View Agent Direct-Connection Plug-In Administration

VMware Horizon 2106

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

https://docs.vmware.com/

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

Contents

View Agent Direct-Connection Plug-In Administration

View Agent Direct-Connection Plugin Administration provides information about installing and configuring View Agent Direct-Connection Plugin. This plug-in is an installable extension to Horizon Agent that allows Horizon Client to directly connect to a virtual machine-based desktop, a published desktop, or an application without using Horizon Connection Server. All the desktop and application features work in the same way as when the user connects through Connection Server.

Intended Audience

This information is intended for an administrator who wants to install, upgrade or configure View Agent Direct-Connection Plug-In in a virtual machine-based desktop or an RDS host. This guide is written for experienced Windows system administrators who are familiar with virtual machine technology and datacenter operations.

Installing View Agent Direct-Connection Plug-In

1

View Agent Direct-Connection (VADC) Plug-In enables Horizon Clients to directly connect to virtual machine-based desktops, published desktops, or applications. VADC Plug-In is an extension to Horizon Agent and is installed on virtual machine-based desktops or RDS hosts.

This chapter includes the following topics:

View Agent Direct-Connection Plug-In System Requirements

View Agent Direct-Connection (VADC) Plug-In is installed on machines where Horizon Agent is already installed. For a list of operating systems that Horizon Agent supports, see "Supported Operating Systems for Horizon Agent" in the *Horizon Installation* document.

VADC Plug-In has the following additional requirements:

- The virtual or physical machine that has VADC Plug-In installed must have a minimum of 128 MB of video RAM to function properly.
- For a virtual machine, you must install VMware Tools before you install Horizon Agent.
- A physical machine supports Windows 10 Enterprise version 1803 or version 1809.

VADC Plug-In support protocol is as follows:

- A virtual machine that has VADC Plug-In installed supports Blast and PCoIP protocols.
- A physical machine that has VADC Plug-In installed supports Blast protocol only.

Note A virtual machine-based desktop that supports VADC can be joined to a Microsoft Active Directory domain, or it can be a member of a workgroup.

Install View Agent Direct-Connection Plug-In

View Agent Direct-Connection (VADC) Plug-In is packaged in a Windows Installer file that you can download from the VMware Web site and install.

Prerequisites

- Verify that Horizon Agent is installed. If your environment does not include Connection Server, install Horizon Agent from the command line and specify a parameter that tells Horizon Agent not to register with Connection Server. See Install Horizon Agent for HTML Access.
- Enable the screen DMA setting for virtual machines on vSphere 6.0 and later. If screen DMA is disabled, users see a black screen when they connect to the remote desktop. For more information on how to set the screen DMA, see the VMware Knowledge Base (KB) article 2144475 http://kb.vmware.com/kb/2144475.

Procedure

1. Download the VADC Plug-In installer file from the VMware download page at http://www.vmware.com/go/downloadview.

   The installer filename is VMware-viewagent-direct-connection-x86_64-y.y.y-xxxxxx.exe for 64-bit Windows or VMware-viewagent-direct-connection--y.y.y-xxxxxx.exe for 32-bit Windows, where y.y.y is the version number and xxxxxx is the build number.
2. Double-click the installer file.
3. (Optional) Change the TCP port number.

   The default port number is 443.
4. (Optional) Choose how to configure the Windows Firewall service.

   By default, **Configure Windows Firewall automatically** is selected and the installer configures Windows Firewall to allow the required network connections.
5. (Optional) Choose whether to disable SSL 3.0.

   By default, **Disable support for SSLv3 automatically (recommended)** is selected and the installer disables SSL 3.0 at the operating system level. This option is not displayed and the installer performs no action if SSL 3.0 is already explicitly enabled or disabled in the registry. If this option is deselected, the installer also performs no action.
6. Follow the prompts and finish the installation.

Install View Agent Direct-Connection Plug-In Silently

You can use the silent installation feature of Microsoft Windows Installer (MSI) to install View Agent Direct-Connection (VADC) Plug-In. In a silent installation, you use the command line and do not have to respond to wizard prompts.

With silent installation, you can efficiently deploy VADC Plug-In in a large enterprise. For more information on Windows Installer, see "Microsoft Windows Installer Command-Line Options" in the *Setting Up Virtual Desktops in Horizon* document. VADC Plug-In supports the following MSI properties.

Table 1-1. MSI Properties for the Silent Installation of View Agent Direct-Connection Plug-In

MSI Property	Description	Default Value
LISTENPORT	The TCP port that VADC Plug-In uses to accept remote connections. By default, the installer will configure Windows Firewall to allow traffic on the port.	443
MODIFYFIREWALL	If set to 1, the installer will configure Windows Firewall to allow traffic on LISTENPORT. If set to 0, the installer will not.	1
DISABLE_SSLV3	If SSL 3.0 is already explicitly enabled or disabled in the registry, the installer ignores this property. Otherwise, the installer disables SSL 3.0 at the operating system level if this property is set to 1, and the installer performs no action if this property is set to 0.	1

Prerequisites

- Verify that Horizon Agent is installed. If your environment does not include Connection Server, install Horizon Agent from the command line and specify a parameter that tells Horizon Agent not to register with Connection Server. See Install Horizon Agent for HTML Access.

Procedure

1. Open a Windows command prompt.
2. Run the VADC Plug-In installer file with command-line options to specify a silent installation. You can optionally specify additional MSI properties.

   The following example installs VADC Plug-In with default options.

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

   The following example installs VADC Plug-In and specifies a TCP port that vadc will listen to for remote connections.

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

View Agent Direct-Connection Plug-In Advanced Configuration

2

You can use the default View Direct-Connection Plug-In configuration settings or customize them through Windows Active Directory group policy objects (GPOs) or by modifying specific Windows registry settings.

This chapter includes the following topics:

View Agent Direct-Connection Plug-In Configuration Settings

The VMware View Agent Configuration ADMX template file (`view_agent_direct_connection.admx`) contains policy settings related to View Agent Direct-Connection Plug-In.

The View Agent Direct-Connection Configuration settings are in the Group Policy Management Editor in **Computer Configuration > Administrative Templates > VMware View Agent Configuration > View Agent Direct-Connection Configuration**.

Table 2-1. View Agent Direct-Connection Plug-In Configuration Settings

Setting	Description
Applications Enabled	This setting supports application launch on remote desktop session hosts. The default setting is enabled.
Client Config Name Value Pairs	List of values to be passed to the client in the form name=value. Example: clientCredentialCacheTimeout=1440.
Client Session Timeout	The maximum length of time in seconds that session is kept active if a client is not connected. The default is 36000 seconds (10 hours).

Table 2-1. View Agent Direct-Connection Plug-In Configuration Settings (continued)

Setting	Description
Client setting: AlwaysConnect	The value can be set to TRUE or FALSE. AlwaysConnect setting is sent to Horizon 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.
Client setting: AutoConnect	This setting overrides any saved Horizon Client preferences. No value is set by default. Enabling this policy will set the value to true, disabling this policy will set the value to false.
Client setting: ScreenSize	ScreenSize setting sent to Horizon Client. If enabled, it overrides any saved client preferences. If not configured or disabled, the client preferences are used.
Multimedia redirection (MMR) Enabled	Determines whether MMR is enabled for client systems. MMR is a Microsoft DirectShow filter that forwards multimedia data from specific codecs on Horizon desktops directly through a TCP socket to the client system. The data is then decoded directly on the client system, where it is played. The default value is disabled. MMR does not work correctly if the client system's video display hardware does not have overlay support. Client systems may have insufficient resources to handle local multimedia decoding.
Reset Enabled	The value can be set to TRUE or FALSE. When set to TRUE, an authenticated Horizon Client can perform an operating system level reboot. The default setting is disabled (FALSE).
Session Timeout	The period of time a user can keep a session open after logging in with Horizon Client. The value is set in minutes. The default is 600 minutes. When this timeout is reached, all of a user's desktop and applications sessions are disconnected.
USB AutoConnect	The value can be 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.
USB Enabled	The value can be 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).
User Idle Timeout	If there is no user activity on the Horizon client for this period of time, the user's desktop and application sessions are disconnected. The value is set in seconds. The default is 900 seconds (15 minutes).

Authentication Settings

The Authentication settings are in the Group Policy Management Editor in **Computer Configuration > Administrative Templates > VMware View Agent Configuration > View Agent Direct-Connection Configuration**. Within this folder is the Log On As Current User settings.

Table 2-2. View Agent Direct-Connection Plug-In Authentication Settings

Setting	Description
Allow Legacy Clients	When disabled, Horizon Client versions older than 5.5 will not authenticate using the Log in as current user feature. If this setting is not configured, older clients are supported.
Allow NTLM Fallback	When enabled, Horizon Client uses NTLM authentication instead of Kerberos when there is no access to the domain controller. If this setting is not configured, NTLM fallback is not allowed.
Require Channel Bindings	When enabled, channel bindings provide an additional security layer to secure NTLM authentication. Horizon Client versions older than 5.5 do not support channel bindings.
Client Credential Cache Timeout	The time period, in minutes, that a Horizon Client allows a user to use a saved password. 0 means never, and -1 means forever. Horizon Client offers users the option of saving their passwords if this setting is set to a valid value. The default is 0 (never).
Disclaimer Enabled	The value can be 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	The disclaimer text shown to Horizon Client users at login. 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`.
X509 Certificate Authentication	Determines if Smart Card X.509 certificate authentication is disabled, allowed, or required.
X509 SSL Certificate Authentication Enabled	Determines if Smart Card X.509 certificate authentication is enabled by a direct SSL connection from a Horizon Client. This option is not required if X.509 certificate authentication is handled via an intermediate SSL termination point. Changing this setting requires a restart of the Horizon Agent.

Protocol and Network Settings

The Protocol and Network settings are in the Group Policy Management Editor in **Computer Configuration > Administrative Templates > VMware View Agent Configuration > View Agent Direct-Connection Configuration**.

Table 2-3. View Agent Direct-Connection Plug-In Configuration Settings

Setting	Description
Default Protocol	The default display protocol used by Horizon Client to connect to the desktop. If the value is not set, then the default value is BLAST.
External Blast Port	The port number sent to Horizon 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.

Table 2-3. View Agent Direct-Connection Plug-In Configuration Settings (continued)

Setting	Description
External Framework Channel Port	The port number sent to the Horizon 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.
External IP Address	The IPV4 address sent to Horizon 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.
External PCoIP Port	The port number sent to Horizon 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 RDP Port	The port number sent to Horizon 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.
HTTPS Port Number	The TCP port on which the plug-in listens for incoming HTTPS requests from Horizon Client. If this value is changed, you must make a corresponding change to the Windows firewall to allow incoming traffic. The default is 443.

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.

For smart card authentication, the certificate authority (CA) that signs the smart card certificates must be in the Windows certificate Store. For information about how to add a certificate authority, see Add a Certificate Authority to the Windows Certificate Store.

Note If a user attempts to log in using a smart card to a Windows 7 or Windows Server 2008 R2 machine and the Smart Card certificate has been signed by an intermediate CA, the attempt may fail because Windows can send the client a trusted issuer list that does not contain intermediate CA names. If this happens, the client will be unable to select an appropriate Smart Card certificate. To avoid this problem, set the registry value `SendTrustedIssuerList` (REG_DWORD) to 0 in the registry key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL`. With this registry value set to 0, Windows does not send a trusted issuer list to the client, which can then select all the valid certificates from the smart card.

Disabling Weak Ciphers in SSL/TLS

To achieve greater security, you can configure the domain policy GPO (group policy object) to ensure that communications that use the SSL/TLS protocol between Horizon Clients and virtual machine-based desktops or RDS hosts do not allow weak ciphers.

Procedure

1. On the Active Directory server, edit the GPO by selecting **Start > Administrative Tools > Group Policy Management**, right-clicking the GPO, and selecting **Edit**.
2. In the Group Policy Management Editor, navigate to the **Computer Configuration > Policies > Administrative Templates > Network > SSL Configuration Settings**.
3. Double-click **SSL Cipher Suite Order**.
4. In the SSL Cipher Suite Order window, click **Enabled**.
5. In the Options pane, replace the entire content of the SSL Cipher Suites text box with the following cipher list:

   ```
   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
   ```

   The cipher suites are listed above on separate lines for readability. When you paste the list into the text box, the cipher suites must be on one line with no spaces after the commas.
6. Exit the Group Policy Management Editor.
7. Restart the VADC machines for the new group policy to take effect.

Results

Note If Horizon Client is not configured to support any cipher that is supported by the virtual desktop operating system, the TLS/SSL negotiation will fail and the client will be unable to connect.

For information on configuring supported cipher suites in Horizon Clients, refer to Horizon Client documentation at https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Replacing the Default Self-Signed TLS Server Certificate

A self-signed TLS server certificate cannot give Horizon 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 Plug-In starts for the first time after installation, it automatically generates a self-signed TLS server certificate and places it in the Windows Certificate Store. The TLS server certificate is presented to Horizon Client during the TLS protocol negotiation to provide information to the client about this desktop. This default self-signed TLS 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 Horizon 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 Connection Server. See "Configuring TLS Certificates for Horizon Servers," in the *Horizon 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 TLS Server Certificates to a large number of desktops using the View Agent Direct-Connection Plug-In, use Active Directory Enrollment to distribute the certificates to each virtual machine.

Authorizing Horizon Client to Access Desktops and Applications

The authorization mechanism that allows a user to access desktops and applications 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 virtual machine-based desktop, published desktop, or published applications. When the plug-in is first installed, this local group is created and contains the Authenticated Users group. Anyone who is successfully authenticated by the plug-in is authorized to access the desktop or applications.

To restrict access to this desktop or RDS host, 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 user is not in this group, the user gets a message after authentication saying that the user is not entitled to access this virtual machine-based desktop or the published desktop and applications that are hosted on this RDS host.

Using Network Address Translation and Port Mapping

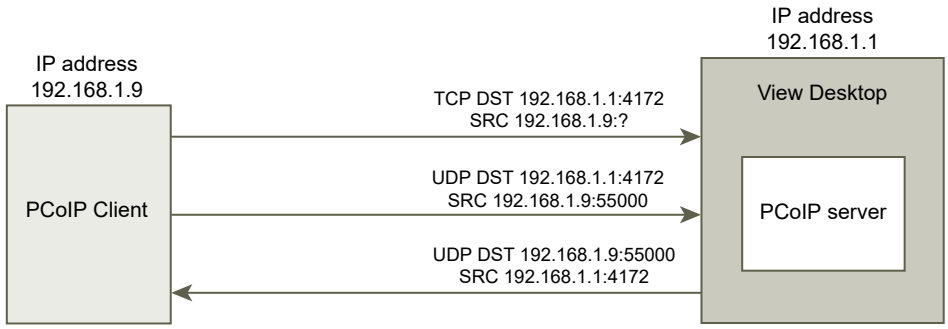
Network Address Translation (NAT) and port mapping configuration are required if Horizon Clients connect to virtual machine-based desktops on different networks.

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

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

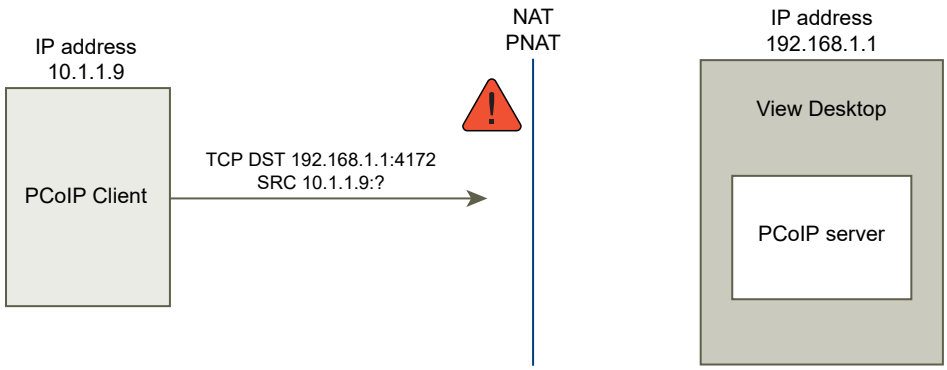
An example deployment of a desktop whose IP address is 192.168.1.1 illustrates the configuration of NAT and port mapping. A Horizon Client system with an IP address of 192.168.1.9 on the same network establishes a PCoIP connection by using TCP and UDP. This connection is direct without any NAT or port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

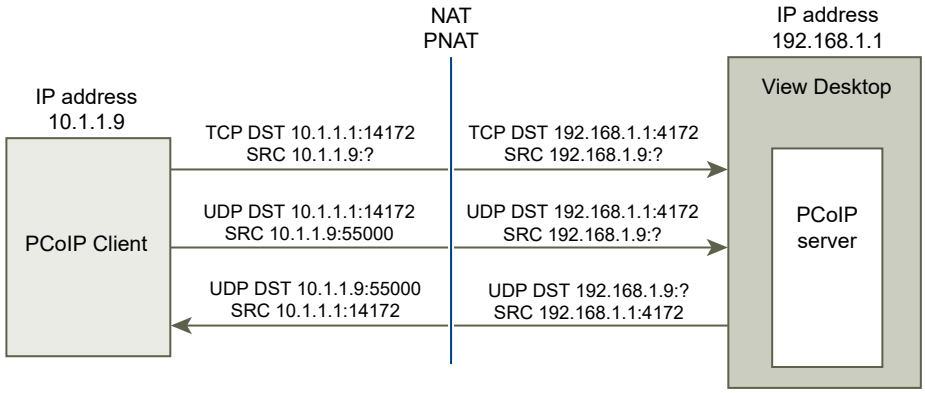


To resolve this problem, you must configure the plug-in to use an external IP address. If `externalIPAddress` is configured as 10.1.1.1 for this desktop, the plug-in gives the client an IP address of 10.1.1.1 when making desktop protocol connections to the desktop. For PCoIP, the PCoIP Secure Gateway 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 plug-in 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 `externalPCoIPPort`in the plug-in to 14172.

In a configuration which uses NAT and port mapping, 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 virtual machine-based desktops to be accessible through a NAT and port mapping device on the same external IP address, you must give each 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.

For 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 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 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. The base port number is used 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 2-4. 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

In this example, Horizon Client connects to IP address 10.20.30.40 and an HTTPS destination port number of (1000 + *n* * 5) where *n* is the desktop number. To connect to desktop 3, the client would connect to 10.20.30.40:1015. This addressing scheme significantly simplifies the configuration setup for each 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 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.

Add a Certificate Authority to the Windows Certificate Store

For smart card authentication, the certificate authority (CA) that signs the smart card certificate must exist in the Windows certificate store. If not, you can add the CA to the Windows certificate store.

Prerequisites

Verify that Microsoft Management Console (MMC) has the Certificates snap-in. See "Add the Certificate Snap-In to MMC" in the *Horizon Installation* document.

Procedure

1. Start MMC.
2. In the MMC console, expand the **Certificates (Local Computer)** node and go to the **Trusted Root Certification Authorities > Certificates** folder.

   If the root certificate is present and there are no intermediate certificates in the certificate chain, exit MMC.
3. Right-click the **Trusted Root Certification Authorities > Certificates** folder and click **All Tasks > Import**.
4. In the **Certificate Import** wizard, click **Next** and browse to the location where the root CA certificate is stored.
5. Select the root CA certificate file and click **Open**.
6. Click **Next**, click **Next**, and click **Finish**.
7. If the smart card certificate is issued by an intermediate CA, import all intermediate certificates in the certificate chain.
   a. Go to the **Certificates (Local Computer) > Intermediate Certification Authorities > Certificates** folder.
   b. Repeat steps 3 through 6 for each intermediate certificate.

Setting Up HTML Access

3

View Agent Direct-Connection (VADC) Plug-In supports HTML Access to virtual machine-based desktops and published desktops and applications.

This chapter includes the following topics:

Install Horizon Agent for HTML Access

To support HTML Access, you must install Horizon Agent on the virtual machine-based desktop with a special parameter.

Prerequisites

- Download the Horizon Agent installer file from the VMware download page at http://www.vmware.com/go/downloadview.

  The installer filename is `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe`, where *YYMM* is the marketing version number, *y.y.y* is the internal version number, and *xxxxxx* is the build number.

Procedure

- Install Horizon Agent from the command line and specify a parameter that tells Horizon Agent not to register with Connection Server.

  This example installs Horizon Agent.

  ```
  VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /v VDM_SKIP_BROKER_REGISTRATION=1
  ```

What to do next

Install View Agent Direct-Connection Plug-In. See Install View Agent Direct-Connection Plug-In.

Set Up Static Content Delivery

If the HTML Access client needs to be served by the desktop, you must perform some setup tasks on the desktop. This enables a user to point a browser directly at a desktop.

Prerequisites

- Download the Horizon HTML Access `portal.war` zip file from the VMware download page at http://www.vmware.com/go/downloadview.

  The filename is `VMware-Horizon-View-HTML-Access-`*`y.y.y`*`-`*`xxxxxx`*`.zip`, where *y.y.y* is the version number and *xxxxxx* is the build number.

Procedure

1. Open **Control Panel**.
2. Navigate to **Programs and Features > Turn Windows features on or off**.
3. Select the check box **Internet Information Services** and click **OK**.
4. In **Control Panel**, navigate to **Administrative Tools > Internet Information Services (IIS) Manager**.
5. Expand the items in the left pane.
6. Right-click **Default Web Site** and select **Edit Bindings...**.
7. Click **Add**.
8. Specify **https**, **All Unassigned**, and port **443**.
9. In the **SSL certificate** field, select the correct certificate.

Option	Action
Certificate **vdm** is present.	Select **vdm** and click **OK**.
Certificate **vdm** is not present.	Select **vdmdefault** and click **OK**.

10. In the **Site Bindings** dialog, remove the entry for **http port 80** and click **Close**.
11. Click **Default Web Site**.
12. Double-click **MIME Types**.
13. If the **File name extension** .json does not exist, in the **Actions** pane, click **Add...**. Otherwise, skip the next 2 steps.
14. For **File name extension**, enter **.json**.
15. For **MIME type**, enter **text/h323** and click **OK**.
16. For **File name extension**, enter **.mem**.
17. For **MIME type**, enter **text/plain** and click **OK**.

18 Copy `VMware-Horizon-View-HTML-Access-y.y.y-xxxxxx.zip` to a temporary folder.

19 Unzip `VMware-Horizon-View-HTML-Access-y.y.y-xxxxxx.zip`.

The result is a file named `portal.war`.

20 Rename `portal.war` to `portal.zip`.

21 Unzip `portal.zip` to the folder `C:\inetpub\wwwroot`.

If necessary, adjust the permissions on the folder to allow files to be added.

The folder `C:\inetpub\wwwroot\portal` is created.

22 Open **Notepad**.

23 Create the file `C:\inetpub\wwwroot\Default.htm` with the following content (replace *<IP address or DNS name of desktop>* with the actual IP address or DNS name of the desktop):

```
<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>
```

Set Up Trusted CA-Signed TLS Server Certificate

You can set up trusted CA-Signed TLS server certificate to ensure that traffic between clients and desktops is not fraudulent.

Prerequisites

- Replace the default self-signed TLS server certificate with a trusted CA-signed TLS server certificate. See Replacing the Default Self-Signed TLS Server Certificate. This creates a certificate that has the Friendly Name value **vdm**.
- If the client's static content is served by the desktop, set up static content delivery. See Set Up Static Content Delivery.
- Familiarize yourself with the Windows Certificate Store. See "Configure Connection Server to Use a New TLS Certificate" in the *Horizon Installation* document.

Procedure

1 In the Windows Certificate Store, navigate to **Personal > Certificates**.

2 Double-click the certificate with Friendly Name **vdm**.

3 Click on the **Details** tab.

4 Copy the **Thumbprint** value.

5 Start the Windows Registry Editor.

6 Navigate to the registry key `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast \Config`.

7 Add a new String (REG_SZ) value, `SSLHash`, to this registry key.

8 Set the `SSLHash` value to the **Thumbprint** value.

Disable HTTP/2 Protocol on Windows 10 and Windows 2016 Desktops

With some web browsers, you might encounter the error ERR_SPDY_PROTOCOL_ERROR when accessing a Windows 10 VADC or Windows 2016 VADC desktop. You can prevent this error by disabling the HTTP/2 protocol on the desktop.

Procedure

1 Start the Windows Registry Editor.

2 Navigate to the registry key `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services \HTTP\Parameters`.

3 Add 2 new REG_DWORD values, `EnableHttp2Tls` and `EnableHttp2Cleartext`, to this registry key.

4 Set both values to **0**.

5 Reboot the desktop.

Setting Up View Agent Direct-Connection on Remote Desktop Services Hosts

4

Horizon supports Remote Desktop Services (RDS) hosts that provide published desktops and applications that users can access from Horizon Client. A published desktop is based on a desktop session to an RDS host. In a typical Horizon deployment, clients connect to desktops and applications through Horizon Connection Server. However, if you install View Agent Direct-Connection Plug-In on an RDS host, clients can connect directly to published desktops or applications without using Connection Server.

This chapter includes the following topics:

Remote Desktop Services Hosts

A Remote Desktop Services (RDS) host is a server computer that hosts applications and desktops for remote access.

In a Horizon deployment, an RDS host is a Windows server that has the Microsoft Remote Desktop Services role, the Microsoft Remote Desktop Session Host service, and Horizon Agent installed. An RDS host can support View Agent Direct-Connection (VADC) if it also has VADC Plug-In installed. For information on setting up an RDS host and installing Horizon Agent, see "Setting Up Remote Desktop Services Hosts" in the *Setting Up Published Desktops and Applications in Horizon* document. For information on installing VADC Plug-In, see Chapter 1 Installing View Agent Direct-Connection Plug-In.

Note When you install Horizon Agent, the installer asks for the hostname or IP address of Connection Server that Horizon Agent will connect to. You can make the installer skip this step by running the installer with a parameter.

```
VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /v "VDM_SKIP_BROKER_REGISTRATION=1"
```

After you set up an RDS host and install VADC Plug-In, you must entitle RDS desktops and applications. See Entitle Published Desktops and Applications.

Entitle Published Desktops and Applications

You must entitle users to published desktops and applications before the users can access the desktops and applications.

If the RDS host is running Windows Server 2012 R2, run **Server Manager** and navigate to **Remote Desktop Services** to configure entitlements.

Desktop Entitlements

To entitle a user to launch a published desktop, perform the following steps:

- Ensure that the user is a member of the local group **View Agent Direct-Connection Users**. By default, all authenticated users are a members of this group.
- For Windows 2012 R2, run **Server Manager** and navigate to **Remote Desktop Services** to configure entitlements. Use the Quick Start wizard to deploy RDSH services.

Application Entitlements

To entitle a user to launch an application, perform the following steps:

- Ensure that the user is a member of the local group **View Agent Direct-Connection Users**. By default, all authenticated users are a members of this group.
- For Windows 2012 R2, run **Server Manager** and navigate to **Remote Desktop Services** to configure entitlements.

Troubleshooting View Agent Direct-Connection Plug-In

5

When using View Agent Direct-Connection Plug-In, you might encounter known issues.

When you investigate a problem with View Agent Direct-Connection Plug-In, make sure that the correct version is installed and running.

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 Knowledge Base (KB) article http://kb.vmware.com/kb/1017939.

This chapter includes the following topics:

Incorrect Graphics Driver is Installed

For PCoIP to work properly, the correct version of the graphics driver must be installed.

Problem

A black screen is displayed when a user connects to a desktop or an application using PCoIP.

Cause

An incorrect version of the graphics driver is running. This could happen if an incorrect version of VMware Tools is installed after the installation of Horizon Agent.

Solution

- Reinstall Horizon Agent.

Insufficient Video RAM

To support PCoIP, a virtual machine that runs a desktop or an RDS host must have a minimum of 128 MB of video RAM.

Problem

A black screen is displayed when a user connects to a desktop or an application using PCoIP.

Cause

The virtual machine does not have enough video RAM.

Solution

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

Enabling Full Logging to Include TRACE and DEBUG information

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

Problem

The Horizon Agent log does not contain TRACE and DEBUG information.

Cause

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

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 Horizon Agent and the plug-in. Search for `wsnm_xmlapi` to find the plug-in log lines.

   When the Horizon Agent is started, the plug-in 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
   ```