

View Agent Direct- Connection 插件管理指南

修改日期：2018 年 12 月 13 日
VMware Horizon 7 7.7



vmware®

您可以从 VMware 网站下载最新的技术文档:

<https://docs.vmware.com/cn/>。

VMware 网站还提供了最近的产品更新。

如果您对本文档有任何意见或建议, 请将反馈信息发送至:

docfeedback@vmware.com

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

北京办公室
北京市
朝阳区新源南路 8 号
启皓北京东塔 8 层 801
www.vmware.com/cn

上海办公室
上海市
淮海中路 333 号
瑞安大厦 804-809 室
www.vmware.com/cn

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

目录

View Agent Direct-Connection 插件管理指南	4
1 安装 View Agent Direct-Connection 插件	5
View Agent Direct-Connection 插件系统要求	5
安装 View Agent Direct-Connection 插件	5
静默安装 View Agent Direct-Connection 插件	6
2 View Agent Direct-Connection 插件高级配置	8
View Agent Direct-Connection 插件配置设置	8
在 SSL/TLS 中禁用弱密码	10
替换默认的自签名 TLS 服务器证书	11
授权 Horizon Client 访问桌面和应用程序	11
使用网络地址转换和端口映射	12
将证书颁发机构添加到 Windows 证书存储区	14
3 设置 HTML Access	16
为 HTML Access 安装 Horizon 7 Agent	16
设置静态内容传送	16
设置由可信 CA 签名的 TLS 服务器证书	18
在 Windows 10 和 Windows 2016 桌面上禁用 HTTP/2 协议	19
4 在远程桌面服务主机上设置 View Agent 直接连接	20
远程桌面服务主机	20
授权已发布的桌面和应用程序	20
5 View Agent Direct-Connection 插件故障排除	22
安装了错误的图形驱动程序	22
视频 RAM 不足	22
启用完整日志记录以包括跟踪和调试信息	23

View Agent Direct-Connection 插件管理指南

《View Agent Direct-Connection 插件管理》提供了有关安装和配置 View Agent Direct-Connection 插件的信息。此插件是 Horizon Agent 的可安装扩展，允许 Horizon Client 直接连接到基于虚拟机的桌面、已发布的桌面或应用程序，而无需使用 Horizon 连接服务器。所有桌面和应用程序功能的工作方式与用户通过连接服务器连接时相同。

目标读者

此信息面向希望在基于虚拟机的桌面或 RDS 主机上安装、升级或配置 View Agent Direct-Connection 插件。本指南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 系统管理员编写。

安装 View Agent Direct-Connection 插件

1

View Agent Direct-Connection (VADC) 插件使 Horizon Client 可以直接连接到基于虚拟机的桌面、已发布的桌面或应用程序。VADC 插件是 Horizon 7 Agent 的扩展，安装在基于虚拟机的桌面或 RDS 主机上。

本章讨论了以下主题：

- [View Agent Direct-Connection 插件系统要求](#)
- [安装 View Agent Direct-Connection 插件](#)
- [静默安装 View Agent Direct-Connection 插件](#)

View Agent Direct-Connection 插件系统要求

View Agent Direct-Connection (VADC) 插件安装在已经安装有 Horizon 7 Agent 的计算机上。有关 Horizon 7 Agent 支持的操作系统列表，请参阅《Horizon 7 安装指南》文档中的“Horizon Agent 支持的操作系统”。

VADC 插件另外还有以下要求：

- 安装了 VADC 插件的虚拟机或物理机必须最少具有 128 MB 视频内存才能使 PCoIP 正常运行。
- 对于虚拟机，您必须在安装 Horizon 7 Agent 之前安装 VMware Tools。

注 支持 VADC 的基于虚拟机的桌面可以加入 Microsoft Active Directory 域，也可以是某个工作组的成员。

安装 View Agent Direct-Connection 插件

View Agent Direct-Connection (VADC) 插件使用 Windows 安装程序文件打包，您可以从 VMware 网站下载并安装该文件。

前提条件

- 确认已安装 Horizon 7 Agent。如果您的环境中不包含 Horizon 7 连接服务器，请从命令行安装 Horizon 7 Agent，并指定告诉 Horizon 7 Agent 不向 Horizon 7 连接服务器注册的参数。请参阅[HTML Access 安装 Horizon 7 Agent](#)。
- 在 vSphere 6.0 及更高版本中为虚拟机启用屏幕 DMA 设置。如果禁用了屏幕 DMA，在连接到远程桌面时，用户将会看到黑屏。有关如何设置屏幕 DMA 的详细信息，请参阅 VMware 知识库 (KB) 文章 2144475 <http://kb.vmware.com/kb/2144475>。

步骤

- 1 从 VMware 下载页面下载 VADC 插件的安装程序文件，网址为：
<http://www.vmware.com/go/downloadview>。

安装程序文件名为 VMware-viewagent-direct-connection-x86_64-y.y.y-xxxxxx.exe（64 位 Windows）或 VMware-viewagent-direct-connection--y.y.y-xxxxxx.exe（32 位 Windows），其中 y.y.y 是版本号，xxxxxx 是内部版本号。

- 2 双击安装程序文件。

- 3 （可选）更改 TCP 端口号。

默认端口号为 443。

- 4 （可选）选择 Windows 防火墙服务的配置方法。

默认情况下，将选择**自动配置 Windows 防火墙**，安装程序会将 Windows 防火墙配置为允许所需的网络连接。

- 5 （可选）选择是否禁用 SSL 3.0。

默认情况下，选择**自动禁用对 SSLv3 的支持 (推荐)**，且安装程序将在操作系统级别禁用 SSL 3.0。如果已经在注册表中明确启用或禁用 SSL 3.0，将不会显示此选项且安装程序不会执行任何操作。取消选择此选项后，安装程序仍然不会执行任何操作。

- 6 按照提示完成安装。

静默安装 View Agent Direct-Connection 插件

您可以使用 Microsoft Windows Installer (MSI) 的静默安装功能安装 View Agent Direct-Connection (VADC) 插件。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 VADC 插件。有关 Windows Installer 的详细信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“Microsoft Windows Installer 命令行选项”。VADC 插件支持以下 MSI 属性。

表 1-1. 用于静默安装 View Agent Direct-Connection 插件的 MSI 属性

MSI 属性	说明	默认值
LISTENPORT	VADC 插件用于接受远程连接的 TCP 端口。默认情况下，安装程序将 Windows 防火墙配置为允许该端口上的流量。	443
MODIFYFIREWALL	如果设置为 1，安装程序会将 Windows 防火墙配置为允许 LISTENPORT 上的流量。如果设置为 0，安装程序将不会这样做。	1
DISABLE_SSLV3	如果已经在注册表中明确启用或禁用 SSL 3.0，安装程序将忽略此属性。否则，如果此属性设置为 1，安装程序将在操作系统级别禁用 SSL 3.0；如果此属性设置为 0，安装程序不会执行任何操作。	1

前提条件

- 确认已安装 Horizon Agent。如果您的环境中不包含 Horizon 连接服务器，请从命令行安装 Horizon Agent，并指定告诉 Horizon Agent 不向 Horizon 连接服务器注册的参数。请参阅[HTML Access 安装 Horizon 7 Agent](#)。

步骤

- 1 打开 Windows 命令提示符。
- 2 使用命令行选项运行 VADC 插件安装程序文件，以指定静默安装。可以选择性地指定其他 MSI 属性。以下示例使用默认选项安装 VADC 插件。

```
VMware-viewagent-direct-connection--y.y.y-xxxxxx.exe /s
```

以下示例将安装 VADC 插件，并为远程连接指定 VADC 将侦听的 TCP 端口。

```
VMware-viewagent-direct-connection--y.y.y-xxxxxx.exe /s /v"/qn LISTENPORT=9999"
```

View Agent Direct-Connection 插件高级配置

2

可以使用默认的 View Direct-Connection 插件配置设置，或者通过 Windows Active Directory 组策略对象 (GPO) 或通过修改特定的 Windows 注册表设置对其进行自定义。

本章讨论了以下主题：

- [View Agent Direct-Connection 插件配置设置](#)
- [在 SSL/TLS 中禁用弱密码](#)
- [替换默认的自签名 TLS 服务器证书](#)
- [授权 Horizon Client 访问桌面和应用程序](#)
- [使用网络地址转换和端口映射](#)
- [将证书颁发机构添加到 Windows 证书存储区](#)

View Agent Direct-Connection 插件配置设置

VMware View Agent 配置 ADMX 模板文件 (view_agent_direct_connection.admx) 中包含与 View Agent Direct-Connection 插件相关的策略设置。

View Agent Direct-Connection 配置设置位于组策略管理编辑器的 **计算机配置 > 管理模板 > VMware View Agent 配置 > View Agent Direct-Connection 配置** 中。

表 2-1. View Agent Direct-Connection 插件配置设置

设置	说明
已启用的应用程序	此设置支持在远程桌面会话主机上启动应用程序。默认设置为启用。
客户端配置名称值对	以 name=value 的格式传递至客户端的值列表。示例： clientCredentialCacheTimeout=1440。
客户端凭据缓存超时	Horizon Client 允许用户使用已保存密码的时段（以分钟为单位）。0 表示从不，-1 表示永久。如果该设置设置为有效值，则 Horizon Client 将为用户提供保存其密码的选项。默认值为 0（从不）。
客户端会话超时	客户端未连接时会话保持活跃状态的最长时间（以秒为单位）。默认值为 36000 秒 (10 小时)。
客户端设置：AlwaysConnect	该值可设置为 TRUE 或 FALSE。AlwaysConnect 设置将发送到 Horizon Client。如果此策略设置为 TRUE，则它将覆盖保存的任何客户端首选项。默认情况下未设置值。启用此策略会将值设置为 TRUE。禁用此策略会将值设置为 FALSE。

表 2-1. View Agent Direct-Connection 插件配置设置（续）

设置	说明
客户端设置: AutoConnect	此设置会覆盖任何已保存的 Horizon Client 首选项。默认情况下未设置值。启用此策略将把值设置为 True ，禁用此策略将把值设置为 False 。
客户端设置: ScreenSize	向 Horizon Client 发送 ScreenSize 设置。如果启用，它将覆盖任何已保存的客户端首选项。如果不配置或已禁用，则使用客户端首选项。
默认协议	Horizon Client 连接到桌面使用的默认显示协议。如果未设置该值，则默认值为 BLAST 。
已启用免责声明	该值可设置为 TRUE 或 FALSE 。如果设置为 TRUE ，则在登录时显示用户要接受的免责声明文本。该文本显示在“免责声明文本”（如果书写）或 GPO Configuration\Windows Settings\Security Settings\Local Policies\Security Options: Interactive Logon 中。 disclaimerEnabled 的默认设置为 FALSE 。
免责声明文本	在登录时向 Horizon Client 用户显示的免责声明文本。“已启用免责声明”策略必须设置为 TRUE 。如果未指定此文本，则默认使用 Windows 策略 Configuration\Windows Settings\Security Settings\Local Policies\Security Options 中的值。
外部 Blast 端口	发送到 Horizon Client 的、用于 HTML5/Blast 协议的目标 TCP 端口号对应的端口号。数字前面的 + 字符表示用于 HTTPS 的端口号中的相对数字。如果外部公开的端口号与服务侦听的端口不匹配，请仅设置该值。通常，该端口号位于 NAT 环境中。默认情况下未设置值。
外部框架通道端口	发送到 Horizon Client 的、用于框架通道协议的目标 TCP 端口号对应的端口号。数字前面的 + 字符表示用于 HTTPS 的端口号中的相对数字。如果外部公开的端口号与服务侦听的端口不匹配，请仅设置该值。通常，该端口号位于 NAT 环境中。默认情况下未设置值。
外部 IP 地址	发送到 Horizon Client 的、用于辅助协议（ RDP 、 PCoIP 、框架通道等）的目标 IP 地址对应的 IPv4 地址。如果外部公开的地址与桌面计算机的地址不匹配，请仅设置该值。通常，该地址位于 NAT 环境中。默认情况下未设置值。
外部 PCoIP 端口	发送到 Horizon Client 的、用于 PCoIP 协议的目标 TCP/UDP 端口号对应的端口号。数字前面的 + 字符表示用于 HTTPS 的端口号中的相对数字。如果外部公开的端口号与服务侦听的端口不匹配，请仅设置该值。通常，该端口号位于 NAT 环境中。默认情况下未设置值。
外部 RDP 端口	发送到 Horizon Client 的、用于 RDP 协议的目标 TCP 端口号对应的端口号。数字前面的 + 字符表示用于 HTTPS 的端口号中的相对数字。如果外部公开的端口号与服务侦听的端口不匹配，请仅设置该值。通常，该端口号位于 NAT 环境中。默认情况下未设置值。
HTTPS 端口号	插件侦听来自 Horizon Client 的传入 HTTPS 请求所用的 TCP 端口。如果此值发生更改，则必须对 Windows 防火墙进行相应更改以允许传入流量。默认值为 443 。
多媒体重定向 (MMR) 已启用	确定是否为客户端系统启用 MMR 。 MMR 是一种 Microsoft DirectShow 筛选器，可直接通过 TCP 套接字将多媒体数据从 Horizon 桌面中的特定编解码器转发至客户端系统。随后，直接在播放数据的客户端系统中解码数据。默认值为禁用。 如果客户端系统的视频显示硬件不支持覆盖功能， MMR 将无法正常运行。客户端系统可能没有足够的资源处理本地多媒体解码。
已启用重置	该值可设置为 TRUE 或 FALSE 。设置为 TRUE 时，通过验证的 Horizon Client 可执行操作系统级别的重新引导。默认设置为禁用 (FALSE)。
会话超时	用户在使用 Horizon Client 登录后可保持会话为打开状态的时间段。此值的单位为分钟。默认值是 600 分钟。达到此超时后，所有用户桌面和应用程序会话都将断开连接。
自动连接 USB	该值可设置为 TRUE 或 FALSE 。插入 USB 设备时将其连接到桌面。如果设置了此策略，它将覆盖保存的任何客户端首选项。默认情况下未设置值。
已启用 USB	该值可设置为 TRUE 或 FALSE 。确定桌面是否可以使用 USB 设备连接客户端系统。默认值为启用。如果出于安全因素阻止使用外部设备，请将设置更改为禁用 (FALSE)。

表 2-1. View Agent Direct-Connection 插件配置设置（续）

设置	说明
用户空闲超时	如果一段时间内在 Horizon Client 上没有用户活动，则用户的桌面和应用程序会话将断开连接。此值的单位为秒。默认值为 900 秒（15 分钟）。
X509 证书身份验证	确定是已禁用、允许还是需要智能卡 X.509 证书身份验证。
X509 SSL 证书身份验证已启用	确定是否通过 Horizon Client 的直接 SSL 连接启用了智能卡 X.509 证书身份验证。如果通过中间 SSL 端点处理 X.509 证书身份验证，则无需使用此选项。更改该设置需要重新启动 Horizon Agent。

外部端口号和外部 IP 地址值用于网络地址转换 (NAT) 和端口映射支持。有关更多信息，请参阅[使用网络地址转换和端口映射](#)。

对于智能卡身份验证，Windows 证书存储区中必须存在可对智能卡证书进行签名的证书颁发机构 (CA)。有关如何添加证书颁发机构的信息，请参阅[将证书颁发机构添加到 Windows 证书存储区](#)。

注 由于 Windows 可能向客户端发送不包含中间 CA 名称的可信颁发者列表，如果用户尝试使用智能卡登录到 Windows 7 或 Windows Server 2008 R2 计算机，并且该智能卡证书由中间 CA 签发，该尝试可能会失败。如果发生这种情况，客户端将无法选择相应的智能卡证书。为避免出现此问题，请在注册表项 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL 中将注册表值 SendTrustedIssuerList (REG_DWORD) 设置为 0。将此注册表值设置为 0 后，Windows 将不会向客户端发送可信颁发者列表，这样之后便可以从智能卡中选择所有有效证书。

在 SSL/TLS 中禁用弱密码

要实现更高的安全性，您可以配置域策略组策略对象 (Group Policy Object, GPO)，以确保在 Horizon Client 和基于虚拟机的桌面或 RDS 主机之间使用 SSL/TLS 协议的通信不允许使用弱密码。

步骤

- 1 在 Active Directory 服务器上编辑 GPO，方法是选择开始 > 管理工具 > 组策略管理，右键单击 GPO，然后选择编辑。
- 2 在组策略管理编辑器中，浏览到计算机配置 > 策略 > 管理模板 > 网络 > SSL 配置设置。
- 3 双击 SSL 密码套件顺序。
- 4 在“SSL 密码套件顺序”窗口中，单击已启用。
- 5 在“选项”窗格中，将“SSL 密码套件”文本框的全部内容替换为以下密码列表：

```
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,
```

```
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA
```

为了便于查看，密码套件已分多行列在上方。将该列表粘贴到文本框中时，密码套件必须位于一行中，并且逗号后不含空格。

6 退出组策略管理编辑器。

7 重新启动 VADC 计算机以使新组策略生效。

注 如果未将 Horizon Client 配置为支持虚拟桌面操作系统支持的任何密码，TLS/SSL 协商将失败，客户端将无法连接。

有关在 Horizon Client 中配置支持的密码套件的信息，请参见 Horizon Client 文档，网址为 https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html。

替换默认的自签名 TLS 服务器证书

自签名 TLS 服务器证书无法为 Horizon Client 提供足够的保护来抵御篡改和窃听威胁。要保护桌面免受这些威胁，您必须替换生成的自签名证书。

View Agent Direct-Connection 插件在完成安装后首次启动时，会自动生成自签名 TLS 服务器证书，并将其放在 Windows 证书存储区中。TLS 协议协商期间，会将 TLS 服务器证书提供给 Horizon Client，以便向客户端提供有关此桌面的信息。此默认的自签名 TLS 服务器证书无法提供有关此桌面的保证，除非将其替换为由客户端信任的、经 Horizon Client 证书检查完全验证过的证书颁发机构 (CA) 签名的证书。

将此证书存储在 Windows 证书存储区的过程以及将其替换为适当 CA 签名证书的过程，与用于 Horizon 7 连接服务器的过程相同。请参阅《Horizon 7 安装指南》文档中的“为 Horizon 7 Server 配置 TLS 证书”，了解有关此证书替换过程的详细信息。

支持具有主题备用名称 (SAN) 的证书和通配证书。

注 要使用 View Agent Direct-Connection 插件将 CA 签名的 TLS 服务器证书分发给大量桌面，请使用 Active Directory 注册功能将证书分发给每个虚拟机。有关更多信息，请参阅：
<http://technet.microsoft.com/en-us/library/cc732625.aspx>。

授权 Horizon Client 访问桌面和应用程序

允许用户直接访问桌面和应用程序的授权机制在名为 View Agent Direct-Connection 用户的本地操作系统内进行控制。

如果用户是该组的成员，会授权用户连接至基于虚拟机的桌面、已发布的桌面或已发布的应用程序。首次安装插件时，会创建此本地组，并且包含“经过身份验证的用户”组。插件成功验证的所有人都将被授权访问桌面或应用程序。

要限制对该桌面或 RDS 主机的访问，您可以修改该组的成员资格以指定用户和用户组列表。这些用户可以为本机用户和用户组，也可以是域用户和用户组。如果用户不在此组中，则在进行身份验证之后用户会收到一条消息，指出用户未经授权访问基于此虚拟机的桌面或者已发布桌面以及该 RDS 主机上托管的应用程序。

使用网络地址转换和端口映射

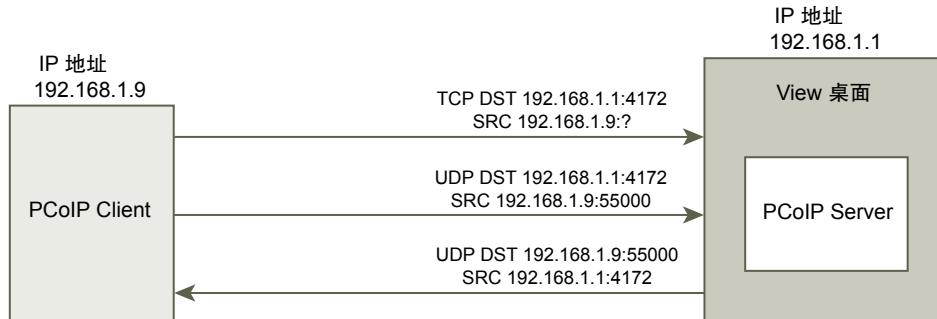
如果 Horizon Client 连接到其他网络上基于虚拟机的桌面，则需要网络地址转换 (NAT) 和端口映射配置。

在此处包含的示例中，您必须在桌面上配置外部寻址信息，以便 Horizon Client 可以使用此信息以通过 NAT 或端口映射设备连接到桌面。此 URL 与 Horizon 7 连接服务器及安全服务器上的外部 URL 和 PCoIP 外部 URL 设置相同。

当 Horizon Client 位于其他网络上且 NAT 设备位于 Horizon Client 和运行此插件的桌面之间时，将需要 NAT 或端口映射配置。例如，如果在 Horizon Client 和桌面之间存在防火墙，则该防火墙充当 NAT 或端口映射设备。

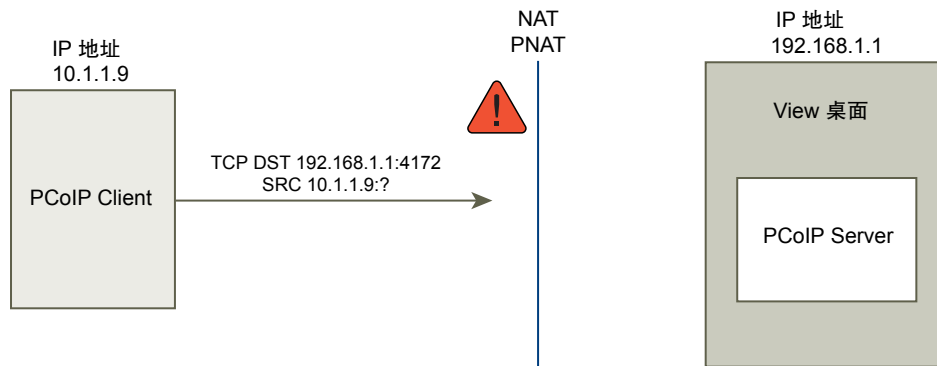
IP 地址为 192.168.1.1 的桌面部署示例说明了 NAT 和端口映射的配置。同一网络上 IP 地址为 192.168.1.9 的 Horizon Client 系统使用 TCP 和 UDP 建立了 PCoIP 连接。这是未使用任何 NAT 或端口映射配置的直接连接。

图 2-1. 从同一网络上的客户端建立直接 PCoIP 连接



如果在客户端和桌面之间添加 NAT 设备以便它们在不同的地址空间中运行，且不对此插件进行任何配置更改，PCoIP 数据包将无法正确路由并会失败。在该示例中，客户端使用不同的地址空间，其 IP 地址为 10.1.1.9。该设置无法正常工作，因为客户端将使用桌面的地址发送 TCP 和 UDP PCoIP 数据包。目标地址 192.168.1.1 将无法在客户端网络中正常使用，且可能会使客户端显示空白屏幕。

图 2-2. 通过 NAT 设备从客户端建立 PCoIP 连接显示失败

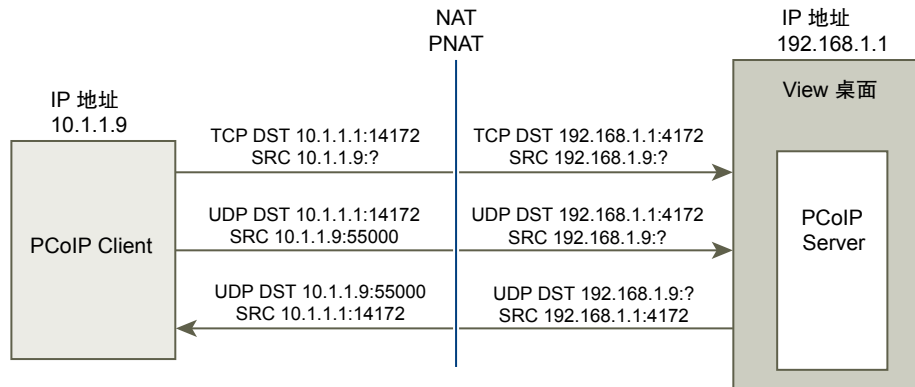


要解决此问题，您必须配置插件使用外部 IP 地址。如果将此桌面的 `externalIPAddress` 配置为 10.1.1.1，此插件将在建立与桌面的桌面协议连接时为客户提供 10.1.1.1 IP 地址。对于 PCoIP，必须在桌面上启动 PCoIP 安全网关服务才能实现此设置。

对于端口映射，如果桌面使用的是标准 PCoIP 端口 4172，而客户端必须使用映射到端口映射设备上端口 4172 的其他目标端口，那么您必须配置插件以实现此设置。如果端口映射设备将端口 14172 映射到 4172，则客户端必须为 PCoIP 使用目标端口 14172。您必须为 PCoIP 配置此设置。将插件中的 `externalPCoIPPort` 配置为 14172。

在使用 NAT 和端口映射的配置中，将 `externalIPAddress` 设置为 10.1.1.1（网络转换为 192.168.1.1），将 `externalPCoIPPort` 设置为 14172（映射到 4172 端口）。

图 2-3. 通过 NAT 设备和端口映射从客户端建立 PCoIP 连接



与 PCoIP 的外部 PCoIP TCP/UDP 端口配置一样，如果 RDP 端口 (3389) 或框架通道端口 (32111) 进行了端口映射，您必须对 `externalRDPPort` 和 `externalFrameworkChannelPort` 进行配置，以指定客户端在通过端口映射设备建立这些连接时所使用的 TCP 端口号。

高级寻址方案

将基于虚拟机的桌面配置为可通过同一外部 IP 地址上的 NAT 和端口映射设备进行访问时，必须为每个桌面提供一组唯一的端口号。然后，这些客户端可以使用相同的目标 IP 地址，但使用唯一的 TCP 端口号进行 HTTPS 连接，以将该连接定向到特定虚拟桌面。

例如，HTTPS 端口 1000 定向到一个桌面，HTTPS 端口 1005 定向到另一桌面，但它们使用的是同一目标 IP 地址。在此情况下，针对桌面协议连接的每个桌面配置唯一外部端口号极其复杂。为此，插件设置 `externalPCoIPPort`、`externalRDPPort` 和 `externalFrameworkChannelPort` 可以采用可选的关系表达式来代替静态值，定义一个相对于客户端使用的基本 HTTPS 端口号的端口号。

如果端口映射设备将端口号 1000 用于 HTTPS 并映射到 TCP 443、端口号 1001 用于 RDP 并映射到 TCP 3389、端口号 1002 用于 PCoIP 并映射到 TCP 和 UDP 4172、端口号 1003 用于框架通道并映射到 TCP 32111，则为了简化配置，可将外部端口号配置为 `externalRDPPort=+1`、`externalPCoIPPort=+2` 和 `externalFrameworkChannelPort=+3`。当 HTTPS 连接来自于使用 HTTPS 目标端口号 1000 的客户端时，系统将相对于该 1000 端口号自动计算外部端口号并分别使用 1001、1002 和 1003。

如果端口映射设备将端口号 1005 用于 HTTPS 并映射到 TCP 443、端口号 1006 用于 RDP 并映射到 TCP 3389、端口号 1007 用于 PCoIP 并映射到 TCP 和 UDP 4172、端口号 1008 用于框架通道并映射到 TCP 32111，则为了部署另一虚拟桌面，请在桌面上使用完全相同的外部端口配置（+1、+2、+3 等）。当 HTTPS 连接来自于使用 HTTPS 目标端口号 1005 的客户端时，系统将相对于该 1005 端口号自动计算外部端口号并分别使用 1006、1007 和 1008。

采用这种方案，所有桌面可以使用相同的配置并共享相同的外部 IP 地址。如果在基本 HTTPS 端口号的基础上以 5 为增量（1000、1005、1010 …）分配端口号，将可以在同一 IP 地址上访问 12,000 多个虚拟桌面。可根据端口映射设备配置使用基本端口号来确定连接要路由到的虚拟桌面。对于在所有虚拟桌面上配置的 `externalIPAddress=10.20.30.40`、`externalRDPPort=+1`、`externalPCoIPPort=+2` 和 `externalFrameworkChannelPort=+3`，虚拟桌面映射将如 NAT 和端口映射表中所述。

表 2-2. NAT 和端口映射值

虚拟机号	桌面 IP 地址	HTTPS	RDP	PCOIP (TCP 和 UDP)	框架通道
0	192.168.0.0	10.20.30.40:1000 -> 192.168.0.0:443	10.20.30.40:1001 -> 192.168.0.0:3389	10.20.30.40:1002 -> 192.168.0.0:4172	10.20.30.40:1003 -> 192.168.0.0:32111
1	192.168.0.1	10.20.30.40:1005 -> 192.168.0.1:443	10.20.30.40:1006 -> 192.168.0.1:3389	10.20.30.40:1007 -> 192.168.0.1:4172	10.20.30.40:1008 -> 192.168.0.1:32111
2	192.168.0.2	10.20.30.40:1010 -> 192.168.0.2:443	10.20.30.40:1011 -> 192.168.0.2:3389	10.20.30.40:1012 -> 192.168.0.2:4172	10.20.30.40:1013 -> 192.168.0.2:32111
3	192.168.0.3	10.20.30.40:1015 -> 192.168.0.3:443	10.20.30.40:1016 -> 192.168.0.3:3389	10.20.30.40:1017 -> 192.168.0.3:4172	10.20.30.40:1018 -> 192.168.0.3:32111

在本示例中，Horizon Client 连接到 IP 地址 10.20.30.40 和 HTTPS 目标端口号 ($1000 + n * 5$)，其中， n 为桌面编号。要连接到桌面 3，客户端应连接到 10.20.30.40:1015。此寻址方案大大简化了每个桌面的配置设置。所有桌面均配置了相同的外部地址和端口配置。NAT 和端口映射配置采用相同模式在 NAT 和端口映射设备内完成，您可在单个公共 IP 地址上访问所有桌面。客户端通常使用解析到此 IP 地址的单个公共 DNS 名称。

将证书颁发机构添加到 Windows 证书存储区

对于智能卡身份验证，Windows 证书存储区中必须存在可对智能卡证书进行签名的证书颁发机构 (CA)。如果不存在，可以将 CA 添加到 Windows 证书存储区中。

前提条件

验证 Microsoft 管理控制台 (MMC) 是否具有证书管理单元。请参阅《Horizon 7 安装指南》文档中的“将证书管理单元添加到 MMC”。

步骤

- 1 启动 MMC。
- 2 在 MMC 控制台中，展开**证书 (本地计算机)** 节点，然后转到**受信任的根证书颁发机构 > 证书**文件夹。
如果存在根证书且证书链中没有中间证书，请退出 MMC。
- 3 右键单击**受信任的根证书颁发机构 > 证书**文件夹，然后单击**所有任务 > 导入**。
- 4 在**证书导入**向导中，单击**下一步**并浏览至存储根 CA 证书的位置。
- 5 选择根 CA 证书文件并单击**打开**。
- 6 连续单击**下一步**，然后单击**完成**。
- 7 如果智能卡证书由中间 CA 颁发，请导入证书链中的所有中间证书。
 - a 转到**证书 (本地计算机) > 中间证书颁发机构 > 证书**文件夹。
 - b 对每个中间证书重复步骤 3 至 6。

设置 HTML Access

View Agent Direct-Connection (VADC) 插件支持使用 HTML Access 访问基于虚拟机的桌面和已发布的桌面。不支持使用 HTML Access 访问已发布的应用程序。

本章讨论了以下主题：

- 为 HTML Access 安装 Horizon 7 Agent
- 设置静态内容传送
- 设置由可信 CA 签名的 TLS 服务器证书
- 在 Windows 10 和 Windows 2016 桌面上禁用 HTTP/2 协议

为 HTML Access 安装 Horizon 7 Agent

要支持 HTML Access，您必须通过特殊参数在基于虚拟机的桌面上安装 Horizon 7 Agent。

前提条件

- 从 VMware 下载页面（网址是 <http://www.vmware.com/go/downloadview>）下载 Horizon Agent 安装程序文件。

安装程序文件名为 VMware-viewagent-y.y.y-xxxxxx.exe（32 位 Windows）或者 VMware-viewagent-x86_64-y.y.y-xxxxxx.exe（64 位 Windows），其中 y.y.y 是版本号，xxxxxx 是内部版本号。

步骤

- ◆ 从命令行安装 Horizon 7 Agent 并指定告诉 Horizon 7 Agent 不向 Horizon 7 连接服务器注册的参数。
该示例安装 32 位版本的 Horizon 7 Agent。

```
VMware-viewagent-y.y.y-xxxxxx.exe /v VDM_SKIP_BROKER_REGISTRATION=1
```

后续步骤

安装 View Agent Direct-Connection 插件。请参阅[安装 View Agent Direct-Connection 插件](#)。

设置静态内容传送

如果 HTML Access 客户端需要由桌面提供服务，您必须在此桌面上执行一些设置任务。设置后，用户可以把浏览器直接指向桌面。

前提条件

- 从 VMware 下载页面（网址是 <http://www.vmware.com/go/downloadview>）下载 Horizon HTML Access portal.war zip 文件。

文件名为 VMware-Horizon-View-HTML-Access-y.y.y-xxxxxx.zip，其中 y.y.y 为版本号，xxxxxx 为内部版本号。

步骤

- 1 打开控制面板。
- 2 导航到**程序和功能 > 打开或关闭 Windows 功能**。
- 3 选中 **Internet 信息服务** 复选框并单击**确定**。
- 4 在**控制面板**中，导航到**管理工具 > Internet 信息服务 (IIS) 管理器**。
- 5 在左侧窗格中展开各项。
- 6 右键单击**默认网站**，然后选择**编辑绑定...**。
- 7 单击**添加**。
- 8 指定 **https**、**所有未分配项**和端口 **443**。
- 9 在 **SSL 证书**字段中，选择正确的证书。

选项	操作
证书 vdm 已存在。	选择 vdm ，然后单击 确定 。
证书 vdm 不存在。	选择 vdmdefault ，然后单击 确定 。

- 10 在**站点绑定**对话框中，移除 **http 端口 80** 对应的条目，然后单击**关闭**。
- 11 单击**默认网站**。
- 12 双击 **MIME 类型**。
- 13 如果文件扩展名 **.json** 不存在，请在**操作**窗格中单击**添加...**。否则，跳过接下来的 2 个步骤。
- 14 对于文件扩展名，输入 **.json**。
- 15 对于 **MIME 类型**，输入**文本/h323**，然后单击**确定**。
- 16 对于文件扩展名，输入 **.mem**。
- 17 对于 **MIME 类型**，输入 **text/plain**，然后单击**确定**。
- 18 将 VMware-Horizon-View-HTML-Access-y.y.y-xxxxxx.zip 复制到临时文件夹中。
- 19 解压缩 VMware-Horizon-View-HTML-Access-y.y.y-xxxxxx.zip。
将生成名为 portal.war 的文件。
- 20 将 portal.war 重命名为 portal.zip。

21 将 portal.zip 解压缩到文件夹 C:\inetpub\wwwroot。

如果需要，调整对该文件夹的权限，以允许添加这些文件。

此时将创建 C:\inetpub\wwwroot\portal 文件夹。

22 打开记事本。

23 创建文件 C:\inetpub\wwwroot\Default.htm，让其包含以下内容（将 *<IP address or DNS name of desktop>* 替换为桌面的实际 IP 地址或 DNS 名称）：

```
<HEAD>
<noscript>
  <meta HTTP-EQUIV="REFRESH" content="0; url=https://<IP address or DNS name of
desktop>/portal/webclient/index.html">
</noscript>
</HEAD>
<script>
  var destination = 'https://<IP address or DNS name of desktop>/portal/webclient/index.html';
  var isSearch = !!window.location.search;
  window.location.href = destination + (isSearch ? window.location.search + '&' : '?') + 'vadc=1'
+ (window.location.hash || '');
</script>
```

设置由可信 CA 签名的 TLS 服务器证书

您可以设置由可信 CA 签名的 TLS 服务器证书，以确保客户端与桌面之间的流量不是欺骗性的。

前提条件

- 将默认自签名 TLS 服务器证书替换为由可信 CA 签名的 TLS 服务器证书。请参阅 [替换默认自签名 TLS 服务器证书](#)。这会创建一个“友好名称”值为 **vdm** 的证书。
- 如果客户端的静态内容由桌面提供，请设置静态内容交付。请参阅[设置静态内容传送](#)。
- 熟悉 Windows 证书存储区。请参阅《Horizon 7 安装指南》文档中的“配置连接服务器、安全服务器或 View Composer 以使用新 TLS 证书”。

步骤

- 1 在 Windows 证书存储区中，导航至**个人 > 证书**。
- 2 双击“友好名称”为 **vdm** 的证书。
- 3 单击**详细信息**选项卡。
- 4 复制**指纹**值。
- 5 启动 Windows 注册表编辑器。
- 6 导航到注册表项 HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config。
- 7 为此注册表项添加新字符串 (REG_SZ) 值 SSLHash。
- 8 将 SSLHash 值设置为**指纹**值。

在 Windows 10 和 Windows 2016 桌面上禁用 HTTP/2 协议

对于某些 Web 浏览器，您可能会在访问 Windows 10 VADC 或 Windows 2016 VADC 桌面时遇到 ERR_SPDY_PROTOCOL_ERROR 错误。您可以在桌面上禁用 HTTP/2 协议以防止出现该错误。

步骤

- 1 启动 Windows 注册表编辑器。
- 2 导航到注册表项
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\HTTP\Parameters。
- 3 在该注册表项中添加 2 个新 REG_DWORD 值：EnableHttp2Tls 和 EnableHttp2Cleartext。
- 4 将两个值设置为 0。
- 5 重新引导桌面。

在远程桌面服务主机上设置 View Agent 直接连接

4

Horizon 7 支持远程桌面服务 (Remote Desktop Services, RDS) 主机，这些主机为用户提供可从 Horizon Client 访问的已发布桌面和应用程序。已发布的桌面基于与 RDS 主机建立的桌面会话。在典型的 Horizon 7 部署中，客户端通过 Horizon 连接服务器连接到桌面和应用程序。但是，如果您在 RDS 主机上安装 View Agent Direct-Connection 插件，客户端可以直接连接到已发布的桌面或应用程序，而无需使用 Horizon 连接服务器。

本章讨论了以下主题：

- [远程桌面服务主机](#)
- [授权已发布的桌面和应用程序](#)

远程桌面服务主机

远程桌面服务 (RDS) 主机是用于托管要远程访问的应用程序和桌面的服务器计算机。

在 Horizon 7 部署中，RDS 主机是已安装 Microsoft 远程桌面服务角色、Microsoft 远程桌面会话主机服务及 Horizon Agent 的 Windows 服务器。如果 RDS 主机还安装了 View Agent Direct Connection (VADC) 插件，则该主机可以支持 VADC。有关设置 RDS 主机和安装 Horizon 7 Agent 的信息，请参阅《在 Horizon 7 中设置已发布的桌面和应用程序》文档中的“设置远程桌面服务主机”。有关安装 VADC 插件的信息，请参阅[第 1 章，安装 View Agent Direct-Connection 插件](#)。

注 安装 Horizon Agent 时，安装程序会要求提供 Horizon Agent 将连接到的 Horizon 连接服务器的主机名或 IP 地址。通过在运行安装程序时设置参数，可以使安装程序跳过此步骤。

```
VMware-viewagent-x86_64-y.y.y-xxxxxx.exe /v "VDM_SKIP_BROKER_REGISTRATION=1"
```

在设置 RDS 主机并安装 VADC 插件之后，您必须授权 RDS 桌面和应用程序。请参阅[授权已发布的桌面和应用程序](#)。

授权已发布的桌面和应用程序

您必须先向用户授予使用已发布桌面和应用程序的权限，然后用户才能访问这些桌面和应用程序。

如果 RDS 主机运行 Windows Server 2008 R2 SP1，请运行 **RemoteApp 管理器** 配置授权。

如果 RDS 主机运行 Windows Server 2012 或 2012 R2，请运行 **服务器管理器** 并导航到 **远程桌面服务** 来配置授权。

桌面授权

要授权用户启动已发布的桌面，请执行以下步骤：

- 确保用户是本地组 **View Agent Direct-Connection** 用户的成员。默认情况下，所有经过身份验证的用户都是此组的成员。
- 对于 Windows Server 2008 R2 SP1，在 **RemoteApp 管理器** 中，确保 RD 会话主机服务器被配置为在 **RD Web 访问** 中显示到此 RD 会话主机服务器的远程桌面连接。
- 对于 Windows 2012 或 2012 R2，运行 **服务器管理器** 并导航到 **远程桌面服务** 来配置授权。

应用程序授权

要授权用户启动应用程序，请执行以下步骤：

- 确保用户是本地组 **View Agent Direct-Connection** 用户的成员。默认情况下，所有经过身份验证的用户都是此组的成员。
- 对于 Windows Server 2008 R2 SP1，在 **RemoteApp 管理器** 中，确保应用程序已在 **RemoteApp** 程序下列出，已设置了 **RD Web 访问**，并为所有用户、此用户或用户所属的组设置了用户分配。
- 对于 Windows 2012 或 2012 R2，运行 **服务器管理器** 并导航到 **远程桌面服务** 来配置授权。

View Agent Direct-Connection 插件故障排除

5

使用 View Agent Direct-Connection 插件时，您可能会遇到某些已知问题。

调查 View Agent Direct-Connection 插件的问题时，请确保已安装并正在运行正确的版本。

如果需要向 VMware 提出支持问题，请始终启用完全日志记录，重现问题，然后生成数据收集工具 (Data Collection Tool, DCT) 日志集。然后，VMware 技术支持人员可以分析这些日志。有关生成 DCT 日志集的详细信息，请参阅 VMware 知识库 (KB) 文章 <http://kb.vmware.com/kb/1017939> 的“收集诊断信息”部分。

本章讨论了以下主题：

- 安装了错误的图形驱动程序
- 视频 RAM 不足
- 启用完整日志记录以包括跟踪和调试信息

安装了错误的图形驱动程序

为使 PCoIP 正常工作，必须安装正确版本的图形驱动程序。

问题

当用户使用 PCoIP 连接到桌面或应用程序时，显示器会显示黑屏。

原因

目前运行的图形驱动程序版本不正确。如果安装 Horizon 7 Agent 后安装的 VMware Tools 版本不正确，则会发生此情况。

解决方案

- ◆ 重新安装 Horizon 7 Agent。

视频 RAM 不足

要支持 PCoIP，运行桌面或 RDS 主机的虚拟机必须至少具有 128 MB 视频 RAM。

问题

当用户使用 PCoIP 连接到桌面或应用程序时，显示器会显示黑屏。

原因

虚拟机具有的视频 RAM 不足。

解决方案

- ◆ 至少为每个虚拟机配置 128 MB 视频 RAM。

启用完整日志记录以包括跟踪和调试信息

View Agent Direct-Connection 插件将日志条目写入标准的 Horizon Agent 日志。默认情况下，日志中不包括 TRACE 和 DEBUG 信息。

问题

Horizon 7 Agent 日志不包含 TRACE 和 DEBUG 信息。

原因

未启用完整日志记录。您必须启用完整日志记录才能在 Horizon Agent 日志中包括 TRACE 和 DEBUG 信息。

解决方案

- 1 打开命令提示符并运行 `C:\Program Files\VMware\VMware View\Agent\DCT\support.bat loglevels`
- 2 输入 **3** 指定完整日志记录。

调试日志文件位于 `%ALLUSERSPROFILE%\VMware\VDM\logs` 中。文件 `debug*.log` 中包含从 Horizon Agent 和插件中记录的信息。搜索 `wsnm_xmlapi` 可找到该插件的日志行。

在 Horizon Agent 启动时，会记录插件版本：

```
2012-10-01T12:09:59.078+01:00 INFO (09E4-0C08) <logloaded> [MessageFrameWork]
Plugin 'wsnm_xmlapi - VMware View Agent XML API Handler Plugin' loaded,
version=e.x.p build= 855808, buildtype=release
```

```
2012-10-01T12:09:59.078+01:00 TRACE (09E4-06E4) <PluginInitThread> [wsnm_xmlapi]
Agent XML API Protocol Handler starting
```