server	32 位	Standard	SP2

重要事项 如果在虚拟机中安装 Windows 7，主机必须安装 ESX/ESXi 4.0 Update 3 或更高版本、ESX/ESXi 4.1 Update 1 或更高版本或者 ESXi 5.0 或更高版本。

基于 Windows 的 View Client 和 View Client with Local Mode 支持的操作系统

用户需要运行 View Client 来连接到他们的 View 桌面。您必须在支持的操作系统上安装 View Client 或 View Client with Local Mode。

表 2–2 中列出了 View Client 支持的 Microsoft Windows 操作系统。有关其他 View 客户端（如适用于 Mac 的 View Client 和适用于 iPad 的 View Client）支持的操作系统信息，请参阅适用于特定客户端的文档。请访问 https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html。

表 2–2 View Client 支持的基于 Windows 的客户端操作系统

操作系统	位数版本	版本	服务包
Windows 7	32 位和 64 位	Home、Enterprise、Professional 和 Ultimate	无和 SP1
Windows XP	32 位	Home 和 Professional	SP3
Windows Vista	32 位	Home、Business、Enterprise 和 Ultimate	SP1 和 SP2

重要事项 仅 Windows 系统和物理机支持 View Client with Local Mode。此外，要使用该功能，您的 VMware 许可中必须包括 View Client with Local Mode。

View Client with Local Mode 是一个完全受支持的功能，在早期版本中是一个被称为 View Client with Offline Desktop 的试验性功能。

注意 VMware 合作伙伴提供用于 VMware View 部署的瘦客户端设备。每个瘦客户端设备的功能和 Linux 操作系统由企业选择使用的供应商、型号和配置决定。有关瘦客户端设备的供应商及型号的信息，请参阅 VMware 网站上的《Thin Client Compatibility Guide》（瘦客户端兼容性指南）。

本地模式桌面的硬件要求

当您检出 View 桌面在本地计算机上运行时，客户端主机上的硬件必须支持本地系统及其中运行的虚拟机。

虚拟硬件

不支持检出使用虚拟硬件版本 8 的 View 桌面。如果使用 vSphere 5 创建作为本地模式桌面资源的虚拟机，请确保创建的虚拟机使用虚拟硬件版本 7。

PC 硬件

表 2–3 描述了各种 View 桌面操作系统的硬件要求。

表 2–3 处理器要求

客户端计算机要求	描述
PC	标准 x86 或 x86-64 兼容
CPU 数量	支持多处理器系统
CPU 速度	对于 Windows XP 本地桌面，CPU 速度至少为 1.3 GHz，建议使用 1.6 GHz。 对于 Windows 7 桌面，CPU 速度至少为 1.3GHz；要实现 Aero 效果，CPU 速度至少为 2.0GHz。
Intel 处理器	Pentium 4、Pentium M（带有 PAE）、Core、Core 2、Core i3、Core i5 和 Core i7 处理器 对于 Windows 7 Aero：Intel Dual Core
AMD 处理器	Athlon、Athlon MP、Athlon XP、Athlon 64、Athlon X2、Duron、Opteron、Turion X2、Turion 64、Sempron、Phenom 和 Phenom II 对于 Windows 7 Aero：Althon 4200+ 及更高版本
64 位操作系统	Intel Pentium 4、Core 2 和 Core i7 处理器（支持 EM64T 和 Intel Virtualization Technology） 多数 AMD64 处理器（最早的修订版 C Opteron 处理器除外）
支持 Windows 7 Aero 的 GPU	nVidia GeForce 8800GT 及更高版本 ATI Radeon HD 2600 及更高版本

磁盘空间

如果您在 View 桌面中对操作系统使用默认安装，实际所需的磁盘空间相当于在物理计算机上安装和运行操作系统及应用程序的所需的空间。

例如，Microsoft 建议为运行 32 位 Windows 7 操作系统的计算机配置 16 GB 的硬盘空间。如果为 32 位 Windows 7 虚拟机配置 16 GB 的虚拟硬盘，则当检出本地桌面时，仅会下载实际使用的磁盘空间容量。对于分配有 16 GB 容量的桌面，实际下载大小约为 7 GB。

桌面下载后，如果配置了 16 GB 的硬盘，使用的磁盘空间量可能会增长到 16 GB。因为在复制过程中拍摄了快照，所以需要额外占用的相应磁盘空间量。例如，如果本地桌面当前使用 7 GB 的磁盘空间，快照将在客户端计算机上额外占用 7 GB 的空间。

支持 IDE 和 SCSI 硬盘。

内存

您需要有足够的内存才能在客户端计算机上运行主机操作系统，另外还需要一定的内存来运行 View 桌面的操作系统以及客户端计算机和 View 桌面上的应用程序。VMware 建议您至少为 Windows XP 和 Windows Vista 系统分配 2 GB 内存，至少为 Windows 7 系统分配 3 GB 内存。有关内存要求的更多信息，请参阅您的客户操作系统和应用程序文档。

可分配到单个计算机中所有虚拟机的内存总量仅受计算机 RAM 容量的限制。每个 View 桌面的最大内存容量为 8 GB（32 位客户端计算机）或 32 GB（64 位客户端计算机）。

显示

建议使用 32 位显卡。在某些图形硬件上运行 Windows Vista 或 Windows 7 虚拟机时，3DMark '06 等 3D 基准测试程序可能无法显示或根本无法显示。

要播放 720p 或更高分辨率的视频，需要使用多处理器系统。

有关 Windows 7 Aero 的 CPU 和 GPU 要求，请参阅表 2–3。

View Portal 的客户端浏览器要求

您可以从客户端系统浏览 View Connection Server 实例并使用 View Portal 来安装基于 Mac 的 View Client、基于 Windows 的 View Client 或 View Client with Local Mode。如果您使用的是 Internet Explorer，View Portal 将在有新版 View Client 可供下载时发出提示。

要使用 View Portal，您必须拥有以下某个 Web 浏览器：

- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9
- Firefox 3.0
- Firefox 3.5

如果您使用的是 Internet Explorer 并且已安装 View Client，当 View Connection Server 提供的版本比在客户端设备上安装的版本新时，您可以选择进行升级。如果当前版本与客户端设备上的版本相同，View Portal 会启动本地系统上安装的 View Client。

注意 View Portal 不支持 Linux。适用于 Linux 的本地客户端仅能通过认证的 VMware 合作伙伴获得。

远程显示协议和软件支持

远程计算机可借助显示协议和软件通过网络连接访问桌面。View Client 支持 Microsoft 远程桌面协议 (RDP) 和 VMware 的 PCoIP。

- 采用 PCoIP 的 VMware View 第 16 页，

  PCoIP 为 LAN 或 WAN 中的广大用户提供了交付的整个桌面环境的最佳桌面体验，包括应用程序、图像、音频和视频等。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。

- Microsoft RDP 第 18 页，

  Microsoft 远程桌面连接 (Remote Desktop Connection, RDC) 使用 RDP 来传输数据。RDP 是一种多通道协议，允许用户远程连接计算机。

- 多媒体重定向 (MMR)第 18 页，

  多媒体重定向 (Multimedia Redirection, MMR) 功能使用虚拟通道将多媒体流直接交付到客户端计算机。

采用 PCoIP 的 VMware View

PCoIP 为 LAN 或 WAN 中的广大用户提供了交付的整个桌面环境的最佳桌面体验，包括应用程序、图像、音频和视频等。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 可以作为使用 Teradici 主机卡的虚拟机和物理机的 View 桌面的显示协议。

PCoIP 功能

PCoIP 的主要功能包括：

- 对于企业防火墙外部的用户，您可将该协议与公司虚拟专用网络或 View 安全服务器结合使用。
- 支持连接到 View Agent 所在的 Windows 桌面。View Agent 支持的操作系统版本在第 13 页，“View Agent 支持的操作系统”中列出。
- 支持来自 View Client 所在 Windows 客户端的连接。View Client 支持的操作系统版本在第 14 页，“基于 Windows 的 View Client 和 View Client with Local Mode 支持的操作系统”中列出。

- Windows XP 和 Vista 客户端可支持 MMR 重定向。Windows 7 View Client 和 Windows 7 View 桌面均不支持 MMR 重定向。
- 支持 USB 重定向。
- 支持音频重定向，可针对 LAN 和 WAN 动态调整音频质量。
- 支持多显示器。您最多可以使用四个显示器，并可以分别调整各显示器的分辨率，每个显示器的最大分辨率为 2560x1600。此外还支持旋转显示和自动调整功能。

  启用 3D 功能后，最多可支持 2 台显示器，其最高分辨率 为 1920 x 1200。
- 支持用 32 位色彩进行虚拟显示。
- 支持 ClearType 字体。
- 支持在本地系统和桌面之间复制和粘贴文本和图像（不超过 1 MB）。支持的文件格式包括文本、图像和 RTF（富文本格式）。您无法在系统之间复制和粘贴系统对象，如文件夹和文件。

视频质量

480p 格式视频

当 View 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。如果操作系统是 Windows 7，而且您希望以高清 Flash 或全屏模式播放视频，此桌面将需要使用双虚拟 CPU。

720p 格式视频

当 View 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 View 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

如果您计划使用 3D 应用程序，如 Windows Aero 主题或 Google Earth，Windows 7 View 桌面必须安装虚拟硬件版本 8（vSphere 5 及更高版本提供）。同时必须打开 **[Windows 7 3D Rendering（Windows 7 3D 呈现）]** 池设置。最多支持 2 台显示器，最高屏幕分辨率为 1920 x 1200。

这种非硬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器 (GPU)。

建议的客户操作系统设置

建议的客户操作系统设置包括：

- 针对 Windows XP 桌面：768 MB RAM 或更多，单个 CPU
- 针对 Windows 7 桌面：1 GB RAM 和双 CPU

客户端硬件要求

客户端硬件要求包括：

- 具有 SSE2 扩展指令集、基于 x86 的处理器，处理器速度为 800 MHz 或更高。
- 具有 NEON（首选）或 WMMX2 扩展指令集的 ARM 处理器，处理器速度为 1 Ghz 或更高。
- 系统要求以外的 RAM，用于支持各种显示器设置。以下公式可用作一般指南：

  ```
  20MB +（24 *（显示器数量） *（显示器宽度） *（显示器高度））
  ```

  作为粗略估计，您可以使用以下计算：

  ```
  1 个显示器：1600 × 1200：64MB
  2 个显示器：1600 × 1200：128MB
  3 个显示器：1600 × 1200：256MB
  ```

Microsoft RDP

Microsoft 远程桌面连接 (Remote Desktop Connection, RDC) 使用 RDP 来传输数据。RDP 是一种多通道协议，允许用户远程连接计算机。

以下是针对不同 Windows 操作系统和功能的 RDP 相关要求和注意事项。

- 对于 Windows XP 和 Windows XP Embedded 系统，应当使用 Microsoft RDC 6.x。
- Windows Vista 附带安装了 RDC 6.x，尽管推荐使用 RDC 7。
- Windows 7 附带安装了 RDC 7。Windows 7 SP1 附带安装了 RDC 7.1。
- 必须拥有 RDC 6.0 或更高版本，才能使用多个显示器。
- 对于 Windows XP 桌面虚拟机，必须安装 Microsoft 知识库 (KB) 文章 323497 和 884020 中列出的 RDP 修补程序。如果未安装 RDP 修补程序，客户端上可能会出现 `Windows Sockets failed error`（Windows 套接字失败错误）消息。
- View Agent 安装程序会为入站 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（通常是 3389 端口）相匹配。如果您更改了 RDP 端口号，则必须更改相关的防火墙规则。

您可以从 Microsoft 网站下载 RDC 版本。

客户端硬件要求

客户端硬件要求包括：

- 具有 SSE2 扩展指令集、基于 x86 的处理器，处理器速度为 800 MHz 或更高。
- 具有 NEON（首选）或 WMMX2 扩展指令集的 ARM 处理器，处理器速度为 600 MHz 或更高。
- 128 MB RAM。

多媒体重定向 (MMR)

多媒体重定向 (Multimedia Redirection, MMR) 功能使用虚拟通道将多媒体流直接交付到客户端计算机。

通过 MMR，多媒体流在客户端系统上进行编码和解码处理。本地硬件格式化并播放媒体内容，从而降低了 ESX/ESXi 主机上的负载需求。

View Client 和 View Client with Local Mode 在以下操作系统上支持 MMR：

- Windows XP
- Windows XP Embedded
- Windows Vista

由于本地解码器必须安装在客户端上，因此 MMR 功能可支持客户端系统支持的媒体文件格式。文件格式包括 MPEG2-1、MPEG-2、MPEG-4 Part 2；WMV 7、8 和 9；WMA；AVI；ACE；MP3；WAV 以及其他。

请使用 Windows Media Player 10 或更高版本，并将其安装到本地计算机（或客户端访问设备）和 View 桌面。

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。

注意 View Client 视频显示硬件必须支持覆盖功能，MMR 才能正常运行。

Windows 7 客户端和 Windows 7 View 桌面不支持 MMR。对于 Windows 7 客户端代理，请使用 RDP 7 中附带的 Windows 媒体重定向功能。

Adobe Flash 要求

您可以减少 Adobe Flash 内容在 View 桌面会话中运行时使用的带宽。减少带宽可以增强整体浏览体验，并且提高桌面上运行的其他应用程序的响应速度。

只能在 Microsoft Windows 上的 Internet Explorer 会话中减少 Adobe Flash 带宽，而可减少带宽的版本也仅限于 Adobe Flash 版本 9 和 10。要使用 Adobe Flash 带宽缩减设置，就不能以全屏模式运行 Adobe Flash。

智能卡身份验证要求

使用智能卡进行用户身份验证的客户端系统必须符合特定要求。

每台使用智能卡进行用户身份验证的客户端系统都必须具有以下软件和硬件：

- View Client
- 一个与 Windows 兼容的智能卡读卡器
- 智能卡中间件
- 产品专用的应用程序驱动程序

您还必须在 View 桌面上安装产品专用的应用程序驱动程序。

View 支持使用 PKCS#11 或 Microsoft CryptoAPI 提供程序的智能卡和智能卡读卡器。您可以选择安装 ActivIdentity ActivClient 软件套件，该套件可提供与智能卡进行交互的工具。

使用智能卡进行身份验证的用户必须拥有智能卡或 USB 智能卡令牌，且每个智能卡都必须包含一个用户证书。

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。该计算机必须具有颁发用户智能卡的授权，且必须是为其颁发证书的域中的成员。

重要事项 当您注册智能卡时，可以选择所得证书的密钥大小。要通过本地桌面使用智能卡，您必须在智能卡注册过程中选择 1024 位或 2048 位密钥大小。不支持具有 512 位密钥的证书。

Microsoft TechNet 网站中包含为 Windows 系统规划和实施智能卡身份验证方面的详细信息。

请参阅第 24 页，“为智能卡身份验证准备 Active Directory”了解有关在 Active Directory 中通过 View 实现智能卡身份验证所需执行任务的信息。

适用于 Mac 的 View Client 或 View Administrator 不支持智能卡身份验证。有关智能卡支持的完整信息，请参阅*《VMware View 体系结构规划指南》*文档。

准备 Active Directory 3

View 使用您现有的 Microsoft Active Directory 基础架构来进行用户身份验证和管理。您必须执行特定的任务来准备 Active Directory，以便能与 View 一起使用。

View 支持下列版本的 Active Directory：

- Windows 2000 Active Directory
- Windows 2003 Active Directory
- Windows 2008 Active Directory

本章讨论了以下主题：

配置域和信任关系

您必须将每个 View Connection Server 主机加入到 Active Directory 域。主机不能是域控制器。将 View 桌面置于与 View Connection Server 主机所在域相同的域，或者置于与 View Connection Server 主机所在域具有双向信任关系的域。

您可以授权 View Connection 主机所在域中的用户和用户组访问 View 桌面和池。您也可以从 View Connection Server 主机所在域中选择用户和用户组，使之成为 View Administrator 中的管理员。要授权或选择其他域中的用户和用户组，您必须在该域和 View Connection Server 主机所在域之间建立双向信任关系。

用户将根据 View Connection Server 主机所在域以及其他任何存在信任协议的用户域的 Active Directory 进行身份验证。

注意 由于安全服务器不会访问包括 Active Directory 在内的任何身份验证存储库，因此它们不需要驻留在 Active Directory 域中。

信任关系和域过滤

为确定可访问的域，View Connection Server 实例会从其所在的域开始遍历信任关系。

对于一组连接良好的小型域，View Connection Server 能够快速确定完整的域列表，但随着域数量的不断增多或域之间连通性能的逐渐降低，确定完整域列表所需的时间也会随之增加。另外，该列表还可能包含您不希望用户在登录 View 桌面时为其提供的域。

您可以使用 `vdmadmin` 命令来配置域的过滤，以限制 View Connection Server 实例能够搜索并向用户显示的域。有关更多信息，请参阅*《VMware View 管理指南》*文档。

为 View 桌面创建组织单位

您应当专门为您的 View 桌面创建一个组织单位 (Organizational Unit, OU)。组织单位是对 Active Directory 的细分，包含用户、组、计算机或其他组织单位。

要避免将组策略设置应用于您的桌面所在域中的其他 Windows 服务器或工作站，您可以为 View 组策略创建一个 GPO 并将其链接到包含您 View 桌面的组织单位。您也可以将组织单位的控制权委托给下级组，如服务器操作员或单独用户。

如果您使用的是 View Composer，应为链接克隆桌面创建一个基于 View 桌面组织单位的独立 Active Directory 容器。拥有 Active Directory 组织单位管理员特权的 View 管理员无需获得域管理员特权即可部署链接克隆桌面。如果您更改了 Active Directory 的管理员凭据，则必须更新 View Composer 中的凭据信息。

为 Kiosk 模式客户端帐户创建组织单位和组

Kiosk 模式的客户端是指运行 View Client 以连接 View Connection Server 实例并启动远程桌面会话的瘦客户端或锁定 PC。如果您在 Kiosk 模式中配置客户端，则应在 Active Directory 中为 Kiosk 模式客户端帐户创建专用组织单位和组。

为 Kiosk 模式的客户端帐户创建专用组织单位和组可使客户端系统免受意外侵袭并简化客户端配置和管理。

有关更多信息，请参阅《VMware View 管理指南》文档。

创建 View 用户组

您应该在 Active Directory 中为不同类型的 View 用户创建用户组。例如，您可以为 View 桌面用户创建名为 "VMware View Users" 的组，为管理 View 桌面的用户创建另一个名为 "VMware View Administrators" 的组。

为 vCenter Server 创建用户帐户

您必须在 Active Directory 中创建一个用户帐户与 vCenter Server 一起使用。当您在 View Administrator 中添加 vCenter Server 实例时可以指定该用户帐户。

该用户帐户必须处于您的 View Connection Server 主机所在域中，或者处于受信任的域中。如果您使用了 View Composer，则必须将该用户帐户添加到 vCenter Server 计算机上的本地 Administrators 组中。

您必须为用户帐户授予在 vCenter Server 中执行特定操作的特权。如果使用 View Composer，则必须为用户帐户授予额外特权。请参阅第 48 页，“配置 vCenter Server 和 View Composer 的用户帐户”了解有关配置这些特权的信息。

为 View Composer 创建用户帐户

如果使用 View Composer，您必须在 Active Directory 中创建一个用户帐户，以供 View Composer 使用。View Composer 需要使用该帐户将链接克隆桌面加入到您的 Active Directory 域。

为确保安全性，您应当创建一个单独的用户帐户，以供 View Composer 使用。通过创建单独的帐户，可以确保该帐户不具有针对其他目的定义的额外特权。您可以为该帐户授予在指定的 Active Directory 容器中创建和移除计算机对象所需的最低特权。例如，View Composer 帐户不需要域管理员特权。

步骤

1 在 Active Directory 中，在您的 View Connection Server 主机所在域或一个受信任的域中创建用户账户。

2 在用于创建和接收链接克隆计算机帐户的 Active Directory 容器中，授予该帐户 **[Create Computer Objects（创建计算机对象）]**、**[Delete Computer Objects（删除计算机对象）]** 和 **[Write All Properties（写入全部属性）]** 权限。

以下列表显示了该用户帐户需要的所有权限，包括默认分配的权限：

- List Contents（列出内容）
- Read All Properties（读取全部属性）
- Write All Properties（写入全部属性）
- Read Permissions（读取权限）
- Create Computer Objects（创建计算机对象）
- Delete Computer Objects（删除计算机对象）

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

下一步

当您为 vCenter Server 配置 View Composer，以及配置和部署链接克隆桌面池时，需要在 View Administrator 中指定该帐户。

配置受限制的组策略

要登录到 View 桌面，用户必须是 View 桌面本地远程桌面用户组的成员。您可以使用 Active Directory 中 [Restricted Groups（受限制的组）] 策略，将用户或用户组添加到每个 View 桌面（已加入到域中）的本地远程桌面用户组中。

[Restricted Groups（受限制的组）] 策略会设置域中计算机的本地组成员关系，使之与 [Restricted Groups（受限制的组）] 策略中定义的成员关系列表设置相匹配。View 桌面用户组的成员始终会添加到每个加入域的 View 桌面的本地远程桌面用户组中。添加新用户时，您只需要将其添加到您的 View 桌面用户组。

前提条件

在 Active Directory 中，为您的域中的 View 桌面用户创建一个组。

步骤

1 在 Active Directory 服务器中，选择 **[Start（开始）] > [Administrative Tools（管理工具）] > [Active Directory Users and Computers（Active Directory 用户和计算机）]**。

2 右键单击域，然后选择 **[Properties（属性）]**。

3 在 **[Group Policy（组策略）]** 选项卡上，单击 **[Open（打开）]** 以打开组策略管理插件。

4 右键单击 **[Default Domain Policy（默认域策略）]**，然后单击 **[Edit（编辑）]**。

5 展开 **[Computer Configuration（计算机配置）]** 区域，然后打开 **[Windows Settings（Windows 设置）\Security Settings（安全设置）]**。

6 右键单击 **[Restricted Groups（受限制的组）]**，然后选择 **[Add Group（添加组）]** 以添加远程桌面用户组。

7 右键单击新的受限制远程桌面用户组，并将 View 桌面用户组添加到组成员列表。

8 单击 **[OK（确定）]** 保存更改。

使用 View 组策略管理模板文件

View 中包含多个针对组件的组策略管理 (ADM) 模板文件。

View Connection Server 在安装时会将 View ADM 模板文件安装到 View Connection Server 主机的*安装目录*\VMware\VMware View\Server\Extras\GroupPolicyFiles 目录中。您必须将这些文件复制到 Active Directory 服务器上的目录中。

通过将这些文件中的策略设置添加到 Active Directory 中新的或现有 GPO，并将其链接到包含 View 桌面的组织单位，您可以优化并保护 View 桌面。

有关使用 View 组策略设置的信息，请参阅《*VMware View 管理指南*》文档。

为智能卡身份验证准备 Active Directory

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

- 为智能卡用户添加 UPN 第 24 页，

  由于智能卡登录依赖用户主体名称 (User Principal Name, UPN)，因此在 View 中使用智能卡进行身份验证的用户的 Active Directory 帐户必须具有有效的 UPN。

- 将根证书添加到受信任的根证书颁发机构第 25 页，

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

- 将中间证书添加到中间证书颁发机构第 25 页，

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

- 将根证书添加到 Enterprise NTAuth 存储第 26 页，

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

为智能卡用户添加 UPN

由于智能卡登录依赖用户主体名称 (User Principal Name, UPN)，因此在 View 中使用智能卡进行身份验证的用户的 Active Directory 帐户必须具有有效的 UPN。

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

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

前提条件

- 通过查看证书属性，获取受信任 CA 的根证书中包含的 SAN。

- 如果您的 Active Directory 服务器上没有“ADSI 编辑”实用程序，请从 Microsoft 网站下载并安装相应的 Windows 支持工具。

步骤

1 在 Active Directory 服务器上，启动“ADSI 编辑”实用程序。

2 在左侧窗格中，展开用户所在的域并双击 `CN=Users`。

3 在右侧窗格中，右键单击用户，然后单击 **[Properties（属性）]**。

4 双击 `userPrincipalName` 属性并键入受信任 CA 证书的 SAN 值。

5 单击 **[OK（确定）]** 保存属性设置。

将根证书添加到受信任的根证书颁发机构

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

步骤

1 在 Active Directory 服务器中，选择 **[Start（开始）] > [All Programs（所有程序）] > [Administrative Tools（管理工具）] > [Active Directory Users and Computers（Active Directory 用户和计算机）]**。

2 右键单击域，然后单击 **[Properties（属性）]**。

3 在 **[Group Policy（组策略）]** 选项卡上，单击 **[Open（打开）]** 以打开组策略管理插件。

4 右键单击 **[Default Domain Policy（默认域策略）]**，然后单击 **[Edit（编辑）]**。

5 展开 **[Computer Configuration（计算机配置）]** 区域，然后打开 **[Windows Settings（Windows 设置）\Security Settings（安全设置）\Public Key（公钥）]**。

6 右键单击 **[Trusted Root Certification Authorities（受信任的根证书颁发机构）]**，然后选择 **[Import（导入）]**。

7 按照向导中的提示导入根证书（如 `rootCA.cer`）并单击 **[OK（确定）]**。

8 关闭 [Group Policy（组策略）] 窗口。

此时，域中的所有系统在其信任的根存储中都有一个根证书的副本。

下一步

如果中间证书颁发机构 (CA) 为您颁发了智能卡登录或域控制器证书，请将此中间证书添加到 Active Directory 中的中间证书颁发机构组策略中。请参阅第 25 页，“将中间证书添加到中间证书颁发机构”。

将中间证书添加到中间证书颁发机构

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

步骤

1 在 Active Directory 服务器中，选择 **[Start（开始）] > [All Programs（所有程序）] > [Administrative Tools（管理工具）] > [Active Directory Users and Computers（Active Directory 用户和计算机）]**.

2 右键单击域，然后单击 **[Properties（属性）]**。

3 在 **[Group Policy（组策略）]** 选项卡上，单击 **[Open（打开）]** 以打开组策略管理插件。

4 右键单击 **[Default Domain Policy（默认域策略）]**，然后单击 **[Edit（编辑）]**。

5 展开 **[Computer Configuration（计算机配置）]** 区域，然后打开 **[Windows Settings（Windows 设置）\Security Settings（安全设置）\Public Key（公钥）]**。

6 右键单击 **[Intermediate Certification Authorities（中间证书颁发机构）]**，然后选择 **[Import（导入）]**。

7 按照向导中的提示导入中间证书（如 `intermediateCA.cer`）并单击 **[OK（确定）]**。

8 关闭 [Group Policy（组策略）] 窗口。

此时，域中的所有系统在其中间证书颁发机构存储区中都有一个中间证书的副本。

将根证书添加到 Enterprise NTAuth 存储

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

步骤

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

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

此时该 CA 即为颁发此类证书的受信任机构。

安装 View Composer 4

要使用 View Composer，您需要创建一个 View Composer 数据库、在 vCenter Server 上安装 View Composer 服务并优化您的 View 基础架构以支持 View Composer。

View Composer 是可选功能。如果您计划部署链接克隆桌面池，请安装 View Composer。

您必须通过许可来安装和使用 View Composer 功能。

本章讨论了以下主题：

准备 View Composer 数据库

您必须创建一个数据库和数据源名 (Data Source Name, DSN) 来存储 View Composer 数据。

View Composer 服务中不包含数据库。如果 vCenter Server 计算机或网络环境中不存在数据库实例，您必须安装一个数据库实例。安装数据库实例后，需要将 View Composer 数据库添加到实例。

您可以将 View Composer 数据库添加到 vCenter Server 数据库所在的实例。您可以在本地（vCenter Server 所在的 Windows Server 计算机）或远程位置（连接网络的 Linux、UNIX 或 Windows Server 计算机）配置数据库。

View Composer 数据库存储有关 View Composer 所用连接和组件的信息：

- vCenter Server 连接
- Active Directory 连接
- View Composer 部署的链接克隆桌面
- View Composer 创建的副本

每个 View Composer 服务实例都必须有自己的 View Composer 数据库。多个 View Composer 服务不能共享一个 View Composer 数据库。

有关支持的数据库版本列表，请参阅第 10 页，“View Composer 的数据库要求”。

要将 View Composer 数据库添加到已安装的数据库实例中，请选择下面一种操作过程。

- 为 View Composer 创建 SQL Server 数据库第 28 页，

  View Composer 可以将链接克隆桌面信息存储在 SQL Server 数据库中。您可以将数据库添加到现有 SQL Server 并为其配置 ODBC 数据源，从而创建一个 View Composer 数据库。

- 为 View Composer 创建 Oracle 数据库第 29 页，

  View Composer 可以将链接克隆桌面信息存储在 Oracle 11g 或 10g 数据库中。您可以将 View Composer 数据库添加到现有 Oracle 实例并为其配置 ODBC 数据源，从而创建一个 View Composer 数据库。您可以使用 Oracle Database Configuration Assistant 或运行 SQL 语句来添加新的 View Composer 数据库。

为 View Composer 创建 SQL Server 数据库

View Composer 可以将链接克隆桌面信息存储在 SQL Server 数据库中。您可以将数据库添加到现有 SQL Server 并为其配置 ODBC 数据源，从而创建一个 View Composer 数据库。

将 View Composer 数据库添加到 SQL Server

您可以向现有 Microsoft SQL Server 实例添加新的 View Composer 数据库，以存储 View Composer 的链接克隆数据。

如果该数据库与 vCenter Server 位于同一系统中，则您可以使用集成 Windows 身份验证（Integrated Windows Authentication）安全模式。如果数据库位于远程系统中，您将无法使用这种方式进行身份验证。

前提条件

- 确认已在 vCenter Server 计算机或网络环境中安装了受支持的 SQL Server 版本。有关详细信息，请参阅第 10 页，“View Composer 的数据库要求”。
- 确认您是使用 SQL Server Management Studio 或 SQL Server Management Studio Express 创建和管理数据源的。您可以从以下网站下载并安装 SQL Server Management Studio Express：

  http://www.microsoft.com/downloadS/details.aspx?familyid=C243A5AE-4BD1-4E3D-94B8-5A0F62BF7796

步骤

1 在 vCenter Server 计算机中，选择 **[Start（开始）]** > **[All Programs（所有程序）]** > **[Microsoft SQL Server 2008]** 或 **[Microsoft SQL Server 2005]**。

2 选择 **[SQL Server Management Studio Express]** 并连接到 vSphere Management 的现有 SQL Server 实例。

3 在 [Object Explorer（对象浏览器）] 面板中，右键单击 [Databases（数据库）] 条目并选择 **[New Database（新建数据库）]**。

4 在 [New Database（新建数据库）] 对话框的 [Database name（数据库名）] 文本框中键入一个名称。

  例如：`viewComposer`

5 单击 **[OK（确定）]**。

  SQL Server Management Studio Express 会将您的数据库添加到 [Object Explorer（对象浏览器）] 面板中的 [Database（数据库）] 条目中。

6 退出 Microsoft SQL Server Management Studio Express。

下一步

按照第 28 页，“将 ODBC 数据源添加到 SQL Server”中的说明操作。

将 ODBC 数据源添加到 SQL Server

将 View Composer 数据库添加到 SQL Server 后，您必须配置一个指向新数据库的 ODBC 连接，以使该数据源能够向 View Composer 服务显示。

以下说明假定您在 Windows Server 2003 SP2 上配置 ODBC 数据源。

前提条件

完成第 28 页，“将 View Composer 数据库添加到 SQL Server”中介绍的步骤。

步骤

1 在 vCenter Server 计算机中，选择 **[Start（开始）] > [Administrative Tools（管理工具）] > [Data Source (ODBC)（数据源 (ODBC)）]**。

2 选择 **[System DSN（系统 DSN）]** 选项卡。

3 单击 **[Add（添加）]**，然后从列表中选择 **[SQL Native Client（SQL 本地客户端）]**。

4 单击 **[Finish（完成）]**。

5 在 [Create a New Data Source to SQL Server（创建 SQL Server 的新数据源）] 设置向导中，键入 View Composer 数据库名和描述。

例如：`ViewComposer`

6 在 [Server（服务器）] 文本框中，键入 SQL Server 数据库名。

请使用*主机名\服务器名*格式，其中*主机名*是计算机名，*服务器名*是 SQL Server 实例。

例如：`VCHOST1\SQLEXP_VIM`

7 单击 **[Next（下一步）]**。

8 请确保已选中 **[Connect to SQL Server to obtain default settings for the additional configuration options（连接到 SQL Server 以获得其他配置选项的默认设置）]** 复选框，且选择了一个身份验证选项。

选项	描述
Windows NT authentication（Windows NT 身份验证）	如果正在使用 SQL Server 本地实例，请选择该选项。该选项也被认为是受信任的身份验证。只有在 vCenter Server 计算机上运行 SQL Server 时才支持 Windows NT 身份验证。
SQL Server authentication（SQL Server 身份验证）	使用 SQL Server 的远程实例时请选择该选项。Windows NT 身份验证在远程 SQL Server 中不受支持。

9 单击 **[Next（下一步）]**。

10 选择 **[Change the default database to（将默认数据库更改为）]** 复选框并从列表中选择 View Composer 数据库的名称。

例如：`ViewComposer`

11 完成并关闭 [Microsoft ODBC Data Source Administrator（Microsoft ODBC 数据源管理器）] 向导。

下一步

在 vCenter Server 计算机上安装新的 View Composer 服务。请参阅第 32 页，“安装 View Composer 服务”。

为 View Composer 创建 Oracle 数据库

View Composer 可以将链接克隆桌面信息存储在 Oracle 11g 或 10g 数据库中。您可以将 View Composer 数据库添加到现有 Oracle 实例并为其配置 ODBC 数据源，从而创建一个 View Composer 数据库。您可以使用 Oracle Database Configuration Assistant 或运行 SQL 语句来添加新的 View Composer 数据库。

- 将 View Composer 数据库添加到 Oracle 11g 或 10g 第 30 页，

  可以使用 Oracle Database Configuration Assistant 将新的 View Composer 数据库添加到现有的 Oracle 11g 或 10g 实例。

- 使用 SQL 语句将 View Composer 数据库添加到 Oracle 实例第 31 页，

  View Composer 数据库必须拥有特定的表空间和特权。您可以使用 SQL 语句在 Oracle 11g 或 10g 数据库实例中创建 View Composer 数据库。

- 为 View Composer 配置 Oracle 数据库用户第 31 页，

  默认情况下，运行 View Composer 数据库的用户已拥有 Oracle 系统管理员权限。要限制运行 View Composer 数据库的用户的安全权限，必须为 Oracle 数据库用户配置特定的权限。

- 将 ODBC 数据源添加到 Oracle 11g 或 10g 第 32 页，

  将 View Composer 数据库添加到 Oracle 11g 或 10g 实例后，您必须配置一个指向新数据库的 ODBC 连接，以使该数据源能向 View Composer 服务显示。

将 View Composer 数据库添加到 Oracle 11g 或 10g

可以使用 Oracle Database Configuration Assistant 将新的 View Composer 数据库添加到现有的 Oracle 11g 或 10g 实例。

前提条件

确认已在 vCenter Server 计算机上安装了受支持的 Oracle 11g 或 10g 版本。请参阅第 10 页，“View Composer 的数据库要求”。

步骤

1 在 vCenter Server 计算机中，启动 **[Database Configuration Assistant（数据库配置助理）]**。

数据库版本	操作
Oracle 11g	选择 **[Start（开始）] > [All Programs（所有程序）] > [Oracle-OraDb11g_home] > [Configuration and Migration Tools（配置和迁移工具）] > [Database Configuration Assistant（数据库配置助理）]**。
Oracle 10g	选择 **[Start（开始）] > [All Programs（所有程序）] > [Oracle-OraDb10g_home] > [Configuration and Migration Tools（配置和迁移工具）] > [Database Configuration Assistant（数据库配置助理）]**。

2 在 [Operations（操作）] 页面上，选择 **[Create a database（创建数据库）]**。

3 在 [Database Templates（数据库模板）] 页面上，选择 **[General Purpose or Transaction Processing（一般用途或事务处理）]** 模板。

4 在 [Database Identification（数据库标识）] 页面上，键入全局数据库名称和 Oracle 系统标识符 (System Identifier, SID) 前缀。

  为简化起见，您可以为这两项使用相同的值。

5 在 [Management Options（管理选项）] 页面上，单击 **[Next（下一步）]** 接受默认设置。

6 在 [Database Credentials（数据库凭据）] 页面上，选择 **[Use the Same Administrative Passwords for All Accounts（为所有帐户使用相同管理密码）]** 并键入密码。

7 在其余的配置页面上，均单击 **[Next（下一步）]** 接受默认设置。

8 在 [Creation Options（创建选项）] 页面上，请验证是否已选中 **[Create Database（创建数据库）]**选项并单击 **[Finish（完成）]**。

9 在 [Confirmation（确认）] 页面中，查看选项并单击 **[OK（确定）]**。

  配置工具会创建数据库。

10 在 [Database Creation Complete（数据库创建完成）] 页面上，单击 **[OK（确定）]**。

下一步

按照第 32 页，“将 ODBC 数据源添加到 Oracle 11g 或 10g”中的说明操作。

使用 SQL 语句将 View Composer 数据库添加到 Oracle 实例

View Composer 数据库必须拥有特定的表空间和特权。您可以使用 SQL 语句在 Oracle 11g 或 10g 数据库实例中创建 View Composer 数据库。

在创建数据库时，您可以自定义数据和日志文件的位置。

前提条件

确认已在 vCenter Server 计算机上安装了受支持的 Oracle 11g 或 10g 版本。有关详细信息，请参阅第 10 页，“View Composer 的数据库要求”.

步骤

1 使用系统帐户登录到 SQL*Plus 会话。

2 执行以下 SQL 语句创建数据库。

```
CREATE SMALLFILE TABLESPACE "VCMP" DATAFILE '/u01/app/oracle/oradata/vcdb/vcmp01.dbf'
SIZE 512M AUTOEXTEND ON NEXT 10M MAXSIZE UNLIMITED LOGGING EXTENT MANAGEMENT LOCAL SEGMENT
SPACE MANAGEMENT AUTO;
```

在该示例中，`VCMP` 是 View Composer 数据库的示例名称，`vcmp01.dbf` 是数据库文件的名称。

在 Windows 环境中，请为 `vcmp01.dbf` 文件指定符合 Windows 规则的路径。

下一步

如果您希望用特定的安全权限运行 View Composer 数据库，请按照第 31 页，“为 View Composer 配置 Oracle 数据库用户”中的说明操作。

按照第 32 页，“将 ODBC 数据源添加到 Oracle 11g 或 10g”中的说明操作。

为 View Composer 配置 Oracle 数据库用户

默认情况下，运行 View Composer 数据库的用户已拥有 Oracle 系统管理员权限。要限制运行 View Composer 数据库的用户的安全权限，必须为 Oracle 数据库用户配置特定的权限。

前提条件

确认 View Composer 数据库是在 Oracle 11g 或 10g 实例中创建的。

步骤

1 使用系统帐户登录到 SQL*Plus 会话。

2 运行以下 SQL 命令创建具有适当权限的 View Composer 数据库用户。

```
CREATE USER "VCMPADMIN" PROFILE "DEFAULT" IDENTIFIED BY "oracle" DEFAULT TABLESPACE

"VCMP" ACCOUNT UNLOCK;
grant connect to VCMPADMIN;
grant resource to VCMPADMIN;
grant create view to VCMPADMIN;
grant create sequence to VCMPADMIN;
grant create table to VCMPADMIN;
```

```
grant create materialized view to VCMPADMIN;
grant execute on dbms_lock to VCMPADMIN;
grant execute on dbms_job to VCMPADMIN;
grant unlimited tablespace to VCMPADMIN;
```

在此示例中，用户名为 `VCMPADMIN`，View Composer 数据库名称为 `VCMP`。

默认情况下，`resource` 角色已拥有 `create procedure`、`create table` 和 `create sequence` 特权。如果 `resource` 角色没有这些特权，请将其明确指定给 View Composer 数据库用户。

将 ODBC 数据源添加到 Oracle 11g 或 10g

将 View Composer 数据库添加到 Oracle 11g 或 10g 实例后，您必须配置一个指向新数据库的 ODBC 连接，以使该数据源能向 View Composer 服务显示。

以下说明假定您在 Windows Server 2003 SP2 上配置 ODBC 数据源。

前提条件

确认已完成第 30 页，“将 View Composer 数据库添加到 Oracle 11g 或 10g”或第 31 页，“使用 SQL 语句将 View Composer 数据库添加到 Oracle 实例”中的步骤。

步骤

1 在 vCenter Server 计算机中，选择 **[Start（开始）] > [Administrative Tools（管理工具）] > [Data Source (ODBC)（数据源 (ODBC)）]**。

2 从 [Microsoft ODBC Data Source Administrator（Microsoft ODBC 数据源管理器）] 向导中选择 **[System DSN（系统 DSN）]** 选项卡。

3 单击 **[Add（添加）]**，然后从列表中选择适当的 Oracle 驱动程序。

例如：**`OraDb11g_home`**

4 单击 **[Finish（完成）]**。

5 在 [Oracle ODBC Driver Configuration（Oracle ODBC 驱动程序配置）] 对话框中，键入要用于 View Composer 的 DSN、对该数据源的描述以及用于连接数据库的用户 ID。

如果为 Oracle 数据库用户 ID 配置了特定的安全权限，就要指定该用户 ID。

注意 安装 View Composer 服务时会使用 DSN。

6 从下拉菜单中选择 [Global Database Name（全局数据库名称）]，指定 **[TNS Service Name（TNS 服务名）]**。

Oracle 数据库配置助理会指定全局数据库名称。

7 要确认数据源，请单击 **[Test Connection（测试连接）]**，然后单击 **[OK（确定）]**。

下一步

在 vCenter Server 计算机上安装新的 View Composer 服务。请参阅第 32 页，“安装 View Composer 服务”。

安装 View Composer 服务

要使用 View Composer，您必须在 vCenter Server 计算机上安装 View Composer 服务。View Manager 使用 View Composer 在 vCenter Server 中创建并部署链接克隆桌面。

您需要在安装 vCenter Server 的 Windows Server 计算机上安装 View Composer 服务。

前提条件

- 确认您的安装符合第 9 页，“View Composer 的要求”中所述的 View Composer 要求。
- 确认您拥有安装和使用 View Composer 的许可。
- 在 vCenter Server 中，在要存储链接克隆桌面的 ESX 主机或群集上创建一个资源池。
- 如果 View Composer 计算机上运行了 Windows 防火墙，请确保 View Composer 服务与 View Connection Server 通信时所用的端口可以访问。您可以将该端口添加到例外列表中，或者停用本地防火墙服务。安装 View Composer 服务时需要指定该端口。
- 如果 View Composer 计算机上运行了 Windows 防火墙，请确保 VMware Universal File Access (UFA) 服务未被阻止。您可以将 UFA 服务添加到例外列表中，或者停用本地防火墙服务。
- 确认您拥有在 [ODBC Data Source Administrator（ODBC 数据源管理器）] 向导中提供的 DSN、域管理员用户名和密码。安装 View Composer 服务时需要输入此信息。

步骤

1 从 VMware 产品页面 http://www.vmware.com/cn/products/ 将 VMware View Composer 安装程序文件下载到安装了 vCenter Server 的 Windows Server 计算机中。

安装程序文件名为 `VMware-viewcomposer-xxxxxx.exe`，其中 *xxxxxx* 是内部版本号。此安装程序文件可在 64 位和 32 位 Windows Server 操作系统上安装 View Composer 服务。

2 要启动 View Composer 安装程序，请双击安装程序文件。

在 Windows Server 2008 计算机上，您可能需要右键单击安装文件并选择 **[Run As Administrator（以管理员身份运行）]**。

3 接受 VMware 许可条款。

4 接受或更改目标文件夹。

5 键入在 Microsoft 或 Oracle [ODBC Data Source Administrator（ODBC 数据源管理器）] 向导中提供的 View Composer 数据库的 DSN。

例如：**`VMware View Composer`**

注意 如果您没有为 View Composer 数据库配置 DSN，请单击 **[ODBC DSN Setup（ODBC DSN 设置）]** 来配置一个名称。

6 键入您在 [ODBC Data Source Administrator（ODBC 数据源管理器）] 向导中提供的域管理员用户名和密码。

如果为 Oracle 数据库用户配置了特定的安全权限，就要指定该用户名称。

7 键入一个端口号或接受默认值。

View Connection Server 使用此端口与 View Composer 服务通信。

8 提供 SSL 证书。

选项	操作
Create default SSL certificate（创建默认 SSL 证书）	单击此单选按钮可为 View Composer 服务创建一个默认的 SSL 证书。
Use an existing SSL certificate（使用现有 SSL 证书）	如果您拥有 View Composer 服务要使用的 SSL 证书，请单击此单选按钮。从列表中选择一个 SSL 证书。

9 单击 **[Install（安装）]** 和 **[Finish（完成）]** 以完成 View Composer 服务的安装。

VMware View Composer 服务会在 vCenter Server 计算机中启动。

为 View Composer 配置基础架构

您可以利用 vSphere、vCenterServer、ActiveDirectory 和基础架构的其他组件中的功能来优化 View Composer 的性能、可用性和可靠性。

为 View Composer 配置 vSphere 环境

要支持 View Composer，您需要在安装和配置 vCenter Server 、ESX 和其他 vSphere 组件时遵循某些最佳实践。

这些最佳实践可让 View Composer 在 vSphere 环境中高效运行。

- 创建链接克隆虚拟机的路径和文件夹信息后，不要在 vCenter Server 中更改这些信息，请通过 View Administrator 来更改文件夹信息。

  如果您在 vCenter Server 中更改此信息，View Manager 将找不到 vCenter Server 中的虚拟机。

- 确保为 ESX 主机上的 vSwitch 设置所配置的端口数足以支持针对 ESX 主机上所运行的链接克隆虚拟机配置的所有虚拟 NIC。
- 在资源池中部署链接克隆桌面时，请确保您的 vSphere 环境拥有足够的 CPU 和内存来托管所需数量的桌面。使用 vSphere Client 来监视资源池的 CPU 和内存的使用情况。
- 用于 View Composer 链接克隆的群集可包含 8 个以上 ESXi 主机，但必须将副本磁盘存储在 NFS 数据存储中。在 VMFS 数据存储中，您只能存储最多包含 8 个 ESX 主机的群集的副本磁盘。
- 使用 vSphere DRS。DRS 可有效地在您的主机之间分配链接克隆虚拟机。

  注意 链接克隆桌面不支持 Storage vMotion。

View Composer 的其他最佳实践

要确保 View Composer 高效运行，请检查您的动态名称服务 (dynamic name service, DNS) 是否正确运行，并交错时间运行防病毒软件扫描。

通过确保 DNS 解析正常运行，您可以克服由 DNS 错误导致的断续问题。View Composer 服务依靠动态名称解析来与其他计算机通信。要测试 DNS 的运行，可按名称对 Active Directory 和 View Connection Server 计算机执行 Ping 操作。

如果交错运行防病毒软件，链接克隆桌面的性能将不会受到影响。如果同时在所有链接克隆中运行防病毒软件，则存储子系统上的每秒 I/O 操作 (IOPS) 将会过多。这样的频繁活动会影响链接克隆桌面的性能。

5 安装 View Connection Server

要使用 View Connection Server，您需要在支持的计算机上安装软件、配置所需组件并选择性地优化组件。

本章讨论了以下主题：

安装 View Connection Server 软件

根据部署的性能、可用性和安全性需求，您可以安装一个 View Connection Server 实例、View Connection Server 副本实例和安全服务器。您必须至少安装一个 View Connection Server 实例。

安装 View Connection Server 时，需要选择一种安装类型。

标准安装	用新的 View LDAP 配置生成一个 View Connection Server 实例。
副本安装	用从已有实例复制的 View LDAP 配置生成一个 View Connection Server 实例。
安全服务器安装	生成一个可在 Internet 和内部网络间添加一个额外安全保护层的 View Connection Server 实例。

安装 View Connection Server 的前提条件

安装 View Connection Server 前，您必须验证安装环境是否符合特定的安装前提条件。

View Connection Server 需要使用一个有效的 View Manager 许可证密钥。以下许可证密钥可以使用：

- View Manager
- 带 View Composer 和 Local Mode 的 View Manager

您必须将 View Connection Server 主机加入到 Active Directory 域。View Connection Server 支持下列版本的 Active Directory：

- Windows 2000 Active Directory
- Windows 2003 Active Directory
- Windows 2008 Active Directory

View Connection Server 主机不能是域控制器。

注意 View Connection Server 不会且不要求对 Active Directory 进行任何模式或配置更新。

不要在已安装 Windows 终端服务器角色的系统上安装 View Connection Server。您必须从要安装 View Connection Server 的任何系统上移除 Windows 终端服务器。

不要在执行任何其他功能或角色的系统上安装 View Connection Server。例如，不要使用同一系统来托管 vCenter Server。

安装 View Connection Server 的系统必须具有静态 IP 地址。

要运行 View Connection Server 安装程序，您必须使用在系统上具有管理员特权的域用户帐户。

使用新配置安装 View Connection Server

要作为单一服务器或 View Connection Server 副本实例组中的首个实例来安装 View Connection Server，您可以使用标准安装选项。

选择标准选项时，安装程序会创建一个新的本地 View LDAP 配置。安装程序会加载模式定义、目录信息树 (DIT) 定义和 ACL，并初始化数据。

安装后，您可以通过 View Administrator 管理多数 View LDAP 配置数据。View Connection Server 会自动维护部分 View LDAP 条目。

前提条件

- 确认您能够以在安装 View Connection Server 的 Windows Server 计算机上具有管理员特权的域用户身份登录。
- 确认您的安装符合第 7 页，“View Connection Server 的要求”中所述的要求。
- 准备环境以进行安装。请参阅第 35 页，“安装 View Connection Server 的前提条件”。
- 熟悉那些必须在 Windows 防火墙上为 View Connection Server 实例打开的网络端口。请参阅第 38 页，“View Connection Server 的防火墙规则”。

步骤

1 从 VMware 产品页面 http://www.vmware.com/cn/products/ 将 View Connection Server 安装程序文件下载到 Windows Server 计算机。

安装程序的文件名为 `VMware-viewconnectionserver-y.y.y-xxxxxx.exe` 或 `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`，其中 *xxxxxx* 是内部版本号，*y.y.y* 是版本号。

2 要启动 View Connection Server 安装程序，请双击安装程序文件。

3 接受 VMware 许可条款。

4 接受或更改目标文件夹。

5 选择 **[View Standard Server]** 安装选项。

6 接受 Microsoft Active Directory 应用程序模式 (Microsoft Active Directory Application Mode, ADAM) 的 Microsoft 软件补充许可协议 (Microsoft Software Supplemental License Agreement)。

7 如果您要在 Windows Server 2008 上安装 View Connection Server，请选择如何配置 Windows 防火墙服务。

选项	操作
Configure Windows Firewall automatically（自动配置 Windows 防火墙）	让安装程序将 Windows 防火墙配置为允许所需的网络连接。
Do not configure Windows Firewall（不配置 Windows 防火墙）	手动配置 Windows 防火墙规则。

如果在 Windows Server 2003 上安装 View Connection Server，您必须手动配置所需的 Windows 防火墙规则。

8 完成安装向导以完成安装 View Connection Server。

VMware View 服务将安装在 Windows Server 计算机中：

- VMware View Connection Server
- VMware View Framework 组件
- VMware View Message Bus 组件
- VMware View 脚本主机
- VMware View Security Gateway 组件
- VMware View PCoIP 安全网关
- VMware View Web 组件
- VMware VDMDS（提供 View LDAP 目录服务）

有关这些服务的信息，请参阅《VMware View 管理指南》文档。

下一步

在 View Connection Server 上执行初始配置。

如果您计划在部署中包含 View Connection Server 副本实例和安全服务器，您必须通过运行 View Connection Server 安装程序文件来安装每个服务器实例。

如果您是在 Windows Server 2008 操作系统上重新安装 View Connection Server 且拥有一个配置为监视性能数据的数据收集器组，请停止并重新启动数据收集器组。

静默安装 View Connection Server

您可以使用 Microsoft Windows Installer (MSI) 的静默安装功能，在多个 Windows 计算机上执行 View Connection Server 的标准安装。在静默安装中，您需要使用命令行，无需响应向导的提示。

通过静默安装，您可以在大型企业中高效部署 View 组件。

前提条件

- 确认您能够以在安装 View Connection Server 的 Windows Server 计算机上具有管理员特权的域用户身份登录。
- 确认您的安装符合第 7 页，“View Connection Server 的要求”中所述的要求。
- 准备环境以进行安装。请参阅第 35 页，“安装 View Connection Server 的前提条件”。
- 确认安装 View Connection Server 的 Windows 计算机具有 MSI 运行时引擎 2.0 版或更高版本。有关详细信息，请参见 Microsoft 网站。
- 熟悉 MSI 安装程序命令行选项。请参阅第 46 页，“Microsoft Windows Installer 命令行选项”。

- 熟悉 View Connection Server 标准安装可用的静默安装属性。请参阅第 38 页，“View Connection Server 标准安装的静默安装属性”。

步骤

1 从 VMware 产品页面 http://www.vmware.com/cn/products/ 将 View Connection Server 安装程序文件下载到 Windows Server 计算机。

安装程序的文件名为 `VMware-viewconnectionserver-y.y.y-xxxxxx.exe` 或 `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`，其中 *xxxxxx* 是内部版本号，*y.y.y* 是版本号。

2 在 Windows Server 计算机上开启命令提示符。

3 在一行中键入安装命令。

例如：`VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=1"`

VMware View 服务将安装在 Windows Server 计算机中。有关详细信息，请参阅第 36 页，“使用新配置安装 View Connection Server”。

View Connection Server 标准安装的静默安装属性

从命令行执行静默安装时，可以包含特定的 View Connection Server 属性。您必须使用 *属性*=*值* 格式，以便 Microsoft Windows Installer (MSI) 解释属性和值。

表 5–1 在标准安装中静默安装 View Connection Server 的 MSI 属性

MSI 属性	描述	默认值
INSTALLDIR	View Connection Server 软件的安装路径和文件夹。 例如：`INSTALLDIR=""D:\abc\my folder""` 括住路径的两组双引号可允许 MSI 安装程序将空格识别为路径的有效部分。	`%ProgramFiles%\VMware\VMware View\Server`
VDM_SERVER_INSTANCE_TYPE	View 服务器的安装类型包括： ■ **1**. 标准安装 ■ **2**. 副本安装 ■ **3**. 安全服务器安装 ■ **4**. View Transfer Server 安装 例如，要执行标准安装，请定义 `VDM_SERVER_INSTANCE_TYPE=1`	1
FWCHOICE	确定是否为 View Connection Server 实例配置防火墙的 MSI 属性。 值为 1 时表示配置防火墙。值为 2 时表示不配置防火墙。 例如：`FWCHOICE=1`	1

View Connection Server 的防火墙规则

在防火墙上必须为 View Connection Server 实例及安全服务器打开某些端口。

在 Windows Server 2008 上安装 View Connection Server 时，安装程序可为您配置所需的 Windows 防火墙规则（可选）。在 Windows Server 2003 R2 上安装 View Connection Server 时，必须手动配置所需的 Windows 防火墙规则。

表 5–2 在 View Connection Server 安装过程中打开的端口

协议	端口	View Connection Server 实例类型
JMS	TCP 4001 传入	标准和副本
JMSIR	TCP 4100 传入	标准和副本
AJP13	TCP 8009 传入	标准和副本
HTTP	TCP 80 传入	标准、副本和安全服务器

表 5–2 在 View Connection Server 安装过程中打开的端口（续）

协议	端口	View Connection Server 实例类型
HTTPS	TCP 443 传入	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

安装 View Connection Server 副本实例

要提供高可用性和负载平衡功能，您可以安装一个或多个复制现有 View Connection Server 实例的 View Connection Server 实例。在完成副本安装后，现有及新安装的 View Connection Server 实例完全相同。

安装副本实例时，View Manager 会从现有 View Connection Server 实例复制 View LDAP 配置数据。

安装后，View Manager 软件会在副本组中所有 View Connection Server 实例上维护相同的 View LDAP 配置数据。更改一个实例时，更新的信息将复制到其他实例。

如果一个副本实例出现故障，组中的其他实例会继续运行。当出现故障的实例恢复活动时，其配置数据将自动更新，以对故障期间发生的更改进行同步。

注意 复制功能由 View LDAP 提供，LDAP 使用的复制技术与 Active Directory 所用技术相同。

前提条件

- 确认网络上至少已安装并配置了一个 View Connection Server 实例。
- 确认您能够以在计划安装副本实例的 Windows Server 计算机上具有管理员特权的域用户身份登录。
- 如果现有 View Connection Server 实例不在副本实例所在的域中，则域用户还必须拥有安装了现有实例的 Windows Server 计算机的 View Administrator 特权。
- 确认您的安装符合第 7 页，“View Connection Server 的要求”中所述的要求。
- 确认安装 View Connection Server 副本实例的计算机已连接到高性能 LAN。请参阅第 9 页，“View Connection Server 副本实例的网络要求”。
- 准备环境以进行安装。请参阅第 35 页，“安装 View Connection Server 的前提条件”。
- 熟悉那些必须在 Windows 防火墙上为 View Connection Server 实例打开的网络端口。请参阅第 38 页，“View Connection Server 的防火墙规则”。

步骤

1 从 VMware 产品页面 http://www.vmware.com/cn/products/ 将 View Connection Server 安装程序文件下载到 Windows Server 计算机。

安装程序的文件名为 `VMware-viewconnectionserver-y.y.y-xxxxxx.exe` 或 `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`，其中 *xxxxxx* 是内部版本号，*y.y.y* 是版本号。

2 要启动 View Connection Server 安装程序，请双击安装程序文件。

3 接受 VMware 许可条款。

4 接受或更改目标文件夹。

5 选择 **[View Replica Server]** 安装选项。

6 输入当前正在复制的现有 View Connection Server 实例的主机名或 IP 地址。

7 接受 Microsoft Active Directory 应用程序模式 (Microsoft Active Directory Application Mode, ADAM) 的 Microsoft 软件补充许可协议 (Microsoft Software Supplemental License Agreement)。

8 如果您要在 Windows Server 2008 上安装 View Connection Server，请选择如何配置 Windows 防火墙服务。

选项	操作
Configure Windows Firewall automatically（自动配置 Windows 防火墙）	让安装程序将 Windows 防火墙配置为允许所需的网络连接。
Do not configure Windows Firewall（不配置 Windows 防火墙）	手动配置 Windows 防火墙规则。

如果在 Windows Server 2003 R2 上安装 View Connection Server，必须手动配置所需的 Windows 防火墙规则。

9 完成安装向导以完成安装副本实例。

VMware View 服务将安装在 Windows Server 计算机中：

- VMware View Connection Server
- VMware View Framework 组件
- VMware View Message Bus 组件
- VMware View 脚本主机
- VMware View Security Gateway 组件
- VMware View PCoIP 安全网关
- VMware View Web 组件
- VMware VDMDS（提供 View LDAP 目录服务）

有关这些服务的信息，请参阅《VMware View 管理指南》文档。

下一步

您无需在 View Connection Server 副本实例上执行初始配置。副本实例会从现有 View Connection Server 实例继承配置。

如果您是在 Windows Server 2008 操作系统上重新安装 View Connection Server 且拥有一个配置为监视性能数据的数据收集器组，请停止并重新启动数据收集器组。

静默安装 View Connection Server 副本实例

您可以使用 Microsoft Windows Installer (MSI) 的静默安装功能，在多个 Windows 计算机上安装 View Connection Server 副本实例。在静默安装中，您需要使用命令行，无需响应向导的提示。

通过静默安装，您可以在大型企业中高效部署 View 组件。

前提条件

- 确认网络上至少已安装并配置了一个 View Connection Server 实例。
- 要安装副本实例，必须作为具有访问 View Administrator 帐户的凭据的用户登录。View Administrator 帐户是在安装 View Connection Server 的第一个实例时指定的。该帐户可以是本地 Administrators 用户组、域用户或用户组帐户。请参阅第 36 页，“使用新配置安装 View Connection Server”。
- 确认您能够以在计划安装副本实例的 Windows Server 计算机上具有管理员特权的域用户身份登录。
- 如果现有 View Connection Server 实例不在副本实例所在的域中，则域用户还必须拥有安装了现有实例的 Windows Server 计算机的 View Administrator 特权。
- 确认您的安装符合第 7 页，“View Connection Server 的要求”中所述的要求。

- 确认安装 View Connection Server 副本实例的计算机已连接到高性能 LAN。请参阅第 9 页，“View Connection Server 副本实例的网络要求”。
- 准备环境以进行安装。请参阅第 35 页，“安装 View Connection Server 的前提条件”。
- 熟悉 MSI 安装程序命令行选项。请参阅第 46 页，“Microsoft Windows Installer 命令行选项”。
- 熟悉 View Connection Server 副本安装可用的静默安装属性。请参阅第 41 页，“View Connection Server 副本实例的静默安装属性”。

步骤

1 从 VMware 产品页面 http://www.vmware.com/cn/products/ 将 View Connection Server 安装程序文件下载到 Windows Server 计算机。

安装程序的文件名为 `VMware-viewconnectionserver-y.y.y-xxxxxx.exe` 或 `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`，其中 *xxxxxx* 是内部版本号，*y.y.y* 是版本号。

2 在 Windows Server 计算机上开启命令提示符。

3 在一行中键入安装命令。

例如：`VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=2 ADAM_PRIMARY_NAME=cs1.companydomain.com"`

VMware View 服务将安装在 Windows Server 计算机中。有关详细信息，请参阅第 39 页，“安装 View Connection Server 副本实例”。

View Connection Server 副本实例的静默安装属性

从命令行执行 View Connection Server 副本实例静默安装时可以包含特定属性。您必须使用 *属性*=*值* 格式，以便 Microsoft Windows Installer (MSI) 解释属性和值。

表 5–3 静默安装 View Connection Server 副本实例的 MSI 属性

MSI 属性	描述	默认值
INSTALLDIR	View Connection Server 软件的安装路径和文件夹。 例如：`INSTALLDIR=""D:\abc\my folder""` 括住路径的两组双引号可允许 MSI 安装程序将空格识别为路径的有效部分。 此 MSI 属性是可选属性。	`%ProgramFiles%\VMware\VMware View\Server`
VDM_SERVER_INSTANCE_TYPE	View 服务器的安装类型包括： ■ **1**. 标准安装 ■ **2**. 副本安装 ■ **3**. 安全服务器安装 ■ **4**. View Transfer Server 安装 要安装副本实例，请定义 `VDM_SERVER_INSTANCE_TYPE=2` 安装副本时，此 MSI 属性是必要属性。	1
ADAM_PRIMARY_NAME	当前正在复制的现有 View Connection Server 实例的主机名或 IP 地址。 例如：`ADAM_PRIMARY_NAME=cs1.companydomain.com` 此 MSI 属性是必要属性。	无
ADAM_PRIMARY_PORT	当前正在复制的现有 View Connection Server 实例的 View LDAP 端口。 例如：`ADAM_PRIMARY_PORT=cs1.companydomain.com` 此 MSI 属性是可选属性。	无
FWCHOICE	确定是否为 View Connection Server 实例配置防火墙的 MSI 属性。 值为 1 时表示配置防火墙。值为 2 时表示不配置防火墙。 例如：`FWCHOICE=1` 此 MSI 属性是可选属性。	1

配置安全服务器的配对密码

安装安全服务器之前，您必须配置安全服务器配对密码。View Connection Server 安装程序会在安装过程中提示您输入该密码。

安全服务器配对密码是一次性密码，允许安全服务器与 View Connection Server 实例配对。密码被提供给 View Connection Server 安装程序后，就会变成无效密码。

步骤

1 在 View Administrator 中，选择 **[View Configuration（View 配置）] > [Servers（服务器）]**。

2 在 [View Server] 窗格中，选择要与安全服务器配对的 View Connection Server 实例。

3 从 **[More Commands（更多命令）]** 下拉菜单中选择 **[Specify Security Server Pairing Password（指定安全服务器配对密码）]**。

4 在 [Pairing password(配对密码）] 和 [Confirm password（确认密码）] 文本框中分别键入密码并指定密码超时值。

您必须在指定的超时期限内使用密码。

5 单击 **[OK（确定）]** 配置密码。

下一步

安装安全服务器。请参阅第 42 页，“安装安全服务器”。

重要事项 如果您在安全服务器配对密码超时期限内未将其提供给 View Connection Server 安装程序，密码会变为无效，且您需要配置一个新密码。

安装安全服务器

安全服务器是一个 View Connection Server 实例，可在 Internet 和您的内部网络之间添加一层额外的安全保护。您可以安装一个或多个安全服务器，以连接到 View Connection Server 实例。

前提条件

- 确定要使用的拓扑结构类型。例如，确定所用的负载平衡解决方案。确定与安全服务器配对的 View Connection Server 实例是否专供外部网络用户使用。有关更多信息，请参阅《VMware View 体系结构规划指南》文档。

  重要事项 如果使用负载平衡程序，必须为负载平衡程序和每个安全服务器指定静态 IP 地址。例如，如果使用具有两个安全服务器的负载平衡程序，则需要 3 个静态 IP 地址。

- 确认您的安装符合第 7 页，“View Connection Server 的要求”中所述的要求。
- 准备环境以进行安装。请参阅第 35 页，“安装 View Connection Server 的前提条件”。
- 确认已安装并配置要与安全服务器配对的 View Connection Server 实例，且该实例正在运行 View Connection Server 4.6 或更高版本。不能将 View 4.6 或更高版本的安全服务器与旧版 View Connection Server 配对。
- 确认计划安装安全服务器的计算机可以访问要与安全服务器配对的 View Connection Server 实例。
- 配置安全服务器的配对密码。请参阅第 42 页，“配置安全服务器的配对密码”。
- 熟悉外部 URL 的格式。请参阅第 56 页，“为 PCoIP 安全网关和安全加密链路连接配置外部 URL”。
- 熟悉那些必须在 Windows 防火墙上为安全服务器打开的网络端口。请参阅第 38 页，“View Connection Server 的防火墙规则”。

步骤

1 从 VMware 产品页面 http://www.vmware.com/cn/products/ 将 View Connection Server 安装程序文件下载到 Windows Server 计算机。

安装程序的文件名为 `VMware-viewconnectionserver-y.y.y-xxxxxx.exe` 或 `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`，其中 *xxxxxx* 是内部版本号，*y.y.y* 是版本号。

2 要启动 View Connection Server 安装程序，请双击安装程序文件。

3 接受 VMware 许可条款。

4 接受或更改目标文件夹。

5 选择 **[View Security Server]** 安装选项。

6 在 **[Server（服务器）]** 文本框中键入要与安全服务器配对的 View Connection Server 实例的主机域名全称或 IP 地址。

安全服务器会将网络流量转发到此 View Connection Server 实例。

7 在 [Password（密码）] 文本框中键入安全服务器配对密码。

如果密码已过期，可以使用 View Administrator 配置一个新密码，然后在安装程序中键入新密码。

8 在 **[External URL（外部 URL）]** 文本框中，为使用 RDP 或 PCoIP 显示协议的 View Client 键入安全服务器的外部 URL。

URL 必须包含协议、客户端可解析的安全服务器名或 IP 地址以及端口号。在网络外运行的安全加密链路客户端会使用该 URL 连接安全服务器。

例如：`https://view.example.com:443`

9 在 **[PCoIP External URL（PCoIP 外部 URL）]** 文本框中，为使用 PCoIP 显示协议的 View Client 键入安全服务器的外部 URL。

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

例如：`100.200.300.400:4172`

URL 中必须包含能供客户端系统连接到安全服务器的 IP 地址和端口号。仅在安全服务器上安装了 PCoIP 安全网关的情况下，您才可以在该文本框中键入内容。

10 如果您在 Windows Server 2008 上安装安全服务器，请选择如何配置 Windows 防火墙服务。

选项	操作
Configure Windows Firewall automatically（自动配置 Windows 防火墙）	让安装程序将 Windows 防火墙配置为允许所需的网络连接。
Do not configure Windows Firewall（不配置 Windows 防火墙）	手动配置 Windows 防火墙规则。

如果在 Windows Server 2003 R2 上安装安全服务器，必须手动配置所需的 Windows 防火墙规则。

11 完成安装向导以完成安装安全服务器。

安全服务器服务将安装在 Windows Server 计算机中：

- VMware View Security Server
- VMware View Framework 组件
- VMware View Security Gateway 组件
- VMware View PCoIP 安全网关

有关这些服务的信息，请参阅《VMware View 管理指南》文档。

安全服务器会出现在 View Administrator 的 [Security Servers（安全服务器）] 窗格中。

下一步

如果您是在 Windows Server 2008 操作系统上重新安装安全服务器且拥有一个配置为监视性能数据的数据收集器组，请停止并重新启动数据收集器组。

静默安装安全服务器

您可以使用 Microsoft Windows Installer (MSI) 的静默安装功能在多个 Windows 计算机上安装安全服务器。在静默安装中，您需要使用命令行，无需响应向导的提示。

通过静默安装，您可以在大型企业中高效部署 View 组件。

前提条件

- 确定要使用的拓扑结构类型。例如，确定所用的负载平衡解决方案。确定与安全服务器配对的 View Connection Server 实例是否专供外部网络用户使用。有关更多信息，请参阅《VMware View 体系结构规划指南》文档。

  重要事项 如果使用负载平衡程序，必须为负载平衡程序和每个安全服务器指定静态 IP 地址。例如，如果使用具有两个安全服务器的负载平衡程序，则需要 3 个静态 IP 地址。

- 确认您的安装符合第 7 页，“View Connection Server 的要求”中所述的要求。
- 准备环境以进行安装。请参阅第 35 页，“安装 View Connection Server 的前提条件”。
- 确认已安装并配置要与安全服务器配对的 View Connection Server 实例，且该实例正在运行 View Connection Server 4.6 或更高版本。不能将 View 4.6 或更高版本的安全服务器与旧版 View Connection Server 配对。
- 确认计划安装安全服务器的计算机可以访问要与安全服务器配对的 View Connection Server 实例。
- 配置安全服务器的配对密码。请参阅第 42 页，“配置安全服务器的配对密码”。
- 熟悉外部 URL 的格式。请参阅第 56 页，“为 PCoIP 安全网关和安全加密链路连接配置外部 URL”。
- 熟悉那些必须在 Windows 防火墙上为安全服务器打开的网络端口。请参阅第 38 页，“View Connection Server 的防火墙规则”。
- 熟悉 MSI 安装程序命令行选项。请参阅第 46 页，“Microsoft Windows Installer 命令行选项”。
- 熟悉安全服务器可用的静默安装属性。请参阅第 45 页，“安全服务器的静默安装属性”。

步骤

1 从 VMware 产品页面 http://www.vmware.com/cn/products/ 将 View Connection Server 安装程序文件下载到 Windows Server 计算机。

  安装程序的文件名为 `VMware-viewconnectionserver-y.y.y-xxxxxx.exe` 或 `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`，其中 *xxxxxx* 是内部版本号，*y.y.y* 是版本号。

2 在 Windows Server 计算机上开启命令提示符。

3 在一行中键入安装命令。

  例如：
  ```
  VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=3
  VDM_SERVER_NAME=cs1.internaldomain.com VDM_SERVER_SS_EXTURL=https://view.companydomain.com:
  443 VDM_SERVER_SS_PCOIP_IPADDR=10.20.30.40 VDM_SERVER_SS_PCOIP_TCPPORT=4172
  VDM_SERVER_SS_PCOIP_UDPPORT=4172 VDM_SERVER_SS_PWD=secret"
  ```

VMware View 服务将安装在 Windows Server 计算机中。有关详细信息，请参阅第 42 页，“安装安全服务器”。

安全服务器的静默安装属性

当您从命令行静默安装安全服务器时，可以加入某些特定的属性。您必须使用 *属性=值* 格式，以便 Microsoft Windows Installer (MSI) 解释属性和值。

表 5–4 静默安装安全服务器的 MSI 属性

MSI 属性	描述	默认值
INSTALLDIR	View Connection Server 软件的安装路径和文件夹。 例如：`INSTALLDIR=""D:\abc\my folder""` 括住路径的两组双引号可允许 MSI 安装程序将空格识别为路径的有效部分。 此 MSI 属性是可选属性。	`%ProgramFiles %\VMware\VMware View\Server`
VDM_SERVER_INSTANCE_TYPE	View 服务器的安装类型包括： ■ **1**. 标准安装 ■ **2**. 副本安装 ■ **3**. 安全服务器安装 ■ **4**. View Transfer Server 安装 要安装安全服务器，请定义 `VDM_SERVER_INSTANCE_TYPE=3` 安装安全服务器时，此 MSI 属性是必要属性。	1
VDM_SERVER_NAME	与安全服务器配对的现有 View Connection Server 实例的主机名或 IP 地址。 例如：`VDM_SERVER_NAME=cs1.internaldomain.com` 此 MSI 属性是必要属性。	无
VDM_SERVER_SS_EXTURL	安全服务器的外部 URL。URL 必须包含协议、可外部解析的安全服务器名和端口号 例如：`VDM_SERVER_SS_EXTURL=https://view.companydomain.com:443` 此 MSI 属性是必要属性。	无
VDM_SERVER_SS_PWD	安全服务器配对密码。 例如：`VDM_SERVER_SS_PWD=secret` 此 MSI 属性是必要属性。	无
FWCHOICE	确定是否为 View Connection Server 实例配置防火墙的 MSI 属性。 值为 1 时表示配置防火墙。值为 2 时表示不配置防火墙。 例如：`FWCHOICE=1` 此 MSI 属性是可选属性。	1
VDM_SERVER_SS_PCOIP_IPADDR	PCoIP 安全网关外部 IP 地址。该属性只在安装安全服务器的操作系统为 Windows Server 2008 R2 或更高版本时才可用。 例如：`VDM_SERVER_SS_PCOIP_IPADDR=10.20.30.40` 如果您打算使用 PCoIP 安全网关组件，此属性为必要属性。	无
VDM_SERVER_SS_PCOIP_TCPPORT	PCoIP 安全网关外部 TCP 端口号。该属性只在安装安全服务器的操作系统为 Windows Server 2008 R2 或更高版本时才可用。 例如：`VDM_SERVER_SS_PCOIP_TCPPORT=4172` 如果您打算使用 PCoIP 安全网关组件，此属性为必要属性。	无
VDM_SERVER_SS_PCOIP_UDPPORT	PCoIP 安全网关外部 UDP 端口号。该属性只在安装安全服务器的操作系统为 Windows Server 2008 R2 或更高版本时才可用。 例如：`VDM_SERVER_SS_PCOIP_UDPPORT=4172` 如果您打算使用 PCoIP 安全网关组件，此属性为必要属性。	无

Microsoft Windows Installer 命令行选项

要以静默方式安装 View 组件，您必须使用 Microsoft Windows Installer (MSI) 命令行选项和属性。View 组件安装程序是 MSI 程序，使用标准的 MSI 功能。您也可以使用 MSI 命令行选项静默卸载 View 组件。

有关 MSI 的详细信息，请参见 Microsoft 网站。有关 MSI 命令行选项的信息，请在 Microsoft Developer Network (MSDN) Library 网站上搜索 MSI 命令行选项。要了解 MSI 命令行的用法，可以在安装了 View 组件的计算机中打开一个命令提示符，并键入 `msiexec /?`。

要以静默方式运行 View 组件安装程序，应当首先禁用引导程序，因为该程序会将安装程序提取到一个临时目录中并启动交互式安装。

表 5–5 显示了用于控制安装程序的引导程序的命令行选项。

表 5–5 View 组件引导程序的命令行选项

选项	描述
`/s`	禁用引导程序的初始屏幕和提取对话框，从而避免显示交互式对话框。 例如：`VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s` 运行静默安装时，必须使用 `/s` 选项。在以上示例中，*xxxxxx* 是内部版本号，*y.y.y* 是版本号。
`/v" MSI 命令行选项"`	指示安装程序传递您在命令行中作为一组选项输入的、括在双引号中的字符串，以便 MSI 进行解释。您必须将命令行条目括在双引号中。在 `/v` 后面及命令行末尾加双引号。 例如：`VMware-viewagent-y.y.y-xxxxxx.exe /s /v"命令行选项"` 要指示 MSI 安装程序解释一个包含空格的字符串，应当将该字符串括在两组双引号中。例如，您可能需要将 View 组件安装在名称中包含空格的安装路径下。 例如：`VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"命令行选项 INSTALLDIR=""d:\abc\my folder"""` 在此示例中，MSI 安装程序会传递安装目录的路径，而不会试图将该字符串解释为两个命令行选项。请注意，最后一个双引号的作用是将整个命令行括住。 运行静默安装时，必须要使用 `/v"命令行选项"` 选项。

您可以通过将命令行选项和 MSI 属性值传递给 MSI 安装程序 `msiexec.exe`，来控制静默安装过程的提示。MSI 安装程序中包含 View 组件的安装代码。安装程序使用您在命令行中输入的值和选项来解释特定于 View 组件的安装选择和设置选项。

表 5–6 显示了传递给 MSI 安装程序的命令行选项和 MSI 属性值。

表 5–6 MSI 命令行选项和 MSI 属性

MSI 选项或属性	描述
`/qn`	指示 MSI 安装程序不显示安装程序向导页面。 例如，您可能希望采用默认的安装选项和功能，以静默方式安装 View Agent： `VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn"` 在以上示例中，*xxxxxx* 是内部版本号，*y.y.y* 是版本号。 或者，也可以使用 `/qb` 选项在非交互式自动安装中显示向导页面。随着安装的进行，向导页面会出现，但是您无法对其进行回应。 运行静默安装时，必须要使用 `/qn` 或 `/qb` 选项。
`INSTALLDIR`	指定 View 组件的可选安装路径。 采用 *安装目录*=*路径* 格式来指定安装路径。如果您要将 View 组件安装在默认路径下，则可以忽略此 MSI 属性。 此 MSI 属性为可选属性。

表 5–6 MSI 命令行选项和 MSI 属性（续）

MSI 选项或属性	描述
ADDLOCAL	确定要安装的特定于组件的功能。在交互式安装中，View 安装程序会显示自定义安装选项供您选择。利用 ADDLOCAL 这一 MSI 属性，您便可以在命令行中指定这些安装选项。 要安装所有可用的自定义安装选项，请输入 ADDLOCAL=ALL。 例如：VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn ADDLOCAL=ALL" 如果不使用 MSI 属性 ADDLOCAL，则会安装默认安装选项。 要单独指定各个安装选项，可输入以逗号分隔的安装选项名称列表。不要在名称之间输入空格。采用以下格式：*ADDLOCAL=值,值,值...*。 例如，您可能希望在客户操作系统安装 View Agent 以及 View Composer Agent 和 PCoIP 功能： VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn ADDLOCAL=Core,SVIAgent,PCoIP" **注意** Core 功能是 View Agent 中的必需功能。 此 MSI 属性为可选属性。
REBOOT	您可以使用 REBOOT=ReallySuppress 选项允许系统配置任务在系统重新启动之前完成。 此 MSI 属性为可选属性。
/l*v *日志文件*	将日志信息写入具有详细输出的指定日志文件。 例如：/l*v ""%TEMP%\vmmsi.log"" 该示例会生成详细的日志文件，类似于在交互式安装过程中生成的日志文件。 可以利用此选项记录专门应用在您的安装中的自定义功能。您可以利用记录的信息在以后的静默安装中指定安装功能。 /l*v 是可选选项。

用 MSI 命令行选项静默卸载 View 产品

您可以使用 Microsoft Windows Installer (MSI) 命令行选项卸载 View 组件。

语法

```
msiexec.exe
/qb
/x
product_code
```

选项

/qb 选项用于显示卸载进度条。要取消显示卸载进度条，请将 /qb 选项替换为 /qn 选项。

/x 选项用于卸载 View 组件。

*产品代码*字符串用于将 View 组件产品文件显示给 MSI 卸载程序。您可以在安装时创建的 %TEMP%\vmmsi.log 文件中搜索 ProductCode 以找到*产品代码*字符串。

关于 MSI 命令行选项的信息，请参阅第 46 页，“Microsoft Windows Installer 命令行选项”。

示例

卸载一个 View Connection Server 实例。

```
msiexec.exe /qb /x {D6184123-57B7-26E2-809B-090435A8C16A}
```

配置 vCenter Server 和 View Composer 的用户帐户

要结合使用 vCenter Server 和 View Manager，您必须配置一个有权在 vCenter Server 中执行操作的用户帐户。要使用 View Composer，您还必须为该 vCenter Server 用户授予额外的特权。要管理以本地模式使用的桌面，除 View Manager 和 View Composer 中所需的特权外，您还必须为该用户授予额外的特权。

您还必须在 Active Directory 中为 View Composer 创建一个域用户。请参阅第 23 页，“为 View Composer 创建用户帐户”。

在何处使用 View Composer 的 vCenter Server 用户和域用户

创建并配置这两个用户帐户后，您需要在 View Administrator 中指定用户名。

- 将 vCenter Server 添加到 View Manager 时，需要指定一个 vCenter Server 用户。
- 为 vCenter Server 配置 View Composer 时，需要为 View Composer 指定一个域用户。
- 您需要在创建链接克隆池时指定 View Composer 的域用户。

为 View Manager、View Composer 和本地模式配置 vCenter Server 用户

要配置一个使 View Manager 有权在 vCenter Server 中操作的用户帐户，您必须为该用户分配一个拥有合适特权的角色。要在 vCenter Server 中使用 View Composer 服务，您必须为用户帐户授予额外的特权。要管理以本地模式使用的桌面，您必须向用户帐户授予 View Manager、View Composer 和本地模式特权。

要支持 View Composer，您还需要让此用户成为 vCenter Server 计算机上的本地系统管理员。

前提条件

- 在 Active Directory 中，在 View Connection Server 域或受信任的域中创建一个用户。请参阅第 22 页，“为 vCenter Server 创建用户帐户”。
- 熟悉此用户帐户所需的特权。请参阅第 50 页，“vCenter Server 用户所需的 View Manager 特权”。
- 如果使用 View Composer，请熟悉所需的其他特权。请参阅第 50 页，“vCenter Server 用户所需的 View Composer 特权”。
- 如果您是管理本地桌面，请熟悉所需的其他特权。请参阅第 51 页，“vCenter Server 用户所需的本地模式特权”。

步骤

1 在 vCenter Server 中，为用户准备一个拥有所需特权的角色。

   - 您可以使用 vCenter Server 中预定义的 Administrator 角色。该角色可以执行 vCenter Server 中所有的操作。
   - 如果您使用 View Composer，您可以创建一个权利有限的角色，为其授予 View Manager 和 View Composer 执行 vCenter Server 操作所需的最低特权。

     在 vSphere Client 中，单击 **[Home（主页）] > [Roles（角色）] > [Add Role（添加角色）]**，输入角色名称，如 **`View Composer Administrator`**，然后选择角色对应的特权。

     此角色必须拥有 View Manager 和 View Composer 在 vCenter Server 中运行所需的所有特权。
   - 如果要管理本地桌面，您可以创建一个权利有限的角色，为其授予 View Manager、View Composer 和本地模式功能执行 vCenter Server 操作所需的最低特权。

在 vSphere Client 中，单击 **[Home（主页）] > [Roles（角色）] > [Add Role（添加角色）]**，输入角色名称，如 **`Local Mode Administrator`**，然后选择角色对应的特权。

此角色必须拥有 View Manager、View Composer 和本地模式功能在 vCenter Server 中运行所需的所有特权。

- 如果您使用不带 View Composer 的 View Manager 且不管理本地桌面，您可以创建一个权利更小的角色，仅为其授予 View Manager 执行 vCenter Server 操作所需的最小特权。

  在 vSphere Client 中，单击 **[Home（主页）] > [Roles（角色）] > [Add Role（添加角色）]**，输入角色名称，如 **`View Manager Administrator`**，然后选择角色对应的特权。

2 在 vSphere Client 中，右键单击清单顶层的 vCenter Server，单击 **[Add Permission（添加权限）]**，然后添加 vCenter Server 用户。

注意 您必须在 vCenter Server 级别定义 vCenter Server 用户。

3 在下拉菜单中选择您创建的管理员角色、View Composer 或 View Manager 角色，并将其分配给 vCenter Server 用户。

4 如果您使用 View Composer，则需要在 vCenter Server 计算机上将 vCenter Server 用户帐户添加到本地系统管理员用户组中。

View Composer 要求 vCenter Server 用户在 vCenter Server 计算机中是系统管理员。

下一步

通过 View Administrator 将 vCenter Server 添加到 View Manager 时，可以指定 vCenter Server 用户。请参阅第 52 页，“将 vCenter Server 实例添加到 View Manager”。

vCenter Server 用户所需的 View Manager 特权

vCenter Server 用户必须具有足够的特权才能使 View Manager 在 vCenter Server 中运行 。为 vCenter Server 用户创建一个拥有所需特权的 View Manager 角色。

表 5–7 View Manager 特权

特权组	您需要启用的特权
Folder（文件夹）	**Create Folder（创建文件夹）** **Delete Folder（删除文件夹）**
Virtual Machine（虚拟机）	在 **[Configuration（配置）]** 中： ■ **Add or remove device（添加或移除设备）** ■ **Advanced（高级）** ■ **Modify device settings（修改设备设置）** 在 **[Interaction（交互）]** 中： ■ **Power Off（关闭）** ■ **Power On（启动）** ■ **Reset（重置）** ■ **Suspend（挂起）** 在 **[Inventory（清单）]** 中： ■ **Create new（新建）** ■ **Remove（移除）** 在 **[Provisioning（置备）]** 中： ■ **Customize（自定义）** ■ **Deploy template（部署模板）** ■ **Read customization specifications（读取自定义规范）**
Resource（资源）	**Assign virtual machine to resource pool（将虚拟机分配给资源池）**

vCenter Server 用户所需的 View Composer 特权

要支持 View Composer，vCenter Server 用户还必须拥有支持 View Manager 所需特权以外的更多特权。为 vCenter Server 用户创建一个拥有 View Manager 特权和以下额外特权的 View Composer 角色。

表 5–8 View Composer 特权

特权组	您需要启用的特权
Datastore（数据存储）	**Allocate space（分配空间）** **Browse Datastore（浏览数据存储）** **Low level file operations（低级别文件操作）**
Virtual machine（虚拟机）	**[Inventory（清单）]**（全部） **[Configuration（配置）]**（全部） **[State（状态）]**（全部） 在 **[Provisioning（置备）]** 中： ■ **Clone virtual machine（克隆虚拟机）** ■ **Allow disk access（允许访问磁盘）**
Resource（资源）	**Assign virtual machine to resource pool（将虚拟机分配给资源池）**

表 5–8 View Composer 特权（续）

特权组	您需要启用的特权
Global（全局）	**Enable Methods（启用方法）** **Disable Methods（禁用方法）** **System tag（系统标记）**
Network（网络）	（全部）

vCenter Server 用户所需的本地模式特权

要管理以本地模式使用的桌面，vCenter Server 用户还必须拥有支持 View Manager 和 View Composer 所需特权以外的更多特权。为 vCenter Server 用户创建一个拥有 View Manager 特权、View Composer 特权和本地模式特权的 Local Mode Administrator 角色。

表 5–9 本地模式特权

特权组	您需要启用的特权
Global（全局）	**设置自定义属性**
Host（主机）	在 **[Configuration（配置）]** 中： **系统管理**

首次配置 View Connection Server

安装 View Connection Server 后，您必须安装产品许可证、将 vCenter Server 和 View Composer 服务添加到 View Manager、添加安全服务器（如果使用）以及设置在您的网络外运行的客户端桌面的外部 URL。

View Administrator 和 View Connection Server

View Administrator 为 View Manager 提供了一个管理界面。

依据您的 View 部署，您可以使用一个或多个 View Administrator 界面。

- 使用一个 View Administrator 界面来管理与单个独立 View Connection Server 或副本 View Connection Server 实例组相关的 View 组件。

  您可以使用任意副本实例的 IP 地址登录 View Administrator。

- 您必须使用单独的 View Administrator 界面来管理每个独立的 View Connection Server 实例和每个副本 View Connection Server 实例组的 View 组件。

您也可以用 View Administrator 管理与 View Connection Server 相关联的安全服务器和 View Transfer Server 实例。

- 每个安全服务器均与一个 View Connection Server 实例相关联。
- 每个 View Transfer Server 实例均可与副本实例组中的任意 View Connection Server 实例进行通信。

登录 View Administrator

要执行初始配置任务，您必须登录 View Administrator。

前提条件

确认您使用的是 View Administrator 支持的 Web 浏览器。请参阅第 9 页，“View Administrator 的要求”。

步骤

1 打开 Web 浏览器并输入以下 URL，其中 *服务器* 是 View Connection Server 实例的主机名或 IP 地址。

`https://服务器/admin`

您可以通过安全连接 (SSL) 来访问 View Administrator。当您第一次连接时，Web 浏览器可能会显示一个页面，警告与该地址相关联的安全证书不是由受信任的证书颁发机构颁发的。这是正常现象，因为 View Connection Server 附带的默认证书是一个自签证书。

2 单击 **[Ignore（忽略）]** 继续使用当前 SSL 证书。

3 使用 View Connection Server 计算机上的管理员凭据登录。

最初，View Connection Server 计算机中本地管理员组 (BUILTIN\Administrators) 的所有成员用户都可以登录 View Administrator。

登录到 View Administrator 后，您可以使用 **[View Configuration（View 配置）] > [Administrators（管理员）]** 更改具有 View Administrators 角色的用户和用户组列表。

安装 View Connection Server 许可证密钥

使用 View Connection Server 前，必须要输入产品的许可证密钥。

首次登录时，View Administrator 会显示 [Product Licensing and Usage（产品许可和使用情况）] 页面。

安装许可证密钥后，View Administrator 将在您登录时显示仪表板页面。

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

注意 View Connection Server 需要使用一个有效的 View 5.0 许可证密钥。从 VMware View 4.0 版本开始，VMware View 许可证密钥的长度为 25 个字符。

步骤

1 如果未显示 [View Configuration（View 配置）] 视图，请单击左侧导航窗格的 **[View Configuration（View 配置）]**。

2 单击 **[Product Licensing and Usage（产品许可和使用情况）]**。

3 在 [Product Licensing（产品许可）] 表中，单击 **[Edit License（编辑许可证）]** 并输入 View Manager 许可证序列号。

4 单击 **[OK（确定）]**。

5 验证许可证的过期日期。

将 vCenter Server 实例添加到 View Manager

您必须配置 View Manager，使其连接到 View 部署中的 vCenter Server 实例。vCenter Server 可创建和管理 View Manager 用作桌面源的虚拟机。

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

前提条件

- 安装 View Connection Server 产品许可证密钥。
- 准备一个有权在 vCenter Server 中执行支持 View Manager 所需操作的 vCenter Server 用户。要使用 View Composer，您必须为该用户授予额外的特权。要管理在本地模式下使用的桌面，除 View Manager 和 View Composer 所需的特权之外，您还必须为用户授予额外特权。

  请参阅第 48 页，“为 View Manager、View Composer 和本地模式配置 vCenter Server 用户”。

- 如果您计划用安全通道 (SSL) 将 View Connection Server 连接到 vCenter Server 实例，请在 vCenter Server 主机上安装服务器 SSL 证书。

步骤

1 在 View Administrator 中，单击 **[View Configuration（View 配置）] > [Servers（服务器）]**。

2 在 [vCenter Server] 面板中，单击 **[Add（添加）]**。

3 在服务器地址文本框中键入 vCenter Server 实例的主机域名全称 (FQDN) 或 IP 地址。

FQDN 包含主机名和域名。例如，在 ***个人服务器主机.公司域.com*** 这段 FQDN 中， ***个人服务器主机*** 是主机名，***公司域.com*** 则是域名。

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

4 键入 vCenter Server 用户的名称。

5 键入 vCenter Server 用户密码。

6 （可选）键入该 vCenter Server 实例的描述。

7 要使用安全通道 (SSL) 连接到 vCenter Server 实例，请确保已选中 **[Connect using SSL（使用 SSL 连接）]**。SSL 连接是默认设置。

8 键入 TCP 端口号。

默认端口为 443。

9 （可选）单击 **[Advanced（高级）]** 来配置 vCenter Server 中的最大并发池操作数量。

a 设置并行部署操作的最大数量。

此设置确定了 View Manager 可在此 vCenter Server 实例中部署完整虚拟机的并发请求的最大数量。默认值为 8。此设置不控制链接克隆部署。

b 设置并行电源操作的最大数量。

该设置确定该 vCenter Server 实例中由 View Manager 管理的虚拟机允许同时发生的电源操作（启动、关机、挂起等）的最大数量。默认值为 5。此设置控制完整虚拟机和链接克隆虚拟机的电源操作。

10 选择是否配置 View Composer。

选项	操作
未使用 View Composer	单击 **[OK（确定）]**。
正在使用 View Composer	配置 View Composer 设置。

下一步

如果该 View Connection Server 实例或副本 View Connection Server 实例组使用多个 vCenter Server 实例，请重复该过程添加其他 vCenter Server 实例。

为 vCenter Server 配置 View Composer 设置

要使用 View Composer，您为 View Manager 配置的初始设置必须与 vCenter Server 中所安装 View Composer 服务的设置相匹配。View Composer 是 View Manager 的一项功能，但它提供的服务直接运行在 vCenter Server 中的虚拟机上。

注意 如果您没有使用 View Composer，则可以跳过此任务。

前提条件

- 您的 Active Directory 管理员必须创建一个域用户，并使该用户具有在包含链接克隆的 Active Directory 域中添加和移除虚拟机的权限。要管理 Active Directory 中的链接克隆虚拟机帐户，域用户必须拥有**[Create Computer Objects（创建计算机对象）]**、**[Delete Computer Objects（删除计算机对象）]**和**[Write All Properties（写入全部属性）]**权限。

  请参阅第 23 页，“为 View Composer 创建用户帐户”。

- 您必须对 View Manager 进行配置，使其连接到 vCenter Server。请参阅第 52 页，“将 vCenter Server 实例添加到 View Manager”。

步骤

1 在 View Administrator 中，打开 [Edit vCenter Server（编辑 vCenter Server）] 对话框。

   a 单击 **[View Configuration（View 配置）] > [Servers（服务器）]**。

   b 在 [vCenter Server] 面板中，选择 vCenter Server 条目。

   c 单击 **[Edit（编辑）]**。

2 选择 **[Enable View Composer（启用 View Composer）]**，并确保端口号与您在 vCenter Server 上安装 View Composer 时指定的端口相同。

   View Manager 会验证 View Composer 服务是否正运行在 vCenter Server 上。

3 单击 **[Add（添加）]**，为 View Composer 帐户信息添加域用户。

   a 键入 Active Directry 域的域名。

   例如：`domain.com`

   b 键入包括域名在内的域用户名。

   例如：`domain.com\admin`

   c 键入帐户密码。

   d 单击 **[OK（确定）]**。

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

4 单击 **[OK（确定）]** 关闭 [Edit vCenter Server（编辑 vCenter Server）] 对话框。

下一步

在安装了 View Composer 服务的每个 vCenter Server 实例中重复该步骤。

配置 View Client 连接

View 客户端通过安全连接与 View Connection Server 或安全服务器主机通信。

用于用户身份验证和 View 桌面选择的初始 View Client 连接将在用户向 View Client 提供域名或 IP 地址时通过 HTTPS 创建。如果您网络环境中的防火墙和负载平衡软件配置正确，此请求将会发送至 View Connection Server 或安全服务器主机。用户通过该连接进行身份验证和桌面选择，但并未连接到 View 桌面。

用户连接到 View 桌面时，View Client 会默认建立第二条指向 View Connection Server 或安全服务器主机的连接。此连接提供了一条通过 HTTPS 传送 RDP 数据和其他数据的安全加密链路，因此称作安全加密链路连接。

用户通过 PCoIP 显示协议连接到 View 桌面时，View Client 可进一步连接到 View Connection Server 或安全服务器主机上的 PCoIP 安全网关。PCoIP 安全网关可确保只有经过身份验证的用户才能通过 PCoIP 与 View 桌面进行通信。

禁用安全加密链路或 PCoIP 安全网关后，将绕过 View Connection Server 或安全服务器主机，而是直接在客户端系统和 View 桌面虚拟机之间建立 View 桌面会话。这种连接类型被称为直接连接。

通常情况下，为了通过 WAN 向连接到安全服务器或 View Connection Server 主机的外部客户端提供安全连接，您需要启用安全加密链路和 PCoIP 安全网关。您可以禁用安全加密链路和 PCoIP 安全网关来允许连接 LAN 的内部客户端与 View 桌面建立直接连接。

某些 View Client 终端（如瘦客户端）不支持安全加密链路连接，而是采用直接连接来传输 RDP 数据，但支持通过 PCoIP 安全网关传输 PCoIP 数据。

默认情况下已启用 SSL 进行客户端连接。您可以禁用 SSL，从而通过 HTTP（而不是 HTTPS）建立初始连接和安全加密链路连接。对于通过防火墙保护通信且连接 LAN 的客户，禁用 SSL 的做法是可以接受的。请参阅第 81 页，“配置 SSL 进行客户端连接”。

配置 PCoIP 安全网关和安全加密链路连接

您可以使用 View Administrator 配置安全加密链路和 PCoIP 安全网关的使用情况。这些组件可确保只有经过身份验证的用户才能与 View 桌面进行通信。

使用 PCoIP 显示协议的客户端可以使用 PCoIP 安全网关。使用 RDP 显示协议的客户端可以使用安全加密链路。

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

在外部客户端直接连接到 View Connection Server 主机的网络配置中，您可以通过在 View Administrator 中编辑 View Connection Server 实例来启用或禁用安全加密链路和 PCoIP 安全网关。

前提条件

- 如果您打算启用 PCoIP 安全网关，请确认 View Connection Server 实例以及与其配对的安全服务器为 View 4.6 或更高版本。
- 如果要将安全服务器与一个已启用 PCoIP 安全网关的 View Connection Server 实例配对，请确认安全服务器为 View 4.6 或更高版本。

步骤

1 在 View Administrator 中，选择 **[View Configuration（View 配置）] > [Servers（服务器）]**。

2 在 View Connection Server 面板中，选择一个 View Connection Server 实例，然后单击 **[Edit（编辑）]**。

3 配置是否使用安全加密链路连接。

选项	描述
禁用安全加密链路	取消选中 **[Use secure tunnel connection to desktop（使用安全加密链路连接桌面）]**。
启用安全加密链路	选中 **[Use secure tunnel connection to desktop（使用安全加密链路连接桌面）]**。

默认启用安全加密链路。

4 配置是否使用 PCoIP 安全网关。

选项	描述
启用 PCoIP 安全网关	选中 **[Use PCoIP Secure Gateway for PCoIP connections to desktop（使用 PCoIP 安全网关与桌面建立 PCoIP 连接）]**
禁用 PCoIP 安全网关	取消选中 **[Use PCoIP Secure Gateway for PCoIP connections to desktop（使用 PCoIP 安全网关与桌面建立 PCoIP 连接）]**

默认禁用 PCoIP 安全网关。

5 单击 **[OK（确定）]** 保存更改。

为 PCoIP 安全网关和安全加密链路连接配置外部 URL

要使用安全加密链路，客户端系统必须能够访问 IP 地址或可以解析成 IP 地址的主机域名全称 (FQDN)，以便客户端连接 View Connection Server 或安全服务器主机。要使用 PCoIP 安全网关，客户端系统必须能够访问允许该客户端连接 View Connection Server 或安全服务器主机的 IP 地址。

从外部使用安全加密链路连接

默认情况下，仅位于同一网络且使用安全加密链路的客户端可以联络 View Connection Server 或安全服务器主机，因此后者能够定位请求的主机。

很多机构都希望用户能通过特定的 IP 地址、客户端可以解析的域名及特定的端口来实现外部连接。该信息可能类似于 View Connection Server 或安全服务器主机的实际地址和端口号，可通过 URL 的形式提供给客户端系统。例如：

- `https://view-example.com:443`
- `https://view.example.com:443`
- `https://example.com:1234`
- `https://100.200.300.400:443`

要在 View Manager 中使用此类地址，您必须将 View Connection Server 或安全服务器主机配置为返回外部 URL 而不是主机 FQDN。

配置外部 URL

您可以配置两种外部 URL。一种 URL 允许客户端系统建立安全加密链路连接。另一种则允许使用 PCoIP 的客户端系统通过 PCoIP 安全网关建立安全加密链路连接。您必须将 PCoIP 外部 URL 指定为 IP 地址，以便客户端系统能够从外部进行连接。

如果您的网络配置中包含安全服务器，请为安全服务器提供外部 URL。与安全服务器配对的 View Connection Server 实例无需使用外部 URL。

在 View Connection Server 实例和安全服务器中配置外部 URL 的过程有所不同。

- 在 View Connection Server 实例中，您可以通过在 View Administrator 中编辑 View Connection Server 设置来设置外部 URL。
- 在安全服务器中，可以在运行 View Connection Server 安装程序时设置外部 URL。您可以使用 View Administrator 来修改安全服务器的外部 URL。

设置 View Connection Server 实例的外部 URL

您需要使用 View Administrator 为 View Connection Server 实例配置外部 URL。

安全加密链路外部 URL 和 PCoIP 外部 URL 都必须是客户端系统用于连接此 View Connection Server 实例的地址。例如，请勿指定该实例的安全加密链路外部 URL 以及与其配对的安全服务器的 PCoIP 外部 URL。

步骤

1 在 View Administrator 中，单击 **[View Configuration（View 配置）] > [Servers（服务器）]**。

2 在 View Connection Server 面板中，选择一个 View Connection Server 实例，然后单击 **[Edit（编辑）]**。

3 在 **[External URL（外部 URL）]** 文本框中键入安全加密链路的外部 URL。

该 URL 必须包含协议、客户端可解析的主机名或 IP 地址以及端口号。

例如：**`https://view.example.com:443`**

4 在 **[PCoIP External URL（PCoIP 外部 URL）]** 文本框中键入 PCoIP 安全网关的外部 URL。

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

例如：`100.200.300.400:4172`

URL 中必须包含能供客户端系统连接到此 View Connection Server 主机的 IP 地址和端口号。如果 PCoIP 安全网关安装在 View Connection Server 实例上，您可以仅在文本框中键入内容。

5 单击 **[OK（确定）]**。

修改安全服务器的外部 URL

您可以使用 View Administrator 来修改安全服务器的外部 URL。

您最初在 View Connection 安装程序中为安全服务器配置外部 URL。

安全加密链路外部 URL 和 PCoIP 外部 URL 都必须是客户端系统用于连接此安全服务器的地址。例如，请勿指定该安全服务器的安全加密链路外部 URL 以及与其配对的 View Connection Server 实例的 PCoIP 外部 URL。

前提条件

确认安全服务器的版本为 View Connection Server 4.6 或更高版本。

步骤

1 在 View Administrator 中，选择 **[View Configuration（View 配置）] > [Servers（服务器）]**。

2 在 [Security Servers（安全服务器）] 面板中，选择安全服务器并单击 **[Edit（编辑）]**。

如果安全服务器未升级到 View Connection Server 4.6 或更高版本，**[Edit（编辑）]** 按钮将不可用。

3 在 **[External URL（外部 URL）]** 文本框中键入安全加密链路的外部 URL。

URL 必须包含协议、客户端可解析的安全服务器主机名或 IP 地址以及端口号。

例如：`https://view.example.com:443`

4 在 **[PCoIP External URL（PCoIP 外部 URL）]** 文本框中键入 PCoIP 安全网关的外部 URL。

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

例如：`100.200.300.400:4172`

URL 中必须包含客户端系统可用以连接安全服务器的 IP 地址和端口号。仅在安全服务器上安装了 PCoIP 安全网关的情况下，您才可以在该文本框中键入内容。

5 单击 **[OK（确定）]** 保存更改。

View Administrator 会将更新的外部 URL 发送到安全服务器。您无需重新启动安全服务器，所作的更改即可生效。

调整 Windows Server 设置以支持您的部署

为支持大规模 View Manager 桌面部署，您可以对安装 View Connection Server 的 Windows Server 计算机进行配置。您可以在每台计算机中调整短周期端口、TCB 哈希表、Java 虚拟机设置和 Windows 页面文件。这些调整可确保计算机拥有充足的资源，可在预期的用户负载下正常运行。

有关 View Connection Server 的硬件和内存要求，请参见第 7 页，“View Connection Server 的硬件要求”。

有关在大规模 View 部署中使用 View Connection Server 的硬件和内存建议，请参阅*《VMware View 体系结构规划指南》*文档中的“Connection Server 虚拟机配置和最大连接数”。

短周期端口

View Manager 使用短周期端口在 View Connection Server 与其管理的 View 桌面之间建立 TCP 连接。为支持大规模 View 桌面部署，您可以增加可用短周期端口的数量。

短周期端口是指当程序请求任何可用的用户端口时，由操作系统创建的短期使用的端口。操作系统会在预定义的范围内（通常介于 1024 和 65535 之间）选择端口号，并在相关的 TCP 连接终止后释放这个端口。

默认情况下，系统在 Windows Server 2003 上最多可以创建约 4,000 个同时运行的短周期端口，在 Windows Server 2008 上最多可创建约 16,000 个。

在 32 位 Windows Server 2003 计算机中，如果某个 View Connection Server 实例可能要使用超过 800 个并发客户端连接，您应当增加可用短周期端口的数量。

计算短周期端口数量

您可以计算每个 View Connection Server 实例支持大量并发客户端连接所需的短周期端口数。

步骤

- 使用以下公式。

  短周期端口数量 = ((5 x 客户端数量) / 服务器数量) + 10

  其中

  客户端数量 计划的并发客户端连接数

  服务器数量 副本服务器组中 View Connection Server 实例的数量

示例：计算短周期端口的数量

例如，您可以规划一个由三个 View Connection Server 实例管理的部署。如表 5–10 中所示，如果您预计会有 3,000 个并发客户端连接，就需要设置 5,010 个短周期端口。

表 5–10 计算短周期端口数量的示例

配置参数	范例值
计划的并发客户端连接数	3,000
副本服务器组中 View Connection Server 实例的数量	3
((5 x 客户端数量) / 服务器数量) + 10 = 每个 View Connection Server 上的短周期端口数量	(5x3,000) / 3 + 10 = 5,010

下一步

使用第 61 页，“用于计算短周期端口和 TCB 哈希表大小的工作表”填写相关的部署值。

增加短周期端口的数量

您可以通过编辑 Windows 注册表来增加运行 View Connection Server 的 Windows Server 计算机上的短周期端口最大值。

Active Directory 组策略可重写注册表项。如果可能，请使用组策略来设置 View Connection Server 上的最大短周期端口数量。

前提条件

计算要在 Windows Server 计算机上配置的短周期端口数量。请参阅第 58 页，“计算短周期端口数量”。

仅在 Windows Server 2003 上得到的端口数大于 4,000，或 Windows Server 2008 上得到的端口数大于 16,000 时修改 Windows 的注册表值。

步骤

1 在 Windows Server 计算机中，启动 Windows 注册表编辑器。

   a 选择 **[Start（开始）] > [Command Prompt（命令提示符）]**。

   b 在命令提示符下，键入 **`regedit`**。

2 在注册表中找到正确的子项，然后单击 **[Parameters]**。

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`

3 单击 **[Edit（编辑）] > [New（新建）]**，然后添加注册表项。

   数值名称：`MaxUserPort`
   数值类型：`DWORD`
   数值数据：`1024 +` *计算出的短周期端口数量*
   有效范围：`5000–65534`（十进制）

4 退出 Windows 注册表编辑器。

5 重新启动 Windows Server 计算机。

增加 TCB 哈希表的大小

传输控制数据块（Transmission Control Block，TCB）可保存与 View Connection Server 客户端及其桌面源之间的 TCP 连接有关的信息。要在 Windows Server 2003 计算机上实现大规模 View 桌面部署，您可以增加 TCB 哈希表的大小。

在 Windows Server 2008 计算机上，您不必增加 TCB 哈希表的大小上限。Windows Server 2008 会默认调整该数值。

TCB 是一种内存驻留数据结构，其中包含套接字编码、传入和传出数据缓冲的位置、已收到或未确认的字节以及其他信息。

为了快速检索这些信息，Windows Server 将 TCB 数据结构存储在一个哈希表中。

默认情况下，Windows Server 2003 会根据 Windows Server 计算机的 CPU 数量配置哈希表的行数。

表 5–11 Windows Server 2003 上的最大 TCB 哈希表大小

CPU 数量	TCB 哈希表的最大行数
1	128
2	512
4	2,048
8	8,192

计算 View Connection Server 实例和安全服务器上的 TCB 哈希表大小时需要分别采用不同的公式。

计算 View Connection Server 的 TCB 哈希表大小

为支持大量 View 桌面，您可以优化每个 View Connection Server 实例上的 TCB 哈希表大小。您可以以行为计算单位优化每个 View connection Server 实例上的 TCB 哈希表大小。

步骤

- 使用以下公式。

  每台 View Connection Server 实例的哈希表行数 = ((5 x 客户端数量) / 服务器数量) + 桌面数量 + 20

  其中

客户端数量	计划的并发客户端连接数
服务器数量	副本服务器组中 View Connection Server 实例的数量
桌面数量	您的部署中 View 桌面资源的数量

示例：计算每台 View Connection Server 上的 TCB 哈希表大小

例如，您的部署中可能会有 3,000 个并发客户端连接、三个 View Connection Server 实例和 6,000 个 View 桌面源。

如表 5–12 中所示，每个 View Connection Server 实例对应的结果是 11,020。

表 5–12 计算每个 View Connection Server 上 TCB 哈希表大小的示例

配置参数	范例值
计划的并发客户端桌面连接数	3,000
View Connection Server 实例的数量	3
View 桌面源的数量	6,000
((5 x 客户端数量) / 服务器数量) + 桌面数量 + 20 = 每台服务器的 TCB 哈希表行数	(5x3,000) / 3 + 6,000 + 20 = 11,020

下一步

使用第 61 页，“用于计算短周期端口和 TCB 哈希表大小的工作表”填写相关的部署值。

计算安全服务器的 TCB 哈希表大小

为支持大量 View 桌面，您可以优化每个安全服务器上的 TCB 哈希表大小。您可以以行为计算单位优化每个 View connection Server 实例上的 TCB 哈希表大小。

步骤

- 使用以下公式。

  哈希表行数 = ((5 x 客户端数量) / 安全服务器数量) + 10

  其中

客户端数量	计划的并发客户端连接数
安全服务器	安全服务器数量

示例：计算每台安全服务器上的 TCB 哈希表大小

例如，您的部署中可能包含 3,000 个并发客户端连接和两台安全服务器。

如表 5–13 中所示，每个安全服务器对应的结果是 7,510。

表 5–13 计算每个安全服务器上 TCB 哈希表大小的示例

配置参数	范例值
计划的并发客户端桌面连接数	3,000
安全服务器数量	2
((5 x 客户端数量) / 安全服务器数量) + 10 = 每台安全服务器上的 TCB 哈希表行数	(5x3,000) / 2 + 10 = 7,510

下一步

使用第 61 页，“用于计算短周期端口和 TCB 哈希表大小的工作表”填写相关的部署值。

增大 Windows Server 上 TCB 哈希表的大小

通过编辑 Windows 注册表来增加运行 View Connection Server 的 Windows Server 计算机上的 TCB 哈希表大小。

Active Directory 组策略可重写注册表项。如果可能，请使用组策略来设置 View Connection Server 中的 TCB 哈希表大小。

步骤

1 在 Windows Server 计算机中，启动 Windows 注册表编辑器。

   a 选择 **[Start（开始）] > [Command Prompt（命令提示符）]**。

   b 在命令提示符下，键入 **`regedit`**。

2 在注册表中找到相应子项，然后单击 **[Parameters]**。

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`

3 单击 **[Edit（编辑）] > [New（新建）]**，然后添加以下注册表项。

   数值名称：`MaxHashTableSize`
   数值类型：`DWORD`
   数值数据：*计算出的哈希表大小*
   有效范围：`64–65536`（十进制）

4 退出 Windows 注册表编辑器。

5 重新启动 Windows Server 计算机。

用于计算短周期端口和 TCB 哈希表大小的工作表

使用这些工作表可计算部署中每个 View Connection Server 实例和安全服务器上的短周期端口数量与 TCB 哈希表大小。

表 5–14 配置参数

配置参数	填入对应值
计划的并发客户端连接数	
View Connection Server 实例的数量	
安全服务器数量	
View 桌面源的数量	

表 5–15 短周期端口数量

短周期端口数量	填入对应值
((5 x 客户端数量) / 服务器数量) + 10 = 每个 View Connection Server 实例上的短周期端口数量	

表 5–16 View Connection Server 的 TCB 哈希表大小

View Connection Server 的哈希表大小	填入对应值
((5 x 客户端数量) / 服务器数量) + 桌面数量 + 20 = 每个 View Connection Server 实例的哈希表行数	

表 5–17 安全服务器的 TCB 哈希表大小

安全服务器的哈希表大小	填入对应值
((5 x 客户端数量) / 安全服务器数量) + 10 = 每台安全服务器上的哈希表行数	

调整 Java 虚拟机大小

View Connection Server 安装程序可调整 View Connection Server 计算机上的 Java 虚拟机 (JVM) 堆内存的大小，以支持大量并发 View 桌面会话。但是，当 View Connection Server 在 32 位 Windows Server 计算机上运行时，为 View Secure Gateway Server 组件配置的 JVM 堆大小有限。要充分调整您的部署，可增大 32 位计算机上的 JVM 堆大小。

在至少有 10 GB 内存的 64 位 Windows Server 计算机上，安装程序将为 View Secure Gateway Server 组件配置大小为 2 GB 的 JVM 堆。此配置支持约 2,000 个并发安全加密链路会话，这是 View Connection Server 可以支持的最大数量。在具有 10 GB 内存的 64 位计算机上，增加 JVM 堆的大小不会带来任何好处。

注意 在 64 位 View Connection Server 计算机上，要部署 50 个或更多的 View 桌面，建议配置 10 GB 内存。仅为小规模的概念验证部署配置小于 10 GB 的内存。

如果 64 位计算机的内存小于 10 GB，则安装程序将为 View Secure Gateway Server 组件配置大小为 512 MB 的 JVM 堆。如果计算机配置有 4 GB 的最小所需内存，则此配置可支持大约 500 个并发安全加密链路会话。此配置支持小规模的概念验证部署绰绰有余。

如果您将 64 位计算机的内存增加到 10 GB 以支持更大规模的部署，View Connection Server 不会增加 JVM 堆的大小。为将 JVM 堆的大小调整到建议值，请重新安装 View Connection Server。

在 32 位 Windows Server 计算机上，View Secure Gateway Server 组件的默认 JVM 堆大小为 512 MB。此 JVM 堆大小可支持约 750 个并发安全加密链路会话。要支持 750 个以上的会话，计算机必须至少配置 3 GB 的内存，并且 JVM 堆大小应增大到 1 GB。大小为 1 GB 的 JVM 堆可支持 1,500 个并发安全加密链路会话，这是 View Connection Server 在 32 位计算机上可以支持的最大数量。

增加 32 位 Windows Server 计算机上的 JVM 堆大小

您可以通过编辑 Windows 注册表来增加安装 View Connection Server 的 32 位 Windows Server 计算机上的 JVM 堆大小。

重要事项 请勿更改 64 位 Windows Server 计算机上的 JVM 堆大小。更改该值可能会使 View Connection Server 的行为变得不稳定。在 64 位计算机上，View Connection Server 安装程序将会对 JVM 堆大小进行设置以适应物理内存。如果您更改了 64 位 View Connection Server 计算机的物理内存，请重新安装 View Connection Server 以重置 JVM 堆大小。

在 32 位计算机上，如果增加 JVM 堆大小后重新安装或升级 View Connection Server 软件，就必须重新增加 JVM 堆大小。该值会在每次重新安装或升级 View Connection Server 软件时重置。

步骤

1 在 Windows Server 计算机中，启动 Windows 注册表编辑器。

a 选择 **[Start（开始）] > [Command Prompt（命令提示符）]**。

b 在命令提示符下，键入 **regedit**。

2 在注册表中找到相应子项，然后单击 **[JvmOptions]**。

```
HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Plugins\wsnm\tunnelService\Params
```

3 单击 **[Edit（编辑）] > [Modify（修改）]**。

Windows 对话框将显示与以下示例类似的注册表项：

```
-Xms128m -Xmx512m -Xss96k -Xrs -XX:+UseConcMarkSweepGC
-Dsimple.http.poller=simple.http.GranularPoller
-Dsimple.http.connect.configurator=com.vmware.vdi.front.SimpleConfigurator
```

4 编辑 -Xmx 参数，将其值改为 **-Xmx1024m**。

对话框将显示以下注册表项。

```
-Xms128m -Xmx1024m -Xss96k -Xrs -XX:+UseConcMarkSweepGC
-Dsimple.http.poller=simple.http.GranularPoller
-Dsimple.http.connect.configurator=com.vmware.vdi.front.SimpleConfigurator
```

5 单击 **[OK（确定）]**，然后退出注册表编辑器。

6 重新启动 Windows Server 计算机。

配置系统页面文件设置

通过更改系统页面文件设置，您可以为安装了 View Connection Server 实例的 Windows Server 计算机优化虚拟内存。

安装 Windows Server 后，Windows 会根据计算机的物理内存计算页面文件的初始大小和最大大小。重新启动计算机后，这些默认值设置将保持不变。

如果 Windows Server 计算机是一个虚拟机，您可以通过 vCenter Server 来修改内存大小。然而，如果 Windows 使用默认设置，系统页面文件的大小就不会根据新的内存大小进行调整。

步骤

1 在安装了 View Connection Server 的 Windows Server 计算机上，导航至 [Virtual Memory（虚拟内存）] 对话框。

默认情况下，**[Custom size（自定义大小）]** 选项会被选中，并会显示页面文件大小的初始大小和最大大小。

2 单击 **[System managed size（系统管理的大小）]**。

Windows 会根据当前的内存使用情况和可用内存空间，不断重新计算系统页面文件的大小。

6 安装 View Transfer Server

执行检入、检出和复制操作时，View Transfer Server 会在本地桌面和数据中心之间传输数据。要安装 View Transfer Server，您需要在 Windows Server 虚拟机上安装软件，将 View Transfer Server 添加至您的 View Manager 部署中，并配置 Transfer Server 存储库。

如果在客户端计算机上部署 View Client with Local Mode，则必须安装并配置 View Transfer Server。

您必须拥有安装 View Transfer Server 和使用本地桌面的许可。

1 安装 View Transfer Server 第 65 页，

View Transfer Server 会下载系统映像文件、同步本地桌面与数据中心中相应远程桌面的数据，并在用户检入和检出本地桌面时传输数据。您需要在运行 Windows Server 的虚拟机上安装 View Transfer Server。

2 将 View Transfer Server 添加到 View Manager 中第 66 页，

View Transfer Server 与 View Connection Server 协同在本地桌面与数据中心之间传输文件和数据。您必须先将 View Transfer Server 添加到 View Manager 部署中，它才可以执行这些任务。

3 配置 Transfer Server 存储库第 67 页，

Transfer Server 存储库存储了本地模式下运行的链接克隆桌面的 View Composer 基础映像。要使 View Transfer Server 能够访问 Transfer Server 存储库，您必须在 View Manager 中配置该存储库。如果您不在本地模式下使用 View Composer 链接克隆，则无需配置 Transfer Server 存储库。

4 View Transfer Server 的防火墙规则第 69 页，

在防火墙上必须为 View Transfer Server 实例打开某些传入 TCP 端口。

5 静默安装 View Transfer Server 第 69 页，

通过在命令行输入安装程序文件名和安装选项，可以静默安装 View Transfer Server。通过静默安装，您可以在大型企业中高效部署 View 组件。

安装 View Transfer Server

View Transfer Server 会下载系统映像文件、同步本地桌面与数据中心中相应远程桌面的数据，并在用户检入和检出本地桌面时传输数据。您需要在运行 Windows Server 的虚拟机上安装 View Transfer Server。

运行期间，View Transfer Server 将被部署到 Apache Web Server 中。安装 View Transfer Server 时，安装程序会将 Apache Web Server 配置为虚拟机上的一项服务。Apache 服务使用端口 80 和 443。

前提条件

- 确认您在要安装 View Transfer Server 的 Windows Server 上具有本地管理员特权。
- 确认您的安装符合第 11 页，“View Transfer Server 的要求”中描述的 View Transfer Server 要求。
- 确认您拥有安装 View Transfer Server 和使用本地桌面的许可。

- 熟悉那些必须在 Windows 防火墙上为 View Connection Server 实例打开的网络端口。请参阅第 69 页，“View Transfer Server 的防火墙规则”。

小心 确认托管 View Transfer Server 的虚拟机上配置了一个 LSI Logic Parallel SCSI 控制器。您无法在具有 SAS 或 VMware 准虚拟控制器的虚拟机上安装 View Transfer Server。

在 Windows Server 2008 虚拟机上，LSI Logic SAS 控制器为默认选中。在安装操作系统之前，必须先将此选项更改为 LSI Logic Parallel 控制器。

步骤

1 从 VMware 产品页面 http://www.vmware.com/cn/products/ 将 View Connection Server 安装程序文件下载到 Windows Server 计算机。

安装程序的文件名为 `VMware-viewconnectionserver-y.y.y-xxxxxx.exe` 或 `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`，其中 *xxxxxx* 是内部版本号，*y.y.y* 是版本号。

2 要启动安装程序，请双击安装程序文件。

3 接受 VMware 许可条款。

4 接受或更改目标文件夹。

5 选择 **[View Transfer Server]**。

6 配置要部署 View Transfer Server 的 Apache Web Server。

您可以接受安装程序提示的网络域、Apache Server 名称和管理员的电子邮件地址的默认值。

7 如果您在 Windows Server 2008 上安装 View Transfer Server，请选择如何配置 Windows 防火墙服务。

选项	操作
Configure Windows Firewall automatically（自动配置 Windows 防火墙）	让安装程序将 Windows 防火墙配置为允许所需的网络连接。
Do not configure Windows Firewall（不配置 Windows 防火墙）	手动配置 Windows 防火墙规则。

如果在 Windows Server 2003 R2 上安装 View Transfer Server，必须手动配置所需的 Windows 防火墙规则。

8 完成安装程序以安装 View Transfer Server。

VMware View Transfer Server、View Transfer Server Control Service 以及 VMware View Framework Component 服务将在虚拟机上安装并启动。

下一步

在 View Administrator 中，将 View Transfer Server 添加到 View Manager 部署。

将 View Transfer Server 添加到 View Manager 中

View Transfer Server 与 View Connection Server 协同在本地桌面与数据中心之间传输文件和数据。您必须先将 View Transfer Server 添加到 View Manager 部署中，它才可以执行这些任务。

您可将多个 View Transfer Server 实例添加到 View Manager 中。这些 View Transfer Server 实例可访问一个公用的 Transfer Server 存储库。它们共享由一个 View Connection Server 实例或副本 View Connection Server 实例组管理的本地桌面的传输负载。

注意 将 View Transfer Server 添加到 View Manager 之后，其 Distributed Resource Scheduler (DRS) 自动化策略将设置为 [Manual（手动）]，这样可有效禁用 DRS。

前提条件

- 确认 View Transfer Server 已安装在 Windows Server 虚拟机上。
- 确认 vCenter Server 已添加到 View Manager 中。View Administrator 中的 **[View Configuration（View 配置）] > [Server（服务器）]** 页面显示了添加到 View Manager 的 vCenter Server 实例。

步骤

1 在 View Administrator 中，单击 **[View Configuration（View 配置）] > [Server（服务器）]**。

2 在 [Transfer Server] 面板中，单击 **[Add（添加）]**。

3 在 [Add Transfer Server（添加 Transfer Server）] 向导中，选择管理 View Transfer Server 虚拟机的 vCenter Server 实例，并单击 **[Next（下一步）]**。

4 选择安装 View Transfer Server 的虚拟机，然后单击 **[Finish（完成）]**。

View Connection Server 会为虚拟机重新配置四个 SCSI 控制器。多个 SCSI 控制器增加了 View Transfer Server 可以同时执行的磁盘传输量。

在 View Administrator 中，View Transfer Server 实例会显示在 [Transfer Server] 面板中。如果未配置 Transfer Server 存储库，View Transfer Server 的状态将从 **[Pending（正在等待处理）]** 变为 **[Missing Transfer Server repository（缺少 Transfer Server 存储库）]**。如果配置了 Transfer Server 存储库，状态将从 **[Pending（正在等待处理）]** 变为 **[Initializing Transfer Server repository（正在初始化 Transfer Server 存储库）]**，最后变成 **[Ready（就绪）]**。

此过程可能需要几分钟。您可以单击 View Administrator 中的刷新按钮查看当前状态。

将 View Transfer Server 实例添加至 View Manager 后，View Transfer Server 虚拟机上的 Apache 服务将会启动。

小心 如果您的 View Transfer Server 虚拟机版本低于硬件版本 7，那么将 View Transfer Server 添加到 View Manager 后，您还必须配置 View Transfer Server 虚拟机的静态 IP 地址。

当 View Transfer Server 虚拟机上添加了多个 SCSI 控制器时，Windows 会删除静态 IP 地址并将虚拟机重新配置为使用 DHCP。虚拟机重新启动后，您必须在虚拟机中重新输入静态 IP 地址。

配置 Transfer Server 存储库

Transfer Server 存储库存储了本地模式下运行的链接克隆桌面的 View Composer 基础映像。要使 View Transfer Server 能够访问 Transfer Server 存储库，您必须在 View Manager 中配置该存储库。如果您不在本地模式下使用 View Composer 链接克隆，则无需配置 Transfer Server 存储库。

如果在您配置 Transfer Server 存储库之前已在 View Manager 中配置了 View Transfer Server，View Transfer Server 会在配置过程中验证 Transfer Server 存储库的位置。

如果打算将多个 View Transfer Server 实例添加到该 View Manager 部署中，则应当在一个网络共享位置配置 Transfer Server 存储库。其他 View Transfer Server 实例无法访问在 View Transfer Server 实例的本地驱动器上配置的 Transfer Server 存储库。

确保 Transfer Server 存储库足够存储 View Composer 生成的基础映像。一个基础映像的大小可能达到数千兆字节。

如果在网络共享位置配置远程 Transfer Server 存储库，则必须提供具有可访问网络共享位置凭据的用户 ID。作为最佳实践，为增强访问 Transfer Server 存储库的安全性，请确保仅限 View 管理员才可通过网络访问资源库。

前提条件

- 确认 View Transfer Server 已安装在 Windows Server 虚拟机上。

- 确认 View Transfer Server 已添加到 View Manager 中。请参阅第 66 页，“将 View Transfer Server 添加到 View Manager 中”。

注意 最佳实践是在配置 Transfer Server 存储库前将 View Transfer Server 添加到 View Manager，但不是强制要求。

步骤

1 为 Transfer Server 存储库配置路径和文件夹。

Transfer Server 存储库可以位于本地驱动器或网络共享位置上。

选项	操作
Local Transfer Server repository（本地 Transfer Server 存储库）	在安装了 View Transfer Server 的虚拟机上，为 Transfer Server 存储库创建路径和文件夹。 例如：`C:\TransferRepository\`
Remote Transfer Server repository（远程 Transfer Server 存储库）	配置网络共享位置的 UNC 路径。 例如：`\\server.domain.com\TransferRepository\` 您添加到 View Manager 部署中的所有 View Transfer Server 实例都必须能通过网络访问该共享驱动器。

2 在 View Administrator 中，单击 **[View Configuration（View 配置）] > [Server（服务器）]**。

3 将所有 View Transfer Server 实例置于维护模式下。

a 在 [Transfer Server] 面板中，选择一个 View Transfer Server 实例。

b 单击 **[Enter Maintenance Mode（进入维护模式）]**，然后单击 **[OK（确定）]**。

View Transfer Server 的状态会变为 **[Maintenance mode（维护模式）]**。

c 重复步骤 3a 和 步骤 3b。

当所有 View Transfer Server 实例均处于维护模式时，当前的传输操作将停止。

4 在 [Transfer Server] 面板中，单击 Transfer Server 存储库旁的 **[None Configured（未配置的）]**。

5 在 Transfer Server 存储库页面的 [General（常规）] 面板中，单击 **[Edit（编辑）]**。

6 键入 Transfer Server 存储库的位置及其他信息。

选项	描述
Network Share（网络共享位置）	■ **[Path（路径）]**：键入您配置的 UNC 路径。 ■ **[Username（用户名）]**：键入具有访问网络共享位置权限的管理员用户的 ID。 ■ **[Password（密码）]**：键入管理员密码。 ■ **[Domain（域）]**：以 NetBIOS 格式键入网络共享位置的域名。不要使用 `.com` 后缀。
Local File System（本地文件系统）	键入在本地 View Transfer Server 虚拟机上配置的路径。

7 单击 **[OK（确定）]**。

如果存储库网络路径或本地驱动不正确，则 [Edit Transfer Server Repository（编辑 Transfer Server 存储库）] 对话框将会显示错误消息，并且不允许您配置位置。您必须键入一个有效位置。

8 在 **[View Configuration（View 配置）] > [Server（服务器）]** 页面上，选择 View Transfer Server 实例，然后单击 **[Exit Maintenance Mode（退出维护模式）]**。

View Transfer Server 的状态将变为 **[Ready（就绪）]**。

View Transfer Server 的防火墙规则

在防火墙上必须为 View Transfer Server 实例打开某些传入 TCP 端口。

在 Windows Server 2008 上安装 View Transfer Server 时，安装程序可为您配置所需的 Windows 防火墙规则（可选）。

在 Windows Server 2003 上安装 View Transfer Server 时，您必须手动配置所需的 Windows 防火墙规则。

表 6–1 列出了必须在防火墙上为 View Transfer Server 实例打开的传入 TCP 端口。

表 6–1 View Transfer Server 实例的 TCP 端口

协议	端口
HTTP	80
HTTPS	443

静默安装 View Transfer Server

通过在命令行输入安装程序文件名和安装选项，可以静默安装 View Transfer Server。通过静默安装，您可以在大型企业中高效部署 View 组件。

设置组策略以允许静默安装 View Transfer Server

必须先配置 Microsoft Windows 组策略以允许使用提升的特权进行安装，才能静默安装 View Transfer Server。

您必须设置针对计算机和本地计算机用户的 Windows Installer 组策略。

前提条件

确认您在要安装 View Transfer Server 的 Windows Server 计算机上具有本地管理员特权。

步骤

1 登录 Windows Server 计算机并单击 **[Start（开始）] > [Run（运行）]**。

2 键入 **`gpedit.msc`** 并单击 **[OK（确定）]**。

3 在 [Group Policy Object Editor（组策略对象编辑器）] 中，单击 **[Local Computer Policy（本地计算机策略）] > [Computer Configuration（计算机配置）]**。

4 展开 **[Administrative Templates（管理模板）]**，打开 **[Windows Installer]** 文件夹，然后双击 **[Always install with elevated privileges（始终使用提升的特权安装）]**。

5 在 **[Always install with elevated privileges Properties（始终使用提升的特权安装属性）]** 窗口中，单击 **[Enabled（启用）]**，然后单击 **[OK（确定）]**。

6 在左侧窗格中，单击 **[User Configuration（用户配置）]**。

7 展开 **[Administrative Templates（管理模板）]**，打开 **[Windows Installer]** 文件夹，然后双击 **[Always install with elevated privileges（始终使用提升的特权安装）]**。

8 在 **[Always install with elevated privileges Properties（始终使用提升的特权安装属性）]** 窗口中，单击 **[Enabled（启用）]**，然后单击 **[OK（确定）]**。

下一步

静默安装 View Transfer Server。

静默安装 View Transfer Server

您可以使用 Microsoft Windows Installer (MSI) 的静默安装功能，在多个 Windows 计算机上安装 View Transfer Server。在静默安装中，您需要使用命令行，无需响应向导的提示。

前提条件

- 确认您在要安装 View Transfer Server 的 Windows Server 上具有本地管理员特权。
- 确认您的安装符合第 11 页，“View Transfer Server 的要求”中描述的 View Transfer Server 要求。
- 确认您拥有安装 View Transfer Server 和使用本地桌面的许可。
- 确认安装 View Transfer Server 的虚拟机具有 MSI 运行时引擎 2.0 版或更高版本。有关详细信息，请参见 Microsoft 网站。
- 熟悉 MSI 安装程序命令行选项。请参阅第 46 页，“Microsoft Windows Installer 命令行选项”。
- 熟悉 View Transfer Server 可用的静默安装属性。请参阅第 71 页，“View Transfer Server 的静默安装属性”。
- 确认已在 Windows Server 计算机上配置静默安装所需的 Windows Installer 组策略。请参阅第 69 页，“设置组策略以允许静默安装 View Transfer Server”。

小心 确认托管 View Transfer Server 的虚拟机上配置了一个 LSI Logic Parallel SCSI 控制器。您无法在具有 SAS 或 VMware 准虚拟控制器的虚拟机上安装 View Transfer Server。

在 Windows Server 2008 虚拟机上，LSI Logic SAS 控制器为默认选中。在安装操作系统之前，必须先将此选项更改为 LSI Logic Parallel 控制器。

步骤

1 从 VMware 产品页面 http://www.vmware.com/cn/products/ 将 View Connection Server 安装程序文件下载到 Windows Server 计算机。

安装程序的文件名为 `VMware-viewconnectionserver-y.y.y-xxxxxx.exe` 或 `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`，其中 *xxxxxx* 是内部版本号，*y.y.y* 是版本号。

2 在 Windows Server 计算机上开启命令提示符。

3 在一行中键入安装命令。

例如：`VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=4"`

VMware View Transfer Server、View Transfer Server Control Service 以及 VMware View Framework Component 服务将在虚拟机上安装并启动。

下一步

在 View Administrator 中，将 View Transfer Server 添加到 View Manager 部署。

View Transfer Server 的静默安装属性

从命令行静默安装 View Transfer Server 时可以包含特定属性。您必须使用 *属性=值* 格式，以便 Microsoft Windows Installer (MSI) 解释属性和值。

表 6–2 View Transfer Server 静默安装的 MSI 属性

MSI 属性	描述	默认值
INSTALLDIR	View Connection Server 软件的安装路径和文件夹。 例如：`INSTALLDIR=""D:\abc\my folder""` 括住路径的两组双引号可允许 MSI 安装程序将空格识别为路径的有效部分。 此 MSI 属性是可选属性。	`%ProgramFiles %\VMware\VMware View\Server`
VDM_SERVER_INSTANCE_TYPE	View 服务器的安装类型包括： ■ **1**. 标准安装 ■ **2**. 副本安装 ■ **3**. 安全服务器安装 ■ **4**. View Transfer Server 安装 要安装 View Transfer Server，请定义 `VDM_SERVER_INSTANCE_TYPE=4` 在标准安装中，此 MSI 属性为可选属性。在所有其他安装类型中，均必须定义此属性。	1
SERVERDOMAIN	安装 View Transfer Server 的虚拟机的网络域。此值与在交互式安装期间配置的 Apache Web Server 网络域相对应。 例如：`SERVERDOMAIN=companydomain.com` 如果使用 MSI 属性 (`SERVERDOMAIN`) 指定自定义的 Apache Web Server 域，还必须指定自定义的 `SERVERNAME` 和 `SERVERADMIN` 属性。 此 MSI 属性是可选属性。	无
SERVERNAME	安装 View Transfer Server 的虚拟机的主机名。此值与在交互式安装期间配置的 Apache Web Server 主机名相对应。 例如：`SERVERNAME=ts1.companydomain.com` 如果使用 MSI 属性 (`SERVERNAME`) 指定自定义的 Apache Web Server 主机名，还必须指定自定义的 `SERVERDOMAIN` 和 `SERVERADMIN` 属性。 此 MSI 属性是可选属性。	无
SERVERADMIN	通过 View Transfer Server 配置的 Apache Web Server 管理员的电子邮件地址。 例如：`SERVERADMIN=admin@companydomain.com` 如果使用 MSI 属性 (`SERVERADMIN`) 指定自定义的 Apache Web Server 管理员，还必须指定自定义的 `SERVERDOMAIN` 和 `SERVERNAME` 属性。 此 MSI 属性是可选属性。	无
FWCHOICE	确定是否为 View Connection Server 实例配置防火墙的 MSI 属性。 值为 1 时表示配置防火墙。值为 2 时表示不配置防火墙。 例如：`FWCHOICE=1` 此 MSI 属性是可选属性。	1

7 配置证书身份验证

您可以为 View Connection Server 实例、安全服务器和 View Transfer Server 实例配置证书身份验证。

本章讨论了以下主题：

替换默认证书

默认的服务器 SSL 证书是在您安装 View Connection Server 时生成的。您可以使用默认证书来进行测试。

重要事项 应尽快替换默认证书。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 CA 签发的证书，不受信任的第三方将有可能伪装成您的服务器并截获流量。

View Connection Server 实例、安全服务器、负载平衡程序和 View Transfer Server 实例需要在收到 SSL 连接时使用服务器 SSL 证书。

- 如果为客户端连接启用 SSL，面向客户端的 View Connection Server 实例、安全服务器和用于终止 SSL 连接的负载平衡程序将需要用到服务器 SSL 证书。
- 如果启用 View Connection Server 实例或安全服务器上的安全加密链路，必须在该服务器上安装一个服务器 SSL 证书。即使使用负载平衡程序终止 SSL 连接，View Client 会和已启用安全加密链路的 View Connection Server 或安全服务器主机建立第二个 HTTPS 连接。
- 如果为本地模式操作和桌面部署启用 SSL，View Transfer Server 实例将需要用到服务器 SSL 证书。
- 如果在 VMware View 中配置智能卡身份验证，面向客户端的 View Connection Server 实例和安全服务器将需要用到根 CA 证书和服务器 SSL 证书。

您可以请求特定于某个 Web 域（如 www.mycorp.com）的服务器 SSL 证书，或者也可以请求可在整个域（如 *.mycorp.com）中使用的通配符服务器 SSL 证书。为简化管理，如果需要在多台服务器上或不同子域中安装证书，您可以选择请求通配符证书。较常见的做法是在安全安装中使用特定于域的证书，与通配符证书相比，CA 通常可以更好地保护特定于域的证书，使其免于丢失。如果使用通配符证书，需要确保私钥可以在服务器之间传输。

将默认证书替换为您的个人证书后，客户端会使用您的证书对服务器进行身份验证。如果您的证书是由 CA 签发，那么 CA 本身的证书通常会嵌入在浏览器中，或是位于客户端可以访问的可信数据库中。客户端接受证书后，会通过发送密钥（由证书中的公钥加密）来做出响应。此密钥用于加密客户端和服务器之间的流量。

您需要用 keytool 和 openssl 实用程序创建并管理 View 的证书。

将 keytool 和 openssl 添加到系统路径

keytool 和 openssl 为密钥和证书管理实用程序。您必须将这些实用程序的路径添加到系统环境 PATH 变量中，以便您可以从主机的任何目录运行这些实用程序。

您可以使用 keytool 实用程序创建密钥存储、生成证书请求、将证书导入密钥存储中以及将私钥添加到密钥存储。您可以使用 openssl 导出证书并创建和导出私钥，以便与 View Transfer Server 配合使用。

步骤

1 在您的 View Connection Server 或安全服务器主机上，右键单击 **[My Computer（我的电脑）]** 并选择 **[Properties（属性）]**。

   a 在 **[Advanced（高级）]** 选项卡上，单击 **[Environment Variables（环境变量）]**。

   b 在 [System Variables（系统变量）] 组中，选择 **[PATH]**，然后单击 **[Edit（编辑）]**。

   c 在 **[Variable Value（变量值）]** 文本框中键入 JRE 目录的路径。使用分号 (;) 来分隔文本框中的条目。

   例如：*安装目录*\VMware\VMware View\Server\jre\bin

2 在您的 View Transfer Server 主机上，右键单击 **[My Computer（我的电脑）]** 并选择 **[Properties（属性）]**。

   a 在 **[Advanced（高级）]** 选项卡上，单击 **[Environment Variables（环境变量）]**。

   b 在 [System Variables（系统变量）] 组中，选择 **[PATH]**，然后单击 **[Edit（编辑）]**。

   c 在 **[Variable Value（变量值）]** 文本框中键入 JRE 和 Apache 目录的路径。使用分号 (;) 来分隔文本框中的条目。

   例如：*安装目录*\VMware\VMware View\Server\httpd\bin;*安装目录*\VMware\VMware View\Server\jre\bin

3 单击 **[OK（确定）]**，直到关闭 [Windows System Properties（Windows 系统属性）] 对话框。

使用现有的 SSL 证书和私钥

如果您的组织已经拥有有效的服务器 SSL 证书，您可以使用该证书替换随 View Connection Server 提供的默认服务器 SSL 证书。

要使用现有证书，您还需要用到附带的私钥。PKCS#12 文件格式（也称为 PFX 文件格式）中包含服务器证书和私钥。PKCS#12 文件类型可带有 .pfx 或 .p12 扩展名。

如果 PKCS#12 文件中包含由根 CA（而不是中间 CA）签发的服务器证书，当您将 View Connection Server 实例或安全服务器配置为使用证书时可以使用现有的 PKCS#12 文件。请参阅第 79 页，“将 View Connection Server 实例或安全服务器配置为使用新证书”。

如果 PKCS#12 文件包含由中间 CA（而不是根 CA）签发的服务器证书，就必须将 PKCS#12 密钥存储转换为 JKS 格式。请参阅第 75 页，“准备要与 VMware View 一起使用的中间证书”。

要在 View Transfer Server 中使用 PKCS#12 文件，必须将 PKCS#12 私钥和服务器证书转换为 PEM 格式。请参阅第 75 页，“准备要与 View Transfer Server 一起使用的 PKCS#12 格式的现有证书”。

准备要与 View Transfer Server 一起使用的 PKCS#12 格式的现有证书

要与 View Transfer Server 实例一起使用的 SSL 证书必须是 PEM 格式的证书。如果您当前拥有 PKCS#12 格式的证书，可以使用 `openssl` 导出 PEM 格式的私钥和服务器证书。

前提条件

确认已将 `openssl` 添加到您主机上的系统 Path 变量中。请参阅第 74 页，“将 keytool 和 openssl 添加到系统路径”。

步骤

1 在 View Transfer Server 系统中，打开命令提示符并使用 `openssl` 从您的 `.p12` 或 `.pfx` 证书文件导出私钥。

例如：**`openssl pkcs12 -in server.pfx -nocerts -out key.pem`**

2 从私钥中移除通行短语并将其保存到 `server.key` 文件。

该步骤可防止 Apache 在每次重新启动时提示您输入通行短语。

例如：**`openssl rsa -in key.pem -out server.key`**

3 从证书文件中导出服务器证书并将其保存到 `server.crt` 文件。

例如：**`openssl pkcs12 -in server.pfx -clcerts -nokeys -out server.crt`**

下一步

将 View Transfer Server 实例配置为使用证书。请参阅第 80 页，“将 View Transfer Server 实例配置为使用新证书”。

准备要与 VMware View 一起使用的中间证书

如果您已经拥有 PKCS#12 密钥存储文件和由中间 CA（而不是根 CA）签发的服务器证书，就必须在将其用于 View 之前将 PKCS#12 密钥存储转换为 JKS 格式。

步骤

1 如果 PKCS#12 密钥存储中尚不包含中间证书，则需要创建 JKS 密钥存储并向其中添加中间证书。

为避免 `keytool` 出现错误，您必须在添加服务器证书前将中间证书添加到密钥存储。

a 将中间证书作为 `intermediateCA.p7` 保存到密钥存储文件所在的目录。

b 将中间证书导入到密钥存储文件。

例如：

`keytool -importcert -keystore keys.jks -storepass secret -trustcacerts -alias intermediateCA -file intermediateCA.p7`

2 将 PKCS#12 文件中的服务器证书和私钥添加到 JKS 密钥存储。

例如：

`keytool -importkeystore -destkeystore keys.jks -deststorepass secret -srckeystore keys.p12 -srcstoretype PKCS12 -srcstorepass clydenw`

如果 JKS 密钥存储不存在，`keytool` 实用程序会创建 JKS 密钥存储。

下一步

将您的 View Connection Server 实例或安全服务器配置为使用证书。请参阅第 79 页，“将 View Connection Server 实例或安全服务器配置为使用新证书”。

创建新的 SSL 证书

您可以使用自签证书或 CA 签发的证书来替换 View Connection Server 附带的默认服务器 SSL 证书。

CA 是确保证书及其创建者身份的第三方受信机构。如果证书是由受信任的 CA 签发，则系统不会向用户显示要求验证证书的消息，且瘦客户端设备可以在无需额外配置的情况下进行连接。如果客户端需要确定所接收数据的来源和完整性，您应当获取一个 CA 签发的证书，而不是使用自签证书。

1 获取由 CA 签发的证书并与 View Connection Server 实例或安全服务器一起使用第 76 页，

   要获取由 CA 签发的证书，您必须使用 `keytool` 生成一个密钥存储文件和一个证书签发请求 (CSR) 文件。出于测试目的，您可以基于不受信任的根从许多 CA 获取免费的临时证书。

2 获取由 CA 签发的证书并与 View Transfer Server 实例一起使用第 77 页，

   要获取由 CA 签发的证书，您必须使用 `openssl` 生成一个私钥文件和一个证书签发请求 (CSR) 文件。出于测试目的，您可以基于不受信任的根从许多 CA 获取免费的临时证书。

3 将根证书导入到密钥存储文件第 78 页，

   如果您的 View Connection Server 实例或安全服务器不信任从 CA 获取的服务器证书的根证书，请先使用 `keytool` 将证书导入到您的密钥存储文件中，然后再添加服务器证书。

4 将中间证书导入到密钥存储文件第 78 页，

   如果您使用的是中间 CA（而不是根 CA）签发的服务器证书，就必须在添加服务器证书前将中间证书添加到密钥存储。

5 将签发的服务器证书导入到密钥存储文件第 79 页，

   如果已经得到 CA 签发的服务器证书，请使用 `keytool` 将证书导入到密钥存储文件。

获取由 CA 签发的证书并与 View Connection Server 实例或安全服务器一起使用

要获取由 CA 签发的证书，您必须使用 `keytool` 生成一个密钥存储文件和一个证书签发请求 (CSR) 文件。出于测试目的，您可以基于不受信任的根从许多 CA 获取免费的临时证书。

前提条件

确定客户端计算机在连接主机时使用的主机域名全称 (FQDN)。

步骤

1 打开命令提示符并使用 `keytool` 创建一个密钥存储文件。

   例如：**`keytool -genkeypair -keyalg "RSA" -keysize 2048 -keystore keys.jks -storepass secret`**

   如果要将中间证书导入到密钥存储文件，必须指定一个 Java 密钥存储文件，如 `keys.jks`。

2 当 keytool 提示您输入姓名时，请键入客户端计算机用来连接主机的主机域名全称 (FQDN)。

选项	操作
View Connection Server 实例	如果您有一个 View Connection Server 实例，请键入 View Connection Server 主机的 FQDN。如果使用负载平衡，请键入负载平衡程序主机的 FQDN。
安全服务器	键入安全服务器主机的 FQDN。

重要事项 如果键入您的姓名，证书将变为无效。

keytool 会在当前目录创建密钥存储文件。

3 请使用 keytool 创建一个具有名称的 CSR 文件，如 certificate.csr。

例如：**keytool -certreq -file certificate.csr -keystore keys.jks -storepass secret**

keytool 会在存储文件所在的目录中创建 CSR 文件。

4 按照 CA 的注册流程将 CSR 文件发送到 CA，并请求获取证书。

在对您的公司进行一些核查后，CA 会签发您请求的证书，使用私钥将其加密，然后将一个有效的证书发送给您。

下一步

如果需要用于 View Transfer Server 实例的证书，请参阅第 77 页，“获取由 CA 签发的证书并与 View Transfer Server 实例一起使用”。

如果 View Connection Server 实例或安全服务器不信任服务器证书的根证书，请先将个根证书导入到密钥存储文件，然后再导入服务器证书。请参阅第 78 页，“将根证书导入到密钥存储文件”。

如果服务器证书由中间 CA 签发，请将中间证书导入到您的密钥存储文件。请参阅第 78 页，“将中间证书导入到密钥存储文件”。

如果已下载了服务器证书，请将其导入到您的密钥存储文件。请参阅第 79 页，“将签发的服务器证书导入到密钥存储文件”。

获取由 CA 签发的证书并与 View Transfer Server 实例一起使用

要获取由 CA 签发的证书，您必须使用 openssl 生成一个私钥文件和一个证书签发请求 (CSR) 文件。出于测试目的，您可以基于不受信任的根从许多 CA 获取免费的临时证书。

前提条件

确定客户端计算机在连接主机时使用的主机域名全称 (FQDN)。

步骤

1 打开命令提示符并使用 openssl 创建一个私钥文件和一个 CSR 文件。

例如：**openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr**

2 当 openssl 提示您输入常用名称时，请键入客户端计算机用来连接 View Transfer Server 主机的主机域名全称 (FQDN)。

重要事项 如果键入您的姓名，证书将变为无效。

openssl 会在当前目录中创建私钥文件和 CSR 文件。

3 请按照 CA 的注册流程将 CSR 文件发送到 CA，并请求获取 PEM 格式的证书。

有些 CA 会提供非 PEM 格式的证书。如果您下载此类型证书，必须将其转换为 PEM 格式。

在对您的公司进行一些核查后，CA 会签发您请求的证书，使用私钥将其加密，然后将一个有效的证书发送给您。

下一步

将 View Transfer Server 实例配置为使用服务器 SSL 证书。请参阅第 80 页，“将 View Transfer Server 实例配置为使用新证书”。

将根证书导入到密钥存储文件

如果您的 View Connection Server 实例或安全服务器不信任从 CA 获取的服务器证书的根证书，请先使用 `keytool` 将证书导入到您的密钥存储文件中，然后再添加服务器证书。

步骤

1 将根证书作为 `rootCA.p7` 保存到密钥存储文件所在的目录。

2 打开命令提示符并使用 `keytool` 将根证书导入到密钥存储文件。

例如：**`keytool -importcert -keystore keys.jks -storepass secret -alias rootCA -file rootCA.p7`**

下一步

如果服务器证书由中间 CA 签发，请将中间证书导入到您的密钥存储文件。请参阅第 78 页，“将中间证书导入到密钥存储文件”。

如果服务器证书由根 CA 签发，请将证书导入到您的密钥存储文件。请参阅第 79 页，“将签发的服务器证书导入到密钥存储文件”。

将中间证书导入到密钥存储文件

如果您使用的是中间 CA（而不是根 CA）签发的服务器证书，就必须在添加服务器证书前将中间证书添加到密钥存储。

前提条件

向中间 CA 索取中间证书。

步骤

1 将中间证书另存为 `intermediateCA.p7` 保存到密钥存储文件所在的目录。

2 将中间证书导入到密钥存储文件。

例如：

`keytool -importcert -keystore keys.jks -storepass secret -trustcacerts -alias intermediateCA -file intermediateCA.p7`

下一步

如果已下载了服务器证书，请将其导入到您的密钥存储文件。请参阅第 79 页，“将签发的服务器证书导入到密钥存储文件”。

将签发的服务器证书导入到密钥存储文件

如果已经得到 CA 签发的服务器证书，请使用 `keytool` 将证书导入到密钥存储文件。

步骤

1 将包含服务器证书的文本文件复制到密钥存储文件所在的目录，并将其保存为 `certificate.p7`。

例如：

```
-----BEGIN PKCS7-----
MIIF+AYJKoZIhvcNAQcCoIIF6TCCBeUCAQExADALBgk
LDCCApWgAwIBAgIQTpY7DsV1n1HeMGgMjMR2PzANBgk
i7coVx71/lCBOlFmx66NyKlZK5mObgvd2dlnsAP+nnS
EhCsdpikSpbtdo18jUubV6z1kQ71CrRQtbi/WtdqxQE
-----END PKCS7-----
```

2 打开命令提示符并使用 `keytool` 将该服务器证书导入到密钥存储文件。

例如：

```
keytool -importcert -keystore keys.jks -storepass secret -keyalg "RSA" -trustcacerts -file
certificate.p7
```

3 如果您指定了临时证书，请在接收到消息 `.... is not trusted.Install reply anyway?` 时键入 **`yes`**。

`keytool` 之所以生成此消息，是因为临时证书不能用于生产环境。

下一步

将您的 View Connection Server 实例或安全服务器配置为使用证书。请参阅第 79 页，“将 View Connection Server 实例或安全服务器配置为使用新证书”。

将 View Connection Server 实例或安全服务器配置为使用新证书

要将 View Connection Server 实例或安全服务器配置为使用新的服务器 SSL 证书，您必须在 View Connection Server 或安全服务器主机上的 `locked.properties` 文件中设置属性。

前提条件

获取一个现有的 PKCS#12 文件，导出一个现有的 Microsoft IIS SSL 服务器证书，或者新建一个 SSL 服务器证书。

步骤

1 将包含证书的密钥存储文件复制到 View Connection Server 或安全服务器主机上的 SSL 网关配置目录。

例如：*安装目录*`\VMware\VMware View\Server\sslgateway\conf\`*密钥存储文件*

密钥存储文件 为密钥存储文件的名称。

例如，如果您使用 `keytool` 实用程序导入您的证书，您的密钥存储文件可能为 `keys.jks`。

如果您已拥有 PKCS#12 文件或已导出现有的 Microsoft IIS SSL 服务器证书，您的密钥文件可能为 `keys.pfx`。

2 将 keyfile、keypass 和 storetype 属性添加到 View Connection Server 或安全服务器主机上的 SSL 网关配置目录中的 locked.properties 文件。

如果还没有 locked.properties 文件，您就必须创建一个。

a 将 keyfile 属性设置为密钥存储文件的名称。

例如：keyfile=keys.jks 或 keyfile=keys.pfx

b 将 keypass 属性设置为密钥存储文件的密码。

例如：keypass=MY_PASS

c 将 storetype 属性设置为与密钥存储文件类型相匹配。

选项	描述
PKCS#12 或 PFX 文件	将 storetype 的值设为 **pkcs12**： storetype=pkcs12
Java 密钥存储文件	将 storetype 的值设置为 **jks**： storetype=jks 必须为 Java 密钥存储文件指定 storetype 属性。

3 重新启动 View Connection Server 服务或安全服务器服务，使所做的更改生效。

下一步

按照第 82 页，“配置适用于 Windows 的 View Client 中的证书检查”中的介绍安装根证书（如尚未安装）和中间证书。

将 View Transfer Server 实例配置为使用新证书

要将 View Transfer Server 实例配置为使用新的服务器 SSL 证书，您必须将您的证书和私钥文件复制到 View Transfer Server 主机。

View Transfer Server 实例中的 Apache Server 需要使用 Base64 编码的 DER (PEM) 证书。证书文件和密钥文件必须使用相应的 .crt 和 .key 扩展名。

前提条件

- 将 openssl 添加到您主机上的系统 Path 变量。请参阅第 74 页，“将 keytool 和 openssl 添加到系统路径”。
- 获取现有的 PKCS#12 文件，导出一个现有的 Microsoft IIS SSL 服务器证书，或者新建一个 SSL 证书。
- 如果您使用的是中间 CA，则需获取一个 PEM 格式的中间证书。
- 如果证书不是 PEM 格式，请将其转换为 PEM 格式。

步骤

1 停止 View Transfer Server 服务。

2 将服务器证书、中间证书（如果有）和私钥文件复制到 View Transfer Server 主机上的*安装目录*\VMware\VMware View\Server\httpd\conf 目录中。

3 在 Apache 配置文件 mod_vprov.conf 中编辑 SSLCertificateFile 和 SSLCertificateKeyFile 对应的条目，以指定服务器证书和私钥文件的名称。

例如：

```
SSLCertificateFile server.crt
SSLCertificateKeyFile server.key
```

4 如果已将中间证书文件复制到 View Transfer Server 主机，请将 `SSLCertificateChainFile` 指令对应的条目添加到 `mod_vprov.conf`。

例如：

```
SSLCertificateChainFile intermediateCA.crt
```

5 重新启动 View Transfer Server 服务以使更改生效。

6 通过 Web 浏览器导航至 View Transfer Server 主机地址，确认已正确配置证书。例如：`https://`*传输服务器主机地址*。

配置 SSL 进行客户端连接

要配置客户端连接在与 View Connection Server 通信时是否使用 SSL，您需要在 View Administrator 中配置全局设置。该设置适用于 View 桌面客户端和运行 View Administrator 的客户端。

全局设置可影响所有由独立的 View Connection Server 实例或副本实例组管理的客户端会话。这些设置并不特定于单个 View Connection Server 实例。

如果已经为智能卡身份验证配置 View Connection Server，就必须为客户端连接启用 SSL。

默认情况下，已启用 SSL 进行客户端连接。

注意 如果为客户端连接禁用 SSL，用户必须在连接 View Connection Server 主机前取消选中 View Client 中的 **[Use secure connection (SSL)（使用安全连接 (SSL)）]** 复选框，且管理员必须键入 HTTP URL 来运行 View Administrator。

重要事项 为客户端连接禁用或启用 SSL 后，所有现有客户端连接都将终止。请选择 View Connection Server 服务的重新启动时间，尽量避免中断桌面用户的工作。

步骤

1 在 View Administrator 中，选择 **[View Configuration（View 配置）] > [Global Settings（全局设置）]**，然后单击 **[Edit（编辑）]**。

2 要配置 SSL 进行客户端连接，请选择或取消选择 **[Require SSL for client connections and View Administrator（需要将 SSL 用于客户端连接和 View Administrator）]**。

3 单击 **[OK（确定）]** 保存更改。

4 重新启动 View Connection Server 服务以使更改生效。

在副本实例组中，您必须在每个 View Connection Server 实例和每个已配对的安全服务器上重新启动该服务。

5 重新配置所有防火墙和负载平衡程序，以允许客户端连接使用新的 SSL 配置。

有关更多信息，请参阅《*VMware View 体系结构规划指南*》文档。

配置 SSL 进行 View Transfer Server 通信

要配置是否将 SSL 用于在托管本地桌面的客户端计算机和 View Transfer Server 之间进行通信和数据传输，请在 View Administrator 中设置 View Connection Server 设置。

View Transfer Server 通信和数据传输的 SSL 设置专用于单个 View Connection Server 实例。您可能希望在为网络用户提供服务的实例上启用 SSL，但在内部用户专用的实例上则将其禁用。

默认情况下，SSL 已被禁止用于 View Transfer Server 通信和数据传输。

注意 这些 SSL 设置不会影响本地数据（始终是加密的）。

步骤

1 在 View Administrator 中，选择 **[View Configuration（View 配置）] > [Servers（服务器）]**。

2 选择 View Connection Server 实例，并单击 **[Edit（编辑）]**。

3 要配置 SSL 以在托管本地桌面的客户端计算机和 View Transfer Server 之间进行通信和数据传输，请选择或取消选择 **[Use SSL for Local Mode operations（为本地模式操作使用 SSL）]**。

这些操作包括检入和检出桌面以及将数据从客户端计算机复制到数据中心。

4 要配置 SSL 以将 View Composer 基础映像文件从 Transfer Server 存储库传输到托管本地桌面的客户端计算机，请选择或取消选择 **[Use SSL when provisioning desktops in Local Mode（部署本地模式桌面时使用 SSL）]**。

5 单击 **[OK（确定）]** 保存更改。

您的更改会立即生效。您无需重新启动 View Transfer Server 服务。

配置适用于 Windows 的 View Client 中的证书检查

可以使用 View Client Configuration ADM 模板文件 (`vdm_client.adm`) 中的安全相关组策略设置在基于 Windows 的 View Client 中配置服务器 SSL 证书检查。

如果您将 View Connection Server 配置为使用 SSL 连接进行客户端连接或 View Administrator 连接，则会执行证书检查。证书验证包括以下所有检查：

- 证书是否已被吊销？是否有可能确定证书是否已被吊销？
- 除了验证发件人身份和加密服务器通信外，证书还有什么其他用途？也就是说，证书类型是否正确？
- 证书是否过期，还是仅在未来有效？也就是说，根据计算机时钟，证书是否有效？
- 证书上的常用名称是否与发送它的服务器主机名称匹配？如果负载平衡器将 View Client 重定向到使用与用户输入的主机名不匹配的证书的服务器，则可能出现不匹配的情况。可能出现不匹配的另一个原因是，用户在客户端输入的是 IP 地址，而不是主机名。
- 证书是否由未知或不受信任的第三方认证机构 (CA) 签署？自签名证书是一种不受信任的 CA 类型。

  要通过这项检查，证书的信任链必须源于设备的本地 证书存储区。

首次设置 View 环境时，将使用默认的自签证书。默认情况下使用的证书验证模式是 **[Warn But Allow（警告但允许）]**。在这种模式下，出现以下任一服务器证书问题时，会显示一个警告，但用户可以选择忽略该警告并继续操作。

- View 服务器提供了一个自签名证书。在这种情况下，如果证书名与用户在 View Client 中提供的 View Connection Server 名称不匹配，这是可以接受的。
- 您的部署中配置的可验证证书已过期或尚未生效。

可以更改默认的证书验证模式。您可以设置为**[No Security（无安全）]** 模式，以便不执行任何证书检查。或者可以设置为**[Full Security（完整安全）]**模式，以便当任何一个检查失败时禁止用户连接到服务器。您还可以允许最终用户自己设置模式。

使用 Client Configuration ADM 模板文件可更改验证模式。View 组件的 ADM 模板文件安装在您的 View Connection Server 主机的 *安装目录*`\VMware\VMware View\Server\Extras\GroupPolicyFiles` 目录中。有关使用这些模板来控制 GPO 设置的信息，请参阅《VMware View 管理指南》文档。

创建事件数据库 8

您可创建一个事件数据库来记录 View Manager 事件的相关信息。如果您没有配置事件数据库，则必须详细查看日志文件才能获取关于事件的信息，而日志文件中仅包含非常有限的信息。

本章讨论了以下主题：

为 View 事件添加数据库和数据库用户

您可以通过将事件数据库添加到现有数据库服务器，从而创建一个事件数据库。然后就可以用企业级报告软件来分析数据库中的事件。

事件数据库的数据库服务器可以单独驻留在 View Connection Server 主机上或驻留在专用服务器上。另外，您也可以使用适当的现有数据库服务器，如托管 View Composer 数据库的服务器。

注意 您无需为此数据库创建 ODBC 数据源。

前提条件

- 确认在 View Connection Server 实例可访问的系统上具有支持的 Microsoft SQL Server 或 Oracle 数据库服务器。有关支持的数据库版本列表，请参阅第 10 页，“View Composer 的数据库要求”。
- 确认您拥有在数据库服务器上创建数据库和用户所需的数据库特权。
- 如果您不熟悉在 Microsoft SQL Server 数据库服务器上创建数据库的过程，请参阅第 28 页，“将 View Composer 数据库添加到 SQL Server”中介绍的步骤。
- 如果您不熟悉在 Oracle 数据库服务器上创建数据库的过程，请参阅第 30 页，“将 View Composer 数据库添加到 Oracle 11g 或 10g”中介绍的步骤。

步骤

1 为服务器添加一个新的数据库，并为其提供一个描述性名称，如 ViewEvents。

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

对于 Microsoft SQL Server 数据库，不要使用集成 Windows 身份验证 (Integrated Windows Authentication) 安全模式方法进行身份验证。一定要使用 SQL Server 身份验证 (SQL Server Authentication) 方法进行身份验证。

数据库随后创建，但在配置 View Administrator 的数据库之前不会安装模式。

下一步

按照第 84 页，“配置事件数据库”中的说明操作。

为事件报告准备 SQL Server 数据库

在使用 View Administrator 在 Microsoft SQL Server 上配置事件数据库之前，您必须配置正确的 TCP/IP 属性并确认该服务器使用了 SQL Server 身份验证 (SQL Server Authentication)。

前提条件

- 为事件报告创建一个 SQL Server 数据库。请参阅第 83 页，“为 View 事件添加数据库和数据库用户”。
- 确认您拥有配置数据库所需的数据库特权。
- 确认数据库服务器使用 SQL Server 身份验证 (SQL Server Authentication) 方法。不要使用 Windows 身份验证 (Windows Authentication)。

步骤

1 打开 SQL Server Configuration Manager 并展开 **[SQL Server*YYYY*Network Configuration（SQL Server YYYY 网络配置）]**。

2 选择 **[Protocols for*server_name*（server_name 使用的协议）]**。

3 在协议列表中，右键单击 **[TCP/IP]** 并选择 **[Properties（属性）]**。

4 将 **[Enabled（启用）]** 属性设置为 **[Yes（是）]**。

5 确认已分配了一个端口，或者在必要时分配一个端口。

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

6 确认该端口未被防火墙阻止。

下一步

使用 View Administrator 将数据库连接到 View Connection Server。按照第 84 页，“配置事件数据库”中的说明操作。

配置事件数据库

事件数据库会将 View 事件的相关信息存储为数据库记录，而不是日志文件记录。

安装 View Connection Server 实例后，您就可以配置事件数据库了。您只需要在 View Connection Server 组中配置一个主机。组中剩余的主机会自动进行配置。

您可以使用 Microsoft SQL Server 或 Oracle 数据库报告工具来查看数据库表中的事件。有关更多信息，请参阅《VMware View Integration》（VMware View 集成指南）文档。

前提条件

配置事件数据库时需要以下信息：

- 数据库服务器的 DNS 名称或 IP 地址。
- 数据库服务器的类型：Microsoft SQL Server 或 Oracle。
- 用来访问数据库服务器的端口号。适用于 Oracle 的默认端口号是 1521；适用于 SQL Server 的默认端口号是 1433。对于 SQL Server，如果数据库服务器是已经命名的实例，或者您使用的是 SQL Server Express，您可能需要确定端口号。有关连接到已命名的 SQL Server 实例的信息，请参阅 http://support.microsoft.com/kb/265808 上的 Microsoft 知识库 (KB) 文章。
- 您在数据库服务器上创建的事件数据库名称。请参阅第 83 页，“为 View 事件添加数据库和数据库用户”。

- 为该数据库创建的用户的用户名和密码。请参阅第 83 页，“为 View 事件添加数据库和数据库用户”。

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

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

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

步骤

1 在 View Administrator 中，选择 **[View Configuration（View 配置）] > [Event Configuration（事件配置）]**。

2 在 **[Event Configuration（事件配置）]** 区域中，单击 **[Edit（编辑）]**，然后在提供的字段中输入信息，最后单击 **[OK（确定）]**。

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

  这些设置可控制事件在 View Administrator 界面中显示的时间长度。这段时间过后，这些事件仅在历史记录数据库表中可用。

  [Database Configuration（数据库配置）] 窗口可显示事件数据库的当前配置。

4 选择 **[Monitoring（监视）] > [Events（事件）]**，确认已成功连接到事件数据库。

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

在 View Administrator 的 [Dashboard（仪表板）] 中，[System Component Status（系统组件状态）] 的 [Reporting Database（报告数据库）] 标题下会显示事件数据库服务器。

安装和启动 View Client 9

您可以从 VMware 网站或由 View Connection Server 提供的 Web 访问页面（即 View Portal）获取基于 Windows 的 View Client 安装程序。安装 View Client 后，您可以为最终用户设置各种启动选项。

有关安装和使用其他 View 客户端（如适用于 Mac 的 View Client 和适用于 iPad 的 View Client）的信息，请参阅适用于特定客户端的文档。请访问 https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html。

本章讨论了以下主题：

安装基于 Windows 的 View Client 或 View Client with Local Mode

最终用户需要从物理机打开 View Client 来连接其虚拟桌面。您可以运行基于 Windows 的安装程序文件来安装 View Client 的所有组件。

如果 View 管理员启用了某些显示选项，那么除了通过 View Client 访问虚拟桌面外，最终用户还可以使用 View Client 配置这些显示选项。例如，最终用户可以选择显示协议或窗口大小，或者使用当前登录凭据进行 View 身份验证。

使用 View Client with Local Mode 时，最终用户会将虚拟桌面的副本下载到他们的本地计算机。之后，最终用户将可以在没有网络连接的情况下使用虚拟桌面。这会最大程度降低延迟并提高性能。

View Client with Local Mode 是一个完全受支持的功能，在早期版本中是一个被称为 View Client with Offline Desktop 的试验性功能。

前提条件

- 确认您可以作为客户端系统的管理员登录。
- 确认客户端系统使用支持的操作系统。请参阅第 14 页，“基于 Windows 的 View Client 和 View Client with Local Mode 支持的操作系统”。
- 确认未安装 View Agent。
- 如果您计划安装 View Client with Local Mode，请确认您的许可中包括 View Client with Local Mode。

- 如果您计划安装 View Client with Local Mode，请确认未安装以下任何产品：VMware View Client、VMware Player、VMware Workstation、VMware ACE 和 VMware Server。
- 确定是否允许使用客户端设备的用户从虚拟桌面访问本地连接的 USB 设备。如果不允许，则必须取消选择向导中显示的 **[USB Redirection]** 组件。
- 如果您计划安装 **[USB Redirection]** 组件，请确认客户端计算机上的 Windows 自动更新功能未关闭。
- 确定是否使用允许最终用户作为当前登录的用户登录到 View Client 及其虚拟桌面这一功能。用户在登录客户端系统时输入的凭据信息会传送到 View Connection Server 实例，并最终传送到虚拟桌面。某些客户端操作系统不支持该功能。
- 如果您不希望要求最终用户提供托管用户虚拟机的 View Connection Server 实例的 IP 地址或主机域名全称 (FQDN)，请确定可在安装期间提供的 IP 地址或 FQDN。

步骤

1 作为拥有管理员特权的用户登录到客户端系统。

2 在客户端系统上，从 VMware 产品页面 http://www.vmware.com/cn/products/ 下载 View Client 安装程序文件。

选择合适的安装程序文件，其中 *xxxxxx* 是内部版本号，*y.y.y* 是版本号。

选项	操作
64 位操作系统上的 View Client	对于 View Client，请选择 `VMware-viewclient-x86_64-y.y.y-xxxxxx.exe`。 对于 View Client with Local Mode，请选择 `VMware-viewclientwithlocalmode-x86_64-y.y.y-xxxxxx.exe`。
32 位操作系统上的 View Client	对于 View Client，请选择 `VMware-viewclient-y.y.y-xxxxxx.exe`。 对于 View Client with Local Mode，请选择 `VMware-viewclientwithlocalmode-y.y.y-xxxxxx.exe`。

3 要启动 View Client 安装程序，请双击安装程序文件。

4 按照提示安装所需组件。

VMware View Client 服务会安装在 Windows 客户端计算机上。View Client 的服务名是 `wsnm.exe`。USB 组件的服务名是 `wsnm_usbctrl.exe`。

下一步

启动 View Client 并确认您可以登录到正确的虚拟桌面。请参阅第 88 页，“启动基于 Windows 的 View Client 或 View Client with Local Mode” 或 第 90 页，“使用 View Portal 安装 View Client”。

启动基于 Windows 的 View Client 或 View Client with Local Mode

在最终用户访问虚拟桌面前，请测试您能否从客户端设备登录虚拟桌面。您可以从 **[Start（开始）]** 菜单或客户端系统上的桌面快捷方式启动 View Client。

在具有网络连接的环境中，用户会话将通过 View Connection Server 进行身份验证。

前提条件

- 确认客户端设备上已安装 View Client 或 View Client with Local Mode。
- 如果您计划使用 View Client with Local Mode，请确认您的许可中包含 View Client with Local Mode，而且 View 桌面可满足本地模式的要求。请参阅《*VMware View 管理指南*》文档中有关设置本地桌面部署的概述主题。

- 确认已创建虚拟桌面池且计划使用的用户帐户有权访问该桌面。请参阅《*VMware View 管理指南*》文档中有关创建桌面池的主题。
- 确认您拥有可访问虚拟桌面的 View Connection Server 实例的主机域名全称 (FQDN) 或 IP 地址。

步骤

1 如果 View Client 在安装后没有自动启动，请双击桌面快捷方式或单击 **[Start（开始）] > [Programs（程序）] > [VMware] > [VMware View Client]**。

2 在 **[Connection Server（连接服务器）]** 下拉菜单中，输入 View Connection Server 的主机名或 IP 地址。

3 确认该对话框中的其他可选设置已按照您的配置显示。

选项	描述
Log in as current user（作为当前用户登录）	根据 View Administrator 中的全局设置，该复选框将会显示或隐藏。如果您计划检出 View 桌面以在本地模式下使用，请不要选中该复选框。
Use secure connection (SSL)（使用安全连接 (SSL)）	如果选中该复选框，则还必须选中 View Administrator 中的 **[Use SSL for client connections（使用 SSL 进行客户端连接）]** 全局设置。
Port（端口）	安全连接的默认端口是 443。
Autoconnect（自动连接）	如果您选中该复选框，则下次启动 View Client 时，**[Connection Server（连接服务器）]** 字段会被禁用，您会连接到选中 **[Autoconnect（自动连接）]** 复选框时指定的服务器。要取消选中该复选框，请取消出现的下一个对话框并单击 **[Options（选项）]** 来显示和更改该设置。

4 单击 **[Connect（连接）]**。

5 输入有权使用至少一个桌面池的用户的凭据，选择域，然后单击 **[Login（登录）]**。

如果使用 **`user@domain`** 格式键入用户名，则该名称会因包含 @ 符号而被视为用户主体名称 (UPN)，此时域下拉菜单将被禁用。

有关创建桌面池以及为用户授予池访问权限的信息，请参阅《*VMware View 管理指南*》文档。

6 （可选）在 **[Display（显示）]** 下拉菜单中，选择显示 View 桌面的窗口大小。

7 （可选）要选择显示协议，请单击列表中桌面旁的向下箭头，再单击 **[Display Protocol（显示协议）]**，然后选择协议。

该选项仅在您的 View administrator 启用它后才可用。

8 从桌面池列表中选择一个桌面，然后单击 **[Connect（连接）]**。

View Client 将尝试连接到指定池中的桌面。

连接成功后，屏幕上将显示客户端窗口。

如果针对 View Connection Server 的身份验证失败或者 View Client 无法连接至桌面，请执行以下任务：

- 确认使用安全 (SSL) 连接的 View Client 设置与 View Administrator 中的全局设置匹配。例如，如果在客户端上取消选中针对安全连接的复选框，则还必须在 View Administrator 中取消选中该复选框。
- 确认 View Connection Server 的安全证书工作正常。如果无法正常工作，桌面上的 View Agent 可能无法使用，而且会在 Transfer Server 状态中显示为尚未就绪。这些现象均出自证书问题引起的其他连接问题。
- 确认 View Connection Server 实例上设置的标签允许从该用户连接。请参阅 *VMware View 管理*文档。
- 确认该用户有权访问此桌面。请参阅 *VMware View 管理*文档。
- 确认客户端计算机允许远程桌面连接。

下一步

- 配置启动选项。

  如果您不希望要求最终用户提供 View Connection Server 的主机名或 IP 地址，或是希望配置其他启动选项，请使用 View Client 命令行选项来创建桌面快捷方式。请参阅 *VMware View 管理*文档。

- 检出可在本地模式下使用的桌面。

  最终用户通过在 View Client with Local Mode 提供的列表中单击桌面旁的向下箭头，确定该桌面是否可以检出。如果可以在本地模式下使用桌面，**[Check out（检出）]** 选项将出现在右键菜单中。只有检出桌面的用户才能访问该桌面，即使某个用户组有权访问桌面也是如此。

使用 View Portal 安装 View Client

通过打开浏览器并浏览到 View Portal 网页可以方便地安装 View Client 或 View Client with Local Mode 应用程序。您可以使用 View Portal 下载适用于 Windows 和 Mac 客户端计算机的完整 View Client 安装程序。

自 View 4.5 起，View Portal 可安装适用于 Windows 的完整 View Client（包含或不包含本地模式）以及适用于 Mac 的 View Client。

注意 View Portal 不支持 Linux。适用于 Linux 的本地客户端仅能通过认证的 VMware 合作伙伴获得。

前提条件

- 确认您拥有 View Connection Server 实例的 URL。
- 确认您可以作为客户端系统的管理员登录。
- 确认已创建虚拟桌面且计划使用的用户帐户有权访问该桌面。
- 确认客户端系统使用支持的操作系统。请参阅第 14 页，“基于 Windows 的 View Client 和 View Client with Local Mode 支持的操作系统”。
- 确认未安装 View Agent。
- 如果您计划安装 View Client with Local Mode，请确认您的许可中包括 View Client with Local Mode。
- 如果您计划安装 View Client with Local Mode，请确认未安装以下任何产品：VMware View Client、VMware Player、VMware Workstation、VMware ACE 和 VMware Server。
- 确定是否允许使用客户端设备的用户从虚拟桌面访问本地连接的 USB 设备。如果不允许，则必须取消选择向导中显示的 **[USB Redirection]** 组件。
- 如果您计划安装 **[USB Redirection]** 组件，请确认客户端计算机上的 Windows 自动更新功能未关闭。

步骤

1 作为拥有管理员特权的用户登录到客户端系统。

2 打开浏览器并输入提供虚拟桌面访问权限的 View Connection Server 实例的 URL。

  Internet Explorer 可确定是否有升级可供使用，而 Firefox 和 Safari 则不具有这个功能。此外，在安装程序列表中，如果客户端使用 32 位系统，则 Internet Explorer 会列出 32 位安装程序，如果如果客户端使用 64 位系统，则 Internet Explorer 会列出 64 位安装程序，而 Firefox 会将 32 位和 64 位安装程序全部列出。

3 按网页上的提示操作。

  如果 View Connection Server 提供的版本比客户端设备上安装的版本新，您可以选择执行升级。如果当前版本与客户端设备上的版本相同，View Portal 会启动客户端计算机上安装的 View Client。

  如果您使用的是旧版本的 View Client 并且客户端连接需要使用智能卡，则 Internet Explorer 浏览器会在 View Portal 检查当前 View Client 版本前提示您插入智能卡。

4 如果 Internet Explorer 提示您插入智能卡，您可以插入智能卡或单击 **[Cancel（取消）]**。

插入智能卡和单击 **[Cancel（取消）]** 的作用相同。

下一步

连接到 View 桌面。请参阅第 88 页，“启动基于 Windows 的 View Client 或 View Client with Local Mode”。

在 Windows 客户端上设置虚拟打印机功能的打印首选项

借助虚拟打印功能，最终用户可从 View 桌面使用本地或网络打印机，而不必在 View 桌面上安装额外的打印驱动程序。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。

打印机被添加到本地 Windows 计算机后，View 会将其加入到 View 桌面的可用打印机列表。无需进行进一步配置。拥有管理员特权的用户仍然可以在 View 桌面上安装打印机驱动程序，且不会与虚拟打印机组件发生冲突。

重要事项 该功能不支持以下类型的打印机：

- 使用 USB 重定向功能连接到 View 桌面中虚拟 USB 端口的 USB 打印机

  必须从 View 桌面断开 USB 打印机，才能在桌面上使用虚拟打印功能。

- 用于打印到文件的 Windows 功能

  在 [Print（打印）] 对话框中选择 **[Print to file（打印到文件）]** 复选框的操作不起作用。使用可创建文件的打印机驱动程序即可以实现操作。例如，您可以使用 PDF 编写程序打印到 PDF 文件。

前提条件

确认已经在 View 桌面上安装 View Agent 的 Virtual Printing 组件。View 桌面文件系统的驱动程序位于 `C:\Program Files\Common Files\VMware\Drivers\Virtual Printer`。

在准备将虚拟机用作 View 桌面时，需要安装 View Agent。有关更多信息，请参阅*《VMware View 管理指南》*文档。

步骤

1 在 View 桌面中，单击 **[Start（开始）] > [Settings（设置）] > [Printers and Faxes（打印机和传真）]**。

2 在 [Printers and Faxes（打印机和传真）] 窗口中，右键单击一个本地可用的打印机并选择 **[Properties（属性）]**。

在 Windows 7 桌面上，即使有其他打印机可用，您可能也只可以看见默认打印机。要查看其他打印机，请右键单击默认的打印机并选择 **[Printer properties（打印机属性）]**。

3 在 [Print Properties（打印属性）] 窗口中，单击 **[ThinPrint Device Setup（ThinPrint 设备设置）]** 选项卡并指定要使用的设置。

4 在 **[General（常规）]** 选项卡上，单击 **[Printing Preferences（打印首选项）]** 并编辑页面和颜色设置。

5 在 **[Advanced（高级）]** 选项卡上，设置双面打印和纵向（长边）或横向（短边）打印首选项。

6 要预览主机中的每一次打印输出，请启用 **[Preview on client before printing（打印前在客户端中预览）]**。

通过预览功能，您可以使用任意打印机及其所有可用属性。

7 在 **[Adjustment（调整）]** 选项卡上，查看自动打印调整的设置。

VMware 建议您保留默认设置。

8 单击 **[OK（确定）]**。

使用 USB 打印机

在 View 环境中，虚拟打印机和重定向的 USB 打印机可以毫无冲突地协同工作。

USB 打印机是一种连接到本地客户端系统 USB 端口的打印机。要将打印作业发送到 USB 打印机，可以使用 USB 重定向功能或虚拟打印功能。

- 只要 View 桌面上也安装了所需的驱动程序，您便可以使用 USB 重定向功能将 USB 打印机附加到 View 桌面中的虚拟 USB 端口。

  如果您使用重定向功能，打印机将不再附加到客户端的物理 USB 端口，正因如此，USB 打印机才不会出现在虚拟打印功能显示的本地打印机列表中。这也意味着您可以从 View 桌面而非本地客户端计算机使用 USB 打印机打印。

- 在 Windows 客户端中，您也可以使用虚拟打印功能将打印作业发送至 USB 打印机。如果您使用虚拟打印功能，您可以从 View 桌面和本地客户端使用 USB 打印机打印，而且无需在 View 桌面上安装打印驱动程序。

静默安装 View Client

通过在命令行界面键入安装程序文件名和安装选项，您可以静默安装 View Client。通过静默安装，您可以在大型企业中高效部署 View 组件。

设置组策略以允许静默安装 View Client with Local Mode

必须先配置 Microsoft Windows 组策略以允许使用提升的特权进行安装，才能静默安装 View Client with Local Mode。

您不需要设置这些组策略，就可以静默安装 View Client。只有在安装 View Client with Local Mode 时才需要这些策略。

您必须设置计算机和客户端计算机用户的 Windows Installer 组策略。

前提条件

确认在安装 View Client with Local Mode 的 Windows 客户端计算机上拥有管理员特权。

步骤

1 登录客户端计算机并单击 **[Start（开始）] > [Run（运行）]**。

2 键入 **gpedit.msc** 并单击 **[OK（确定）]**。

3 在 [Group Policy Object Editor（组策略对象编辑器）] 中，单击 **[Local Computer Policy（本地计算机策略）] > [Computer Configuration（计算机配置）]**。

4 展开 **[Administrative Templates（管理模板）]**，打开 **[Windows Installer]** 文件夹，然后双击 **[Always install with elevated privileges（始终使用提升的特权安装）]**。

5 在 **[Always install with elevated privileges Properties（始终使用提升的特权安装属性）]** 窗口中，单击 **[Enabled（启用）]**，然后单击 **[OK（确定）]**。

6 在左侧窗格中，单击 **[User Configuration（用户配置）]**。

7 展开 **[Administrative Templates（管理模板）]**，打开 **[Windows Installer]** 文件夹，然后双击 **[Always install with elevated privileges（始终使用提升的特权安装）]**。

8 在 **[Always install with elevated privileges Properties（始终使用提升的特权安装属性）]** 窗口中，单击 **[Enabled（启用）]**，然后单击 **[OK（确定）]**。

下一步

静默安装 View Client with Local Mode。

静默安装 View Client

您可以使用 Microsoft Windows Installer (MSI) 的静默安装功能，在多个 Windows 计算机上安装 View Client 或 View Client with Local Mode。在静默安装中，您需要使用命令行，无需响应向导的提示。

前提条件

- 确认您可以作为客户端系统的管理员登录。
- 确认客户端系统使用支持的操作系统。请参阅第 14 页，“基于 Windows 的 View Client 和 View Client with Local Mode 支持的操作系统”。
- 如果您计划安装 View Client with Local Mode，请确认您的许可中包括 View Client with Local Mode。
- 如果您计划安装 View Client with Local Mode，请确认未安装以下任何产品：VMware View Client、VMware Player、VMware Workstation、VMware ACE 和 VMware Server。
- 确定是否使用允许最终用户作为当前登录的用户登录到 View Client 及其虚拟桌面这一功能。用户在登录客户端系统时输入的凭据信息会传送到 View Connection Server 实例，并最终传送到虚拟桌面。某些客户端操作系统不支持该功能。
- 如果您不希望要求最终用户提供托管用户虚拟机的 View Connection Server 实例的 IP 地址或主机域名全称 (FQDN)，请确定可在安装期间提供的 IP 地址或 FQDN。
- 熟悉 MSI 安装程序命令行选项。请参阅第 46 页，“Microsoft Windows Installer 命令行选项”。
- 熟悉 View Client 可用的静默安装 (MSI) 属性。请参阅第 94 页，“View Client 的静默安装属性”。
- 确定是否允许最终用户从虚拟桌面访问本地连接的 USB 设备。如果不允许，请将 MSI 属性 `ADDLOCAL` 设置为您想要使用的功能列表并忽略 USB 功能。有关详细信息，请参阅第 94 页，“View Client 的静默安装属性”。
- 如果安装 View Client with Local Mode，请确认已在客户端计算机上配置了静默安装所需的 Windows Installer 组策略。请参阅第 92 页，“设置组策略以允许静默安装 View Client with Local Mode”。

步骤

1 在客户端系统上，从 VMware 产品页面 http://www.vmware.com/cn/products/ 下载 View Client 安装程序文件。

选择合适的安装程序文件，其中 *xxxxxx* 是内部版本号，*y.y.y* 是版本号。

选项	操作
64 位操作系统上的 View Client	对于 View Client，请选择 `VMware-viewclient-x86_64-y.y.y-xxxxxx.exe`。 对于 View Client with Local Mode，请选择 `VMware-viewclientwithlocalmode-x86_64-y.y.y-xxxxxx.exe`。
32 位操作系统上的 View Client	对于 View Client，请选择 `VMware-viewclient-y.y.y-xxxxxx.exe`。 对于 View Client with Local Mode，请选择 `VMware-viewclientwithlocalmode-y.y.y-xxxxxx.exe`。

2 在 Windows 客户端计算机上打开命令提示符。

3 在一行中键入安装命令。

以下示例会安装带有单点登录功能和 USB 重定向功能的 View Client，并为 View Client 用户配置了默认的 View Connection Server 实例：`VMware-viewclient-y.y.y-xxxxxx.exe /s /v"/qn REBOOT=ReallySuppress VDM_SERVER=cs1.companydomain.com ADDLOCAL=Core,TSSO,USB"`

以下示例会安装 View Client with Local Mode：`VMware-viewclientwithlocal-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,MVDI"`

注意 必须使用 `Core` 功能。

VMware View Client 服务会安装在 Windows 客户端计算机上。

下一步

启动 View Client 并确认您可以登录到正确的虚拟桌面。请参阅第 88 页，“启动基于 Windows 的 View Client 或 View Client with Local Mode” 或 第 90 页，“使用 View Portal 安装 View Client”。

View Client 的静默安装属性

通过命令行静默安装 View Client 时，您可以包含特定属性。您必须使用 *属性*=*值* 格式，以便 Microsoft Windows Installer (MSI) 解释属性和值。

表 9–1 显示了您可以在命令行中使用的 View Client 静默安装属性。

表 9–1 View Client 静默安装的 MSI 属性

MSI 属性	描述	默认值
INSTALLDIR	View Client 软件的安装路径和文件夹。 例如：`INSTALLDIR=""D:\abc\my folder""` 括住路径的两组双引号可允许 MSI 安装程序将空格识别为路径的一部分。 此 MSI 属性为可选属性。	`%ProgramFiles%\VMware\VMware View\Client`
VDM_SERVER	View Client 用户默认连接的 View Connection Server 实例的主机域名全称 (FQDN) 或 IP 地址。配置此属性时，View Client 用户不需要提供此 FQDN 或 IP 地址。 例如：`VDM_SERVER=cs1.companydomain.com` 此 MSI 属性为可选属性。	无
DESKTOP_SHORTCUT	配置 View Client 的桌面快捷方式图标。 值为 1 时表示安装快捷方式。值为 0 时表示不安装快捷方式。 此 MSI 属性为可选属性。	1
QUICKLAUNCH_SHORTCUT	配置 View Client 快速启动托盘上的快捷方式图标。 值为 1 时表示安装快捷方式。值为 0 时表示不安装快捷方式。 此 MSI 属性为可选属性。	1
STARTMENU_SHORTCUT	配置 [Start（开始）] 菜单中的 View Client 快捷方式。 值为 1 时表示安装快捷方式。值为 0 时表示不安装快捷方式。 此 MSI 属性为可选属性。	1

在静默安装命令中，您可以使用 MSI 属性 `ADDLOCAL=` 指定 View Client 安装程序配置的功能。每个静默安装功能都对应一个设置选项，您可以在交互安装过程中选择这些选项。

表 9–2 显示了您可以在命令行界面键入的 View Client 功能及相应的交互安装选项。

表 9–2 View Client 静默安装功能和交互自定义安装选项

静默安装功能	交互安装中的自定义安装选项
Core 使用 MSI 属性 ADDLOCAL= 指定单个功能时，必须包含 **Core**。 指定 ADDLOCAL=ALL 时，会安装所有 View Client 和 View Client with Local Mode 功能（包括 Core）。	无。 在交互安装过程中，会默认安装核心 View Client 功能。
MVDI 安装 View Client with Local Mode 和通过 ADDLOCAL= 指定单个功能时使用此功能。 指定 ADDLOCAL=ALL 时，会安装所有 View Client with Local Mode 功能（包括 MVDI）。	无。 交互安装 View Client with Local Mode 时，会默认安装 MVDI 功能。 交互安装 View Client 时，将无法使用 MVDI 功能。
ThinPrint	虚拟打印
TSSO	单点登录 (SSO)
USB	USB 重定向

索引

U

V