VMware View 安全性指南

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-000575-00

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 安全性

《VMware View 安全性》提供了对 VMware View™ 安全功能的简明参考。

- 所需的系统和数据库登录帐户。
- 安全性相关配置选项和设置。
- 必须受到保护的资源，如安全性相关的配置文件和密码，以及对安全操作的建议访问控制。
- 日志文件的位置及其用途。
- 必须打开或启用以确保 VMware View 正常运行的外部接口、端口和服务。

目标读者

本书所述信息面向 IT 决策制定者、体系结构人员、管理员和其他必须熟悉 VMware View 安全组件的读者。本参考指南应当与《VMware View 强化指南》(VMware View Hardening Guide) 和其他 VMware View 文档结合使用。

VMware View 安全性参考

配置安全的 View 环境时，可以在多个位置更改设置并做出调整，以保护您的系统。

- VMware View 帐户第 8 页，

  您必须设置管理 VMware View 组件的系统和数据库帐户。

- VMware View 安全性设置第 8 页，

  VMware View 中包含一些设置，您可以使用它们来调整配置的安全性。您可以使用 View Administrator、编辑组配置文件或使用“ADSI 编辑”实用程序来访问设置（视情况而定）。

- VMware View 资源第 15 页，

  VMware View 中包含若干配置文件和类似资源，必须为它们提供保护。

- VMware View 日志文件第 15 页，

  VMware View 软件会创建记录其组件安装和运行情况的日志文件。

- VMware View TCP 和 UDP 端口第 16 页，

  View 使用 TCP 和 UDP 端口进行组件之间的网络访问。您可能要重新配置防火墙，以允许相应端口上的访问。

- View Connection Server 主机上的服务第 20 页，

  View Manager 的运行依赖于 View Connection Server 主机上运行的若干服务。如果您想调整这些服务的运行，就需要先熟悉这些服务。

- 安全服务器上的服务第 21 页，

  View Manager 的运行依赖于安全服务器上运行的若干服务。如果您想调整这些服务的运行，就需要先熟悉这些服务。

- View Transfer Server 主机上的服务第 21 页，

  本地桌面的传输操作依赖于 View Transfer Server 主机上运行的服务。如果您想调整这些服务的运行，就需要先熟悉这些服务。

VMware View 帐户

您必须设置管理 VMware View 组件的系统和数据库帐户。

表 1 VMware View 系统帐户

VMware View 组件	所需帐户
View Client	在 Active Directory 中为有权访问 View 桌面的用户配置用户帐户。用户帐户必须是远程桌面用户组的成员，但无需 View 管理员特权。
View Client with Local Mode	在 Active Directory 中为有权访问本地模式 View 桌面的用户配置用户帐户。用户帐户不需要 View 管理员特权。 作为桌面的标准最佳实践，请确保 为每个要在本地模式下 使用的 View 桌面的本地管理员帐户 创建一个唯一的密码。
vCenter Server	在 Active Directory 中配置一个有权在 vCenter Server 中执行所需 View Manager 支持操作的用户帐户。 有关所需特权的信息，请参阅《VMware View 安装指南》文档。
View Composer	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。 用户帐户不应是 View 管理帐户。为该帐户授予在指定的 Active Directory 容器中创建和移除计算机对象所需的最低特权。例如，该帐户不需要域管理员特权。 有关所需特权的信息，请参阅《VMware View 安装指南》文档。
View Connection Server、Security Server 或 View Transfer Server	最初，View Connection Server 计算机上本地管理员组 (BUILTIN\Administrators) 的所有用户成员都能登录到 View Administrator。 在 View Administrator 中，您可以使用 **[View Configuration（View 配置）] > [Administrators（管理员）]** 更改 View 管理员列表。 有关所需特权的信息，请参阅《VMware View 管理指南》文档。

表 2 VMware View 数据库帐户

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

为减少安全漏洞风险，请采取以下措施：

- 在您的组织使用的数据库服务器以外的服务器上配置 View 数据库。
- 不允许一个用户帐户访问多个数据库。
- 配置单独帐户访问 View Composer 和事件数据库。

VMware View 安全性设置

VMware View 中包含一些设置，您可以使用它们来调整配置的安全性。您可以使用 View Administrator、编辑组配置文件或使用“ADSI 编辑”实用程序来访问设置（视情况而定）。

View Administrator 中的安全性相关全局设置

用于客户端会话和连接的安全性相关全局设置可通过 View Administrator 中的 **[View Configuration（View 配置）] > [Global Settings（全局设置）]** 访问。

表 3 安全性相关的全局设置

设置	描述
Disable Single Sign-On for Local Mode operations（对本地模式操作禁用单点登录）	确定在用户登录本地桌面时是否启用单点登录。 默认情况下禁用此设置。
Enable automatic status updates（启用自动状态更新）	确定 View Manager 是否定期更新 View Administrator 中的全局状态窗格和仪表板。如果启用此设置，已登录 View Administrator 的任何用户的空闲会话都不会超时。 默认情况下禁用此设置。
Message security mode（消息安全模式）	确定是否对 View Manager 组件之间传输的 JMS 消息进行签发和验证。 如果设置为 **[Disabled（禁用）]**，消息安全模式将被禁用。 如果设置为 **[Enabled（启用）]**，View 组件将拒绝未签名的消息。 如果设置为 **[Mixed（混合）]**，消息安全模式将被启用，但不会强制用于 View Manager 3.0 之前的 View 组件。 默认设置为 **[Disabled（禁用）]**。
Reauthenticate secure tunnel connections after network interruption（网络中断后对安全加密链路连接重新进行身份验证）	如果 View 客户端通过安全加密链路连接到 View 桌面，则可以确定在网络中断后是否必须重新对用户凭据进行身份验证。 该设置在默认情况下为启用状态。
Require SSL for client connections and View Administrator（需要将 SSL 用于客户端连接和 View Administrator）	确定 View Connection Server 和 View 桌面客户端之间，以及 View Connection Server 和访问 View Administrator 的客户端之间是否使用安全的 SSL 通信通道。 该设置在默认情况下为启用状态。
Session timeout（会话超时）	确定在用户登录 View Connection Server 后，能够将会话保持多长时间。 默认值是 600 分钟。

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

View Administrator 中的安全性相关服务器设置

安全性相关的服务器设置可通过 View Administrator 中的 **[View Configuration（View 配置）] > [Server（服务器）]** 访问。

表 4 安全性相关的服务器设置

设置	描述
Connect using SSL（使用 SSL 连接）	如果启用，View 将使用 SSL 加密与 vCenter Server 进行通信。 该设置在默认情况下为启用状态。
Use PCoIP Secure Gateway for PCoIP connections to desktop（使用 PCoIP 安全网关与桌面建立 PCoIP 连接）	如果启用，当用户使用 PCoIP 显示协议连接至 View 桌面时，View Client 会和 View Connection Server 或安全服务器主机再建立一条安全连接。 如果禁用，将绕开 View Connection Server 或安全服务器主机，直接在客户端系统和 View 桌面虚拟机之间建立桌面会话。 默认情况下禁用此设置。
Use secure tunnel connection to desktop（使用安全加密链路连接桌面）	如果启用，当用户连接至 View 桌面时，View Client 会和 View Connection Server 或安全服务器主机建立另一条 HTTPS 连接。 如果禁用，将绕开 View Connection Server 或安全服务器主机，直接在客户端系统和 View 桌面虚拟机之间建立桌面会话。 该设置在默认情况下为启用状态。

表 4 安全性相关的服务器设置（续）

设置	描述
Use secure tunnel connection for Local Mode operations（为本地模式操作使用安全加密链路连接）	如果启用，本地桌面将使用安全加密链路进行通信。网络流量将通过 View Connection Server 或安全服务器（如已配置）传送。 如果禁用，数据传输将直接在本地桌面和数据中心内相应的远程桌面间进行。 默认情况下禁用此设置。
Use SSL for Local Mode operations（为本地模式操作使用 SSL）	如果启用，客户端计算机与数据中心之间的通信和数据传输将使用 SSL 加密。这些操作包括检入和检出桌面、将数据从客户端计算机复制到数据中心，但不包括传输 View Composer 基础映像。 默认情况下禁用此设置。
Use SSL when provisioning desktops in Local Mode（部署本地模式桌面时使用 SSL）	如果启用，将 View Composer 基础映像文件从 Transfer Server 存储库传输到客户端计算机时将使用 SSL 加密。 默认情况下禁用此设置。

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

View Agent 配置模板中的安全性相关设置

View Agent 的 ADM 模板文件 (`vdm_agent.adm`) 中提供了安全性相关设置。除非另作说明，上述设置中仅包含一项 [Computer Configuration（计算机配置）] 设置。

安全性设置存储在客户计算机注册表的 `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Agent\Configuration` 位置。

表 5 View Agent 配置模板中的安全性相关设置

设置	注册表值名称	描述
`AllowDirectRDP`	`AllowDirectRDP`	确定非 View 客户端是否可以使用 RDP 直接连接到 View 桌面。如果禁用此设置，View Agent 将只允许通过 View Client 建立的受 View 管理的连接。 **重要事项** 为确保 View 正常运行，每个桌面的客户操作系统中都必须运行 Windows 终端服务。您可以使用此设置防止用户通过 RDP 直接连接到其桌面。 该设置在默认情况下为启用状态。
`AllowSingleSignon`	`AllowSingleSignon`	确定是否通过单点登录 (SSO) 将用户连接到 View 桌面。启用此设置后，用户在与 View Client 连接时只需输入凭据。禁用此设置时，用户必须在进行远程连接时重新进行身份验证。 该设置在默认情况下为启用状态。
`CommandsToRunOnConnect`	`CommandsToRunOnConnect`	指定在会话首次连接时运行的一组命令或命令脚本。 默认情况下未指定列表。
`CommandsToRunOnReconnect`	`CommandsToRunOnReconnect`	指定在会话断开后重新连接时运行的一组命令或命令脚本。 默认情况下未指定列表。
`ConnectionTicketTimeout`	`VdmConnectionTicketTimeout`	指定 View 连接票证的有效时间（以秒为单位）。 如果未配置此设置，则使用默认超时时限 120 秒。
`CredentialFilterExceptions`	`CredentialFilterExceptions`	指定不允许加载代理 CredentialFilter 的可执行文件。文件名不得包含路径或后缀。使用分号分隔多个文件名。 默认情况下未指定列表。

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

View Client 配置模板中的安全性设置

View Client 的 ADM 模板文件 (vdm_client.adm) 中提供了安全性相关设置。除非特别说明，上述设置中仅包含一项 [Computer Configuration（计算机配置）] 设置。如果 [User Configuration（用户配置）] 设置可用，而且您为它定义了一个值，它将覆盖等效的 [Computer Configuration（计算机配置）] 设置。

安全性设置存储在主机注册表的 HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client\Security 位置。

表 6 View Client 配置模板中的安全性设置

设置	注册表值名称	描述
Allow command line credentials（允许命令行凭据）	AllowCmdLineCredentials	确定是否可以通过 View Client 命令行选项提供用户凭据。启用此设置后，当用户从命令行运行 View Client 时 smartCardPIN 和 password 选项不可用。 该设置在默认情况下为启用状态。
Brokers Trusted For Delegation（获得委派信任的 Broker）	BrokersTrustedForDelegation	指定接受用户身份和凭据信息（在用户选中了 **[Log in as current user（作为当前用户登录）]** 复选框时传送）的 View Connection Server 实例。如果您未指定任何 View Connection Server 实例，所有 View Connection Server 实例都会接受该信息。 使用以下某种格式添加 View Connection Server 实例： ■ **domain\system$** ■ **system$@domain.com** ■ View Connection Server 服务的服务主体名称（Service Principal Name，SPN）。

表 6 View Client 配置模板中的安全性设置（续）

设置	注册表值名称	描述
Certificate verification mode（证书验证模式）	CertCheckMode	配置 View Client 执行的证书检查的级别。您可以选择其中一种模式： ■ [No Security（无安全）]。View 不执行证书检查。 ■ [Warn But Allow（警告但允许）]。出现以下服务器证书问题时，会显示一个警告，但用户可以继续连接到 View Connection Server： ■ View 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。 发生其他证书错误状况时，View 会显示一个错误对话框，并阻止用户连接到 View Connection Server。 [Warn But Allow（警告但允许）] 为默认值。 ■ [Full Security（完整安全）]。如果发生任何类型的证书错误，用户将无法连接到 View Connection Server。View 将向用户显示证书错误。 要允许 View Client 执行任意类型的证书检查，您必须在 View Administrator 中选中 [Global Settings（全局设置）] 的 **Require SSL for client connections and View Administrator（需要将 SSL 用于客户端连接和 View Administrator）]**。 配置该组策略设置后，用户可以在 View Client 中查看选定的证书验证模式，但无法配置设置。SSL 配置对话框会通知用户：管理员已锁定该设置。 未配置或禁用该设置时，View Client 用户可以配置 SSL 并选择证书验证模式。 对于 Windows 客户端来说，如果您不希望将该设置配置为组策略，您可以通过将 CertCheckMode 值名称添加到客户端计算机上的以下注册表项来启用证书验证。 HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security 使用以下注册表项值： ■ **0** 实施 [No Security（无安全）]。 ■ **1** 实施 [Warn But Allow（警告但允许）]。 ■ **2** 实施 [Full Security（完整安全）]。 如果您在注册表项中配置了组策略设置和 CertCheckMode 设置，组策略设置优先于注册表项值。
Default value of the 'Log in as current user' checkbox（“作为当前用户登录”复选框的默认值）	LogInAsCurrentUse	指定 View Client 连接对话框上 **[Log in as current user（作为当前用户登录）]** 复选框的默认值。 这项设置优先于 View Client 安装期间指定的默认值。 如果用户通过命令行运行 View Client 并指定了 [logInAsCurrentUser] 选项，则该值将覆盖此设置。 如果选中了 **[Log in as current user（作为当前用户登录）]** 复选框，用户在登录客户端系统时提供的身份和凭据信息会传送到 View Connection Server 实例，最后传送到 View 桌面。如果取消选择该复选框，用户必须多次输入身份和凭据信息，才能访问 View 桌面。 [User Configuration（用户配置）] 设置与 [Computer Configuration（计算机配置）] 设置均可用。 默认情况下禁用这些设置。

表 6 View Client 配置模板中的安全性设置（续）

设置	注册表值名称	描述
Display option to Log in as current user（显示“作为当前用户登录”选项））	LogInAsCurrentUser_Display	确定 **[Log in as current user（作为当前用户登录）]** 复选框是否显示在 View Client 连接对话框上。 如果显示该复选框，用户可以选择或取消选择该复选框并覆盖其默认值。如果该复选框隐藏，用户将无法从 View Client 连接对话框中覆盖其默认值。 您可以通过 **[Default value of the ‘Log in as current user’ checkbox（“作为当前用户登录”复选框的默认值）]** 策略设置指定 [Log in as current user（作为当前用户登录）] 复选框的默认值。 [User Configuration（用户配置）] 设置与 [Computer Configuration（计算机配置）] 设置均可用。 默认情况下启用这些设置。
Enable jump list integration（启用跳转列表集成）	EnableJumplist	确定在 Windows 7 及更高版本系统的任务栏上的 View Client 图标中是否显示跳转列表。使用跳转列表，用户可连接最近使用的 View Connection Server 实例和 View 桌面。 共享 View Client 时，您可能不希望用户查看最近使用的桌面名称。因此，您可以通过禁用此设置来禁用跳转列表。 该设置在默认情况下为启用状态。
Enable Single Sign-On for smart card authentication（为智能卡身份验证启用单点登录）	EnableSmartCardSSO	确定是否为智能卡身份验证启用单点登录。启用单点登录后，View Client 会将加密的智能卡 PIN 存储到临时内存，然后再将其提交到 View Connection Server。如果禁用单点登录，View Client 将不显示自定义 PIN 对话框。 默认情况下禁用此设置。
Ignore bad SSL certificate date received from the server（忽略从服务器中收到的无效 SSL 证书日期）	IgnoreCertDateInvalid	确定是否忽略与无效的服务器证书日期关联的错误。在服务器发送过期证书时会发生这些错误。 该设置在默认情况下为启用状态。 此设置仅适用于 View 4.6 及更低版本。
Ignore certificate revocation problems（忽略证书撤消问题）	IgnoreRevocation	确定是否忽略与撤消的服务器证书关联的错误。当服务器发出一个已撤消的证书以及客户端无法验证证书的撤消状态时，会出现这种错误。 默认情况下禁用此设置。 此设置仅适用于 View 4.6 及更低版本。
Ignore incorrect SSL certificate common name (host name field)（忽略不正确的 SSL 证书公用名（主机名字段））	IgnoreCertCnInvalid	确定是否忽略与错误的服务器证书公用名关联的错误。在证书上的公用名与发送该证书的服务器主机名不匹配时会发生这些错误。 默认情况下禁用此设置。 此设置仅适用于 View 4.6 及更低版本。
Ignore incorrect usage problems（忽略用法不正确的问题）	IgnoreWrongUsage	确定是否忽略与服务器证书使用不当关联的错误。如果服务器发送的证书专用于某一用途，而不是用来验证发送者的身份和对服务器通信进行加密，则会发生这些错误。 默认情况下禁用此设置。 此设置仅适用于 View 4.6 及更低版本。
Ignore unknown certificate authority problems（忽略未知证书颁发机构问题）	IgnoreUnknownCa	确定是否忽略与未知的服务器证书的证书颁发机构 (CA) 关联的错误。如果服务器发送的证书是由不受信任的第三方证书颁发机构签发的，则会发生这些错误。 默认情况下禁用此设置。 此设置仅适用于 View 4.6 及更低版本。

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

View Client 配置模板的脚本定义部分中的安全性相关设置

View Client 的 ADM 模板文件 (vdm_client.adm) 的脚本定义部分提供了安全性相关设置。除非另作说明，上述设置中包含一项 [Computer Configuration（计算机配置）] 设置和一项 [User Configuration（用户配置）] 设置。如果定义 [User Configuration（用户配置）] 设置，它将覆盖等效的 [Computer Configuration（计算机配置）] 设置。

脚本定义设置存储在主机注册表的 HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client 位置。

表 7 脚本定义部分中的安全性相关设置

设置	注册表值名称	描述
Connect all USB devices to the desktop on launch（启动时将所有 USB 设备连接到桌面）	connectUSBOnStartup	确定桌面启动时是否将客户端系统中所有可用的 USB 设备都连接到桌面。 默认情况下禁用此设置。
Connect all USB devices to the desktop when they are plugged in（插入 USB 设备时将其连接到桌面）	connectUSBOnInsert	确定将 USB 设备插入客户端系统时是否将其都连接到桌面 默认情况下禁用此设置。
Logon Password（登录密码）	Password	指定 View Client 在登录过程中使用的密码。该密码由 Active Directory 存储在纯文本中。 默认情况下未定义此设置。

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

View LDAP 中的安全性相关设置

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

表 8 View LDAP 中的安全性相关设置

名称 - 值对	属性	描述
cs-allowunencryptedstartsession	pae-NameValuePair	允许在单点登录到可信域（支持安全支持提供程序接口 (Security Support Provider Interface, SSPI) 协商）以外的桌面时实施静态密钥保护。静态密钥保护 与 SSPI 相比安全性较低。 如果设置为 **[0]**，将不允许密钥保护。该设置适用于所有桌面均位于可信域的情况。如果 SSPI 协商失败，会话将无法开始。 如果设置为 **[1]**，就可以在 SSPI 协商失败时 使用 静态密钥保护。该设置适用于部分桌面位于可信域以外的情况。 默认设置为 **[1]**。
	pae-OVDIKeyCipher	指定当用户检入和检出本地桌面时， View Connection Server 用于加密虚拟磁盘 (.vmdk) 文件的加密密钥密码。 您可以将加密密钥密码值设置为 **AES-128**、**AES-192** 或 **AES-256**。 默认值为 **AES-128**。
	pae-SSOCredentialCacheTimeout	设置单点登录 (SSO) 超时限制（分钟），超过此时间限制后，用户的 SSO 凭据将不再有效。 默认值为 **15**。 值为 **-1** 时表示未设置 SSO 超时限制。 **[0]** 值为禁用 SSO。

VMware View 资源

VMware View 中包含若干配置文件和类似资源，必须为它们提供保护。

表 9 View Connection Server 和 Security Server 资源

资源	位置	保护
LDAP 设置	不适用。	LDAP 数据会作为基于角色的访问控制的一部分，自动得到保护。
LDAP 备份文件	*<驱动器盘符>*:\Programdata\VMWare\VDM\backups (Windows Server 2008) *<驱动器盘符>*:\Documents and Settings\All Users\Application Data\VMWare\VDM\backups (Windows Server 2003)	由访问控制保护。
locked.properties（证书属性文件）	*安装目录*\VMware\VMware View\Server\sslgateway\conf	可由访问控制提供保护。确保该文件不被 View 管理员以外的任何用户访问。
日志文件	*%ALLUSERSPROFILE%*\Application Data\VMware\VDM\logs *<驱动器盘符>*:\Documents and Settings\All Users\Application Data\VMware\VDM\logs	由访问控制保护。
web.xml（Tomcat 配置文件）	*安装目录*\VMware View\Server\broker\web apps\ROOT\Web INF	由访问控制保护。

表 10 View Transfer Server 资源

资源	位置	保护
httpd.conf（Apache 配置文件）	*安装目录*\VMware\VMware View\Server\httpd\conf	可由访问控制提供保护。确保该文件不被 View 管理员以外的任何用户访问。
日志文件	*<驱动器盘符>*:\ProgramData\VMware\VDM\logs (Windows Server 2008 R2) *%ALLUSERSPROFILE%*\Application Data\VMware\VDM\logs（Windows Server 2003 和 Windows Server 2003 R2） *<驱动器盘符>*:\Program Files\Apache Group\Apache2\logs（Apache 服务器）	由访问控制保护。

VMware View 日志文件

VMware View 软件会创建记录其组件安装和运行情况的日志文件。

注意 VMware View 日志文件专门供 VMware 支持部门使用。VMware 建议您配置并使用事件数据库来监视 View。有关更多信息，请参阅《VMware View 安装指南》和《VMware View Integration》（VMware View 集成指南）文档。

表 11 VMware View 日志文件

VMware View 组件	文件路径和其他信息
所有组件（安装日志）	*%临时目录%*\vminst.log_*日期_时间戳* *%临时目录%*\vmmsi.log_*日期_时间戳*
View Agent	Windows XP 客户操作系统： *<驱动器盘符>*:\Documents and Settings\All Users\Application Data\VMware\VDM\logs Windows Vista 和 Windows 7 客户操作系统： *<驱动器盘符>*:\ProgramData\VMware\VDM\logs 如果配置了用户数据磁盘 (UDD)，*<驱动器盘符>* 可能与 UDD 对应。 PCoIP 日志名为 pcoip_agent*.log 和 pcoip_server*.log。
View Applications	SQL Server 或 Oracle 数据库服务器上配置的 View 事件数据库。 Windows 应用程序事件日志。默认情况下禁用。
View Client with Local Mode	Windows XP 主机操作系统： C:\Documents and Settings*%用户名%*\Local Settings\Application Data\VMware\VDM\Logs\ Windows Vista 和 Windows 7 主机操作系统： C:\Users*%用户名%*\AppData\VMware\VDM\Logs\
View Composer	链接克隆桌面上的 *%系统驱动器%*\Windows\Temp\vmware-viewcomposer-ga-new.log。 View Composer 日志中包含有关 QuickPrep 和 Sysprep 脚本执行情况的信息。日志记录脚本执行的开始时间和结束时间，以及所有输出或错误消息。
View Connection Server 或 Security Server	服务器上的 *%ALLUSERSPROFILE%*\Application Data\VMware\VDM\logs*.txt。 服务器上的 *<驱动器盘符>*:\Documents and Settings\All Users\Application Data\VMware\VDM\logs*.txt。 日志目录可在 View 公共配置 ADM 模板文件 (vdm_common.adm) 的日志配置设置中进行配置。 PCoIP 安全网关日志被写入到名为 SecurityGateway_*.log 的文件，该文件位于安全服务器日志目录的 PCoIP Secure Gateway 子目录中。
View Services	SQL Server 或 Oracle 数据库服务器上配置的 View 事件数据库。 Windows 系统事件日志。
View Transfer Server	Windows Server 2008 R2： *<驱动器盘符>*:\ProgramData\VMware\VDM\logs*.txt Windows Server 2003 和 Windows Server 2003 R2： *%ALLUSERSPROFILE%*\Application Data\VMware\VDM\logs*.txt Apache 服务器： *<驱动器盘符>*:\Program Files\Apache Group\Apache2\logs\error.log

VMware View TCP 和 UDP 端口

View 使用 TCP 和 UDP 端口进行组件之间的网络访问。您可能要重新配置防火墙，以允许相应端口上的访问。

表 12 View 使用的 TCP 和 UDP 端口（不包括本地模式）

源	端口	目标	端口	协议	描述
安全服务器	4172	View Agent 4.5 或更早版本	50002（可通过组策略更改）	UDP	PCoIP（仅 AES-128-GCM）（如果使用 PCoIP 安全网关）。
安全服务器	4172	View Agent 4.6 或更高版本	4172	UDP	PCoIP（仅 AES-128-GCM）（如果使用 PCoIP 安全网关）。

表 12 View 使用的 TCP 和 UDP 端口（不包括本地模式）（续）

源	端口	目标	端口	协议	描述
安全服务器	4172	View Client 4.5 或更早版本	50002（无法更改）	UDP	PCoIP（仅 AES-128-GCM）（如果使用 PCoIP 安全网关）。
安全服务器	4172	View Client 4.6 或更高版本	4172	UDP	PCoIP（仅 AES-128-GCM）（如果使用 PCoIP 安全网关）。
安全服务器	*	View Connection Server	4001	TCP	JMS 流量。
安全服务器	*	View Connection Server	8009	TCP	AJP13 转发的 Web 流量。
安全服务器	*	View 桌面	3389	TCP	指向 View 桌面的 Microsoft RDP 流量。
安全服务器	*	View 桌面	9427	TCP	Wyse MMR 重定向。
安全服务器	*	View 桌面	32111	TCP	USB 重定向。
安全服务器	*	View 桌面 4.5 或更早版本	50002（可通过组策略更改）	TCP	PCoIP (HTTPS)（如果使用 PCoIP 安全网关）。
安全服务器	*	View 桌面 4.6 或更高版本	4172	TCP	PCoIP (HTTPS)（如果使用 PCoIP 安全网关）。
View Agent 4.5 或更早版本	50002（可通过组策略更改）	View Client 4.5 或更早版本	50002（无法更改）	UDP	PCoIP（AES-128-GCM 或 SALSA20）（如果未使用 PCoIP 安全网关）。
View Agent 4.5 或更早版本	50002（可通过组策略更改）	View Client 4.6 或更高版本	4172	UDP	PCoIP（AES-128-GCM 或 SALSA20）（如果未使用 PCoIP 安全网关）。
View Agent 4.6 或更高版本	4172	View Client 4.5 或更早版本	50002（无法更改）	UDP	PCoIP（AES-128-GCM 或 SALSA20）（如果未使用 PCoIP 安全网关）。
View Agent 4.6 或更高版本	4172	View Client 4.6 或更高版本	4172	UDP	PCoIP（AES-128-GCM 或 SALSA20）（如果未使用 PCoIP 安全网关）。
View Agent 4.5 或更早版本	50002（可通过组策略更改）	View Connection Server 或 Security Server	4172	UDP	PCoIP（仅 AES-128-GCM）（如果使用 PCoIP 安全网关）。
View Agent 4.6 或更高版本	4172	View Connection Server 或 Security Server	4172	UDP	PCoIP（仅 AES-128-GCM）（如果使用 PCoIP 安全网关）。
View Client	*	View Connection Server 或 Security Server	80	TCP	HTTP 访问（如果为客户端连接禁用 SSL）。
View Client	*	View Connection Server 或 Security Server	443	TCP	HTTPS 访问（如果为客户端连接启用 SSL）。
View Client	*	View Connection Server 或 Security Server	4172	TCP	PCoIP (HTTPS)（如果使用 PCoIP 安全网关）。
View Client	*	View 桌面	3389	TCP	指向 View 桌面的 Microsoft RDP 流量（如果使用直接连接而不是安全加密链路连接）。
View Client	*	View 桌面	9427	TCP	Wyse MMR 重定向（如果使用直接连接而不是安全加密链路连接）。

表 12 View 使用的 TCP 和 UDP 端口（不包括本地模式）（续）

源	端口	目标	端口	协议	描述
View Client	*	View 桌面	32111	TCP	USB 重定向（如果使用直接连接而不是安全加密链路连接）。
View Client 4.5 或更早版本	*	View Agent 4.5 或更早版本	50002（可通过组策略更改）	TCP	PCoIP (HTTPS)（如果未使用 PCoIP 安全网关）。
View Client 4.5 或更早版本	50002（无法更改）	View Agent 4.5 或更早版本	50002（可通过组策略更改）	UDP	PCoIP（AES-28-GCM 或 SALSA20）（如果未使用 PCoIP 安全网关）。
View Client 4.5 或更早版本	*	View Agent 4.6 或更高版本	4172	TCP	PCoIP (HTTPS)（如果未使用 PCoIP 安全网关）。
View Client 4.5 或更早版本	50002（无法更改）	View Agent 4.6 或更高版本	4172	UDP	PCoIP（AES-28-GCM 或 SALSA20）（如果未使用 PCoIP 安全网关）。
View Client 4.5 或更早版本	50002（无法更改）	View Connection Server 或 Security Server	4172	UDP	PCoIP（仅 AES-128-GCM）（如果使用 PCoIP 安全网关）。
View Client 4.6 或更高版本	*	View Agent 4.5 或更早版本	50002（可通过组策略更改）	TCP	PCoIP (HTTPS)（如果未使用 PCoIP 安全网关）。
View Client 4.6 或更高版本	4172	View Agent 4.5 或更早版本	50002（可通过组策略更改）	UDP	PCoIP（AES-28-GCM 或 SALSA20）（如果未使用 PCoIP 安全网关）。
View Client 4.6 或更高版本	*	View Agent 4.6 或更高版本	4172	TCP	PCoIP (HTTPS)（如果未使用 PCoIP 安全网关）。
View Client 4.6 或更高版本	4172	View Agent 4.6 或更高版本	4172	UDP	PCoIP（AES-28-GCM 或 SALSA20）（如果未使用 PCoIP 安全网关）。
View Client 4.6 或更高版本	4172	View Connection Server 或 Security Server	4172	UDP	PCoIP（仅 AES-128-GCM）（如果使用 PCoIP 安全网关）。
View Connection Server	*	vCenter Server 或 View Composer	80	TCP	SOAP 消息（如果对 vCenter Servers 或 View Composer 访问禁用 SSL）。
View Connection Server	*	vCenter Server 或 View Composer	443	TCP	SOAP 消息（如果对 vCenter Servers 或 View Composer 访问启用 SSL）。
View Connection Server	4172	View Agent 4.5 或更早版本	50002（可通过组策略更改）	UDP	PCoIP（仅 AES-128-GCM）（如果使用经过 View Connection Server 的 PCoIP 安全网关）。
View Connection Server	4172	View Agent 4.6 或更高版本	4172	UDP	PCoIP（仅 AES-128-GCM）（如果使用经过 View Connection Server 的 PCoIP 安全网关）。
View Connection Server	4172	View Client 4.5 或更早版本	50002（无法更改）	UDP	PCoIP（仅 AES-128-GCM）（如果使用经过 View Connection Server 的 PCoIP 安全网关）。

表 12 View 使用的 TCP 和 UDP 端口（不包括本地模式）（续）

源	端口	目标	端口	协议	描述
View Connection Server	4172	View Client 4.6 或更高版本	4172	UDP	PCoIP（仅 AES-128-GCM）（如果使用经过 View Connection Server 的 PCoIP 安全网关）。
View Connection Server	*	View Connection Server	4100	TCP	JMS 路由器之间的流量。
View Connection Server	*	View 桌面	3389	TCP	指向 View 桌面的 Microsoft RDP 流量（如果使用经过 View Connection Server 的安全加密链路连接）。
View Connection Server	*	View 桌面	4172	TCP	PCoIP (HTTPS)（如果使用经过 View Connection Server 的 PCoIP 安全网关）。
View Connection Server	*	View 桌面	9427	TCP	Wyse MMR 重定向（如果使用经过 View Connection Server 的安全加密链路连接）。
View Connection Server	*	View 桌面	32111	TCP	USB 重定向（如果使用经过 View Connection Server 的安全加密链路连接）。
View 桌面	*	View Connection Server 实例	4001	TCP	JMS 流量。
View Composer 服务	*	ESXi 主机	902	TCP	在 View Composer 自定义链接克隆磁盘时使用，这些磁盘包括 View Composer 内部磁盘和永久磁盘及系统一次性磁盘（如已指定）。

您需要打开额外数量的端口，本地模式功能才能正常运行。

表 13 本地模式使用的 TCP 和 UDP 端口

源	端口	目标	端口	协议	描述
安全服务器	*	View Transfer Server	80	TCP	View 桌面下载和数据复制（如果为本地模式操作使用安全加密链路连接并禁用 SSL）。
安全服务器	*	View Transfer Server	443	TCP	View 桌面下载和数据复制（如果为本地模式操作使用安全加密链路连接并启用 SSL）。
View Client with Local Mode	*	View Transfer Server	80	TCP	View 桌面下载和数据复制（如果为本地模式操作使用直接连接而不是安全加密链路连接，且禁用 SSL）。

表 13 本地模式使用的 TCP 和 UDP 端口（续）

源	端口	目标	端口	协议	描述
View Client with Local Mode	*	View Transfer Server	443	TCP	View 桌面下载和数据复制（如果为本地模式操作使用直接连接而不是安全加密链路连接，且启用 SSL）。
View Connection Server	*	ESX 主机	902	TCP	在检出本地桌面时使用。
View Connection Server	*	View Transfer Server	80	TCP	View 桌面下载和数据复制（如果为本地模式操作使用经过 View Connection Server 的安全加密链路连接且禁用 SSL）。
View Connection Server	*	View Transfer Server	443	TCP	View 桌面下载和数据复制（如果为本地模式操作使用经过 View Connection Server 的安全加密链路连接且启用 SSL）。
View Connection Server	*	View Transfer Server	4001	TCP	用于支持本地模式的 JMS 流量。
View Transfer Server	*	ESX 主机	902	TCP	为本地模式发布 View Composer 程序包。

View Connection Server 主机上的服务

View Manager 的运行依赖于 View Connection Server 主机上运行的若干服务。如果您想调整这些服务的运行，就需要先熟悉这些服务。

表 14 View Connection Server 主机服务

服务名称	启动类型	描述
VMware View Connection Server	自动	提供连接代理服务。必须运行此服务 View Manager 才能正常运行。如果启动或停止此服务，会同时启动或停止 Framework、Message Bus、Security Gateway 和 Web 服务。此服务不会启动或停止 VMwareVDMDS 服务或 VMware View 脚本主机服务。
VMware View Framework 组件	手动	为 View Manager 提供事件日志、安全和 COM+ 框架服务。必须运行此服务 View Manager 才能正常运行。
VMware View Message Bus 组件	手动	在 View Manager 组件之间提供消息传递服务。必须运行此服务 View Manager 才能正常运行。
VMware View PCoIP 安全网关	手动	提供 PCoIP 安全网关服务。如果客户端通过 PCoIP 安全网关连接到 View Connection Server，则必须运行此服务。
VMware View 脚本主机	自动（如果已启用）	对您删除虚拟机时运行的第三方脚本提供支持。默认情况下，此服务已被禁用。如果您需要运行脚本，应启用此服务。
VMware View Security Gateway 组件	手动	为 View Manager 提供安全加密链路服务。必须运行此服务 View Manager 才能正常运行。
VMware View Web 组件	手动	为 View Manager 提供 Web 服务。必须运行此服务 View Manager 才能正常运行。
VMware VDMDS	自动	为 View Manager 提供 LDAP 目录服务。必须运行此服务 View Manager 才能正常运行。升级 VMware View 期间也必须运行此服务，以确保正确迁移现有数据。

安全服务器上的服务

View Manager 的运行依赖于安全服务器上运行的若干服务。如果您想调整这些服务的运行，就需要先熟悉这些服务。

表 15 安全服务器服务

服务名称	启动类型	描述
VMware View Security Server	自动	提供安全服务器服务。必须运行此服务，安全服务器才能正确运行。如果您启动或停止此服务，会同时启动或停止 Framework 和 Security Gateway 服务。
VMware View Framework 组件	手动	提供事件日志、安全和 COM+ 框架服务。必须运行此服务，安全服务器才能正确运行。
VMware View PCoIP 安全网关	手动	提供 PCoIP 安全网关服务。如果客户端通过 PCoIP 安全网关连接到安全服务器，则必须运行此服务。
VMware View Security Gateway 组件	手动	提供安全加密链路服务。必须运行此服务，安全服务器才能正确运行。

View Transfer Server 主机上的服务

本地桌面的传输操作依赖于 View Transfer Server 主机上运行的服务。如果您想调整这些服务的运行，就需要先熟悉这些服务。

View Transfer Server 上安装的所有服务都必须运行，才能保证 View Manager 中本地桌面的正确运行。

表 16 View Transfer Server 主机服务

服务名称	启动类型	描述
VMware View Transfer Server	自动	提供协调 View Transfer Server 相关服务的服务。如果您启动或停止此服务，会同时启动或停止 View Transfer Server Control 服务和 Framework 服务。
VMware View Transfer Server Control 服务	手动	为 View Transfer Server 提供管理能力并处理与 View Connection Server 的通信。
VMware View Framework 组件	手动	为 View Manager 提供事件日志、安全和 COM+ 框架服务。
Apache2.2 服务	自动	为以本地模式运行 View 桌面的客户端计算机提供数据传输能力。 当您将 View Transfer Server 添加到 View Manager 时，Apache2.2 服务即会启动。

索引