VMware Horizon View Agent Direct-Connection 插件管理

Horizon View 5.3

View Agent 5.3

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-001290-00

vmware®

最新的技术文档可以从 VMware 网站下载：

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

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 Horizon View Agent Direct-Connection 插件管理 5

1 设置和安装 VMware Horizon View Agent Direct-Connection 插件 7

VMware Horizon View Agent Direct-Connection 插件的系统要求 7

安装 VMware Horizon View Agent Direct-Connection 插件 7

卸载 VMware Horizon View Agent Direct-Connection 插件 8

2 VMware Horizon View Agent Direct Connection 插件高级配置 9

VMware Horizon View Agent Direct-Connection 插件配置设置 9

在 SSL/TLS 中禁用弱密码 11

替换默认的 自签名 SSL 服务器证书 12

授权 View Client 访问 View 桌面 12

使用网络地址转换和端口映射 12

3 排除 VMware Horizon View Agent Direct-Connection 插件故障 17

启用完整记录以包含 TRACE 和 DEBUG 信息 17

索引 19

VMware Horizon View Agent Direct-Connection 插件管理

*VMware Horizon View Agent Direct-Connection 插件管理*介绍了有关安装和配置 VMware Horizon View Agent Direct-Connection 插件的信息。此插件是 View Agent 的选装组件，能让 View Client 直接连接到 View 桌面而无需使用 View 连接服务器。

利用虚拟桌面上运行的 VMware Horizon View Agent Direct-Connection 插件，客户端可以直接连接到 虚拟桌面。View 桌面的所有功能，包括 PCoIP、HTML5 访问、RDP、USB 重定向和会话管理都以同样的方式运行，就像 用户已通过 View 连接服务器建立了连接。

目标 读者

本文所含信息面向 任何希望在 VMware 虚拟桌面上安装、升级或使用 VMware Horizon View Agent Direct-Connection 插件的人员。本指南专供 有经验的 Windows 系统管理员阅读，他们需熟悉虚拟 机技术和数据中心的运作。

设置和安装 VMware Horizon View Agent Direct-Connection 插件

1

安装 Horizon View Agent Direct-Connection 插件的过程中需要确认 View 桌面满足特定的系统要求，然后才能在虚拟机上运行插件安装程序。

本章讨论了以下主题：

- 第 7 页，“VMware Horizon View Agent Direct-Connection 插件的系统要求”
- 第 7 页，“安装 VMware Horizon View Agent Direct-Connection 插件”
- 第 8 页，“卸载 VMware Horizon View Agent Direct-Connection 插件”

VMware Horizon View Agent Direct-Connection 插件的系统要求

Horizon View Agent Direct-Connection 插件必须安装到满足特定软件要求的 View 虚拟桌面上。

表 1-1 Horizon View Agent Direct-Connection 插件的系统要求

vSphere 版本	操作系统版本	软件
所述版本的 View Agent 所支持的 任何 vSphere 版本。 **重要事项** 所有虚拟桌面都必须在 vSphere 5.x ESXi 主机上托管。	所述版本的 View Agent 所支持的 任何操作系统版本。	■ View Agent 5.3 或 更高版本 ■ 您必须在安装 VMware Tools 后安装 Horizon View Agent。

重要事项 每个 View 虚拟桌面必须配置至少 128MB 的视频 RAM 才能保证 PCoIP 正常工作。

虚拟桌面可以 加入到 Microsoft Active Directory 域中，或是成为 工作组的成员。

安装 VMware Horizon View Agent Direct-Connection 插件

您必须将 Horizon View Agent Direct-Connection 插件安装到运行 View Agent 的 Windows 虚拟机。

前提条件

确定虚拟机运行的是受支持版本的 View Agent，配置了足够的视频 RAM 且运行于受支持版本的 ESXi。请参阅第 7 页，“VMware Horizon View Agent Direct-Connection 插件的系统要求”。

步骤

1 以管理员身份登录虚拟机并启动适合当前操作系统的安装程序。

操作系统	安装程序
64 位 Windows	`VMware-viewagent-direct-connection-x86_64-x.y.z-nnnnnn.exe`
32 位 Windows	`VMware-viewagent-direct-connection-x.y.z-nnnnnn.exe`

安装程序确认安装了正确版本的 Windows 操作系统和 View Agent。

2 也可以在“配置信息”对话框中输入插件在监听 View Client 的传入 HTTPS 请求时所用的 TCP 端口号。

默认的 TCP 端口号是 443，多数情况下不应更改，但如有必要，可以在安装过后更改。

自动配置 Windows 防火墙复选框为默认选中。该选项可添加此 TCP 端口的防火墙规则以允许从 View client 进行连接。如果 Windows 防火墙正在运行且此规则尚未创建，View Client 将无法进行连接。

下一步

使用 View Client 访问此虚拟机，测试已完成的安装环境。在 View Client 中，您需要指定运行此插件的 View 桌面的名称或 IP 地址，而不是指定 View 连接服务器实例或安全服务器的名称或 IP 地址。您将接受和往常一样的身份验证，而选择和连接桌面时的用户体验与通过 View 连接服务器连接时相比并无差异。

卸载 VMware Horizon View Agent Direct-Connection 插件

您可以像卸载其他 Windows 应用程序那样卸载 Horizon View Agent Direct-Connection 插件。

步骤

1 打开**控制面板 > 程序和功能**

2 选择 **VMware View Agent Direct-Connection 插件**

3 选择**卸载**

Horizon View Agent Direct-Connection 插件被移除，View Agent 随即重新启动。

VMware Horizon View Agent Direct Connection 插件高级配置 2

您可以使用 默认的 Horizon View Direct-Connection 插件配置设置或 通过 Windows Active Directory 组策略 (GPO) 对其进行自定义，也可以 使用特定的 Windows 注册表设置。

本章讨论了以下主题：

- 第 9 页， “VMware Horizon View Agent Direct-Connection 插件配置设置”
- 第 11 页， “在 SSL/TLS 中禁用弱密码”
- 第 12 页， “替换默认的 自签名 SSL 服务器证书”
- 第 12 页， “授权 View Client 访问 View 桌面”
- 第 12 页， “使用网络地址转换和端口映射”

VMware Horizon View Agent Direct-Connection 插件配置设置

Horizon View Agent Direct-Connection 插件的 所有配置设置都存储在 各 View 桌面的本地注册表中。您可以借助本地策略编辑器使用 Windows Active Directory 组策略 (GPO) 管理这些设置， 也可以直接修改注册表来管理这些设置。

该插件采用 默认值。但您也可以更改默认设置。这些注册表值 可以在下面的注册表项中设置：

```
HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Agent\Configuration\XMLAPI
```

表 2-1 Direct-Connection 插件 配置设置

设置	注册表值	类型	描述
HTTPS 端口号	httpsPortNumber	REG_SZ	插件监听来自 View Client 的传入 HTTPS 请求时所在的 TCP 端口号。如果该值发生变化，您必须 对 Windows 防火墙进行相应更改以便允许新值。
会话超时	sessionTimeout	REG_SZ	用户在登录 View Client 后 能让会话保持打开的时间。此值的单位为分钟。如果该策略 未经配置或被禁用，默认值就是 600 分钟。如果桌面 会话超时，会话将被终止，View Client 会与桌面 断开连接。
启用免责声明	disclaimerEnabled	REG_SZ	该值可设置为 TRUE 或 FALSE。如果设为 TRUE，则在登录时显示免责声明文本 由用户接受。所示文本来自 'Disclaimer Text'（如已编写）或 GPO Configuration\Windows Settings\Security Settings\Local Policies\Security Options:Interactive logon。disclaimerEnabled 的默认设置为 FALSE。

表 2-1 Direct-Connection 插件 配置设置 （续）

设置	注册表值	类型	描述
免责声明文本	disclaimerText	REG_SZ	在登录时向 View Client 用户显示的 免责声明文本。Disclaimer Enabled 策略必须设置为 TRUE。如果未指定该文本，将默认 使用 Windows 策略值 Configuration\Windows Settings\Security Settings\Local Policies\Security Options。
客户端设置：始终连接	alwaysConnect	REG_SZ	该值可设置为 TRUE 或 FALSE。AlwaysConnect 设置会发送到 View Client。如果该策略设置为 TRUE，它将覆盖任何已保存的客户端首选项。默认情况下不指定任何值。启用该策略即可将值设置为 TRUE。禁用该策略会将值设置为 FALSE。
外部 PCoIP 端口	externalPCoIPPort	REG_SZ	发送到 View Client 的端口号，用于 PCoIP 协议所用的目标 TCP/UDP 端口号。编号前面的 A + 字符表示 HTTPS 所用端口号的 相对编号。只有在外部显示的端口号 与服务监听所在的端口不匹配时，才应设置该值。通常情况下， 此端口号是在 NAT 环境中。默认情况下不指定任何值。
外部 Blast 端口	externalBlastPort	REG_SZ	发送到 View Client 的端口号，用于 HTML5/Blast 协议所用的目标 TCP 端口号。编号前面的 A + 字符表示 HTTPS 所用端口号的 相对编号。只有在外部显示的端口号 与服务监听所在的端口不匹配时，才当设置该值。通常情况下， 此端口号是在 NAT 环境中。默认情况下不指定任何值。
外部 RDP 端口	externalRDPPort	REG_SZ	发送到 View Client 的端口号，用于 RDP 协议所用的目标 TCP 端口号。编号前面的 A + 字符表示 HTTPS 所用端口号的 相对编号。只有在外部显示的端口号 与服务监听所在的端口不匹配时，才应当设置该值。通常情况下，此端口号是在 NAT 环境中。默认情况下不指定任何值。
外部 IP 地址	externalIPAddress	REG_SZ	发送到 View Client 的 IP v4 地址，用于 备用协议（RDP、PCoIP、 Framework 通道等 ）所用的目标 IP 地址。只有在外部显示的 地址与桌面计算机地址不匹配时，才应当设置该值。通常情况下， 该地址是在 NAT 环境中。默认情况下不指定任何值。
外部 Framework 通道端口	externalFrameworkChannelPort	REG_SZ	发送到 View Client 的端口号，用于 Framework Channel 协议所用的目标 TCP 端口号。编号前面的 A + 字符表示 HTTPS 所用端口号的 相对编号。只有在外部显示的端口号 与服务监听所在的端口不匹配时，才应当设置该值。通常情况下， 此端口号是在 NAT 环境中。默认情况下不指定任何值。
启用 USB	usbEnabled	REG_SZ	该值可设置为 TRUE 或 FALSE。确定桌面是否能使用连接到 客户端系统的 USB 设备。默认设置为启用。要 出于安全因素阻止使用外部设备，请将设置更改为 禁用 (FALSE)。
客户端设置：USB 自动连接	usbAutoConnect	REG_SZ	该值可设置为 TRUE 或 FALSE。在插入 USB 设备时连接此类设备到桌面。如果设置了该策略，它将覆盖任何已保存的客户端 首选项。默认情况下不指定任何值。

表 2-1 Direct-Connection 插件 配置设置 （续）

设置	注册表值	类型	描述
启用重置	resetEnabled	REG_SZ	该值可设置为 TRUE 或 FALSE。如果设为 TRUE，经过身份验证的 View client 可以执行 操作系统级重启。默认设置为禁用 (FALSE)。
客户端凭据缓存超时	clientCredentialCacheTimeout	REG_SZ	View client 允许用户使用所保存密码 的时间（分钟）。0 表示从不允许，-1 表示始终允许。如果设置为有效值，View Client 将 允许用户保存密码 。默认值是 0（从不）。

View Client 设置不会 改变插件的行为。这些设置会发送到 View Client 进行解释。

外部端口号和 外部 IP 地址值被用于网络地址转换 (NAT) 和 端口映射支持。有关详细信息，请参阅 第 12 页，“使用网络地址转换和端口映射”.

您可以设置那些 覆盖这类注册表设置的策略，方法是使用本地策略编辑器或 Active directory 中的组策略对象 (GPO)。策略设置优先于 常规注册表设置。可以使用 GPO 模板文件来 配置策略。在默认位置安装 View Agent 和插件后， 可在以下位置找到模板文件：

```
C:\Program Files\VMware\VMware View\Agent\extras\view_agent_direct_connection.adm
```

您可以将此模板 文件导入到 Active Directory 或本地组策略编辑器以简化 这些配置设置的管理。有关以此类方式管理策略设置的详细信息，请参阅 Microsoft Policy Editor and GPO handling（Microsoft 策略编辑器和 GPO 处理）文档。 插件的策略设置存储在以下注册表项位置：

```
HKEY_LOCAL_MACHINE Software\Policies\VMware, Inc.\VMware VDM\Agent\Configuration\XMLAPI
```

在 SSL/TLS 中禁用弱密码

通过这套 View 桌面强化流程，您可以让 View Client 与 View 桌面之间基于 SSL/TLS 协议的通信不使用弱加密密码。

禁用弱密码的配置存储在 Windows 注册表中。必须在运行 View Agent Direct-Connection 插件的所有桌面操作系统中更改这些设置。

注意 这些设置会在所有方面影响操作系统对 SSL/TLS 的使用。

SSL 3.0 和 TLS 1.0 (RFC2246) 与 INTERNET-DRAFT `56-bit Export Cipher Suites For TLS draft-ietf-tls-56-bit-ciphersuites-00.txt` 提供了使用不同密码套件的选项。每个密码套件都拥有密钥交换、验证、加密和 MAC 算法可用于 SSL/TLS 会话。

前提条件

您要熟悉如何使用 `Regedt32.exe` 注册表编辑器编辑 Windows 注册表项。

步骤

- 启动注册表编辑器 `Regedt32.exe`，找到以下注册表项：
  `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL`

下一步

表 2-2 密码套件更新

Windows XP SP3	Windows Vista 及更高版本
1 在子项 `\Ciphers\DES 56/56` 中添加一个 DWORD 值 `Enabled`，将其设置为 `0x0`。 2 在子项 `\Hashes\MD5` 中添加一个 DWORD 值 `Enabled` 并设置为 `0x0`。 这些更新可确保只有以下密码能用于 Windows XP SP3： ■ SSLv3 168 位 DES-CBC3-SHA ■ SSLv3 128 位 RC4-SHA ■ TLSv1 168 位 DES-CBC3-SHA ■ TLSv1 128 位 RC4-SHA	1 在子项 `\Hashes` 中创建一个子项 `MD5`。 2 在子项 `\Hashes \MD5` 中添加一个 DWORD 值 `Enabled` 并设置为 `0x0`。 这些更新可确保只有以下密码能用于 Windows Vista 及更高版本： ■ SSLv3 168 位 DES-CBC3-SHA ■ SSLv3 128 位 RC4-SHA ■ TLSv1 256 位 AES256-SHA ■ TLSv1 128 位 AES128-SHA ■ TLSv1 168 位 DES-CBC3-SHA ■ TLSv1 128 位 RC4-SHA

替换默认的 自签名 SSL 服务器证书

自签名 SSL 服务器证书无法为 View Client 提供足够的保护来抵御 篡改和窃取的威胁。为保护您的桌面免受这类 威胁，您必须替换已生成的自签名证书。

当 View Agent Direct-Connection 插件在安装后初次启动时，会 自动生成一个自签名 SSL 定位器证书并将其存放到 Windows 证书存储区。SSL 服务器证书会在 SSL 协议的协商期间呈现给 View Client 以便向客户端提供此 View 桌面的信息。这个默认的自签名 SSL 服务器证书无法 为此桌面提供保障，除非它已经被替换为 客户端信任的证书签发机构 (CA) 签发的证书，并且 经过了完整的 View Client 证书检查。

在 Windows 证书存储区内存储该证书以及替换为 相应 CA 签发证书所用的流程与 View 连接服务器（5.1 或更高版本）所用的流程完全相同。有关证书替换流程的详细信息，请参阅《VMware Horizon View 安装指南》中的 "Configuring SSL Certificates for View Servers"（为 View Server 配置 SSL 证书）。

包含使用者 备用名称 (SAN) 的证书和通配证书均可得到支持。

注意 要将 CA 签发的 SSL 服务器证书分发至大量 View 桌面（使用 View Agent Direct-Connection 插件），请使用 Active Directory Enrollment 向 每个虚拟机分发证书。有关详细信息，请参阅：http://technet.microsoft.com/en-us/library/cc732625.aspx

授权 View Client 访问 View 桌面

该授权机制允许 View Client 用户直接访问 View 桌面，由一个名为 **View Agent Direct-Connection Users** 的本地操作系统组进行控制。

如果用户是该组成员，他将被授权与桌面直接连接。初次安装插件时，会创建该本地组并加入 Authenticated Users 组。成功经过该插件身份验证的用户将得到访问桌面的授权。

要限制对此桌面的访问，您可以修改该组的成员身份以指定用户和用户组列表。这些用户可以是本地或域中的用户和用户组。如果 View Client 用户不在该组中，他将在身份验证后看到一条消息，提示其无权访问此桌面。

使用网络地址转换和端口映射

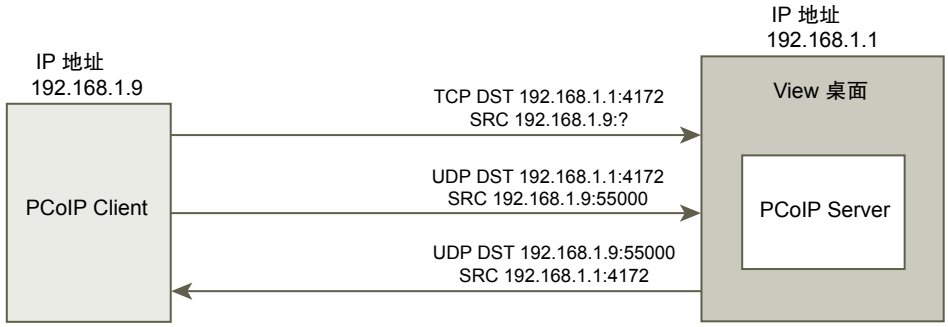
如果 View Client 连接到位于不同网络的 View 桌面，则需要进行网络地址转换 (NAT) 和端口映射配置。

在本文档所提供的示例中，您必须在 View 桌面上配置外部寻址信息以便 View Client 使用此信息通过 NAT 或端口映射设备连接 View 桌面。 此 URL 与 View 连接服务器和安全服务器上的“外部 URL”及“PCoIP 外部 URL”设置相同。

如果 View Client 位于不同的网络上，且 View Client 和运行插件的 View 虚拟桌面之间存在 NAT 设备，则需要进行 NAT 或端口映射配置。 例如，如果 View Client 和 View 虚拟桌面之间有防火墙，则防火墙将作为 NAT 或端口映射设备。

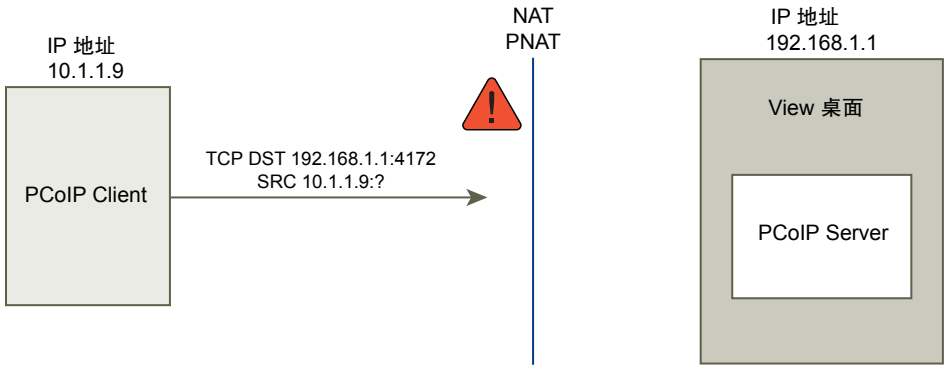
示例中，IP 地址为 192.168.1.1 的 View 桌面部署展示了 NAT 和端口映射的配置。 IP 地址为 192.168.1.9 且位于同一网络的 View Client 系统使用 TCP 和 UDP 建立了一个 PCoIP 连接。 此连接为直接连接，未使用任何 NAT 或端口映射配置。

图 2-1 来自位于同一网络的客户端的直接 PCoIP



如果您在客户端和桌面之间添加 NAT 设备以便其在不同的地址空间工作，但却未对插件进行任何配置更改，则 PCoIP 数据包将无法正确路由并将发生故障。 在本例中，客户端所使用的是不同的地址空间，且 IP 地址为 10.1.1.9。 本设置出现故障的原因是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 无法从客户端网络工作，而且可能会造成客户端显示白屏。

图 2-2 通过 NAT 设备从客户端发送 PCoIP 显示故障

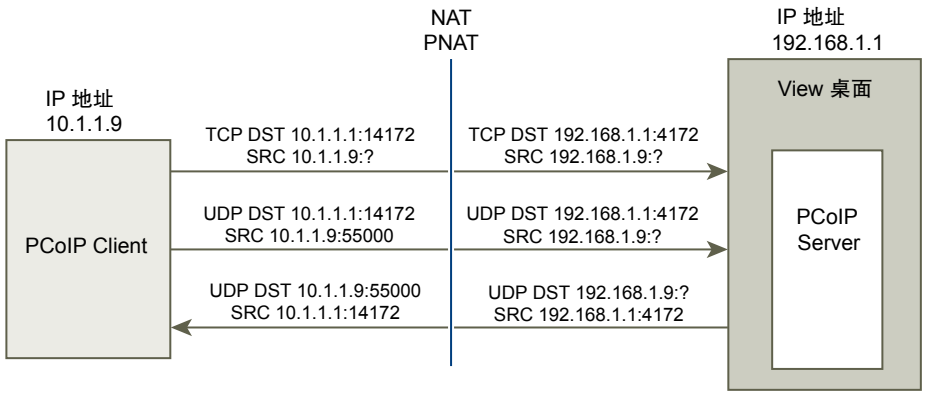


要解决此问题，您必须配置插件使用外部 IP 地址。 对于本桌面，如果 `externalIPAddress` 配置为 10.1.1.1， 则在与桌面进行桌面协议连接时，插件将为客户端分配 IP 地址 10.1.1.1。对于 PCoIP，必须在桌面上针对此设置启动 PCoIP 安全网关服务。

对于端口映射，如果桌面使用标准 PCoIP 端口 4172，但客户端必须使用其他目标端口通过端口映射设备映射到端口 4172，则您必须针对此设置配置插件。 如果端口映射设备将端口 14172 映射到 4172，则客户端必须对 PCoIP 使用目标端口 14172。 您必须针对 PCoIP 对此设置进行配置。 将插件中的 `externalPCoIPPort` 设置为 14172。

配置中使用了 NAT 和端口映射， 且 `externalIPAdress` 设置为 10.1.1.1，并经网络转换为 192.168.1.1，且 `externalPColPPort` 设置为 14172，并经端口映射为 4172。

图 2-3 通过 NAT 设备和端口映射从客户端发送 PCoIP



与 PCoIP 的外部 PCoIP TCP/UDP 端口配置相同，如果 RDP 端口 (3389) 或 Framework Channel 端口 (32111) 需要端口映射，则您必须配置 `externalRDPPort` 和 `externalFrameworkChannelPort` 以指定客户端通过端口映射设备进行连接时所需使用的 TCP 端口号。

高级寻址方案

在配置多个 View 桌面以便通过位于同一外部 IP 地址的 NAT 和端口映射设备进行访问时，必须为每个 View 桌面指定唯一的一组端口号。之后，客户端可以使用相同的目标 IP 地址，但需要用唯一的 TCP 端口号用于 HTTPS 连接才能将其指向特定的虚拟桌面。

寻址方案示例

在本示例中，HTTPS 端口 1000 指向了一个桌面，HTTPS 端口 1005 则指向另一个桌面，两者使用了同一个目标 IP 地址。此时如果为每个 View 桌面配置唯一的外部端口号用于桌面协议连接，所需的操作将非常复杂。因此，插件设置 `externalPCoIPPort`、`externalRDPPort` 和 `externalFrameworkChannelPort` 可使用可选的关系表达式替代静态值，相对于客户端所用的基础 HTTPS 端口号来定义一个其他端口号。

如果端口映射设备将端口号 1000 用于 HTTPS，则映射到 TCP 443；如果将端口号 1001 用于 RDP，则映射到 TCP 3389；端口号 1002 用于 PCoIP，则映射到 TCP 和 UDP 4172；端口号 1003 用于 framework 通道，则映射到 TCP 32111。为简化配置，外部端口号可以配置为 `externalRDPPort=+1`、`externalPCoIPPort=+2` 和 `externalFrameworkChannelPort=+3`。当 HTTPS 连接由使用 HTTPS 目标端口号 1000 的客户端传入时，外部端口号会相对于端口号 1000 自动进行计算，分别使用 1001、1002 和 1003 编号。

在部署其他虚拟桌面时，如果端口映射设备将端口号 1005 用于 HTTPS，则映射到 TCP 443；如果将端口号 1006 用于 RDP，则映射到 TCP 3389；端口号 1007 用于 PCoIP，则映射到 TCP 和 UDP 4172；端口号 1008 用于 framework 通道，则映射到 TCP 32111，桌面（+1、+2、+3，以此类推）上的外部端口配置完全一致。当 HTTPS 连接由使用 HTTPS 目标端口号 1005 的客户端传入时，外部端口号会相对于端口号 1005 自动进行计算，分别使用 1006、1007 和 1008 编号。

此方案允许所有 View 桌面采用相同配置，并共享相同的外部 IP 地址。因此，以数字 5 为增量（1000、1005、1010 等）为基础 HTTPS 端口分配端口号时，可以在同一个 IP 地址上访问超过 12,000 个虚拟桌面，并基于端口映射设备的配置使用基础端口号确定连接指向的虚拟桌面。对于配置到所有虚拟桌面的 `externalIPAddress=10.20.30.40`、`externalRDPPort=+1`、`externalPCoIPPort=+2` 和 `externalFrameworkChannelPort=+3` 设置，指向虚拟桌面的映射将符合 NAT 和端口映射表的描述。

表 2-3 NAT 和端口映射值

VM 编号	桌面 IP 地址	HTTPS	RDP	PCOIP（TCP 和 UDP）	Framework 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

View Client 可连接到 IP 地址 10.20.30.40 和 HTTPS 目标端口号（1000 + *n* * 5，其中 *n* 是 View 桌面编号）。为连接 View 桌面 3，客户端需要连接到 10.20.30.40:1015。这一寻址方案能显著简化各 View 桌面的配置设置。所有桌面都配置了相同的外部地址和端口配置。NAT 和端口映射配置会通过这一方式在 NAT 和端口映射设备内完成，所有 View 桌面都可以在单独的公共 IP 地址上访问。客户端通常使用可解析为该 IP 地址的单个公共 DNS 名称。

排除 VMware Horizon View Agent Direct-Connection 插件故障

3

在使用 Horizon View Agent Direct-Connection 插件时，您可能会遇到某些已知问题需要解决。

在检查 Horizon View Agent Direct-Connection 插件问题时，确保安装并运行了正确版本。在上面的示例中，插件版本的详细信息为 `version=e.x.p build-855808, buildtype=release`。插件名称 VMware View Agent XML API Handler Plugin 已被记录。

如果需要向 VMware 提交与支持有关的问题，请始终启用完整记录、重现问题并生成 Data Collection Tool (DCT) 日志集。VMware 技术支持人员将分析这些日志。有关生成 DCT 日志集的详细信息，请参考 VMware View 知识库文章 http://kb.vmware.com/kb/1017939 关于收集诊断信息的内容。

启用完整记录以包含 TRACE 和 DEBUG 信息

Horizon View Agent Direct-Connection 插件可将日志条目写入到标准 View Agent 日志。但默认情况下，TRACE 和 DEBUG 信息并未包含在日志中。

问题

Horizon View Agent Direct-Connection 插件可将日志条目写入到标准 View Agent 日志。但默认情况下，TRACE 和 DEBUG 信息并未包含在标准 View Agent 日志中。

原因

完整记录未启用。您必须启用完整记录才能在 View Agent 日志中包含 TRACE 和 DEBUG 信息。

解决方案

1 打开命令行提示符界面并运行 `C:\Program Files\VMware\VMware View\Agent\DCT\support.bat loglevels`

2 输入 **3** 开启完整记录。

调试日志文件位于 `%ALLUSERSPROFILE%\VMware\VDM\logs`。文件 `debug*.log` 包含了从 View Agent 和插件中记录的信息。搜索 `wsnm_xmlapi` 以寻找插件日志行。

View Agent 启动时，将记录插件版本：

```
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
```

为虚拟机配置的视频 RAM 不足

必须为虚拟机配置足够的视频 RAM。

问题

在使用 PCoIP 时出现黑屏。

原因

为虚拟机配置了不足量的视频 RAM，如 16MB 或 32MB。

解决方案

- 为每个虚拟机配置至少 128MB 的视频 RAM。

安装了错误的 图形驱动程序

必须安装正确版本的 Horizon View Agent 图形驱动程序。图形 驱动程序可能已在安装 Horizon View Agent 后降级。如果 在安装 Horizon View Agent 后安装了错误版本的 VMware Tools，就可能出现 这种情况。

问题

由于图形驱动程序降级，在使用 PCoIP 时出现黑屏。

原因

安装了 错误版本的图形驱动程序。

解决方案

- 重新安装 Horizon View Agent。

索引

A

安装 Horizon View Agent Direct-Connection 插件 **7**

C

错误的图形 驱动程序 **18**

D

端口映射 **12, 14**

H

Horizon View Agent Direct-Connection 插件 **5**

Horizon View Agent direct-connection 插件高级配置 配置 **9**

Horizon View Agent Direct-Connection 插件可实现完整记录 **17**

J

禁用弱密码 **11**

P

排除 Horizon View Agent Direct-Connection 插件故障 **17**

S

视频 RAM 不足 **18**

授权 View Client **12**

SSL 服务器 证书, 替换 **12**

V

View Agent Direct-Connection 插件的配置设置 **9**

W

网络地址转换 **12**

X

卸载 Horizon View Agent Direct-Connection 插件 **8**

系统要求, Horizon View Agent Direct-Connection 插件 **7**