Administración del complemento View Agent Direct-Connection

VMware Horizon 7 7.2

vmware®

Puede encontrar la documentación técnica más actualizada en el sitio web de WMware en:

https://docs.vmware.com/es/

En el sitio web de VMware también están disponibles las últimas actualizaciones del producto.

Si tiene algún comentario sobre esta documentación, envíelo a la siguiente dirección de correo electrónico:

docfeedback@vmware.com

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

VMware, Inc.
Paseo de la Castellana 141. Planta 8.
28046 Madrid.
Tel.:+ 34 91 418 58 01
Fax: + 34 91 418 50 55
www.vmware.com/es

Contenido

Administración del complemento View Agent Direct-Connection

La guía *Administración del complemento View Agent Direct-Connection* proporciona información sobre la instalación y la configuración del complemento View Agent Direct-Connection. Este complemento es una extensión que se puede instalar de View Agent que permite a Horizon Client conectarse directamente a un escritorio basado en máquina virtual, a un escritorio de los Servicios de Escritorio remoto (RDS) o a una aplicación sin usar el servidor de conexión de View. Todas las funciones de las aplicaciones y de los escritorios siguen funcionando del mismo modo que cuando el usuario se conecta a través del servidor de conexión de View.

Público al que se dirige

Esta información se dirige a un administrador que desee instalar, actualizar o configurar el complemento View Agent Direct-Connection en un escritorio basado en máquina virtual o un host RDS. Asimismo, está destinada a administradores de sistemas Windows con experiencia que estén familiarizados con la tecnología de las máquinas virtuales y las operaciones de los centros de datos.

Instalar el complemento View Agent Direct-Connection 1

El complemento View Agent Direct-Connection (VADC) habilita instancias de Horizon Client para que se conecten directamente a escritorios basados en máquinas virtuales, escritorios RDS o aplicaciones. El complemento VADC es una extensión de View Agent y se instala en escritorios basados en máquinas virtuales o hosts RDS.

Este capítulo cubre los siguientes temas:

Requisitos del sistema del complemento View Agent Direct-Connection

El complemento View Agent Direct-Connection (VADC) se instala en equipos donde View Agent ya está instalado. Para ver una lista de los sistemas operativos compatibles con View Agent, consulte el artículo sobre los sistemas operativos compatibles con View Agent en el documento *Instalación de View*.

El complemento VADC tiene los siguientes requisitos adicionales:

- La máquina virtual o el equipo físico que tengan instalado el complemento VADC deben tener un mínimo de 128 MB de RAM de vídeo para que PCoIP funcione correctamente.
- En una máquina virtual, debe instalar VMware Tools antes de instalar View Agent.
- Un equipo físico debe tener una tarjeta de host Teradici. No es necesario instalar VMware Tools.

NOTA: Un escritorio basado en una máquina virtual que admita VADC puede conectarse a un dominio de Microsoft Active Directory o puede ser miembro de un grupo de trabajo.

Instalar el complemento View Agent Direct-Connection

El complemento View Agent Direct-Connection (VADC) se encuentra en un paquete de un archivo de Windows Installer que puede descargar desde el sitio web de VMware e instalarlo.

Prerequisitos

- Compruebe que View Agent esté instalado. Si su entorno no incluye el servidor de conexión de View, instale View Agent desde la línea de comando y especifique un parámetro para que View Agent no se registre con el servidor de conexión de View. Consulte "Instale View Agent para HTML Access," página 21.

- Habilite la opción DMA de la pantalla para las máquinas virtuales en vSphere 6.0 y versiones posteriores. Si la DMA de la pantalla está deshabilitada, los usuarios verán una pantalla negra al conectarse al escritorio remoto. Para obtener más información sobre cómo establecer la DMA de la pantalla, consulte el artículo 2144475 de la base de conocimientos (KB) de VMware http://kb.vmware.com/kb/2144475.

Procedimiento

1 Descargue el archivo de instalación del complemento VADC desde el sitio de descargas de VMware disponible en http://www.vmware.com/go/downloadview.

   El nombre del archivo de instalación es VMware-viewagent-direct-connection-x86_64-y.y.y-xxxxxx.exe para Windows de 64 bits o VMware-viewagent-direct-connection--y.y.y-xxxxxx.exe para Windows de 32 bits, donde y.y.y es el número de la versión y xxxxxx es el número de compilación.

2 Haga doble clic en el archivo de instalación.

3 (Opcional) Cambie el número de puerto TCP.

   El puerto predeterminado es el 443.

4 (Opcional) Elija cómo configurar el servicio del Firewall de Windows.

   De forma predeterminada, la opción **Configurar el Firewall de Windows automáticamente** está seleccionada y el instalador configura el firewall para permitir las conexiones de red necesarias.

5 (Opcional) Seleccione si desea deshabilitar SSL 3.0.

   De forma predeterminada, la opción **Deshabilitar la compatibilidad con SSLv3 automáticamente (recomendado)** está seleccionada y el instalador deshabilita SSL 3.0 en el nivel de sistema operativo. Esta opción no se muestra y el instalador no realiza ninguna acción si SSL 3.0 ya aparece habilitado o deshabilitado explícitamente en el registro. Si esta opción no está seleccionada, el instalador tampoco realiza ninguna acción.

6 Siga los pasos que se le indican y finalice la instalación.

Instalar silenciosamente el complemento View Agent Direct-Connection

Puede usar la función de instalación silenciosa de Microsoft Windows Installer (MSI) para instalar el complemento View Agent Direct-Connection (VADC). En una instalación silenciosa, puede usar la línea de comando y no es necesario que responda a los mensajes del asistente.

La instalación silenciosa le permite implementar el complemento VADC correctamente en una empresa de gran tamaño. Para obtener más información sobre Windows Installer, consulte "Opciones de la línea de comando de Microsoft Windows Installer" en el documento *Configurar escritorios virtuales en Horizon 7*. El complemento VADC admite las siguientes propiedades MSI.

Tabla 1-1. Propiedades MSI de la instalación silenciosa del complemento View Agent Direct-Connection

Propiedad MSI	Descripción	Valor predeterminado
LISTENPORT	El puerto TCP que el complemento VADC usa para aceptar las conexiones remotas. De forma predeterminada, el instalador configurará el Firewall de Windows para permitir el tráfico en el puerto.	443
MODIFYFIREWALL	Si está establecido en 1, el instalador configurará el Firewall de Windows para que permita el tráfico en LISTENPORT. Si está establecido en 0, el instalador no lo hará.	1
DISABLE_SSLV3	Si SSL 3.0 ya está explícitamente habilitado o deshabilitado en el registro, el instalador ignora esta propiedad. De lo contrario, el instalador deshabilita SSL 3.0 en el nivel de sistema operativo si esta propiedad está establecida en 1 y no realiza ninguna acción si lo está en 0.	1

Prerequisitos

- Compruebe que Horizon Agent esté instalado. Si su entorno no incluye el servidor de conexión de Horizon, instale Horizon Agent desde la línea de comandos y especifique un parámetro para que Horizon Agent no se registre con el servidor de conexión de Horizon. Consulte "Instale View Agent para HTML Access," página 21.

Procedimiento

1 Abra un símbolo de sistema de Windows.

2 Ejecute el archivo de instalación del complemento VADC con las opciones de la línea de comando para especificar una instalación silenciosa. De forma opcional, puede especificar propiedades MSI adicionales.

El siguiente ejemplo instala el complemento VADC con las opciones predeterminadas.

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

El siguiente ejemplo instala el complemento VADC y especifica un puerto TCP que VADC escuchará para las conexiones remotas.

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

Configuración avanzada del complemento View Agent Direct-Connection

2

Puede usar las opciones de configuración predeterminadas del complemento View Direct-Connection o personalizarlas con los Objetos de directivas de grupo (GPO) de Windows Active Directory o modificando la configuración específica del registro de Windows.

Este capítulo cubre los siguientes temas:

Opciones de configuración del complemento View Agent Direct-Connection

Todas las opciones de configuración del complemento View Agent Direct-Connection se almacenan en el registro local de cada host RDS o escritorio basado en máquina virtual. Puede administrar estas opciones con los objetos de directivas de grupo (GPO) de Active Directory, a través del editor de directivas locales o si modifica directamente el registro.

Los valores de registro se encuentran en la clave de registro de `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Agent\Configuration\XMLAPI`.

Tabla 2-1. Opciones de configuración del complemento View Agent Direct-Connection

Configuración	Valor de registro	Tipo	Descripción
Número de puerto HTTPS	httpsPortNumber	REG_SZ	El puerto TCP en el que el complemento escucha las solicitudes HTTPS entrantes desde Horizon Client. Si este valor cambia, debe realizar el cambio correspondiente en el firewall de Windows para permitir el tráfico entrante.
Tiempo de espera de la sesión	sessionTimeout	REG_SZ	Periodo de tiempo durante el que un usuario puede mantener una sesión abierta tras iniciar sesión con Horizon Client. Este valor se expresa en minutos. El valor predeterminado es 600 minutos. Cuando se llega a este tiempo de espera, todas las sesiones de las aplicaciones y los escritorios de los usuarios se desconectan.

Tabla 2-1. Opciones de configuración del complemento View Agent Direct-Connection (Continua)

Configuración	Valor de registro	Tipo	Descripción
Protocolo predeterminado	protocoloPredeterminado	REG_SZ	El protocolo de visualización predeterminado que usa Horizon Client para conectarse al escritorio. Si no se establece el valor, el valor predeterminado es BLAST.
Renuncia de responsabilidad habilitada	disclaimerEnabled	REG_SZ	El valor se puede establecer en `TRUE` o `FALSE`. Si se establece en `TRUE`, aparece un texto de renuncia de responsabilidad que el usuario debe aceptar al iniciar sesión. El texto se muestra en "Texto de renuncia de responsabilidad" si está escrito, o bien en el GPO `Configuration\Windows Settings\Security Settings\Local Policies\Security Options: Interactive logon`. El valor predeterminado de disclaimerEnabled es `FALSE`.
Texto de renuncia de responsabilidad	disclaimerText	REG_SZ	El texto de renuncia de responsabilidad que se muestra a los usuarios de Horizon Client al iniciar sesión. La directiva de renuncia de responsabilidad habilitada debe estar establecida en `TRUE`. Si no se especifica el texto, se usa el valor de la directiva de Windows de forma predeterminada `Configuration\Windows Settings\Security Settings\Local Policies\Security Options`.
Opción de cliente: AlwaysConnect	alwaysConnect	REG_SZ	El valor se puede establecer en `TRUE` o `FALSE`. La opción AlwaysConnect se envía a Horizon Client. Si esta directiva está establecida en `TRUE`, sobrescribe las preferencias de cliente guardadas. No se establece ningún valor de forma predeterminada. Al habilitar esta directiva, se establece el valor en `TRUE`. Al deshabilitar esta directiva, se establece el valor en `FALSE`.
Puerto PCoIP externo	externalPCoIPPort	REG_SZ	El número de puerto enviado a Horizon Client como número de puerto TCP/UDP de destino que se usa para el protocolo PCoIP. Un carácter + delante del número indica un número relativo al número de puerto que se utiliza para HTTPS. Establezca este valor solamente si el número de puerto externo de exposición no coincide con el puerto en el que el servicio está realizando la escucha. Normalmente, este número de puerto se encuentra en un entorno NAT. No se establece ningún valor de forma predeterminada.
Puerto Blast externo	externalBlastPort	REG_SZ	El número de puerto enviado a Horizon Client como número de puerto TCP de destino que se usa para el protocolo HTML5/Blast. Un carácter + delante del número indica un número relativo al número de puerto que se utiliza para HTTPS. Establezca este valor solamente si el número de puerto externo de exposición no coincide con el puerto en el que el servicio está realizando la escucha. Normalmente, este número de puerto se encuentra en un entorno NAT. No se establece ningún valor de forma predeterminada.

Tabla 2-1. Opciones de configuración del complemento View Agent Direct-Connection (Continua)

Configuración	Valor de registro	Tipo	Descripción
Puerto RDP externo	externalRDPPort	REG_SZ	El número de puerto enviado a Horizon Client como número de puerto TCP de destino que se usa para el protocolo RDP. Un carácter + delante del número indica un número relativo al número de puerto que se utiliza para HTTPS. Establezca este valor solamente si el número de puerto externo de exposición no coincide con el puerto en el que el servicio está realizando la escucha. Normalmente, este número de puerto se encuentra en un entorno NAT. No se establece ningún valor de forma predeterminada.
Dirección IP externa	externalIPAddress	REG_SZ	La dirección IPV4 enviada a Horizon Client como dirección IP de destino usada para protocolos secundarios (RDP, PCoIP, canal de marco de trabajo, etc). Establezca este valor solamente si la dirección externa de exposición no coincide con la dirección del equipo de escritorio. Normalmente, esta dirección se encuentra en un entorno NAT. No se establece ningún valor de forma predeterminada.
Puerto del canal de marco de trabajo externo	externalFrameworkChannelPort	REG_SZ	El número de puerto enviado a Horizon Client como número de puerto TCP de destino que se usa para el protocolo del canal del marco de trabajo. Un carácter + delante del número indica un número relativo al número de puerto que se utiliza para HTTPS. Establezca este valor solamente si el número de puerto externo de exposición no coincide con el puerto en el que el servicio realiza las tareas de escucha. Normalmente, este número de puerto se encuentra en un entorno NAT. No se establece ningún valor de forma predeterminada.
USB habilitado	usbEnabled	REG_SZ	El valor se puede establecer en `TRUE` o `FALSE`. Determina si los escritorios pueden usar los dispositivos USB conectados al sistema cliente. Está habilitada de forma predeterminada. Si desea evitar el uso de dispositivos externos por razones de seguridad, deshabilite la opción (`FALSE`).
Opción de cliente: conectar automáticamente el dispositivo USB	usbAutoConnect	REG_SZ	El valor se puede establecer en `TRUE` o `FALSE`. Cuando los dispositivos USB están conectados, también se conectan a los escritorios. Si esta directiva está establecida, sobrescribe las preferencias de cliente guardadas. No se establece ningún valor de forma predeterminada.
Restablecimiento habilitado	resetEnabled	REG_SZ	El valor se puede establecer en `TRUE` o `FALSE`. Cuando se establece en `TRUE`, un Horizon Client autenticado puede realizar un reinicio a nivel de sistema operativo. Esta opción aparece como deshabilitada de forma predeterminada (`FALSE`).
Tiempo de espera de la caché de las credenciales del cliente	clientCredentialCacheTimeout	REG_SZ	El periodo de tiempo, en minutos, durante el que un Horizon Client permite que un usuario utilice una contraseña guardada. 0 significa nunca y -1, siempre. Horizon Client ofrece a los usuarios la posibilidad de guardar las contraseñas si esta opción está configurada con un valor válido. El valor predeterminado es 0 (nunca).

Tabla 2-1. Opciones de configuración del complemento View Agent Direct-Connection (Continua)

Configuración	Valor de registro	Tipo	Descripción
Tiempo de espera inactivo del usuario	userIdleTimeout	REG_SZ	Si no hay actividad en Horizon Client durante este periodo de tiempo, las sesiones de las aplicaciones y los escritorios del usuario se desconectan. Este valor se expresa en segundos. El valor predeterminado es 900 segundos (15 minutos).
Compatibilidad con tarjetas inteligentes	x509CertAuth	REG_SZ	Indica la compatibilidad de la autenticación de tarjeta inteligente según los siguientes valores: ■ `0`: no permitido ■ `1`: opcional ■ `2`: obligatoria El valor predeterminado es `0`.
Origen del certificado de tarjeta inteligente	x509SSLCertAuth	REG_SZ	Indica que el certificado de tarjeta inteligente se obtiene desde la negociación SSL. El valor debe estar establecido en `TRUE` cuando `x509CertAuth` esté configurado como 1 o 2. El valor predeterminado es FALSE. Si desea cambiar esta opción, es necesario reiniciar el servicio de View Agent.
Pares de valores del nombre de la configuración cliente	BioMetricsTimeout	REG_SZ	Indica si la autenticación biométrica es compatible y, si es así, el periodo de tiempo durante el cual se puede usar. 0 significa que la autenticación biométrica no es compatible. -1 significa que es compatible sin ningún límite de tiempo. Un número positivo indica la cantidad de minutos durante los cuales se puede utilizar. El valor predeterminado es 0 (no compatible).

Los números de puertos externos y los valores de las direcciones IP externas se usan para la Traducción de direcciones de red (NAT) y la compatibilidad de asignación de puertos. Si desea obtener más información, consulte "Usar la Traducción de direcciones de red y la asignación de puertos," página 17.

Puede establecer directivas que reemplacen estas opciones de registro mediante el editor de directivas locales o los Objetos de directivas de grupo (GPO) de Active Directory. Las opciones de directivas tienen preferencia ante las opciones normales de registro. Se proporciona una plantilla de GPO para configurar las directivas. Cuando View Agent y el complemento están instalados en la ubicación predeterminada, el archivo de plantilla se encuentra en la siguiente ruta:

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

Puede importar este archivo de plantilla en Active Directory o en el editor de directivas de grupo local para simplificar la gestión de estas opciones de configuración. Consulte la documentación del editor de directivas de Microsoft y del GPO para obtener más información sobre la administración de la configuración de directivas. La configuración de las directivas del complemento se almacena en la clave de registro:

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

Para la autenticación de tarjeta inteligente, la entidad de certificación (CA) que firma los certificados debe aparecer en el almacén de certificados de Windows. Para obtener más información sobre cómo agregar una entidad de certificación, consulte "Agregar una entidad de certificación al almacén de certificados de Windows," página 19.

NOTA: Si un usuario intenta iniciar sesión con una tarjeta inteligente en equipos Windows 7 o Windows Server 2008 R2 y una CA intermedia firmó el certificado de tarjeta inteligente, este intento deriva en un error debido a que Windows puede enviar al cliente una lista de emisores de confianza que no contienen nombres de CA intermedias. Si esto sucede, es posible que el cliente no pueda seleccionar un certificado de tarjeta inteligente apropiado. Para evitar este problema, establezca el valor de registro `SendTrustedIssuerList` (REG_DWORD) en 0 en la clave de registro `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL`. Si este valor de registro está establecido en 0, Windows no envía una lista de emisores de confianza al cliente, que entonces puede seleccionar todos los certificados válidos de la tarjeta inteligente.

Deshabilitar cifrados débiles en SSL/TLS

Si desea que la seguridad sea mayor, puede configurar el GPO (objeto de directiva de grupo) de la directiva del dominio para garantizar que la comunicación que usa el protocolo SSL/TLS entre las instancias de Horizon Client y los escritorios basados en máquina virtual no permita cifrados débiles.

Procedimiento

1 En el servidor de Active Directory, para editar el GPO seleccionando, seleccione **Inicio > Herramientas administrativas > Administración de directivas de grupo**, haga clic en el GPO y seleccione **Editar**.

2 En el Editor de administración de directivas de grupo, diríjase a **Configuración del equipo > Directivas > Plantillas administrativas > Red > Opciones de configuración SSL**.

3 Haga doble clic en **Orden de conjuntos de cifrado SSL**.

4 En la ventana Orden de conjuntos de cifrado SSL, haga clic en **Habilitado**.

5 En el panel Opciones, reemplace todo el contenido del cuadro de texto Conjunto de claves de cifrado SSL por la siguiente lista de cifrado:

```
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
```

Los conjuntos de claves de cifrado aparecen en la parte superior en líneas separadas para que se puedan leer con facilidad. Cuando copie la lista en el cuadro de texto, los conjuntos de claves de cifrado deben estar en una línea y sin espacios después de las comas.

6 Salga del Editor de administración de directivas de grupo.

7 Reinicie los equipos VADC para que se aplique la nueva directiva de grupo.

NOTA: Si Horizon Client no está configurado para admitir los cifrados compatibles con el sistema operativo del escritorio virtual, se producirá un error en la negociación TLS/SSL y el cliente no se podrá conectar.

Para obtener información sobre la configuración de conjuntos de claves de cifrado en Horizon Client, consulte la documentación de Horizon Client disponible en https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Reemplazar el certificado SSL de servidor autofirmado predeterminado

Un certificado SSL de servidor autofirmado no proporciona protección suficiente a Horizon Client ante amenazas de manipulación y escuchas secretas. Para proteger los escritorios de dichas amenazas, debe reemplazar el certificado autofirmado generado.

Cuando el complemento View Agent Direct-Connection se inicia por primera vez después de la instalación, genera automáticamente un certificado SSL de servidor autofirmado y lo envía al almacén de certificados de Windows. El certificado SSL de servidor se presenta a Horizon Client durante la negociación del protocolo SSL para proporcionar al cliente información sobre este escritorio. El certificado SSL de servidor autofirmado predeterminado no puede garantizar la seguridad de este escritorio, a menos que se reemplace por un certificado firmado por una entidad de certificación (CA) en la que el cliente confíe y que esté totalmente validado por la comprobación de certificados de Horizon Client.

El procedimiento para almacenar este certificado en el almacén de certificados de Windows y el procedimiento para reemplazarlo por un certificado firmado por una CA son los mismos que los que se usan para el servidor de conexión de View (versión 5.1 o posterior). Consulte "Configurar los certificados SSL para los View Server" en el documento *Instalación de View* para obtener más detalles sobre el procedimiento de reemplazo de los certificados.

Los certificados con Nombre alternativo del firmante (SAN) y los certificados comodines son compatibles.

NOTA: Para distribuir los certificados SSL de servidor firmados por una CA a un gran número de escritorios con el complemento View Agent Direct-Connection, utilice la Directiva de registro de Active Directory para distribuir los certificados a todas las máquinas virtuales. Si desea obtener más información, consulte http://technet.microsoft.com/en-us/library/cc732625.aspx.

Autorizar el acceso de Horizon Client a escritorios y aplicaciones

El mecanismo de autorización que permite a un usuario acceder a escritorios y aplicaciones directamente se controla a través de un grupo de sistemas operativos locales llamado **Usuarios de View Agent Direct-Connection**.

Si un usuario es miembro de este grupo, está autorizado a conectarse al escritorio basado en máquina virtual, a un escritorio RDS o a las aplicaciones. Cuando el complemento se instala por primera vez, se crea el grupo local que contiene el grupo de usuarios autenticados. Todos los usuarios que el complemento autentique correctamente están autorizados para acceder al escritorio o a las aplicaciones.

Para restringir el acceso a este escritorio o host RDS, puede modificar la pertenencia a este grupo para especificar una lista de usuarios y grupos de usuarios. Estos usuarios pueden ser locales o bien usuarios de dominios y grupos de usuarios. Si el usuario no está en este grupo, recibirá un mensaje tras autenticarse para informarle que no tiene autorización para acceder a este escritorio basado en máquina virtual ni al escritorio RDS y las aplicaciones que se alojan en este host RDS.

Usar la Traducción de direcciones de red y la asignación de puertos

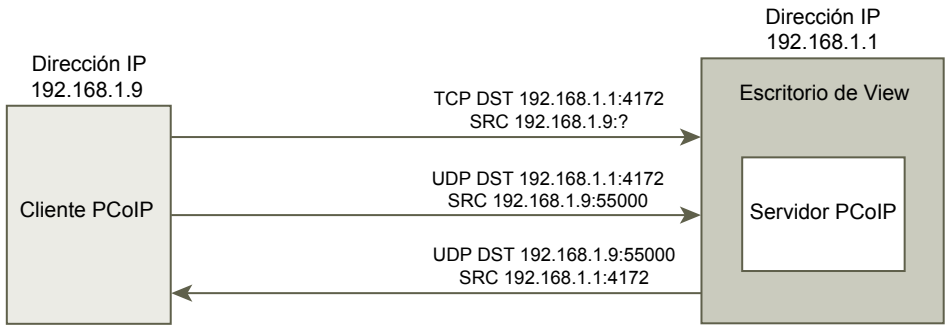
La configuración de la asignación de puertos y la Traducción de direcciones de red (NAT) son necesarias si Horizon Client se conecta a escritorios basados en máquinas virtuales en diferentes redes.

En los ejemplos incluidos en esta guía, debe configurar la información del direccionamiento externo en el escritorio para que Horizon Client pueda usar esta información para conectarse al escritorio usando NAT o un dispositivo de asignación de puertos. La URL es la misma que la URL externa y la URL externa de PCoIP del servidor de conexión de View y del servidor de seguridad.

Cuando Horizon Client está en una red diferente y un dispositivo NAT se encuentra entre Horizon Client y el escritorio que ejecuta el complemento, es necesaria una configuración de asignación de puertos o de NAT. Por ejemplo, si existe un firewall entre Horizon Client y el escritorio, este firewall actúa como un dispositivo de asignación de puertos o NAT.

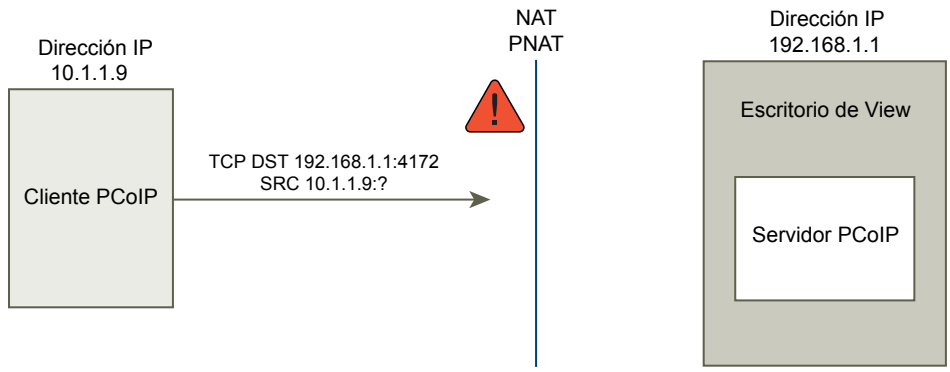
Un ejemplo de implementación de un escritorio cuya dirección IP sea 192.168.1.1 muestra la configuración de NAT y de la asignación de puertos. Un sistema Horizon Client con una dirección IP 192.168.1.9 en la misma red establece una conexión PCoIP usando TCP y UDP. Esta conexión es directa sin ninguna configuración de asignación de puertos o NAT.

Figura 2-1. PCoIP directo desde un cliente de la misma red



Si agrega un dispositivo NAT entre el cliente y el escritorio para que trabajen en diferentes espacios de direcciones y no realicen ningún cambio en la configuración del complemento, los paquetes PCoIP no se enrutan correctamente y se produce un error. En este ejemplo, el cliente usa un espacio de direcciones diferente y tiene una dirección IP 10.1.1.9. Esta configuración produce un error porque el cliente usará la dirección del escritorio para enviar el TCP y los paquetes UDP PCoIP. La dirección de destino 192.168.1.1 no funcionará desde la red del cliente y puede causar que el cliente muestre una pantalla en blanco.

Figura 2-2. El PCoIP desde un cliente a través del dispositivo NAT muestra el error

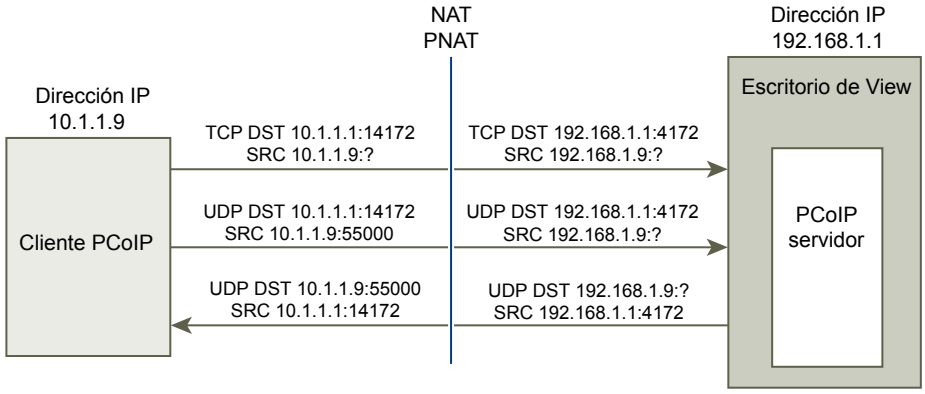


Para resolver este problema, debe configurar el complemento para que use una dirección IP externa. Si `externalIPAddress` está configurada como 10.1.1.1 en este escritorio, el complemento proporciona una dirección IP 10.1.1.1 al cliente al establecer conexiones del protocolo de escritorios con el escritorio. Para PCoIP, el servicio de puerta de enlace segura de PCoIP debe iniciarse en el escritorio para esta configuración.

Para la asignación de puertos, cuando el escritorio use el puerto 4172 PCoIP estándar, pero el cliente deba usar un puerto de destino diferente, asignado al puerto 4172 en el dispositivo de asignación de puertos, debe configurar el complemento para que admita esta disposición de puertos. Si el dispositivo asigna el puerto 14172 al puerto 4172, el cliente debe usar un puerto de destino 14172 para PCoIP. Debe realizar esta configuración para PCoIP. Establezca `externalPCoIPPort` en el complemento como 14172.

En una configuración que use NAT y la asignación de puertos, `externalIPAdress` se configura como 10.1.1.1, que es la red traducida como 192.168.1.1 y `externalPColPPort` se configura como 14172 que es el puerto asignado 4172.

Figura 2-3. El PCoIP desde un cliente a través del dispositivo NAT y de asignación de puertos



Al igual que en la configuración del puerto externo PCoIP TCP/UDP, si el puerto RDP (3389) o el puerto del canal del marco de trabajo (32111) están asignados a algún puerto, debe configurar `externalRDPPort` y `externalFrameworkChannelPort` para especificar los números de puertos TCP que el cliente usará para establecer estas conexiones a través de un dispositivo de asignación de puertos.

Esquema de direccionamiento avanzado

Cuando configure escritorios basados en máquinas virtuales para que sean accesibles a través un dispositivo de asignación de puertos y NAT en la misma dirección IP externa, debe proporcionar a cada escritorio un conjunto único de números de puerto. Los clientes pueden usar la misma dirección IP de destino, pero deben usar un número de puerto TCP único para que la conexión HTTPS dirija la conexión a un escritorio virtual específico.

Por ejemplo, el puerto HTTPS 1000 se dirige a un escritorio y el puerto HTTPS 1005 se dirige a otro, pero ambos puertos utilizan la misma dirección IP de destino. En este caso, sería demasiado complejo configurar números de puerto externos únicos para cada escritorio de las conexiones del protocolo del escritorio. Por esta razón, las opciones del complemento `externalPCoIPPort`, `externalRDPPort` y `externalFrameworkChannelPort` pueden utilizar una expresión relacional opcional en lugar de un valor estadístico para definir un número de puerto relacionado con el número de puerto HTTPS base utilizado por el cliente.

Si el dispositivo de asignación de puertos usa el número de puerto 1000 para HTTPS, asignado a TCP 443; el número de puerto 1001 para RDP, asignado a TCP 3389; el número de puerto 1002 para PCoIP, asignado a TCP y UDP 4172; y el número de puerto 1003 para el canal del marco de trabajo, asignado a TCP 32111, para simplificar la configuración, los números del puerto externo se pueden configurar para que sean

externalRDPPort=+1, externalPCoIPPort=+2 y externalFrameworkChannelPort=+3. Cuando la conexión HTTPS ingrese desde un cliente que use el número de puerto de destino 1000 HTTPS, los números de los puertos externos se calcularán de forma automática de acuerdo a este número de puerto y usará 1001, 1002 y 1003 respectivamente.

Para implementar otro escritorio virtual, si el dispositivo de asignación de puertos usa el número de puerto 1005 para HTTPS, asignado a TCP 443; el número de puerto 1006 para RDP, asignado a TCP 3389; el número de puerto 1007 para PCoIP, asignado a TCP y UDP 4172; y el número de puerto 1008 para el canal del marco de trabajo, asignado a TCP 32111, con la misma configuración del puerto externo en el escritorio (+1, +2, +3 y sucesivamente) cuando la conexión HTTPS ingresa desde un cliente que usa el número de puerto de destino 1005 HTTPS, los números de puerto externos se calcularán automáticamente según el número de puerto 1005 y usará 1006, 1007 y 1008 respectivamente.

Este esquema permite que todos los escritorios estén configurados correctamente y que todos compartan la misma dirección IP externa. Si se asignan los números de puerto siguiendo un incremento de cinco (1000, 1005, 1010,...) al número de puerto HTTPS base, será posible que más de 12.000 escritorios accedan a la misma dirección IP. El número de puerto base se usa para determinar el escritorio virtual al que se enruta la conexión, según la conexión del dispositivo de asignación de puertos. En externalIPAddress=10.20.30.40, externalRDPPort=+1, externalPCoIPPort=+2 y externalFrameworkChannelPort=+3 configurados en todos los escritorios virtuales, la asignación a los escritorios virtuales debe corresponder a la descrita en la tabla de asignación de puertos y NAT.

Tabla 2-2. Valores de asignación de puertos y NAT

#MV	Dirección IP del escritorio	HTTPS	RDP	PCOIP (TCP y UDP)	Canal de marco de trabajo
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

En este ejemplo, Horizon Client se conecta a la dirección IP 10.20.30.40 y a número de puerto de destino HTTPS (1000 + *n* * 5) donde *n* es el número de escritorio. Para conectarse al escritorio 3, el cliente tiene que conectarse a 10.20.30.40:1015. Este esquema de direccionamiento simplifica de forma significativa las opciones de configuración de cada escritorio. Todos los escritorios están configurados con la misma dirección externa y la misma configuración de puertos. La configuración de la asignación de puertos y NAT se realiza a través del dispositivo de asignación de puertos y NAT con este patrón coherente y se puede acceder a todos los escritorios a través de una única dirección IP pública. El cliente usará normalmente un único nombre DNS público que resuelva esta dirección IP.

Agregar una entidad de certificación al almacén de certificados de Windows

Para la autenticación de tarjeta inteligente, la entidad de certificación (CA) que firma el certificado debe aparecer en el almacén de certificados de Windows. Si no es así, puede agregar la CA a dicho almacén.

Prerequisitos

Verifique que Microsoft Management Console (MMC) cuente con el complemento Certificados. Consulte "Agregar el complemento Certificados a MMC" en el documento *Instalación de View*.

Procedimiento

1 Inicie MMC.

2 En la consola MMC, expanda el nodo **Certificados (equipo local)** y diríjase a la carpeta **Entidades de certificación raíz de confianza > Certificados**.

Si el certificado raíz está presente y no hay ningún certificado intermedio en la cadena de certificados, cierre MMC.

3 Haga clic con el botón secundario en la carpeta **Entidades de certificación raíz de confianza > Certificados** y, a continuación, en **Todas las tareas > Importar**.

4 En el asistente Importación de certificado, haga clic en **Siguiente** y busque la ubicación en la que está almacenada el certificado CA raíz.

5 Seleccione el archivo del certificado CA raíz y haga clic en **Abrir**.

6 Haga clic en **Siguiente**, vuelva a hacer clic en **Siguiente** y, a continuación, haga clic en **Finalizar**.

7 Si una CA intermedia expide un certificado de tarjeta inteligente, importe todos los certificados intermedios a la cadena de certificados.

a Diríjase a la carpeta **Certificados (equipo local) > Entidades de certificación intermedias > Certificados**.

b Repita los pasos del 3 al 6 en cada certificado intermedio.

Configurar HTML Access 3

El complemento View Agent Direct-Connection (VADC) admite HTML Access para los escritorios basados en máquinas virtuales y escritorios RDS. HTML Access no es compatible con aplicaciones RDS.

Este capítulo cubre los siguientes temas:

Instale View Agent para HTML Access

Para admitir HTML Access, debe instalar View Agent en el escritorio basado en máquina virtual con un parámetro especial.

Prerequisitos

- Descargue el archivo de instalación de View Agent desde el sitio de descargas de VMware disponible en http://www.vmware.com/go/downloadview.

  El nombre del archivo es `VMware-viewagent-y.y.y-xxxxxx.exe` para Windows 32 bits o `VMware-viewagent-x86_64-y.y.y-xxxxxx.exe` para Windows de 64 bits, donde *y.y.y* es el número de la versión y *xxxxxx* es el número de compilación.

Procedimiento

- Instale View Agent desde la línea de comando y especifique un parámetro para que View Agent no se registre con el servidor de conexión de View.

  Este ejemplo instala la versión de 32 bits de View Agent.

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

Qué hacer a continuación

Instale el complemento View Agent Direct-Connection. Consulte "Instalar el complemento View Agent Direct-Connection," página 7.

Configurar el envío de contenido estático

Si el cliente de HTML Access necesita ser atendido por un escritorio, debe realizar algunas tareas de configuración en el escritorio. Esto permite que un usuario pueda dirigirse a un navegador directamente desde un escritorio.

Prerequisitos

- Descargue el archivo zip `portal.war` de View HTML Access desde el sitio de descargas de VMware disponible en http://www.vmware.com/go/downloadview.

  El nombre del archivo es `VMware-Horizon-View-HTML-Access-y.y.y-xxxxxx.zip`, donde *y.y.y* es el número de versión y *xxxxxx* es el número de compilación.

Procedimiento

1 Abra **Panel de control**.

2 Diríjase a **Programas y características > Activar o desactivar las características de Windows**.

3 Seleccione la casilla **Internet Information Services** y haga clic en **Aceptar**.

4 En **Panel de control**, diríjase a **Herramientas administrativas > Administrador de Internet Information Services (IIS)**.

5 Expanda los elementos del panel situado a la izquierda.

6 Haga clic con el botón secundario en **Sitio Web predeterminado** y seleccione **Modificar enlaces...**

7 Haga clic en **Agregar**.

8 Especifique **https**, **Sin asignar** y puerto **443**.

9 En el campo **Certificado SSL**, seleccione el certificado adecuado.

Opción	Acción
El certificado **vdm** está presente.	Seleccione **vdm** y haga clic en **Aceptar**.
El certificado **vdm** no está presente.	Seleccione **vdmdefault** y haga clic en **Aceptar**.

10 En el diálogo **Enlaces de sitios**, elimine la entrada de **http puerto 80** y haga clic en **Cerrar**.

11 Haga clic en **Sitio Web predeterminado**.

12 Haga doble clic en **Tipos MIME**.

13 Si la **Extensión del nombre de archivo** .json no existe, en el panel **Acciones**, haga clic en **Agregar...**. De lo contrario, omita los dos pasos siguientes.

14 En **Extensión del nombre de archivo**, introduzca **.json**.

15 En **Tipo de MIME**, introduzca **text/h323** y haga clic en **Aceptar**.

16 En **Extensión del nombre de archivo**, introduzca **.mem**.

17 En **Tipo de MIME**, introduzca **texto/sin formato** y haga clic en **Aceptar**.

18 Copie `VMware-Horizon-View-HTML-Access-y.y.y-xxxxxx.zip` en una carpeta temporal.

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

Como resultado, aparecerá un archivo denominado `portal.war`.

20 Cambie el nombre de `portal.war` a `portal.zip`.

21 Descomprima `portal.zip` en la carpeta `C:\inetpub\wwwroot`.

Si es necesario, modifique los permisos de la carpeta para permitir que se agreguen archivos.

Se crea la carpeta `C:\inetpub\wwwroot\portal`.

22 Abra el **Bloc de notas**.

23 Cree el archivo `C:\inetpub\wwwroot\Default.htm` con el siguiente contenido (reemplace *<dirección IP o nombre DNS del escritorio>* por la dirección IP o nombre DNS del escritorio actual):

```
<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>
```

Configurar un certificado SSL de servidor firmado por una CA de confianza

Puede establecer un certificado SSL de servidor firmado por una CA de confianza para asegurar que el tráfico entre clientes y escritorios no sea fraudulento.

Prerequisitos

- Reemplace el certificado SSL del servidor autofirmado predeterminado por un certificado SSL de servidor firmado por una CA de confianza. Consulte "Reemplazar el certificado SSL de servidor autofirmado predeterminado," página 16. Esto crea un certificado que tiene el valor Nombre descriptivo **vdm**.
- Si el escritorio se encarga del contenido estático del cliente, configure una entrega de contenido estático. Consulte "Configurar el envío de contenido estático," página 22.
- Familiarícese con el almacén de certificados de Windows. Consulte "Configurar el servidor de conexión de View, el servidor de seguridad o View Composer para usar un nuevo certificado SSL" en el documento *Instalación de View*.

Procedimiento

1 En el almacén de certificados de Windows, diríjase a **Personal > Certificados**.

2 Haga doble clic en el certificado con el Nombre descriptivo **vdm**.

3 Haga clic en la pestaña **Detalles**.

4 Copie el valor **Huella digital**.

5 Inicie el Editor de registros de Windows.

6 Diríjase a la clave del registro `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config`.

7 Agregue un nuevo valor de cadena (REG_SZ), `SslHash`, a esta clave de registro.

8 Configure el valor `SslHash` con el valor **Thumbprint**.

Deshabilitar el protocolo HTTP/2 en escritorios Windows 10 y Windows 2016

En algunos navegadores, es posible que se encuentre el error ERR_SPDY_PROTOCOL_ERROR al acceder a un escritorio VADC para Windows 10 o a un escritorio VADC para Windows 2016. Para evitar este error, deshabilite el protocolo HTTP/2 en el escritorio.

Procedimiento

1 Inicie el Editor del Registro de Windows.

2 Diríjase a la clave de registro `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\HTTP\Parameters`.

3 Agregue dos nuevos valores REG_DWORD, `EnableHttp2Tls` y `EnableHttp2Cleartext`, a esta clave de registro.

4 Configure ambos valores en **0**.

5 Reinicie el escritorio.

Configurar View Agent Direct Connection en los hosts de los Servicios de Escritorio remoto

4

Horizon 7 admite los hosts de los Servicios de Escritorio remoto (RDS) que proporcionan aplicaciones y escritorios RDS a los que los usuarios pueden acceder desde Horizon Client. Un escritorio RDS se basa en una sesión de escritorio de un host RDS. En una implementación de Horizon 7 típica, los clientes se conectan a escritorios y aplicaciones a través del servidor de conexión de Horizon. Sin embargo, si instala el complemento View Agent Direct-Connection en un host RDS, los clientes se pueden conectar directamente a las aplicaciones o los escritorios RDS sin usar el servidor de conexión de Horizon.

Este capítulo cubre los siguientes temas:

Hosts de los Servicios de Escritorios remotos

Un host de los Servicios de Escritorios remotos (RDS) es un equipo servidor que aloja aplicaciones y escritorios para el acceso remoto.

En una implementación de Horizon 7, un host RDS es un servidor de Windows que tiene la función de los Servicios de Escritorios remotos de Microsoft, el servicio del host de sesión de Escritorio remoto de Microsoft y Horizon Agent instalados. Un host RDS puede admitir View Agent Direct Connection (VADC) si también tiene instalado el complemento VADC. Para obtener información sobre cómo configurar un host RDS y cómo instalar Horizon 7 Agent, consulte la sección "Configurar hosts de los Servicios de Escritorio remoto" en el documento *Configurar aplicaciones y escritorios publicados en Horizon 7*. Para obtener más información sobre la instalación del complemento VADC, consulte Capítulo 1, "Instalar el complemento View Agent Direct-Connection," página 7.

NOTA: Cuando instala Horizon Agent, el instalador solicita el nombre de host o la dirección IP del servidor de conexión de Horizon a la que se conectará Horizon Agent. Puede hacer que el instalador omita este paso al ejecutarlo con un parámetro.

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

Después de configurar un host RDS e instalar el complemento VADC, debe autorizar las aplicaciones y los escritorios RDS. Consulte "Autorizar aplicaciones y escritorios RDS," página 25.

Autorizar aplicaciones y escritorios RDS

Debe autorizar a los usuarios para que puedan utilizar las aplicaciones y los escritorios RDS antes de que puedan acceder a ellos.

Si el host RDS ejecuta Windows Server 2008 R2 SP1, ejecute **Administrador de RemoteApp** para configurar las autorizaciones.

Si el host RDS ejecuta Windows Server 2012 o 2012 R2, ejecute **Administrador de servidores** y diríjase a **Servicios de Escritorio remoto** para configurar las autorizaciones.

Autorizaciones de escritorios

Para autorizar que un usuario pueda iniciar un escritorio RDS, siga estos pasos:

- Asegúrese de que el usuario sea miembro del grupo local **Usuarios de View Agent Direct-Connection**. De forma predeterminada, todos los usuarios autenticados son miembros de este grupo.
- Para Windows Server 2008 R2 SP1, en **Administrador de RemoteApp**, compruebe que el servidor del host de la sesión del escritorio remoto esté configurado en **Mostrar una conexión a Escritorio remoto para este servidor host de sesión de Escritorio remoto en Acceso web de RD**.
- Para Windows 2012 o 2012 R2, ejecute **Administrador de servidores** y diríjase a **Servicios de Escritorio remoto** para configurar las autorizaciones.

Autorizaciones de aplicaciones

Para autorizar que un usuario inicie una aplicación, siga estos pasos:

- Asegúrese de que el usuario sea miembro del grupo local **Usuarios de View Agent Direct-Connection**. De forma predeterminada, todos los usuarios autenticados son miembros de este grupo.
- Para Windows Server 2008 R2 SP1, en **Administrador de RemoteApp**, compruebe que la aplicación aparezca en **Programas RemoteApp**, que esté configurada para **Acceso web de RD** y que tenga establecidas las asignaciones para todos los usuarios, para este usuario o para un grupo del que el usuario es miembro.
- Para Windows 2012 o 2012 R2, ejecute **Administrador de servidores** y diríjase a **Servicios de Escritorio remoto** para configurar las autorizaciones.

Solucionar los problemas del complemento View Agent Direct-Connection

5

Al usar el complemento View Agent Direct-Connection, es posible que se produzcan problemas conocidos.

Cuando investigue un problema con el complemento View Agent Direct-Connection, asegúrese de que la versión correcta esté instalada y en ejecución.

Si es necesario enviar un problema de compatibilidad a VMware, habilite siempre el registro completo, reproduzca el problema y genere un conjunto de registros con la herramienta de recopilación de datos (DCT). Es entonces cuando el equipo de soporte técnico de VMware puede analizar esos registros. Para obtener más información sobre cómo generar un conjunto de registros DCT, consulte el artículo de la base de conocimientos sobre cómo recopilar información de diagnóstico para VMware View, disponible en http://kb.vmware.com/kb/1017939.

Este capítulo cubre los siguientes temas:

Versión incorrecta de controlador de gráficos instalada

Para que PCoIP funcione correctamente, se debe instalar la versión correcta del controlador de gráficos.

Problema

Aparece una pantalla negra cuando un usuario se conecta a un escritorio o a una aplicación con PCoIP.

Origen

Se está ejecutando una versión incorrecta de los controladores de gráficos. Esto puede ocurrir si se instaló una versión incorrecta de VMware Tools después de instalar View Agent.

Solución

- Vuelva a instalar View Agent.

RAM de vídeo insuficiente

Para admitir PCoIP, una máquina virtual que ejecute un escritorio o un host RDS debe tener, como mínimo, 128 MB de RAM de vídeo.

Problema

Aparece una pantalla negra cuando un usuario se conecta a un escritorio o a una aplicación con PCoIP.

Origen

La máquina virtual no cuenta con RAM de vídeo suficiente.

Solución

- Configure al menos 128 MB de RAM de vídeo para cada máquina virtual.

Habilitar el registro completo para incluir la información de TRACE y DEBUG

El complemento View Agent Direct-Connection escribe entradas en el registro estándar de View Agent. De forma predeterminada, la información de TRACE y DEBUG no se encuentran en el registro.

Problema

View Agent no contiene la información de TRACE y DEBUG.

Origen

El registro completo no está habilitado. Debe habilitarlo para incluir la información de TRACE y DEBUG en el registro de View Agent.

Solución

1. Abra una ventana de símbolo de sistema y ejecute `C:\Program Files\VMware\VMware View\Agent\DCT\support.bat loglevels`.
2. Introduzca **3** para habilitar el registro completo.

   Los archivos de registro de depuración se encuentran en `%ALLUSERSPROFILE%\VMware\VDM\logs`. El archivo `debug*.log` registra la información de View Agent y el complemento. Busque `wsnm_xmlapi` para encontrar las líneas del registro del complemento.

   Cuando se inicia View Agent, se registra la versión del complemento:

   ```
   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
   ```

Índice