VMware Horizon View Agent Direct-Connection Plugin Administration

Horizon View 5.3

View Agent 5.3

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-001290-00

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

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

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

Copyright © 2013 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

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

Contents

VMware Horizon View Agent Direct-Connection Plugin Administration

VMware Horizon View Agent Direct-Connection Plugin Administration provides information about installing and configuring VMware Horizon View Agent Direct-Connection Plugin. This plugin is an installable extension to View Agent that allows a View Client to directly connect to a View desktop without using View Connection Server.

With VMware Horizon View Agent Direct-Connection Plugin running on a virtual desktop, the client can connect directly to the virtual desktop. All the View desktop features of PCoIP, HTML5 Access, RDP, USB redirection, and session management work in the same way, as if the user had connected through View Connection Server.

Intended Audience

This information is intended for anyone who wants to install, upgrade, or use VMware Horizon View Agent Direct-Connection Plugin in the VMware virtual desktop. The guide is written for experienced Windows system administrators who are familiar with virtual machine technology and datacenter operations.

Set Up and Install VMware Horizon View Agent Direct-Connection Plugin

1

Installing the Horizon View Agent Direct-Connection Plugin involves verifying that the View desktop meets certain system requirements and then running the plugin installer on the virtual machine.

This chapter includes the following topics:

VMware Horizon View Agent Direct-Connection Plugin System Requirements

Horizon View Agent Direct-Connection Plugin must be installed on a View virtual desktop that meets certain software requirements.

Table 1-1. System Requirements for Horizon View Agent Direct-Connection Plugin

vSphere Versions	Operating System Versions	Software
Any vSphere version that the stated View Agent version supports. IMPORTANT All virtual desktops must be hosted on vSphere 5.x ESXi hosts.	Any operating system version that the stated View Agent version supports.	■ View Agent 5.3 or later ■ You must install Horizon View Agent after you install VMware Tools.

IMPORTANT Each View virtual desktop must be configured with a minimum of 128MB of video RAM for PCoIP to function correctly.

The virtual desktop can be joined to a Microsoft Active Directory Domain, or it can be a member of a Workgroup.

Install VMware Horizon View Agent Direct-Connection Plugin

You must install the Horizon View Agent Direct-Connection Plugin on a Windows virtual machine that is running View Agent.

Prerequisites

Confirm that the virtual machine is running a supported version of View Agent, has a sufficient amount of video RAM configured, and is running on a supported version of ESXi. See "VMware Horizon View Agent Direct-Connection Plugin System Requirements," on page 7.

Procedure

1 Log in to the virtual machine as an administrator and launch the installer that is appropriate for your operating system.

Operating System	Installer
Windows 64-bit	`VMware-viewagent-direct-connection-x86_64-x.y.z-nnnnnn.exe`
Windows 32-bit	`VMware-viewagent-direct-connection-x.y.z-nnnnnn.exe`

The installer confirms that the correct version of the Windows operating system and View Agent is installed.

2 Optionally, enter the TCP port number used by the plugin to listen for incoming HTTPS requests from View Clients in the Configuration Information dialog box.

The default TCP port number is 443 and should not be changed in most cases, but the port number can be changed later after installation, if required.

The **Configure Windows Firewall automatically** checkbox is selected by default. This selection adds a firewall rule for this TCP port to allow connections from View clients. If the Windows firewall is running and this rule has not been created, the View Clients will not be able to connect.

What to do next

Test the completed installation by using View Client to access this virtual machine. In the View Client, instead of specifying the name or IP address of a View Connection Server instance or security server, you specify the name or IP address of a View desktop running this plugin. You authenticate as normal and the user experience for selecting and connecting to the desktop is the same as when connecting through View Connection Server.

Uninstall VMware Horizon View Agent Direct-Connection Plugin

You can uninstall the Horizon View Agent Direct-Connection Plugin just as you do other Windows applications.

Procedure

1 Go to **Control Panel > Programs and Features.**

2 Select **VMware View Agent Direct-Connection Plugin.**

3 Select **Uninstall.**

The Horizon View Agent Direct-Connection Plugin is removed, and the View Agent is restarted.

VMware Horizon View Agent Direct-Connection Plugin Advanced Configuration

2

You can use the default Horizon View Direct-Connection Plugin configuration settings or customize them through Windows Active Directory group policies (GPOs) or by using specific Windows registry settings.

This chapter includes the following topics:

VMware Horizon View Agent Direct-Connection Plugin Configuration Settings

All configuration settings for Horizon View Agent Direct-Connection Plugin are stored in the local registry on each View desktop. You can manage these settings using Windows Active Directory group policies (GPOs), through the local policy editor, or by directly modifying the registry.

The plugin works with the default values. You can, however, change the defaults. These registry values can be set in the registry key:

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

Table 2-1. Direct-Connection Plugin Configuration Settings

Setting	Registry Value	Type	Description
HTTPS Port Number	httpsPortNumber	REG_SZ	TCP port number on which the plugin listens for incoming HTTPS requests from View Client. If this value is changed, you must make a corresponding change to the Windows firewall so that the new is allowed.
Session Timeout	sessionTimeout	REG_SZ	Period of time a user can keep a session open after logging in with View Client. The value is set in minutes. If this policy is not configured or disabled, the default is 600 minutes. When a desktop session times out, the session is terminated and View Client is disconnected from the desktop.

Table 2-1. Direct-Connection Plugin Configuration Settings (Continued)

Setting	Registry Value	Type	Description
Disclaimer Enabled	disclaimerEnabled	REG_SZ	Value is set to TRUE or FALSE. If set to TRUE, show disclaimer text for user acceptance at login. The text is shown from 'Disclaimer Text' if written, or from the GPO Configuration\Windows Settings\Security Settings\Local Policies\Security Options: Interactive logon. The default setting for disclaimerEnabled is FALSE.
Disclaimer Text	disclaimerText	REG_SZ	Disclaimer text shown to View Client users at log in. The Disclaimer Enabled policy must be set to TRUE. If the text is not specified, the default is to use the value from Windows policy Configuration\Windows Settings\Security Settings\Local Policies\Security Options.
Client setting: AlwaysConnect	alwaysConnect	REG_SZ	Value is set to TRUE or FALSE. AlwaysConnect setting is sent to View Client. If this policy is set to TRUE, it overrides any saved client preferences. No value is set by default. Enabling this policy sets the value to TRUE. Disabling this policy sets the value to FALSE.
External PCoIP Port	externalPCoIPPort	REG_SZ	Port number sent to View Client for the destination TCP/UDP port number that is used for the PCoIP protocol. A + character in front of the number indicates a relative number from the port number used for HTTPS. Only set this value if the externally exposed port number does not match the port that the service is listening on. Typically, this port number is in a NAT environment. No value is set by default.
External Blast Port	externalBlastPort	REG_SZ	Port number sent to View Client for the destination TCP port number that is used for the HTML5/Blast protocol. A + character in front of the number indicates a relative number from the port number used for HTTPS. Only set this value if the externally exposed port number does not match the port that the service is listening on. Typically, this port number is in a NAT environment. No value is set by default.
External RDP Port	externalRDPPort	REG_SZ	Port number sent to View Client for the destination TCP port number that is used for the RDP protocol. A + character in front of the number indicates a relative number from the port number used for HTTPS. Only set this value if the externally exposed port number does not match the port that the service is listening on. Typically, this port number is in a NAT environment. No value is set by default.
External IP Address	externalIPAddress	REG_SZ	IP v4 address sent to View Client for the destination IP address that is used for secondary protocols (RDP, PCoIP, Framework channel, and so on). Only set this value if the externally exposed address does not match the address of the desktop machine. Typically, this address is in a NAT environment. No value is set by default.

Table 2-1. Direct-Connection Plugin Configuration Settings (Continued)

Setting	Registry Value	Type	Description
External Framework Channel Port	externalFrameworkChannelPort	REG_SZ	The port number sent to the View Client for the destination TCP port number that is used for the Framework Channel protocol. A + character in front of the number indicates a relative number from the port number used for HTTPS. Only set this value if the externally exposed port number does not match the port where the service is listening. Typically, this port number is in a NAT environment. No value is set by default.
USB Enabled	usbEnabled	REG_SZ	Value is set to `TRUE`or `FALSE`. Determines whether desktops can use USB devices connected to the client system. The default value is enabled. To prevent the use of external devices for security reasons, change the setting to disabled (`FALSE`).
Client setting: USB AutoConnect	usbAutoConnect	REG_SZ	Value is set to `TRUE` or `FALSE`. Connect USB devices to the desktop when they are plugged in. If this policy is set, it overrides any saved client preferences. No value is set by default.
Reset Enabled	resetEnabled	REG_SZ	Value is set to `TRUE`or `FALSE`. When set to `TRUE`, an authenticated View client can perform an operating system level reboot. The default setting is disabled (`FALSE`).
Client Credential Cache Timeout	clientCredentialCacheTimeout	REG_SZ	Time, in minutes, that a View client allows a user to use a saved password. 0 means never, and -1 means forever. View Client offers users the option of saving their passwords if this setting is set to a valid value. The default is 0 (never).

View Client settings do not change the behavior of the plugin. These settings are sent to the View Client for interpretation.

The External Port numbers and External IP Address values are used for Network Address Translation (NAT) and port mapping support. For more information see, "Using Network Address Translation and Port Mapping," on page 13.

You can set policies that override these registry settings by using the Local Policy Editor or by using Group Policy Objects (GPOs) in Active directory. Policy settings have precedence over normal registry settings. A GPO template file is supplied to configure policies. When the View Agent and plugin are installed in the default location, the template file has the following location:

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

You can import this template file into Active Directory or the Local Group Policy Editor to simplify the management of these configuration settings. See the Microsoft Policy Editor and GPO handling documentation for details of managing policy settings in this way. Policy settings for the plugin are stored in the registry key:

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

Disabling Weak Ciphers in SSL/TLS

You can ensure that View Client to View desktop communications that use SSL/TLS protocol do not allow weak cryptographic ciphers by using this View desktop hardening procedure.

The configuration for disabling weak ciphers is stored in the Windows registry. Changes to these settings must be done on all desktop operating systems that run View Agent Direct-Connection Plugin.

NOTE These settings affect all use of SSL/TLS on the operating system.

Both SSL 3.0 and TLS 1.0 (RFC2246) with INTERNET-DRAFT `56-bit Export Cipher Suites For TLS draft-ietf-tls-56-bit-ciphersuites-00.txt` provide options to use different cipher suits. Each cipher suite determines the key exchange, authentication, encryption, and MAC algorithms used within a SSL/TLS session.

Prerequisites

You need to have experience editing Windows registry keys using the `Regedt32.exe` registry editor.

Procedure

- Start Registry Editor `Regedt32.exe`, and locate this registry key:`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL`

What to do next

Table 2-2. Cipher Suites Updates

Windows XP SP3	Windows Vista and Later
1 In subkey`\Ciphers\DES 56/56` add a DWORD value `Enabled` with a value of `0x0`. 2 In subkey`\Hashes\MD5` add a DWORD value `Enabled` with a value of `0x0`. These updates ensure that only the following ciphers are available on Windows XP SP3: ■ SSLv3 168 bits DES-CBC3-SHA ■ SSLv3 128 bits RC4-SHA ■ TLSv1 168 bits DES-CBC3-SHA ■ TLSv1 128 bits RC4-SHA	1 In subkey `\Hashes`create a subkey `MD5`. 2 In subkey `\Hashes \MD5`add a DWORD value `Enabled` with a value of `0x0`. These updates ensure that only the following ciphers are available on Windows Vista and later: ■ SSLv3 168 bits DES-CBC3-SHA ■ SSLv3 128 bits RC4-SHA ■ TLSv1 256 bits AES256-SHA ■ TLSv1 128 bits AES128-SHA ■ TLSv1 168 bits DES-CBC3-SHA ■ TLSv1 128 bits RC4-SHA

Replacing the Default Self-Signed SSL Server Certificate

A self-signed SSL server certificate cannot give View Client sufficient protection against threats of tampering and eavesdropping. To protect your desktops from these threats, you must replace the generated self-signed certificate.

When View Agent Direct-Connection Plugin starts for the first time after installation, it automatically generates a self-signed SSL server certificate and places it in the Windows Certificate Store. The SSL server certificate is presented to View Client during the SSL protocol negotiation to provide information to the client about this View desktop. This default self-signed SSL server certificate cannot give guarantees about this desktop, unless it is replaced by a certificate signed by a Certificate Authority (CA) that is trusted by the client and is fully validated by the View Client certificate checks.

The procedure for storing this certificate in the Windows Certificate Store and the procedure for replacing it with a proper CA signed certificate, are the same as those used for View Connection Server (version 5.1 or later). See "Configuring SSL Certificates for View Servers," in the VMware Horizon View Installation document for details on this certificate replacement procedure.

Certificates with Subject Alternative Name (SAN) and wildcard certificates are supported.

NOTE To distribute the CA signed SSL Server Certificates to a large number of View desktops using the View Agent Direct-Connection Plugin, use Active Directory Enrollment to distribute the certificates to each virtual machine. For more information see: http://technet.microsoft.com/en-us/library/cc732625.aspx

Authorizing View Client to Access the View Desktop

The authorization mechanism that allows a View Client user to access the View desktop directly is controlled within a local operating system group called **View Agent Direct-Connection Users**.

If a user is a member of this group, that user is authorized to connect to the desktop directly. When the plugin is first installed, this local group is created and contains the Authenticated Users group. Anyone who is successfully authenticated by the plugin is authorized to access the desktop.

To restrict access to this desktop, you can modify the membership of this group to specify a list of users and user groups. These users can be local or domain users and user groups. If the View Client user is not in this group, the user gets a message after authentication saying that the user is not entitled to access this desktop.

Using Network Address Translation and Port Mapping

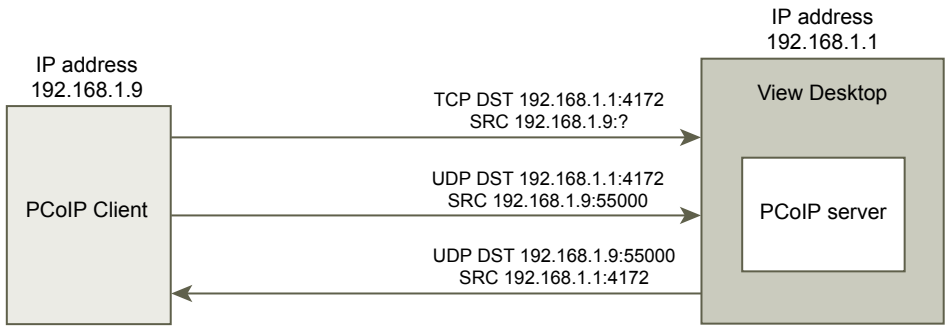
Network Address Translation (NAT) and port mapping configuration are required if View Clients connect to View desktops on different networks.

In the examples included here, you must configure external addressing information on the View desktop so that View Client can use this information to connect to the View desktop by using NAT or a port mapping device. This URL is the same as the External URL and PCoIP External URL settings on View Connection Server and security server.

When View Client is on a different network and a NAT device is between View Client and the View virtual desktop running the plugin, a NAT or port mapping configuration is required. For example, If there is a firewall between the View Client and the View virtual desktop the firewall is acting as a NAT or port mapping device.

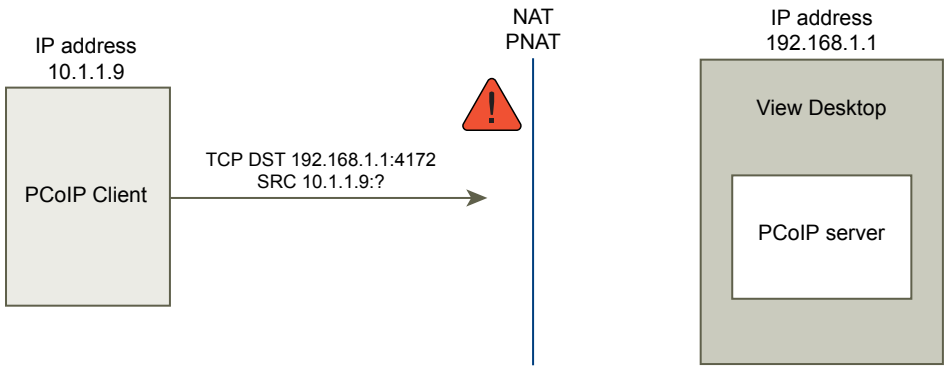
An example deployment of a View desktop whose IP address is 192.168.1.1 illustrates the configuration of NAT and port mapping. A View Client system with an IP address of 192.168.1.9 on the same network establishes a PCoIP connection by using TCP and UDP. This connection is direct without any NAT or port mapping configuration.

Figure 2-1. Direct PCoIP from a Client on the Same Network



If you add a NAT device between the client and desktop so that they are operating in a different address space and do not make any configuration changes to the plugin, the PCoIP packets will not be routed correctly and will fail. In this example, the client is using a different address space and has an IP address of 10.1.1.9. This setup fails because the client will use the address of the desktop to send the TCP and UDP PCoIP packets. The destination address of 192.168.1.1 will not work from the client network and might cause the client to display a blank screen.

Figure 2-2. PCoIP From a Client via a NAT Device Showing the Failure

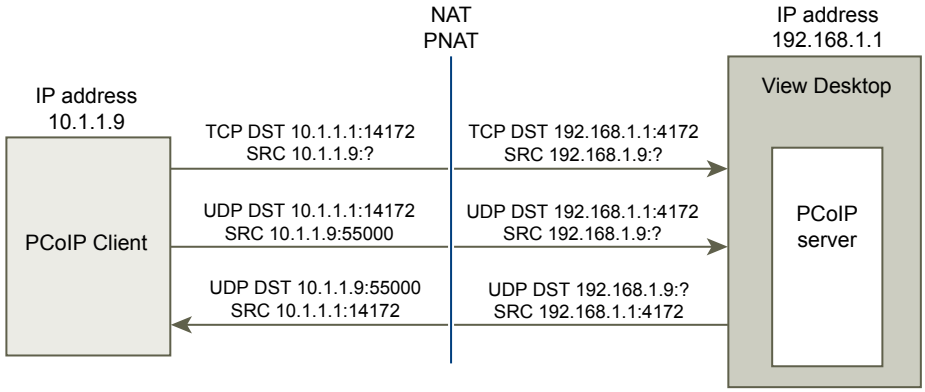


To resolve this problem, you must configure the plugin to use an external IP address. If `externalIPAddress` is configured as 10.1.1.1 for this desktop, the plugin gives the client an IP address of 10.1.1.1 when making desktop protocol connections to the desktop. For PCoIP, the PCoIP Secure Gateway service must be started on the desktop for this setup.

For port mapping, when the desktop uses the standard PCoIP port 4172, but the client must use a different destination port, mapped to port 4172 at the port mapping device, you must configure the plugin for this setup. If the port mapping device maps port 14172 to 4172, the client must use a destination port of 14172 for PCoIP. You must configure this setup for PCoIP. Set `externalPCoIPPortin` the plugin to 14172.

In a configuration which uses NAT and port mapping, and the `externalIPAdress` is set to 10.1.1.1, which is network translated to 192.168.1.1, and `externalPColPPort` is set to 14172, which is port mapped to 4172.

Figure 2-3. PCoIP From a Client via a NAT Device and Port Mapping



As with the external PCoIP TCP/UDP port configuration for PCoIP, if the RDP port (3389) or the Framework Channel port (32111) is port mapped, you must configure `externalRDPPort` and `externalFrameworkChannelPort` to specify the TCP port numbers that the client will use to make these connections through a port mapping device.

Advanced Addressing Scheme

When you configure several View desktops to be accessible through a NAT and port mapping device on the same external IP address, you must give each View desktop a unique set of port numbers. The clients can then use the same destination IP address, but use a unique TCP port number for the HTTPS connection to direct the connection to a specific virtual desktop.

Addressing Scheme Examples

In this example, HTTPS port 1000 directs to one desktop and HTTPS port 1005 directs to another, with both using the same destination IP address. In this case, configuring unique external port numbers for every View desktop for the desktop protocol connections would be too complex. For this reason, the plugin settings `externalPCoIPPort`,`externalRDPPort`, and `externalFrameworkChannelPort` can take an optional relational expression instead of a static value to define a port number relative to the base HTTPS port number used by the client.

If the port mapping device uses port number 1000 for HTTPS, mapped to TCP 443; port number 1001 for RDP, mapped to TCP 3389; port number 1002 for PCoIP, mapped to TCP and UDP 4172; and port number 1003 for the framework channel, mapped to TCP 32111, to simplify configuration, the external port numbers can be configured to be `externalRDPPort`=+1, `externalPCoIPPort`=+2 and `externalFrameworkChannelPort`=+3. When the HTTPS connection comes in from a client that used an HTTPS destination port number of 1000, the external port numbers would automatically be calculated relative to this port number of 1000 and would use 1001, 1002 and 1003 respectively.

To deploy another virtual desktop, if the port mapping device used port number 1005 for HTTPS, mapped to TCP 443; port number 1006 for RDP, mapped to TCP 3389; port number 1007 for PCoIP, mapped to TCP and UDP 4172; and port number 1008 for the framework channel, mapped to TCP 32111, with exactly the same external port configuration on the desktop (+1, +2, +3, and so on) when the HTTPS connection comes in from a client that used an HTTPS destination port number of 1005, the external port numbers would automatically be calculated relative to this port number of 1005 and use 1006, 1007, and 1008 respectively.

This scheme allows all View desktops to be identically configured and yet all share the same external IP address. Allocating port numbers in increments of five (1000, 1005, 1010 …) for the base HTTPS port number would therefore allow over 12,000 virtual desktops to be accessed on the same IP address. and using the base port number to determine the virtual desktop to route the connection to, based on the port mapping device configuration. For an `externalIPAddress`=10.20.30.40, `externalRDPPort`=+1, `externalPCoIPPort`=+2 and `externalFrameworkChannelPort`=+3 configured on all virtual desktops, the mapping to virtual desktops would be as described in the NAT and port mapping table.

Table 2-3. NAT and Port Mapping Values

VM#	Desktop IP Address	HTTPS	RDP	PCOIP (TCP and UDP)	Framework Channel
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 would connect to IP address 10.20.30.40 and an HTTPS destination port number of (1000 + *n* * 5) where *n* is the View desktop number. To connect to View desktop 3, the client would connect to 10.20.30.40:1015. This addressing scheme significantly simplifies the configuration setup for each View desktop. All desktops are configured with identical external address and port configurations. The NAT and port mapping configuration is done within the NAT and port mapping device with this consistent pattern, and all View desktops can be accessed on a single public IP address. The client would typically use a single public DNS name that resolves to this IP address.

Troubleshooting the VMware Horizon View Agent Direct-Connection Plugin 3

When using the Horizon View Agent Direct-Connection Plugin, you might encounter some known issues and have to troubleshoot them.

When you investigate a problem with the Horizon View Agent Direct-Connection Plugin, make sure that the correct version is installed and running. In the example above, the plugin version details are `version=e.x.p build-855808, buildtype=release`. The plugin name VMware View Agent XML API Handler Plugin is logged.

If a support issue needs to be raised with VMware, always enable full logging, reproduce the problem, and generate a Data Collection Tool (DCT) log set. VMware technical support can then analyze these logs. For details on generating a DCT log set, refer to Collecting diagnostic information for VMware View KB article http://kb.vmware.com/kb/1017939.

Enabling Full Logging to Include TRACE and DEBUG information

The Horizon View Agent Direct-Connection plugin writes log entries to the standard View Agent log. TRACE and DEBUG information is not included in the log by default.

Problem

The Horizon View Agent Direct-Connection Plugin writes log entries to the standard View Agent log. TRACE and DEBUG information is not included in the standard View Agent logs by default.

Cause

Full logging is not enabled. You must enable full logging to include TRACE and DEBUG information in the View Agent logs.

Solution

1 Open a command prompt and run `C:\Program Files\VMware\VMware View\Agent\DCT\support.bat loglevels`

2 Enter **3** for full logging.

The debug log files are located in `%ALLUSERSPROFILE%\VMware\VDM\logs`. The file `debug*.log` has information logged from the View Agent and the plugin. Search for `wsnm_xmlapi` to find the plugin log lines.

When the View Agent is started, the plugin version is logged:

```
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
```

Insufficient Video RAM Configured for the Virtual Machine

The correct amount of Video RAM must be configured for the virtual machine.

Problem

A black screen is displayed when using PCoIP.

Cause

An insufficient of video RAM such as 16MB or 32MB was configured for the virtual machine.

Solution

- Configure at least 128MB of video RAM for each virtual machine.

Incorrect Graphics Driver is Installed

The correct version of the Horizon View Agent graphics driver must be installed. The graphics driver might have been downgraded after Horizon View Agent was installed. This might happen if an incorrect version of VMware Tools is installed after Horizon View Agent.

Problem

A black screen is displayed when using PCoIP due to a downgraded graphics driver.

Cause

The incorrect version of graphics driver was installed.

Solution

- Reinstall Horizon View Agent.

Index