



# **Citrix Virtual Apps and Desktops 7 1912 LTSR**

## Contents

<b>Citrix Virtual Apps and Desktops 7 1912 Long Term Service Release (LTSR)</b>	<b>12</b>
<b>Novedades</b>	<b>13</b>
<b>Cumulative Update 9 (CU9)</b>	<b>14</b>
<b>Problemas resueltos</b>	<b>18</b>
<b>Cumulative Update 8 (CU8)</b>	<b>22</b>
<b>Problemas resueltos</b>	<b>27</b>
<b>Cumulative Update 7 (CU7)</b>	<b>33</b>
<b>Problemas resueltos</b>	<b>38</b>
<b>Cumulative Update 6 (CU6)</b>	<b>43</b>
<b>Problemas resueltos</b>	<b>48</b>
<b>Cumulative Update 5 (CU5)</b>	<b>53</b>
<b>Problemas resueltos</b>	<b>57</b>
<b>Cumulative Update 4 (CU4)</b>	<b>63</b>
<b>Problemas resueltos</b>	<b>67</b>
<b>Cumulative Update 3 (CU3)</b>	<b>76</b>
<b>Problemas resueltos</b>	<b>81</b>
<b>Cumulative Update 2 (CU2)</b>	<b>90</b>
<b>Problemas resueltos</b>	<b>96</b>
<b>Cumulative Update 1 (CU1)</b>	<b>111</b>
<b>Problemas resueltos</b>	<b>116</b>
<b>1912 LTSR (versión inicial)</b>	<b>125</b>
<b>Problemas resueltos</b>	<b>133</b>
<b>Problemas conocidos</b>	<b>138</b>

<b>Elementos retirados</b>	<b>150</b>
<b>Requisitos del sistema</b>	<b>162</b>
<b>Información técnica general</b>	<b>174</b>
<b>Active Directory</b>	<b>184</b>
<b>Bases de datos</b>	<b>187</b>
<b>Métodos de entrega</b>	<b>195</b>
<b>Puertos de red</b>	<b>199</b>
<b>HDX</b>	<b>204</b>
<b>Transporte adaptable</b>	<b>215</b>
<b>Canales virtuales ICA de Citrix</b>	<b>223</b>
<b>Doble salto en Citrix Virtual Apps and Desktops</b>	<b>233</b>
<b>Instalación y configuración</b>	<b>236</b>
<b>Antes de la instalación</b>	<b>238</b>
<b>Entornos de virtualización de Microsoft Azure Resource Manager</b>	<b>247</b>
<b>Entornos de virtualización de Microsoft System Center Virtual Machine Manager</b>	<b>268</b>
<b>Entornos de virtualización de Citrix Hypervisor</b>	<b>271</b>
<b>Entornos de Microsoft System Center Configuration Manager</b>	<b>275</b>
<b>Entornos de virtualización de VMware</b>	<b>277</b>
<b>Entornos de virtualización de Nutanix</b>	<b>286</b>
<b>Entornos de virtualización de Microsoft Azure</b>	<b>288</b>
<b>Instalar componentes principales</b>	<b>291</b>
<b>Instalar VDA</b>	<b>304</b>
<b>Instalación desde la línea de comandos</b>	<b>321</b>
<b>Instalar agentes VDA mediante scripts</b>	<b>334</b>

<b>Instalar agentes VDA mediante SCCM</b>	<b>337</b>
<b>Crear un sitio</b>	<b>340</b>
<b>Crear catálogos de máquinas</b>	<b>345</b>
<b>Administrar catálogos de máquinas</b>	<b>367</b>
<b>Crear grupos de entrega</b>	<b>375</b>
<b>Administrar grupos de entrega</b>	<b>382</b>
<b>Crear grupos de aplicaciones</b>	<b>407</b>
<b>Administrar grupos de aplicaciones</b>	<b>416</b>
<b>Acceso con Remote PC</b>	<b>421</b>
<b>App-V</b>	<b>433</b>
<b>AppDisks</b>	<b>448</b>
<b>Publicar contenido</b>	<b>480</b>
<b>VDI de servidor</b>	<b>486</b>
<b>Capa de personalización de usuarios</b>	<b>488</b>
<b>Personal vDisk</b>	<b>506</b>
<b>Instalación y actualización</b>	<b>514</b>
<b>Configurar y administrar</b>	<b>517</b>
<b>Herramientas</b>	<b>530</b>
<b>Pantallas, mensajes y solución de problemas</b>	<b>533</b>
<b>Migrar Personal vDisk a App Layering</b>	<b>543</b>
<b>Eliminar componentes</b>	<b>557</b>
<b>Actualización y migración</b>	<b>559</b>
<b>Cambios en 7.x</b>	<b>564</b>
<b>Actualizar la versión de una implementación</b>	<b>572</b>

<b>Actualizar un servidor de trabajo XenApp 6.5 a un nuevo VDA</b>	<b>592</b>
<b>Migrar XenApp 6.x</b>	<b>594</b>
<b>Protección</b>	<b>625</b>
<b>Recomendaciones y consideraciones de seguridad</b>	<b>627</b>
<b>Integrar Citrix Virtual Apps and Desktops con Citrix Gateway</b>	<b>636</b>
<b>Administración delegada</b>	<b>637</b>
<b>Tarjetas inteligentes</b>	<b>646</b>
<b>Implementaciones de tarjeta inteligente</b>	<b>653</b>
<b>Autenticación PassThrough y Single Sign-On con tarjetas inteligentes</b>	<b>660</b>
<b>Transport Layer Security (TLS)</b>	<b>662</b>
<b>Transport Layer Security (TLS)</b>	<b>675</b>
<b>Protocolo TLS en Universal Print Server</b>	<b>692</b>
<b>Seguridad de canales virtuales</b>	<b>703</b>
<b>Dispositivos</b>	<b>709</b>
<b>Dispositivos USB genéricos</b>	<b>710</b>
<b>Dispositivos móviles y de pantalla táctil</b>	<b>711</b>
<b>Puertos serie</b>	<b>714</b>
<b>Teclados especiales</b>	<b>720</b>
<b>Dispositivos TWAIN</b>	<b>722</b>
<b>Cámaras web</b>	<b>723</b>
<b>Gráficos</b>	<b>724</b>
<b>HDX 3D Pro</b>	<b>726</b>
<b>Aceleración de GPU para SO Windows multisesión</b>	<b>727</b>
<b>Aceleración de GPU para SO Windows de sesión única</b>	<b>730</b>

<b>Thinwire</b>	<b>735</b>
<b>Marca de agua de sesión basada en texto</b>	<b>742</b>
<b>Contenido multimedia</b>	<b>744</b>
<b>Funciones de audio</b>	<b>747</b>
<b>Redirección de contenido de explorador web</b>	<b>757</b>
<b>Conferencias de vídeo de HDX y compresión de vídeo para cámaras web de HDX</b>	<b>767</b>
<b>Redirección multimedia HTML5</b>	<b>770</b>
<b>Optimización para Microsoft Teams</b>	<b>774</b>
<b>Supervisión, solución de problemas y asistencia para Microsoft Teams</b>	<b>800</b>
<b>Redirección de Windows Media</b>	<b>808</b>
<b>Redirección de contenido general</b>	<b>809</b>
<b>Redirección de carpetas del cliente</b>	<b>810</b>
<b>Redirección del host al cliente</b>	<b>812</b>
<b>Redirección bidireccional de contenido</b>	<b>815</b>
<b>Acceso a aplicaciones locales y redirección de URL</b>	<b>817</b>
<b>Consideraciones sobre unidades del cliente y redirección de USB genérico</b>	<b>827</b>
<b>Imprimir</b>	<b>839</b>
<b>Ejemplo de configuración de la impresión</b>	<b>848</b>
<b>Prácticas recomendadas, consideraciones de seguridad y operaciones predeterminadas</b>	<b>851</b>
<b>Directivas y preferencias de impresión</b>	<b>854</b>
<b>Aprovisionar impresoras</b>	<b>856</b>
<b>Mantener el entorno de impresión</b>	<b>865</b>
<b>Directivas</b>	<b>871</b>
<b>Trabajar con directivas</b>	<b>873</b>

<b>Plantillas de directiva</b>	<b>877</b>
<b>Crear directivas</b>	<b>882</b>
<b>Comparar, priorizar, modelar y solucionar problemas de directivas</b>	<b>889</b>
<b>Configuraciones predeterminadas de directivas</b>	<b>893</b>
<b>Referencia para configuraciones de directivas</b>	<b>924</b>
<b>Configuraciones de la directiva ICA</b>	<b>929</b>
<b>Configuraciones de la directiva Reconexión automática de clientes</b>	<b>937</b>
<b>Configuraciones de directiva de Sonido</b>	<b>940</b>
<b>Configuraciones de directiva de Ancho de banda</b>	<b>942</b>
<b>Configuraciones de directiva de Redirección bidireccional de contenido</b>	<b>948</b>
<b>Configuraciones de la directiva Redirección de contenido de explorador web</b>	<b>951</b>
<b>Configuraciones de directiva de Sensores del cliente</b>	<b>959</b>
<b>Configuraciones de directiva de Interfaz de usuario de escritorio</b>	<b>960</b>
<b>Configuraciones de directiva de Supervisión de usuario final</b>	<b>962</b>
<b>Configuración de directiva de Enhanced Desktop Experience</b>	<b>962</b>
<b>Configuraciones de directiva de Redirección de archivos</b>	<b>963</b>
<b>Configuraciones de directiva de Gráficos</b>	<b>968</b>
<b>Configuraciones de directiva de Almacenamiento en caché</b>	<b>975</b>
<b>Configuraciones de directiva de Framehawk</b>	<b>976</b>
<b>Configuraciones de directiva de Keep Alive</b>	<b>977</b>
<b>Configuraciones de directiva de Acceso a aplicaciones locales</b>	<b>978</b>
<b>Configuraciones de directiva de Experiencia móvil</b>	<b>978</b>
<b>Configuraciones de directiva de Multimedia</b>	<b>979</b>
<b>Configuraciones de directiva de Conexiones de multisequencia</b>	<b>990</b>

<b>Configuraciones de directiva de Redirección de puertos</b>	<b>993</b>
<b>Configuraciones de directiva de Impresión</b>	<b>995</b>
<b>Configuraciones de directiva de Impresoras del cliente</b>	<b>998</b>
<b>Configuraciones de directiva de Controladores</b>	<b>1002</b>
<b>Configuraciones de directiva de Universal Print Server</b>	<b>1004</b>
<b>Configuraciones de directiva de Impresión universal</b>	<b>1009</b>
<b>Configuraciones de directiva de Seguridad</b>	<b>1012</b>
<b>Configuraciones de directiva de Límites de servidor</b>	<b>1014</b>
<b>Configuraciones de directiva de Límites de sesión</b>	<b>1014</b>
<b>Configuraciones de la directiva Fiabilidad de la sesión</b>	<b>1016</b>
<b>Configuraciones de directiva de Marca de agua de la sesión</b>	<b>1018</b>
<b>Parámetros de directiva de control de zona horaria</b>	<b>1021</b>
<b>Configuraciones de directiva de Dispositivos TWAIN</b>	<b>1022</b>
<b>Configuraciones de directiva de Dispositivos USB</b>	<b>1023</b>
<b>Configuraciones de directiva de Presentación visual</b>	<b>1032</b>
<b>Configuraciones de directiva de Imágenes en movimiento</b>	<b>1034</b>
<b>Configuraciones de directiva de Imágenes fijas</b>	<b>1036</b>
<b>Configuraciones de directiva de WebSockets</b>	<b>1038</b>
<b>Configuraciones de la directiva Administración de carga</b>	<b>1039</b>
<b>Configuraciones de directiva de Profile Management</b>	<b>1040</b>
<b>Configuraciones avanzadas de directiva</b>	<b>1041</b>
<b>Configuraciones básicas de directiva</b>	<b>1044</b>
<b>Configuraciones de directiva de Multiplataforma</b>	<b>1048</b>
<b>Configuraciones de directiva de Sistema de archivos</b>	<b>1050</b>

<b>Configuraciones de directiva de Exclusiones</b>	<b>1050</b>
<b>Configuraciones de directiva de Sincronización</b>	<b>1052</b>
<b>Configuraciones de directiva de Redirección de carpetas</b>	<b>1054</b>
<b>Configuraciones de directiva de AppData(Roaming)</b>	<b>1055</b>
<b>Configuraciones de directiva de Contactos</b>	<b>1056</b>
<b>Configuraciones de directiva de Escritorio</b>	<b>1056</b>
<b>Configuraciones de directiva de Documentos</b>	<b>1057</b>
<b>Configuraciones de directiva de Descargas</b>	<b>1058</b>
<b>Configuraciones de directiva de Favoritos</b>	<b>1058</b>
<b>Configuraciones de directiva de Vínculos</b>	<b>1059</b>
<b>Configuraciones de directiva de Música</b>	<b>1060</b>
<b>Configuraciones de directiva de Imágenes</b>	<b>1061</b>
<b>Configuraciones de directiva de Juegos guardados</b>	<b>1061</b>
<b>Configuraciones de directiva de Menú Inicio</b>	<b>1062</b>
<b>Configuraciones de directiva de Búsquedas</b>	<b>1063</b>
<b>Configuraciones de directiva de Vídeos</b>	<b>1063</b>
<b>Configuraciones de directiva de Registro</b>	<b>1064</b>
<b>Configuraciones de directiva de Gestión de perfiles</b>	<b>1069</b>
<b>Configuraciones de directiva de Registro del sistema</b>	<b>1073</b>
<b>Configuraciones de directiva para Perfiles de usuario de streaming</b>	<b>1074</b>
<b>Configuración de directiva de personalización de usuario</b>	<b>1076</b>
<b>Configuraciones de directiva de Virtual Delivery Agent</b>	<b>1077</b>
<b>Configuraciones de directiva de HDX 3D Pro</b>	<b>1079</b>
<b>Configuraciones de directiva de Supervisión</b>	<b>1080</b>

<b>Configuraciones de directiva de IP virtual</b>	<b>1084</b>
<b>Configurar la redirección de puertos COM y puertos LPT mediante el Registro</b>	<b>1085</b>
<b>Configuración de directivas de Connector for Configuration Manager 2012</b>	<b>1086</b>
<b>Administrar</b>	<b>1090</b>
<b>Licencias</b>	<b>1092</b>
<b>Licencias de varios tipos</b>	<b>1095</b>
<b>Preguntas frecuentes sobre licencias</b>	<b>1103</b>
<b>Aplicaciones</b>	<b>1116</b>
<b>Aplicaciones de la Plataforma universal de Windows</b>	<b>1128</b>
<b>Zonas</b>	<b>1131</b>
<b>Conexiones y recursos</b>	<b>1144</b>
<b>Caché de host local</b>	<b>1159</b>
<b>Administrar las claves de seguridad</b>	<b>1170</b>
<b>IP virtual y bucle invertido virtual</b>	<b>1187</b>
<b>Delivery Controllers</b>	<b>1191</b>
<b>Registro de VDA</b>	<b>1195</b>
<b>Sesiones</b>	<b>1207</b>
<b>Usar búsquedas en Studio</b>	<b>1215</b>
<b>Etiquetas</b>	<b>1216</b>
<b>Compatibilidad con IPv4/IPv6</b>	<b>1226</b>
<b>Perfiles de usuario</b>	<b>1229</b>
<b>Recopilar rastreos de Citrix Diagnostic Facility (CDF) durante el inicio del sistema</b>	<b>1236</b>
<b>Citrix Insight Services</b>	<b>1239</b>
<b>Citrix Scout</b>	<b>1251</b>

<b>Supervisar</b>	<b>1269</b>
<b>Registro de configuraciones</b>	<b>1270</b>
<b>Registros de eventos</b>	<b>1276</b>
<b>Director</b>	<b>1277</b>
<b>Instalación y configuración</b>	<b>1282</b>
<b>Configuración avanzada</b>	<b>1285</b>
<b>Configurar la autenticación con tarjetas inteligentes PIV</b>	<b>1289</b>
<b>Configurar el análisis de red</b>	<b>1292</b>
<b>Administración delegada y Director</b>	<b>1294</b>
<b>Implementación segura de Director</b>	<b>1297</b>
<b>Configurar sitios locales con Citrix Analytics for Performance</b>	<b>1300</b>
<b>Análisis de sitios</b>	<b>1306</b>
<b>Alertas y notificaciones</b>	<b>1317</b>
<b>Filtrar datos para solucionar fallos</b>	<b>1332</b>
<b>Supervisar tendencias históricas en un sitio</b>	<b>1334</b>
<b>Solucionar problemas de implementaciones</b>	<b>1340</b>
<b>Solucionar problemas de aplicaciones</b>	<b>1341</b>
<b>Sondeo de aplicaciones</b>	<b>1345</b>
<b>Sondeo de escritorios</b>	<b>1350</b>
<b>Solucionar problemas de máquinas</b>	<b>1355</b>
<b>Solucionar problemas de usuarios</b>	<b>1364</b>
<b>Diagnosticar problemas de inicio de sesión</b>	<b>1366</b>
<b>Diagnosticar problemas de inicio de sesión de los usuarios</b>	<b>1372</b>
<b>Remedar usuarios</b>	<b>1380</b>

<b>Enviar mensajes a usuarios</b>	<b>1381</b>
<b>Resolver fallos de aplicación</b>	<b>1382</b>
<b>Restaurar conexiones de escritorio</b>	<b>1383</b>
<b>Restaurar sesiones</b>	<b>1384</b>
<b>Generar informes de sistema de canales HDX</b>	<b>1385</b>
<b>Restablecer un perfil de usuario</b>	<b>1386</b>
<b>Grabar sesiones</b>	<b>1390</b>
<b>Tabla de compatibilidad de funciones</b>	<b>1392</b>
<b>Granularidad y retención de datos</b>	<b>1396</b>
<b>Motivos de fallo y solución de problemas en Citrix Director</b>	<b>1404</b>
<b>SDK y API</b>	<b>1429</b>
<b>Plantillas voluntarias de accesibilidad de productos WCAG 2.0</b>	<b>1431</b>

## Citrix Virtual Apps and Desktops 7 1912 Long Term Service Release (LTSR)

May 24, 2024

### Importante:

La estrategia de ciclos de vida para las versiones Current Release (CR) y las versiones Long Term Service (LTSR) del producto se describe en [Hitos del ciclo de vida](#).

Citrix Virtual Apps and Desktops es una solución de virtualización que proporciona a los equipos de TI control sobre máquinas virtuales, aplicaciones, licencias y seguridad, al tiempo que permiten un acceso desde cualquier lugar y cualquier dispositivo.

El programa Long Term Service Release (LTSR o Servicio a largo plazo) de Citrix Virtual Apps and Desktops ofrece estabilidad y funcionalidad a largo plazo para las versiones de Citrix Virtual Apps and Desktops.

Cumulative Update 9 (CU9) es la actualización más reciente de la versión 1912 LTSR. Las versiones LTSR también están disponibles para la versión 7.15 de XenApp y XenDesktop. Si no conoce el programa LTSR, no es necesario instalar la versión inicial de 1912 LTSR. En su lugar, le recomendamos que comience directamente por 1912 LTSR CU9.

- Para obtener información sobre casos de uso, consulte <https://www.citrix.com/products/citrix-virtual-apps-and-desktops/>.
- Para obtener información sobre los componentes y las tecnologías de las implementaciones de Citrix Virtual Apps and Desktops, consulte [Información técnica general](#).

### Versiones anteriores

La documentación de otras versiones disponibles actualmente se encuentra en [Citrix Virtual Apps and Desktops](#).

Para versiones incluso anteriores, la documentación se archiva en [Documentación antigua](#).

### Citrix Virtual Apps and Desktops en Citrix Cloud

La oferta de Citrix Cloud Virtual Apps and Desktops es Citrix DaaS. Para ver la documentación del servicio, consulte [Citrix DaaS](#).

## Descargas

[Citrix Virtual Apps and Desktops 7 1912 LTSR CU9](#)

## Enlaces útiles

- [Citrix Supportability Pack](#)
- [Preguntas frecuentes de LTSR \(FAQ\)](#)
- [Opciones de servicio de Citrix Virtual Apps and Desktops](#)
- [Fechas de la vida útil del producto](#)
- [Programa LTSR para Receiver para Windows](#)

## Cambios en el nombre y el número de versión de los productos Citrix

Para obtener información sobre los cambios efectuados en 2018 en nombres de producto y números de versión, consulte [Nuevos nombres y números](#).

## Novedades

May 24, 2024

### Acerca de esta versión

Acerca de la actualización [Cumulative Update 9 \(CU9\)](#)

Acerca de la actualización [Cumulative Update 8 \(CU8\)](#)

Acerca de la actualización [Cumulative Update 7 \(CU7\)](#)

Acerca de la actualización [Cumulative Update 6 \(CU6\)](#)

Acerca de la actualización [Cumulative Update 5 \(CU5\)](#)

Acerca de la actualización [Cumulative Update 4 \(CU4\)](#)

Acerca de [Cumulative Update 3 \(CU3\)](#)

Acerca de [Cumulative Update 2 \(CU2\)](#)

Acerca de [Cumulative Update 1 \(CU1\)](#)

Acerca de [1912 LTSR \(versión inicial\)](#)

## Cumulative Update 9 (CU9)

May 24, 2024

Fecha de publicación: 30 de abril de 2024

### Acerca de esta versión

Citrix Virtual Apps and Desktops 7 1912 LTSR Cumulative Update 9 (CU9) corrige más de 15 problemas notificados desde la publicación de 1912 LTSR CU8.

[1912 LTSR \(información general\)](#)

[1912 LTSR \(funciones e información sobre la actualización de la versión\)](#)

[Problemas resueltos desde Citrix Virtual Apps and Desktops 7 1912 LTSR CU8](#)

[Problemas conocidos en esta versión](#)

[Elementos eliminados y obsoletos](#)

[Fechas de elegibilidad de Subscription Advantage de los productos Citrix](#)

### Descargas

[Citrix Virtual Apps and Desktops 7 1912 LTSR CU9](#)

#### Importante:

Citrix License Administration Console alcanzó el final de su vida útil y el final de su desarrollo en el Servidor de licencias 11.17.2.0\_BUILD\_40000 Use [Citrix Licensing Manager](#).

### Nuevas implementaciones

¿Cómo implemento la actualización CU9 desde cero?

Puede configurar un nuevo entorno de Citrix Virtual Apps and Desktops basado en CU9 con el metainstalador de CU9. Antes de ello, le recomendamos que se familiarice con el producto:

Consulte la sección [Citrix Virtual Apps and Desktops 7 1912 LTSR \(versión inicial\)](#) y lea atentamente las secciones [Información técnica general](#), [Instalar y configurar](#) y [Proteger](#) antes de planificar la implementación. Compruebe que la configuración cumple los [requisitos del sistema](#) de todos los componentes.

## Implementaciones existentes

¿Qué actualizo?

CU9 ofrece actualizaciones de [componentes base](#) de 1912 LTSR. Recuerde: Citrix recomienda actualizar todos los componentes de LTSR de la implementación a CU9. Por ejemplo: Si Citrix Provisioning forma parte de su implementación LTSR, actualice los componentes de Citrix Provisioning a CU9. Si Citrix Provisioning no forma parte de la implementación, no necesita instalarlo ni actualizarlo.

## Componentes base de Citrix Virtual Apps and Desktops 7 1912 LTSR CU9

---

<b>Componente base de 1912 LTSR</b>	<b>Versión como se muestra en Programas y características</b>	<b>Notas</b>
VDA de sesión única	1912.0.9000.9299	
VDA multisesión	1912.0.9000.9299	
Delivery Controller	1912.0.9000.9299	
Citrix Studio	1912.0.9000.85	
Citrix Director	1912.0.9000.14	
Administración de directivas de grupo de Citrix	7.24.9000.0	
Extensión del cliente de directivas de grupo de Citrix	7.24.9000.0	
Citrix StoreFront	1912.0.9000.17	
Citrix Provisioning	1912.80.iso	
Universal Print Server	1912.0.9000.15	
Grabación de sesiones	1912.0.9000	
Linux VDA	1912.0.9000	Consulte la <a href="#">documentación de Linux VDA</a> para ver las plataformas compatibles
Profile Management	1912.0.9000.3	
Servicio de autenticación federada de Citrix	1912.0.9000.14	
Redirección de contenido del explorador web	15.19.9000.16	

---

## Componentes compatibles de Citrix Virtual Apps and Desktops 7 1912 LTSR CU9

Los siguientes componentes, en las versiones que se indican a continuación, son compatibles con entornos LTSR. Estos componentes no dan derecho a las ventajas de LTSR (ciclo de vida ampliado y actualizaciones acumulativas de correcciones solamente). Citrix puede pedirle que actualice estos componentes a una versión más reciente dentro de sus entornos 1912 LTSR.

Componentes y funciones compatibles	Versión como se muestra en Programas y características
App Layering	22.11
Directivas de protección de aplicaciones	1912 LTSR CU8
HDX RealTime Optimization Pack	2.9 LTSR CU7
Servidor de licencias	11.17.2.0, compilación 47000
Capa de personalización de usuarios	23.12.4
Reproductor web de grabación de sesiones	1912.0.9000
Autoservicio de restablecimiento de contraseñas	1912.0.8000
Windows 10 de 32 bits	Consulte la <a href="#">documentación de la versión inicial</a>
Workspace Environment Management	2305
XenApp y XenDesktop 7.15 LTSR VDA (versión más reciente)*	Solo la actualización acumulativa más reciente

### Nota:

Windows 10 de 32 bits solo es compatible durante 18 meses a partir de la publicación inicial de 1912 LTSR. Windows 10 32 de bits solo es compatible en Windows 10 Enterprise 2019 LTSC.

\* La compatibilidad con VDA de XenApp y XenDesktop 7.15 LTSR en este caso es solo para Windows 7 y Windows 2008 R2. XenApp y XenDesktop 7.15 LTSR dejará de ser compatible a partir de agosto de 2022. La compatibilidad con Citrix para Windows 7 y Windows 2008 R2 finalizará cuando Microsoft finalice el soporte para el sistema operativo o cuando finalice la compatibilidad con XenApp y XenDesktop 7.15 LTSR, lo que ocurra primero. Para obtener más información, consulte la [tabla de productos de Citrix](#).

## Versiones compatibles de la aplicación Citrix Workspace

Todas las versiones admitidas de la aplicación Citrix Workspace son compatibles con Citrix Virtual Apps and Desktops 1912 LTSR. Para obtener información sobre el ciclo de vida de la aplicación Citrix Workspace, consulte [Lifecycle Milestones for Citrix Workspace app and Citrix Receiver](#).

Para mayor comodidad, considere la posibilidad de suscribirse al [feed RSS de la aplicación Citrix Workspace](#) para recibir una notificación cuando una nueva versión de la aplicación Citrix Workspace esté disponible.

## **Exclusiones importantes de Citrix Virtual Apps and Desktops 7 1912 LTSR CU9**

Las siguientes funciones, componentes y plataformas no dan derecho a las ventajas y prestaciones del ciclo de vida de 1912 LTSR. Específicamente, se excluyen las ventajas de actualizaciones acumulativas y el ciclo de vida ampliado. Las actualizaciones de los componentes y funciones excluidos están disponibles a través de las versiones publicadas regularmente.

---

### **Componentes y funciones excluidos**

---

AppDisks

AppDNA

Citrix SCOM Management Pack

Framehawk

Personal vDisk

Integración de StoreFront con Citrix Online

---

---

### **Plataformas Windows excluidas\***

---

Windows 2008 de 32 bits (para Universal Print Server)

---

\* Citrix se reserva el derecho a actualizar el soporte que ofrece para las plataformas en función de los hitos de los ciclos de vida de los proveedores externos.

## **Datos de análisis de instalación y actualización**

Cuando se usa el programa de instalación del producto completo para implementar o actualizar los componentes de XenApp o XenDesktop, se recopila información anónima sobre el proceso de instalación y se guarda en la máquina donde se está realizando la instalación o actualización del componente. Esta información se utiliza para ayudar a Citrix a mejorar la experiencia de instalación de sus clientes.

## Migrar XenApp 6.5

El proceso de migración de XenApp 6.5 permite realizar una transición eficaz y rápida desde una comunidad XenApp 6.5 a un sitio con 1912 LTSR. Esta transición puede resultarle útil en caso de implementaciones que contienen una gran cantidad de aplicaciones y directivas de grupo Citrix, porque reduce el riesgo de que se produzcan errores accidentales al mover manualmente las aplicaciones y las directivas de grupo Citrix al nuevo sitio de XenApp.

Después de instalar los componentes principales de 1912 LTSR y crear un sitio, el proceso de migración sigue estos pasos:

- Ejecute el instalador de 1912 en cada servidor de trabajo de XenApp 6.5. Este instalador actualiza automáticamente el servidor a un nuevo Virtual Delivery Agent para SO de servidor listo para usar en el nuevo sitio.
- Ejecute los cmdlets de exportación de PowerShell en un Controller de XenApp 6.5, que exporta las configuraciones de aplicaciones y directivas de Citrix a archivos XML.
- Si fuera necesario, modifique los archivos XML para seleccionar con exactitud lo que quiere importar al sitio nuevo. Al adaptar los archivos, puede importar las configuraciones de directivas y aplicaciones al sitio de 1912 LTSR por fases: algunas configuraciones ahora y otras más tarde.
- Ejecute los cmdlets de importación de PowerShell en el nuevo Controller de 1912, el cual importa las configuraciones contenidas en los archivos XML al nuevo sitio de XenApp.

Vuelva a configurar el nuevo sitio según sea necesario y, a continuación, haga pruebas en él.

Para obtener más información, consulte [Migrar XenApp 6.x](#).

## Problemas resueltos

June 27, 2024

Se han solucionado estos problemas desde Citrix Virtual Apps and Desktops 7 1912 LTSR CU8:

### Citrix Provisioning

La [documentación de Citrix Provisioning 1912 CU9](#) ofrece información específica acerca de las actualizaciones de esta versión.

### Delivery Controller

- La tarea de crear o actualizar el catálogo de máquinas falla en la zona de disponibilidad B, pero funciona bien en las zonas de disponibilidad A y C porque no se pudo iniciar una instancia de

servicio de volúmenes en su conexión a la nube. Ejecute el siguiente comando para actualizar la tabla de la base de datos de configuración del sitio para usar la nueva plantilla VolumeWorkerTemplate en el servidor SQL.

```
UPDATE HostingUnitServiceSchema.VolumeServiceConfigurationBaseTemplate  
SET TemplateId = 'ami-09b42976632b27e9b'  
WHERE RegionName = 'ap-southeast-2'
```

**Nota:** La zona de disponibilidad podría ser diferente para diferentes clientes.

[CVADHELP-24094]

- Las actualizaciones de la tabla `MonitorData.ResourceUtilization` de la base de datos de supervisión están demoradas. [CVADHELP-22724]

## Linux Virtual Delivery Agent

La documentación de Linux Virtual Delivery Agent 1912 CU9 no contiene problemas resueltos.

## Metainstalador

- Autorización de carga: si va a cargar las recopilaciones de diagnósticos en Citrix, debe tener una cuenta de Citrix o Citrix Cloud. (Estas son las credenciales que debe utilizar para acceder a las descargas de Citrix o para acceder a la central de control de Citrix Cloud.) Una vez validadas las credenciales de cuenta, se emite un token.

Si se autentica con una cuenta de Citrix o Citrix Cloud, debe hacer clic en un enlace para acceder a Citrix Cloud mediante HTTPS con su explorador web predeterminado. Después de introducir sus credenciales de Citrix Cloud, se muestra el token. Copie el token y luego péguelo en Citrix Scout. A continuación, puede seguir en el asistente de Scout.

El token se almacena localmente en la máquina que ejecuta Citrix Scout. Para habilitar el uso de este token la próxima vez que ejecute Recopilar o Rastrear y reproducir, marque la casilla Guardar el token y omitir este paso en el futuro.

Debe volver a autorizar cada vez que seleccione Programar en la página de inicio de Citrix Scout. No puede usar un token almacenado al crear o cambiar una programación.

[CVADHELP-24415]

## Profile Management

La [documentación de Profile Management 1912 CU9](#) ofrece información específica acerca de las actualizaciones de esta versión.

## Grabación de sesiones

La [documentación de Grabación de sesiones 1912 CU9](#) ofrece información específica acerca de las actualizaciones de esta versión.

## StoreFront

La [documentación de StoreFront 1912 CU9](#) ofrece información específica acerca de las actualizaciones de esta versión.

## Universal Print Server

### Impresión

- Es posible que las impresoras conectadas a Universal Print Server no aparezcan en las sesiones para imprimir. Este problema se produce cuando se actualiza el archivo `httpd.conf` de Universal Print Server. [CVADHELP-21139]
- Cuando utiliza la versión 1912 CU5 de VDA y la versión 2012 R2 del sistema operativo, se producen errores en varios trabajos de impresión desde el servidor de impresión UPS de Citrix de producción y se muestra este mensaje de error:  
`CCgpcStream::Open: WaitForMultipleObjects time out. InternalUpcRemoteOpenSt  
: Failed to Open Stream. Abort Job.`  
[CVADHELP-22354]

## VDA para SO de sesión única

### Impresión

- El intento de imprimir un archivo en impresoras locales mediante la aplicación Citrix Workspace para Mac con macOS Sonoma podría fallar y mostrarse este mensaje de error:  
`Error: Printer not activated. Error code -41`  
[CVADHELP-23839]
- Al reiniciar un VDA con las directivas de Universal Print Server habilitadas, es posible que no se inicie el equilibrio de carga de Universal Print Server. [CVADHELP-23714]
- Es posible que las impresoras locales no se redirijan a la sesión durante el primer inicio. Sin embargo, sí se redirigen durante los siguientes inicios. [CVADHELP-23334]

## Sesión/Conexión

- Es posible que `CtxSvcHost (CtxSmartCardSvc)` se cierre inesperadamente al cerrar sesión en el VDA. [CVADHELP-23172]
- Es posible que falte la clave de redirección de Microsoft Teams `MSTeamsRedirSupport` en `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream` del Registro al conectarse de nuevo a un dispositivo de usuario a través de una sesión de usuario. El problema se produce cuando aún existe una sesión RDP. [CVADHELP-19993]
- Si no se puede acceder a las impresoras o a los servidores de impresión, es posible que el inicio y el cierre de sesión tarden mucho en responder. [CVADHELP-23637]
- El proceso `WebSocketService.exe` no se inicia después de reiniciar un VDA el día bisiesto. [CVADHELP-24771]
- Microsoft Teams 2.1 no está optimizado de forma predeterminada en el VDA. [CVADHELP-24767]

## VDA para SO multisesión

### Impresión

- El intento de imprimir un archivo en impresoras locales mediante la aplicación Citrix Workspace para Mac con macOS Sonoma podría fallar y mostrarse este mensaje de error:  
`Error: Printer not activated. Error code -41`  
[CVADHELP-23839]
- Al reiniciar un VDA con las directivas de Universal Print Server habilitadas, es posible que no se inicie el equilibrio de carga de Universal Print Server. [CVADHELP-23714]
- Es posible que las impresoras locales no se redirijan a la sesión durante el primer inicio. Sin embargo, sí se redirigen durante los siguientes inicios. [CVADHELP-23334]

## Sesión/Conexión

- Si el agente de Grabación de sesiones no está instalado en el VDA y ejecuta los comandos de PowerShell `Get-BrokerSessionRecordingStatus`, `Start-BrokerSessionRecording` o `Stop-BrokerSessionRecording`, el VDA se borra del registro y se registra de nuevo en el Delivery Controller unos segundos después. Esta acción no afecta a las sesiones existentes. Si el agente de Grabación de sesiones está instalado en el VDA, los comandos de PowerShell funcionan sin problemas. [CVADHELP-23686]

- El proceso `WebSocketService.exe` puede consumir más memoria de la esperada en los VDA. [CVADHELP-23870]
- Es posible que `CtxSvcHost (CtxSmartCardSvc)` se cierre inesperadamente al cerrar sesión en el VDA. [CVADHELP-23172]
- El proceso `WebSocketService.exe` no se inicia después de reiniciar un VDA el día bisiesto. [CVADHELP-24771]

### Excepciones del sistema

- Al actualizar un VDA de 1912 LTSR CU5 a CU6, se produce una excepción irre recuperable en `Wdica.sys` y aparece una pantalla azul con un código de comprobación de errores: `0x000000CE`. [CVADHELP-22365]

## Cumulative Update 8 (CU8)

November 28, 2023

Fecha de publicación: 11 de septiembre de 2023

### Acerca de esta versión

Citrix Virtual Apps and Desktops 7 1912 LTSR Cumulative Update 8 (CU8) corrige más de 50 problemas notificados desde la publicación de 1912 LTSR CU7.

[1912 LTSR \(información general\)](#)

[1912 LTSR \(funciones e información sobre la actualización de la versión\)](#)

[Problemas resueltos desde Citrix Virtual Apps and Desktops 7 1912 LTSR CU7](#)

[Problemas conocidos en esta versión](#)

[Elementos eliminados y obsoletos](#)

[Fechas de elegibilidad de Subscription Advantage de los productos Citrix](#)

### Descargas

[Citrix Virtual Apps and Desktops 7 1912 LTSR CU8](#)

**Importante:**

Citrix License Administration Console alcanzó el final de su vida útil y el final de su desarrollo en el Servidor de licencias 11.17.2.0\_BUILD\_40000 Use [Citrix Licensing Manager](#).

## Nuevas implementaciones

¿Cómo implemento la actualización CU8 desde cero?

Puede configurar un nuevo entorno de Citrix Virtual Apps and Desktops basado en CU8 con el metainstalador de CU8. Antes de ello, le recomendamos que se familiarice con el producto:

Consulte la sección [Citrix Virtual Apps and Desktops 7 1912 LTSR \(versión inicial\)](#) y lea atentamente las secciones [Información técnica general](#), [Instalar y configurar](#) y [Proteger](#) antes de planificar la implementación. Compruebe que la configuración cumple los [requisitos del sistema](#) de todos los componentes.

## Implementaciones existentes

¿Qué actualizo?

CU8 ofrece actualizaciones de [componentes base](#) de 1912 LTSR. Recuerde: Citrix recomienda actualizar todos los componentes de LTSR de la implementación a CU8. Por ejemplo: Si Citrix Provisioning forma parte de su implementación LTSR, actualice los componentes de Citrix Provisioning a CU8. Si Citrix Provisioning no forma parte de la implementación, no necesita instalarlo ni actualizarlo.

## Componentes base de Citrix Virtual Apps and Desktops 7 1912 LTSR CU8

---

<b>Componente base de 1912 LTSR</b>	<b>Versión como se muestra en Programas y características</b>	<b>Notas</b>
VDA de sesión única	1912.0.8000	
VDA multisesión	1912.0.8000	
Delivery Controller	1912.0.8000	
Citrix Studio	1912.0.8000	
Citrix Director	1912.0.8000	
Administración de directivas de grupo de Citrix	7.24.8000	

<b>Componente base de 1912 LTSR</b>	<b>Versión como se muestra en Programas y características</b>	<b>Notas</b>
Extensión del cliente de directivas de grupo de Citrix	7.24.8000	
Citrix StoreFront	1912.0.8000	
Citrix Provisioning	1912.80.iso	
Universal Print Server	1912.0.8000	
Grabación de sesiones	1912.0.8000	
Linux VDA	1912.0.8000	Consulte la <a href="#">documentación de Linux VDA</a> para ver las plataformas compatibles.
Profile Management	1912.0.8000	
Servicio de autenticación federada de Citrix	1912.0.8000	
Redirección de contenido del explorador web	15.19.8000	

### Componentes compatibles de Citrix Virtual Apps and Desktops 7 1912 LTSR CU8

Los siguientes componentes, en las versiones que se indican a continuación, son compatibles con entornos LTSR. Estos componentes no dan derecho a las ventajas de LTSR (ciclo de vida ampliado y actualizaciones acumulativas de correcciones solamente). Citrix puede pedirle que actualice estos componentes a una versión más reciente dentro de sus entornos 1912 LTSR.

<b>Componentes y funciones compatibles</b>	<b>Versión como se muestra en Programas y características</b>
App Layering	22.11
Directivas de protección de aplicaciones	1912 LTSR CU8
HDX RealTime Optimization Pack	2.9 LTSR CU7
Servidor de licencias	11.17.2.0, compilación 44000
Capa de personalización de usuarios	23.6.2
Reproductor web de grabación de sesiones	1912.0.8000
Autoservicio de restablecimiento de contraseñas	1912.0.8000
Windows 10 de 32 bits	Consulte la <a href="#">documentación de la versión inicial</a>

Componentes y funciones compatibles	Versión como se muestra en Programas y características
Workspace Environment Management	2305
XenApp y XenDesktop 7.15 LTSR VDA (versión más reciente)*	Solo la actualización acumulativa más reciente

**Nota:**

Windows 10 de 32 bits solo es compatible durante 18 meses a partir de la publicación inicial de 1912 LTSR. Windows 10 32 de bits solo es compatible en Windows 10 Enterprise 2019 LTSC.

\* La compatibilidad con VDA de XenApp y XenDesktop 7.15 LTSR en este caso es solo para Windows 7 y Windows 2008 R2. XenApp y XenDesktop 7.15 LTSR dejará de ser compatible a partir de agosto de 2022. La compatibilidad con Citrix para Windows 7 y Windows 2008 R2 finalizará cuando Microsoft finalice el soporte para el sistema operativo o cuando finalice la compatibilidad con XenApp y XenDesktop 7.15 LTSR, lo que ocurra primero. Para obtener más información, consulte la [tabla de productos de Citrix](#).

**Versiones compatibles de la aplicación Citrix Workspace**

Todas las versiones admitidas de la aplicación Citrix Workspace son compatibles con Citrix Virtual Apps and Desktops 1912 LTSR. Para obtener información sobre el ciclo de vida de la aplicación Citrix Workspace, consulte [Lifecycle Milestones for Citrix Workspace app and Citrix Receiver](#).

Para mayor comodidad, considere la posibilidad de suscribirse al [feed RSS de la aplicación Citrix Workspace](#) para recibir una notificación cuando una nueva versión de la aplicación Citrix Workspace esté disponible.

**Exclusiones importantes de Citrix Virtual Apps and Desktops 7 1912 LTSR CU8**

Las siguientes funciones, componentes y plataformas no dan derecho a las ventajas y prestaciones del ciclo de vida de 1912 LTSR. Específicamente, se excluyen las ventajas de actualizaciones acumulativas y el ciclo de vida ampliado. Las actualizaciones de los componentes y funciones excluidos están disponibles a través de las versiones publicadas regularmente.

**Componentes y funciones excluidos**

AppDisks

AppDNA

---

## Componentes y funciones excluidos

---

Citrix SCOM Management Pack

Framehawk

Personal vDisk

Integración de StoreFront con Citrix Online

---

---

## Plataformas Windows excluidas\*

---

Windows 2008 de 32 bits (para Universal Print Server)

---

\* Citrix se reserva el derecho a actualizar el soporte que ofrece para las plataformas en función de los hitos de los ciclos de vida de los proveedores externos.

## Datos de análisis de instalación y actualización

Cuando se usa el programa de instalación del producto completo para implementar o actualizar los componentes de XenApp o XenDesktop, se recopila información anónima sobre el proceso de instalación y se guarda en la máquina donde se está realizando la instalación o actualización del componente. Esta información se utiliza para ayudar a Citrix a mejorar la experiencia de instalación de sus clientes.

## Migrar XenApp 6.5

El proceso de migración de XenApp 6.5 permite realizar una transición eficaz y rápida desde una comunidad XenApp 6.5 a un sitio con 1912 LTSR. Esta transición puede resultarle útil en caso de implementaciones que contienen una gran cantidad de aplicaciones y directivas de grupo Citrix, porque reduce el riesgo de que se produzcan errores accidentales al mover manualmente las aplicaciones y las directivas de grupo Citrix al nuevo sitio de XenApp.

Después de instalar los componentes principales de 1912 LTSR y crear un sitio, el proceso de migración sigue estos pasos:

- Ejecute el instalador de 1912 en cada servidor de trabajo de XenApp 6.5. Este instalador actualiza automáticamente el servidor a un nuevo Virtual Delivery Agent para SO de servidor listo para usar en el nuevo sitio.
- Ejecute los cmdlets de exportación de PowerShell en un Controller de XenApp 6.5, que exporta las configuraciones de aplicaciones y directivas de Citrix a archivos XML.

- Si fuera necesario, modifique los archivos XML para seleccionar con exactitud lo que quiere importar al sitio nuevo. Al adaptar los archivos, puede importar las configuraciones de directivas y aplicaciones al sitio de 1912 LTSR por fases: algunas configuraciones ahora y otras más tarde.
- Ejecute los cmdlets de importación de PowerShell en el nuevo Controller de 1912, el cual importa las configuraciones contenidas en los archivos XML al nuevo sitio de XenApp.

Vuelva a configurar el nuevo sitio según sea necesario y, a continuación, haga pruebas en él.

Para obtener más información, consulte [Migrar XenApp 6.x](#).

## Problemas resueltos

May 24, 2024

Se han solucionado estos problemas desde Citrix Virtual Apps and Desktops 7 1912 LTSR CU7:

### Citrix Director

- Una vez establecida una sesión, el nombre simplificado de la máquina que aparece en la página Detalles de la máquina en Citrix Director se revierte al nombre del grupo de entrega. [CVADHELP-18746]

### Directiva de Citrix

- Es posible que el servicio CseEngine.exe consuma más memoria que la prevista en los VDA. [CVADHELP-19226]
- El valor de la directiva sobre canales virtuales **VirtualChannelWhiteList** del parámetro HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Citrix\VCPolicies podría dañarse y no aplicarse en el VDA tras el reinicio. Este problema se produce al eliminar archivos de la carpeta C:\ProgramData\Citrix\GroupPolicy o al cortar el contenido de la carpeta y pegarlo en una ubicación diferente. [CVADHELP-21420]
- El valor de Modelado de directivas de grupo muestra el valor inhabilitado en lugar del valor real. Por ejemplo, el valor de **Límite de memoria de presentación** aparece inhabilitado, en lugar de mostrarse el valor real, 65536 KB. [CVADHELP-22484]
- Es posible que no se puedan aplicar directivas de usuario de Citrix en diferentes dominios al actualizar VDA a la versión LTSR CU7. [CVADHELP-22992]

## Citrix Provisioning

La [documentación de Citrix Provisioning 1912 CU8](#) ofrece información específica acerca de las actualizaciones de esta versión.

## Citrix Studio

- Al intentar agregar máquinas a un grupo de entrega, es posible que la página de asignación de máquinas desaparezca. Como resultado, los usuarios no aparecen asignados en la página Asignación de máquinas y las máquinas están configuradas como **Sin asignar**. [CVADHELP-20000]
- Al agregar una aplicación App-V, es posible que el campo **Entrega** aparezca en blanco. Este problema se produce cuando se agrega la aplicación y se cambia el nombre de la misma con respecto a su nombre predeterminado. [CVADHELP-21138]

## Delivery Controller

- Si la agregación de sitios o los grupos de entrega con directivas intermediarias específicas se habilitan, al iniciar una aplicación o un escritorio se crea otra sesión en lugar de conectarse de nuevo a una existente. [CVADHELP-19879]
- Cuando la memoria reservada es inferior a la memoria configurada, es posible que no se puedan encender máquinas virtuales y que aparezca este mensaje de error:

**Invalid memory setting: Memory reservation (sched.mem.min) should be equal to mem-size (94208). The virtual machine failed to start. Failed to turn on the MemSched module. Error parsing scheduler-specific configuration parameters.**

[CVADHELP-21052]

- Al intentar crear una nueva conexión de alojamiento en la máquina maestra del grupo de XenServer, el proceso puede fallar y mostrarse este mensaje de error:

**No se puede contactar con el servidor host. Compruebe que la conexión tiene una dirección de host válida y que el servidor host está encendido y funcionando correctamente.**

**No se pudo obtener la lista de hosts de XenServer.**

[CVADHELP-21320]

- Es posible que Citrix Broker Service (Brokerservice.exe) se cierre inesperadamente tras desconectarse del servidor de licencias. [CVADHELP-21615]
- Es posible que la cantidad de sesiones que se muestran en Citrix Studio y Citrix Director no coincida. Citrix Studio muestra menos sesiones activas que Citrix Director. [CVADHELP-21727]

- Es posible que algunos contadores de rendimiento XML de Citrix no se agreguen al gráfico de la pantalla de rendimiento. [CVADHELP-21785]
- Los intentos de importar la caché de host local (LHC) pueden fallar con un ID de evento 505. El problema se produce si ha agregado el valor de Registro **XmlStaTicketLifetimeInSeconds** al comando **Set-BrokerServiceConfigurationData**. [CVADHELP-22967]
- Con esta corrección, Machine Creation Services es compatible con vSAN 8. [CVADHELP-23415]

## Linux Virtual Delivery Agent

La [documentación de Linux Virtual Delivery Agent 1912 CU8](#) proporciona información específica acerca de las actualizaciones de esta versión.

## Metainstalador

- Al instalar VDA para un sistema operativo multisesión con la opción **Habilitar conexiones con una máquina de servidor** habilitada y actualizar la versión del VDA, se muestra el texto **Componentes adicionales para la imagen maestra de MCS** en el asistente de actualización, en lugar de **Componentes adicionales para habilitar conexiones con broker con servidores**.

### Nota:

Esta corrección se aplica a partir de Citrix Virtual Apps and Desktops 1912 LTSR CU8 y desde las actualizaciones de 1912 LTSR CU a 1912 LTSR CU8 y versiones posteriores. Sin embargo, la corrección no se aplica a las versiones CU de XenApp y XenDesktop 7.15 LTSR ni a las actualizaciones desde XenApp y XenDesktop 7.15 LTSR a Citrix Virtual Apps and Desktops 1912 LTSR CU.

[CVADHELP-21557]

## Optimización de Microsoft Teams

- Es posible que el servicio de redirección de vídeo HTML5 de Citrix HDX (WebSocketService.exe) se cierre de forma inesperada al utilizar Microsoft Teams. [CVADHELP-22561]

## Profile Management

La [documentación de Profile Management 1912 CU8](#) ofrece información específica acerca de las actualizaciones de esta versión.

## Grabación de sesiones

La documentación de Grabación de sesiones 1912 CU8 no contiene problemas resueltos.

## StoreFront

La [documentación de StoreFront 1912 CU8](#) ofrece información específica acerca de las actualizaciones de esta versión.

## VDA para SO de sesión única

### Instalación, desinstalación y actualización

- Después de actualizar un VDA a 1912 LTSR CUx o 2203 LTSR CUx, es posible que no se restaure el valor de **ApplicationLaunchWaitTimeoutMS** en la clave de Registro HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI. [CVADHELP-22758]

### Teclado

- En la versión 1912 CU5 de VDA que se ejecuta en las versiones 21H1 o 21H2 de Microsoft Windows 10, es posible que el teclado no esté sincronizado correctamente con el dispositivo de punto final en la sesión HDX. [CVADHELP-21534]

### Sesión/Conexión

- Es posible que no se pueda habilitar SSL en los VDA cuando la plantilla de certificado se haya creado con el **proveedor de almacenamiento de claves** como proveedor de **criptografía**. [CVADHELP-21485]
- Es posible que los sitios web internos de determinadas aplicaciones de terceros con VDA instalado no permitan el acceso sin un aviso. [CVADHELP-22081]
- Con el protocolo Enlightened Data Transport (EDT) habilitado, es posible que las sesiones de Citrix se bloqueen al actualizar el VDA de la versión 1912 LTSR CU6 a la versión 1912 LTSR CU7. [CVADHELP-23370]
- Si el agente de grabación de sesiones no está instalado en el VDA y ejecuta los comandos de PowerShell **Get-BrokerSessionRecordingStatus**, **Start-BrokerSessionRecording** y **Stop-BrokerSessionRecording**, el VDA anula el registro y vuelve a registrarse en el Delivery Controller al cabo de unos segundos. Esta acción no afecta a las sesiones existentes. Si

el agente de Grabación de sesiones está instalado en el VDA, los comandos de PowerShell funcionan sin problemas. [CVADHELP-23491]

### Tarjetas inteligentes

- Al iniciar una sesión con una tarjeta inteligente e intentar desbloquear una sesión bloqueada, es posible que reciba una solicitud para introducir una contraseña en lugar del PIN de la tarjeta inteligente. Este problema se produce al instalar el parche KB5018410 de Microsoft. [CVADHELP-21665]

### Excepciones del sistema

- Es posible que los VDA generen un código de comprobación de errores, 000000CA, si se inserta y se extrae rápidamente un dispositivo USB. [CVADHELP-21459]
- Durante el inicio de la sesión, es posible que los VDA sufran una excepción grave en la inicialización del canal virtual personalizado ControlUP y aparezca una pantalla azul. [CVADHELP-21885]
- Es posible que el servicio HTML5 Video Redirection Service (CtxHdxWebSocketService) se cierre de forma inesperada. [CVADHELP-22012]
- Es posible que el controlador de impresora universal de PDF de Citrix se cierre inesperadamente por un error en el módulo acfpdfuamd64.dll. [CVADHELP-22085]
- Los VDA podrían sufrir una excepción irrecoverable en Wdica.sys y provocar un pantallazo azul. [CVADHELP-22482]
- Es posible que el proceso del indicador de estado de los gráficos, GfxStatusIndicator.exe, se cierre repetidamente. [CVADHELP-23142]

### VDA para SO multisesión

#### Teclado

- Al abrir dos instancias de una aplicación y definir el parámetro **DisableToggler** en cinco segundos, es posible que tenga que esperar unos 30 segundos antes de poder escribir en la segunda aplicación. [CVADHELP-22491]

#### Sesión/Conexión

- Es posible que el estado de la grabación en el reproductor de Grabación de sesiones no cambie de **En directo** a **Completo** una vez completada la grabación e incluso después de cerrar sesión.

El problema se produce en Microsoft Windows 10 o en una aplicación publicada. [CVADHELP-17556]

- Es posible que no se pueda habilitar SSL en los VDA al crear la plantilla de certificados con el proveedor de almacenamiento de claves como el proveedor Criptografía. [CVADHELP-21485]
- Es posible que no se puedan abrir archivos PDF con Adobe Acrobat Reader DC en servidores de Citrix y que se muestre este mensaje de error:

#### **Werfault.exe - Application Error**

**The application was unable to start correctly (0xc0000142). Click Ok to close the application.**

[CVADHELP-21779]

- Es posible que Grabación de sesiones siga grabando a pesar de haber cerrado o desconectado la sesión. [CVADHELP-22097]
- Es posible que la sesión de usuario se actualice continuamente al iniciar una sesión de Linux que ejecute Ubuntu a través de la GUI del Subsistema de Windows para Linux (WSLg). [CVADHELP-22198]
- Al abrir dos instancias de una aplicación y definir el parámetro **DisableToggler** en cinco segundos, es posible que tenga que esperar unos 30 segundos antes de poder escribir en la segunda aplicación. [CVADHELP-22679]
- Tras actualizar un VDA de 1912 LTSR CU5 a CU6 o CU7, es posible que no se restauren los valores de **LogoffCheckerStartupDelayInSeconds** y **SeamlessFlags** en la clave de Registro HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI. [CVADHELP-22783]
- Al reconectarse a una sesión después de cambiar el valor de PPP del cliente, es posible que el nuevo valor no se aplique a la sesión. [CVADHELP-23007]
- Con el protocolo Enlightened Data Transport (EDT) habilitado, es posible que las sesiones de Citrix se bloqueen al actualizar un VDA de la versión 1912 LTSR CU6 a la versión 1912 LTSR CU7. [CVADHELP-23370]

### **Tarjetas inteligentes**

- Al iniciar una sesión con una tarjeta inteligente e intentar desbloquear una sesión bloqueada, es posible que reciba una solicitud para introducir una contraseña en lugar del PIN de la tarjeta inteligente. Este problema se produce al instalar el parche KB5018410 de Microsoft. [CVADHELP-21665]

## Excepciones del sistema

- Es posible que el proceso de Terminal Services se cierre inesperadamente por el módulo con errores, RPM.dll. [CVADHELP-21108]
- Es posible que el proceso Service Host (svchost.exe) consuma más memoria de la esperada en un VDA para SO multisesión cuando se instala el componente UiPath Remote Runtime. [CVADHELP-21678]
- Durante el inicio de la sesión, es posible que los VDA sufran una excepción grave en la inicialización del canal virtual personalizado ControlUP y aparezca una pantalla azul. [CVADHELP-21885]
- Es posible que el servicio HTML5 Video Redirection Service (CtxHdxWebSocketService) se cierre de forma inesperada. [CVADHELP-22012]
- Es posible que el controlador de impresora universal de PDF de Citrix se cierre inesperadamente por un error en el módulo acfpdfuamd64.dll. [CVADHELP-22085]
- Al actualizar un VDA de 1912 LTSR CU5 a CU6, se produce una excepción irrecoverable en Wdica.sys y aparece una pantalla azul con un código de comprobación de errores: 0x000000CE. [CVADHELP-22365]
- Los VDA podrían sufrir una excepción irrecoverable en Wdica.sys y provocar un pantallazo azul. [CVADHELP-22482]

## Cumulative Update 7 (CU7)

May 5, 2023

Fecha de publicación: 15 de marzo de 2023

### Acerca de esta versión

Citrix Virtual Apps and Desktops 7 1912 LTSR Cumulative Update 7 (CU7) corrige más de 55 problemas notificados desde la publicación de 1912 LTSR CU6.

[1912 LTSR \(información general\)](#)

[1912 LTSR \(funciones e información sobre la actualización de la versión\)](#)

[Problemas resueltos desde Citrix Virtual Apps and Desktops 7 1912 LTSR CU6](#)

[Problemas conocidos en esta versión](#)

[Elementos eliminados y obsoletos](#)

[Fechas de elegibilidad de Subscription Advantage de los productos Citrix](#)

## Descargas

[Citrix Virtual Apps and Desktops 7 1912 LTSR CU7](#)

### Importante:

Citrix License Administration Console alcanzó el final de su vida útil y el final de su desarrollo en el Servidor de licencias 11.17.2.0\_BUILD\_40000 Utilice [Citrix Licensing Manager](#).

## Nuevas implementaciones

¿Cómo implemento la actualización CU7 desde cero?

Puede configurar un nuevo entorno de Citrix Virtual Apps and Desktops basado en CU7 con el metainstalador de CU7. Antes de ello, le recomendamos que se familiarice con el producto:

Consulte la sección [Citrix Virtual Apps and Desktops 7 1912 LTSR \(versión inicial\)](#) y lea atentamente las secciones [Información técnica general](#), [Instalar y configurar](#) y [Proteger](#) antes de planificar la implementación. Compruebe que la configuración cumple los [requisitos del sistema](#) de todos los componentes.

## Implementaciones existentes

¿Qué actualizo?

CU7 ofrece actualizaciones de [componentes base](#) de 1912 LTSR. Recuerde: Citrix recomienda actualizar todos los componentes de LTSR de la implementación a CU7. Por ejemplo: Si Citrix Provisioning forma parte de su implementación LTSR, actualice los componentes de Citrix Provisioning a CU7. Si Citrix Provisioning no forma parte de la implementación, no necesita instalarlo ni actualizarlo.

## Componentes base de Citrix Virtual Apps and Desktops 7 1912 LTSR CU7

---

Componente base de 1912 LTSR	Versión como se muestra en Programas y características	Notas
VDA de sesión única	1912.0.7000	
VDA multisesión	1912.0.7000	

---

<b>Componente base de 1912 LTSR</b>	<b>Versión como se muestra en Programas y características</b>	<b>Notas</b>
Delivery Controller	1912.0.7000	
Citrix Studio	1912.0.7000	
Citrix Director	1912.0.7000	
Administración de directivas de grupo de Citrix	7.24.7000	
Extensión del cliente de directivas de grupo de Citrix	7.24.7000	
Citrix StoreFront	1912.0.7000	
Citrix Provisioning	1912.37.iso	
Universal Print Server	1912.0.7000	
Grabación de sesiones	1912.0.7000	
Linux VDA	1912.0.7000	Consulte la <a href="#">documentación de Linux VDA</a> para ver las plataformas compatibles.
Profile Management	1912.0.7000	
Servicio de autenticación federada de Citrix	1912.0.7000	
Redirección de contenido del explorador web	15.19.7000	

### Componentes compatibles de Citrix Virtual Apps and Desktops 7 1912 LTSR CU7

Los siguientes componentes, en las versiones que se indican a continuación, son compatibles con entornos LTSR. Estos componentes no dan derecho a las ventajas de LTSR (ciclo de vida ampliado y actualizaciones acumulativas de correcciones solamente). Citrix puede pedirle que actualice estos componentes a una versión más reciente dentro de sus entornos 1912 LTSR.

<b>Componentes y funciones compatibles</b>	<b>Versión como se muestra en Programas y características</b>
App Layering	22.11
Directivas de protección de aplicaciones	1912 LTSR CU7
HDX RealTime Optimization Pack	2.9 LTSR CU6

Componentes y funciones compatibles	Versión como se muestra en Programas y características
Servidor de licencias	11.17.2.0, compilación 40000
Capa de personalización de usuarios	22.11.3
Reproductor web de grabación de sesiones	1912.0.7000
Optimización de Teams	1912.12.0
Autoservicio de restablecimiento de contraseñas	1912.0.7000
Windows 10 de 32 bits	Consulte la <a href="#">documentación de la versión inicial</a>
Workspace Environment Management	2212
XenApp y XenDesktop 7.15 LTSR VDA (versión más reciente)*	Solo la actualización acumulativa más reciente

**Nota:**

Windows 10 de 32 bits solo es compatible durante 18 meses a partir de la publicación inicial de 1912 LTSR. Windows 10 32 de bits solo es compatible en Windows 10 Enterprise 2019 LTSC.

\* La compatibilidad con VDA de XenApp y XenDesktop 7.15 LTSR en este caso es solo para Windows 7 y Windows 2008 R2. XenApp y XenDesktop 7.15 LTSR dejará de ser compatible a partir de agosto de 2022. La compatibilidad con Citrix para Windows 7 y Windows 2008 R2 finalizará cuando Microsoft finalice el soporte para el sistema operativo o cuando finalice la compatibilidad con XenApp y XenDesktop 7.15 LTSR, lo que ocurra primero. Para obtener más información, consulte la [tabla de productos de Citrix](#).

**Versiones compatibles de la aplicación Citrix Workspace**

Todas las versiones admitidas de la aplicación Citrix Workspace son compatibles con Citrix Virtual Apps and Desktops 1912 LTSR. Para obtener información sobre el ciclo de vida de la aplicación Citrix Workspace, consulte [Lifecycle Milestones for Citrix Workspace app and Citrix Receiver](#).

Para mayor comodidad, considere la posibilidad de suscribirse al [feed RSS de la aplicación Citrix Workspace](#) para recibir una notificación cuando una nueva versión de la aplicación Citrix Workspace esté disponible.

**Exclusiones importantes de Citrix Virtual Apps and Desktops 7 1912 LTSR CU7**

Las siguientes funciones, componentes y plataformas no dan derecho a las ventajas y prestaciones del ciclo de vida de 1912 LTSR. Específicamente, se excluyen las ventajas de actualizaciones acumula-

tivas y el ciclo de vida ampliado. Las actualizaciones de los componentes y funciones excluidos están disponibles a través de las versiones publicadas regularmente.

---

### **Componentes y funciones excluidos**

---

AppDisks

AppDNA

Citrix SCOM Management Pack

Framehawk

Personal vDisk

Integración de StoreFront con Citrix Online

---

---

### **Plataformas Windows excluidas\***

---

Windows 2008 de 32 bits (para Universal Print Server)

---

\* Citrix se reserva el derecho a actualizar el soporte que ofrece para las plataformas en función de los hitos de los ciclos de vida de los proveedores externos.

### **Datos de análisis de instalación y actualización**

Cuando se usa el programa de instalación del producto completo para implementar o actualizar los componentes de XenApp o XenDesktop, se recopila información anónima sobre el proceso de instalación y se guarda en la máquina donde se está realizando la instalación o actualización del componente. Esta información se utiliza para ayudar a Citrix a mejorar la experiencia de instalación de sus clientes.

### **Migrar XenApp 6.5**

El proceso de migración de XenApp 6.5 permite realizar una transición eficaz y rápida desde una comunidad XenApp 6.5 a un sitio con 1912 LTSR. Esta transición puede resultarle útil en caso de implementaciones que contienen una gran cantidad de aplicaciones y directivas de grupo Citrix, porque reduce el riesgo de que se produzcan errores accidentales al mover manualmente las aplicaciones y las directivas de grupo Citrix al nuevo sitio de XenApp.

Después de instalar los componentes principales de 1912 LTSR y crear un sitio, el proceso de migración sigue estos pasos:

- Ejecute el instalador de 1912 en cada servidor de trabajo de XenApp 6.5. Este instalador actualiza automáticamente el servidor a un nuevo Virtual Delivery Agent para SO de servidor listo para usar en el nuevo sitio.
- Ejecute los cmdlets de exportación de PowerShell en un Controller de XenApp 6.5, que exporta las configuraciones de aplicaciones y directivas de Citrix a archivos XML.
- Si fuera necesario, modifique los archivos XML para seleccionar con exactitud lo que quiere importar al sitio nuevo. Al adaptar los archivos, puede importar las configuraciones de directivas y aplicaciones al sitio de 1912 LTSR por fases: algunas configuraciones ahora y otras más tarde.
- Ejecute los cmdlets de importación de PowerShell en el nuevo Controller de 1912, el cual importa las configuraciones contenidas en los archivos XML al nuevo sitio de XenApp.

Vuelva a configurar el nuevo sitio según sea necesario y, a continuación, haga pruebas en él.

Para obtener más información, consulte [Migrar XenApp 6.x](#).

## Problemas resueltos

June 19, 2023

Se han solucionado estos problemas desde Citrix Virtual Apps and Desktops 7 1912 LTSR CU6:

### Citrix Director

- Cuando se instalan un VDA y un Delivery Controller en la misma máquina, es posible que el VDA no sea visible en la vista **Filtro > Máquinas > Todas las máquinas** de Citrix Director. [CVADHELP-20271]

### Directiva de Citrix

- Con esta corrección, se han solucionado varios problemas de memoria. [ CVADHELP-19916, CVADHELP-20908, CVADHELP-20909]
- El valor de configuración de la directiva puede aparecer como **Kpbs**, en lugar de **Kbps**. [CVADHELP-21527]

### Citrix Provisioning

La [documentación de Citrix Provisioning 1912 CU7](#) ofrece información específica acerca de las actualizaciones de esta versión.

## Citrix Studio

- Al intentar crear un nuevo sitio de Citrix Virtual Apps and Desktops con los permisos DBCreator, Securityadmin y Public desde la consola de Citrix Studio, la operación puede fallar. [CVADHELP-20594]

## Delivery Controller

- Si algunos controladores de dominio están apagados, es posible que Citrix Studio muestre los identificadores de seguridad (SID) de las máquinas en lugar de los nombres de las cuentas. [CVADHELP-19312]

## Linux Virtual Delivery Agent

La [documentación de Linux Virtual Delivery Agent 1912 CU7](#) proporciona información específica acerca de las actualizaciones de esta versión.

## Licencias

- Es posible que Citrix Studio (complemento de PowerShell para administración de licencias) no pueda comunicarse con los servidores de licencias cuando se permitan conjuntos de cifrado seguros. [CVADHELP-20056]

## Optimización de Microsoft Teams

- Es posible que las llamadas de Microsoft Teams se desconecten poco después de la conexión inicial. [CVADHELP-20042]
- Es posible que el servicio HTML5 Video Redirection Service (CtxHdxWebSocketService) se cierre de forma inesperada. [CVADHELP-21074]

## Profile Management

La [documentación de Profile Management 1912 CU7](#) ofrece información específica acerca de las actualizaciones de esta versión.

## Problemas de seguridad

- Esta corrección soluciona un problema de seguridad. Para obtener más información, consulte el artículo [CTX559370](#) de Knowledge Center.

## Grabación de sesiones

La documentación de Grabación de sesiones 1912 CU7 no contiene problemas resueltos.

## StoreFront

La [documentación de StoreFront 1912 CU7](#) ofrece información específica acerca de las actualizaciones de esta versión.

## Universal Print Server

### Servidor

- Al intentar imprimir un documento desde Citrix Universal Print Server en impresoras de sesión compartida, la operación puede fallar. El problema se produce después de actualizar a Citrix Virtual Apps and Desktops 1912 LTSR CU4. [CVADHELP-19431]

## VDA para SO de sesión única

### Teclado

- Es posible que el teclado virtual no aparezca automáticamente en una aplicación publicada al colocar el cursor en un campo modificable. [CVADHELP-21419]

## Sesión/Conexión

- Cuando la funcionalidad seguridad basada en virtualización (VBS) está activada, al acceder a una estación de trabajo con acceso con Remote PC a través de un dispositivo de usuario y, a continuación, desconectar, es posible que aparezca una pantalla en negro al establecer contacto físicamente con la estación de trabajo e iniciar sesión en el sistema. [CVADHELP-20342]
- Los intentos de volver a conectarse a una sesión pueden fallar. [CVADHELP-20439]
- Es posible que el proceso de gráficos de software de Citrix (Ctxgfx.exe) se cierre de forma inesperada cuando la directiva de **marcas de agua de sesión** esté habilitada en el VDA. [CVADHELP-20607]
- Al tomar el control de la sesión de usuario actualmente conectada desde una consola local de un VDA físico, es posible que todas o algunas de las pantallas que están conectadas al VDA físico permanezcan en modo de ahorro de energía. [CVADHELP-20619]

- Durante la reconexión de una sesión, el indicador de estado de la batería puede desaparecer si el cable de alimentación está enchufado. [CVADHELP-20768]
- Al conectar un monitor, la ventana integrada puede desaparecer. [CVADHELP-21084]
- Con la versión más reciente de Chrome, la extensión de redirección de contenido del explorador puede fallar y provocar que la llamada de Microsoft Teams optimizado se desconecte. [CVADHELP-21336]

### Excepciones del sistema

- Es posible que los VDA sufran una excepción irrecuperable y muestren una pantalla azul cuando se desconecte y vuelva a conectar una sesión que utiliza el protocolo Enlightened Data Transport (EDT). [CVADHELP-20293]
- El proceso wfshell.exe puede cerrarse de manera imprevista debido a un error en el módulo CtxUiMon.dll. [CVADHELP-20312]
- Si Microsoft Azure Information Protection (AIP) está instalado y Citrix Hook está habilitado, es posible que las aplicaciones de Microsoft 365 se cierren de manera imprevista. [CVADHELP-20642]
- Es posible que el servicio CseEngine.exe consuma más memoria que la prevista en los VDA. [CVADHELP-20909]
- Al iniciar un escritorio publicado, abrir el **Explorador de archivos** y hacer clic en la unidad C local redirigida en **Red >\ Cliente**, es posible que el **Explorador de archivos** se cierre de manera imprevista. [CVADHELP-21089]
- Los VDA podrían sufrir una excepción irrecuperable en tdica.sys y provocar un pantallazo azul. El problema se produce al intentar volver a conectarse a una sesión. [CVADHELP-21318]

### Experiencia de usuario

- Al iniciar sesión desde Citrix Gateway cuando el **atributo de nombre del SSO de LDAP** está establecido en **UserPrincipalName**, es posible que la marca de agua de Citrix muestre el nombre de inicio de sesión de forma incorrecta. [CVADHELP-21815]

### VDA para SO multisesión

#### Teclado

- Es posible que el teclado virtual no aparezca automáticamente en una aplicación publicada al colocar el cursor en un campo modificable. [CVADHELP-21419]

## Impresión

- En los clientes Mac, es posible que el tamaño de papel predeterminado de la impresora no se conserve después de cerrar sesión y volver a iniciarla. [CVADHELP-21161]

## Sesión/Conexión

- Al iniciar una aplicación desde un VDA como usuario anónimo, puede aparecer un mensaje de error que indica lo siguiente:

### **Nombre de usuario y contraseña incorrectos.**

[CVADHELP-19802]

- El protector de pantalla puede aparecer en una sesión reconectada desde una aplicación publicada integrada a través de un VDA que tenga habilitado el protector de pantalla. [CVADHELP-20431]
- Con esta corrección, puede usar comodines en la ruta del proceso mientras agrega canales virtuales a la lista de permitidos. Para obtener más información, consulte la documentación sobre Seguridad de canales virtuales. [CVADHELP-20478]
- Durante la reconexión de una sesión, el indicador de estado de la batería puede desaparecer si el cable de alimentación está enchufado. [CVADHELP-20768]
- Es posible que los VDA dejen de responder cuando RPM demore un proceso de cierre de sesión al no liberar el bloqueo como es debido. [CVADHELP-20892]
- Es posible que la función Lista de canales virtuales permitidos no funcione en Microsoft Teams. [CVADHELP-21287]
- Con la versión más reciente de Chrome, la extensión de redirección de contenido del explorador puede fallar y provocar que la llamada de Microsoft Teams optimizado se desconecte. [CVADHELP-21336]

## Excepciones del sistema

- El proceso wfshell.exe puede cerrarse de manera imprevista debido a un error en el módulo CtxUiMon.dll. [CVADHELP-20312]
- Es posible que el servicio CseEngine.exe consuma más memoria que la prevista en los VDA. [CVADHELP-20909]
- Al iniciar un escritorio publicado, abrir el **Explorador de archivos** y hacer clic en la unidad C local redirigida en **Red >\ Cliente**, es posible que el **Explorador de archivos** se cierre de manera imprevista. [CVADHELP-21089]

## Experiencia de usuario

- Al iniciar sesión desde Citrix Gateway cuando el **atributo de nombre del SSO de LDAP** está establecido en **UserPrincipalName**, es posible que la marca de agua de Citrix muestre el nombre de inicio de sesión de forma incorrecta. [CVADHELP-21815]

## Cumulative Update 6 (CU6)

December 15, 2022

Fecha de publicación: 31 de octubre de 2022

### Acerca de esta versión

Citrix Virtual Apps and Desktops 7 1912 LTSR Cumulative Update 6 (CU6) corrige más de 35 problemas notificados desde la publicación de 1912 LTSR CU5.

[1912 LTSR \(información general\)](#)

[1912 LTSR \(funciones e información sobre la actualización de la versión\)](#)

[Problemas resueltos desde Citrix Virtual Apps and Desktops 7 1912 LTSR CU5](#)

[Problemas conocidos en esta versión](#)

[Elementos eliminados y obsoletos](#)

[Fechas de elegibilidad de Subscription Advantage de los productos Citrix](#)

### Descargas

[Citrix Virtual Apps and Desktops 7 1912 LTSR CU6](#)

#### Importante:

Citrix License Administration Console alcanzó el final de su vida útil y el final de su desarrollo en el Servidor de licencias 11.17.2.0\_BUILD\_37000. Utilice [Citrix Licensing Manager](#).

### Nuevas implementaciones

¿Cómo implemento la actualización CU6 desde cero?

Puede configurar un nuevo entorno de Citrix Virtual Apps and Desktops basado en CU6 con el metainstalador de CU6. Antes de ello, le recomendamos que se familiarice con el producto:

Consulte la sección [Citrix Virtual Apps and Desktops 7 1912 LTSR \(versión inicial\)](#) y lea atentamente las secciones [Información técnica general](#), [Instalar y configurar](#) y [Proteger](#) antes de planificar la implementación. Compruebe que la configuración cumple los [requisitos del sistema](#) de todos los componentes.

## Implementaciones existentes

¿Qué actualizo?

CU6 ofrece actualizaciones de [componentes base](#) de 1912 LTSR. Recuerde: Citrix recomienda actualizar todos los componentes de LTSR de la implementación a CU6. Por ejemplo: Si Citrix Provisioning forma parte de su implementación LTSR, actualice los componentes de Citrix Provisioning a CU6. Si Citrix Provisioning no forma parte de la implementación, no necesita instalarlo ni actualizarlo.

## Componentes base de Citrix Virtual Apps and Desktops 7 1912 LTSR CU6

<b>Componente base de 1912 LTSR</b>	<b>Versión como se muestra en Programas y características</b>	<b>Notas</b>
VDA de sesión única	1912.0.6000	
VDA multisesión	1912.0.6000	
Delivery Controller	1912.0.6000	
Citrix Studio	1912.0.6000	
Citrix Director	1912.0.6000	
Administración de directivas de grupo de Citrix	7.24.6000	
Extensión del cliente de directivas de grupo de Citrix	7.24.6000	
Citrix StoreFront	1912.0.6000	
Citrix Provisioning	1912.31.iso	
Universal Print Server	1912.0.6000	
Grabación de sesiones	1912.0.6000	

<b>Componente base de 1912 LTSR</b>	<b>Versión como se muestra en Programas y características</b>	<b>Notas</b>
Linux VDA	1912.0.6000	Consulte la <a href="#">documentación de Linux VDA</a> para ver las plataformas compatibles.
Profile Management	1912.0.6000	
Servicio de autenticación federada de Citrix	1912.0.6000	
Redirección de contenido del explorador web	15.19.6000	
Citrix Probe Agent	2009	<a href="#">Descargas</a>

### Componentes compatibles de Citrix Virtual Apps and Desktops 7 1912 LTSR CU6

Los siguientes componentes, en las versiones que se indican a continuación, son compatibles con entornos LTSR. Estos componentes no dan derecho a las ventajas de LTSR (ciclo de vida ampliado y actualizaciones acumulativas de correcciones solamente). Citrix puede pedirle que actualice estos componentes a una versión más reciente dentro de sus entornos 1912 LTSR.

<b>Componentes y funciones compatibles</b>	<b>Versión como se muestra en Programas y características</b>
App Layering	22.08
Directivas de protección de aplicaciones	1912 LTSR CU6
HDX RealTime Optimization Pack	2.9 LTSR CU5
Servidor de licencias	11.17.2.0, compilación 40000
Capa de personalización de usuarios	22.6.1
Reproductor web de grabación de sesiones	1912.0.6000
Optimización de Teams	1912.0.0
Autoservicio de restablecimiento de contraseñas	1912.0.6000
Windows 10 de 32 bits	Consulte la <a href="#">documentación de la versión inicial</a>
Workspace Environment Management	2206
XenApp y XenDesktop 7.15 LTSR VDA (versión más reciente)*	Solo la actualización acumulativa más reciente

**Nota:**

Windows 10 de 32 bits solo es compatible durante 18 meses a partir de la publicación inicial de 1912 LTSR. Windows 10 32 de bits solo es compatible en Windows 10 Enterprise 2019 LTSC.

\* La compatibilidad con VDA de XenApp y XenDesktop 7.15 LTSR en este caso es solo para Windows 7 y Windows 2008 R2. XenApp y XenDesktop 7.15 LTSR dejará de ser compatible a partir de agosto de 2022. La compatibilidad con Citrix para Windows 7 y Windows 2008 R2 finalizará cuando Microsoft finalice el soporte para el sistema operativo o cuando finalice la compatibilidad con XenApp y XenDesktop 7.15 LTSR, lo que ocurra primero. Para obtener más información, consulte la [tabla de productos de Citrix](#).

## **Versiones compatibles de la aplicación Citrix Workspace**

Todas las versiones admitidas de la aplicación Citrix Workspace son compatibles con Citrix Virtual Apps and Desktops 1912 LTSR. Para obtener información sobre el ciclo de vida de la aplicación Citrix Workspace, consulte [Lifecycle Milestones for Citrix Workspace app and Citrix Receiver](#).

Para mayor comodidad, considere la posibilidad de suscribirse al [feed RSS de la aplicación Citrix Workspace](#) para recibir una notificación cuando una nueva versión de la aplicación Citrix Workspace esté disponible.

## **Exclusiones importantes de Citrix Virtual Apps and Desktops 7 1912 LTSR CU6**

Las siguientes funciones, componentes y plataformas no dan derecho a las ventajas y prestaciones del ciclo de vida de 1912 LTSR. Específicamente, se excluyen las ventajas de actualizaciones acumulativas y el ciclo de vida ampliado. Las actualizaciones de los componentes y funciones excluidos están disponibles a través de las versiones publicadas regularmente.

---

### **Componentes y funciones excluidos**

---

AppDisks

AppDNA

Citrix SCOM Management Pack

Framehawk

Personal vDisk

Integración de StoreFront con Citrix Online

---

---

## Plataformas Windows excluidas\*

---

Windows 2008 de 32 bits (para Universal Print Server)

---

\* Citrix se reserva el derecho a actualizar el soporte que ofrece para las plataformas en función de los hitos de los ciclos de vida de los proveedores externos.

## Datos de análisis de instalación y actualización

Cuando se usa el programa de instalación del producto completo para implementar o actualizar los componentes de XenApp o XenDesktop, se recopila información anónima sobre el proceso de instalación y se guarda en la máquina donde se está realizando la instalación o actualización del componente. Esta información se utiliza para ayudar a Citrix a mejorar la experiencia de instalación de sus clientes.

## Migrar XenApp 6.5

El proceso de migración de XenApp 6.5 permite realizar una transición eficaz y rápida desde una comunidad XenApp 6.5 a un sitio con 1912 LTSR. Esta transición puede resultarle útil en caso de implementaciones que contienen una gran cantidad de aplicaciones y directivas de grupo Citrix, porque reduce el riesgo de que se produzcan errores accidentales al mover manualmente las aplicaciones y las directivas de grupo Citrix al nuevo sitio de XenApp.

Después de instalar los componentes principales de 1912 LTSR y crear un sitio, el proceso de migración sigue estos pasos:

- Ejecute el instalador de 1912 en cada servidor de trabajo de XenApp 6.5. Este instalador actualiza automáticamente el servidor a un nuevo Virtual Delivery Agent para SO de servidor listo para usar en el nuevo sitio.
- Ejecute los cmdlets de exportación de PowerShell en un Controller de XenApp 6.5, que exporta las configuraciones de aplicaciones y directivas de Citrix a archivos XML.
- Si fuera necesario, modifique los archivos XML para seleccionar con exactitud lo que quiere importar al sitio nuevo. Al adaptar los archivos, puede importar las configuraciones de directivas y aplicaciones al sitio de 1912 LTSR por fases: algunas configuraciones ahora y otras más tarde.
- Ejecute los cmdlets de importación de PowerShell en el nuevo Controller de 1912, el cual importa las configuraciones contenidas en los archivos XML al nuevo sitio de XenApp.

Vuelva a configurar el nuevo sitio según sea necesario y, a continuación, haga pruebas en él.

Para obtener más información, consulte [Migrar XenApp 6.x](#).

## Problemas resueltos

March 21, 2023

Se han solucionado estos problemas desde Citrix Virtual Apps and Desktops 7 1912 LTSR CU5:

### Citrix Director

- En Citrix Director, es posible que la página **Detalles de la sesión** muestre directivas aplicadas dos veces si las directivas tienen definidos parámetros de equipo y de usuario. [CVADHELP-19205]

### Directiva de Citrix

- Tras actualizar la versión 1912 LTSR CU3 de Citrix Virtual Apps and Desktops a la versión CU4 o CU5, es posible que los VDA no se registren en Delivery Controller y que permanezcan sin registrarse. [CVADHELP-19834]
- Es posible que se genere una consulta de DNS incorrecta cuando CseEngine.exe busca un objeto de directiva de grupo (GPO). [CVADHELP-20361]

### Citrix Provisioning

La [documentación de Citrix Provisioning 1912 CU6](#) ofrece información específica acerca de las actualizaciones de esta versión.

### Citrix Studio

- Es posible que no se puedan crear conexiones de host con Azure en Citrix Studio debido a una excepción. [CVADHELP-18741]
- Es posible que las operaciones que impliquen catálogos de máquinas en Citrix Studio, como el acceso, la creación, la eliminación o la enumeración de catálogos, sean lentas. Este problema se produce si se utiliza un hipervisor de Nutanix para alojar la conexión. [CVADHELP-19652]

### Delivery Controller

- Citrix Broker Service (Brokerservice.exe) podría dejar de responder y desconectarse. [CVADHELP-16352]

- Después de actualizar XenApp y XenDesktop 7.6 a XenApp y XenDesktop 7.15 LTSR CU6 o a una versión posterior, o bien a Citrix Virtual Apps and Desktops 1912 LTSR y crear un catálogo de Machine Creation Services (MCS), es posible que la opción **Tamaño de caché en disco (GB)** esté inhabilitada y no pueda habilitarse. Para habilitar la solución, reinicie el servicio de host y abra Citrix Studio de nuevo tras la actualización de DBSchema. [CVADHELP-17705]
- Al actualizar un catálogo de Machine Creation Services, si selecciona la máquina virtual y, a continuación, la instantánea correspondiente, puede aparecer este mensaje de error:

**Se ha producido un error inesperado. Póngase en contacto con la asistencia técnica de Citrix.**

[CVADHELP-17794]

- Es posible que no se puedan encender máquinas después de restaurar la conexión con System Center Virtual Machine Manager (SCVMM). [CVADHELP-18400]
- Es posible que Citrix Broker Service (Brokerservice.exe) se cierre de forma inesperada por un error en el módulo LicPolEng.dll. [CVADHELP-19674]
- Al usar una dirección IP estática para crear una máquina VDA con versión 2203 LTSR a partir de una imagen maestra, es posible que Machine Creation Services (MCS) no habilite DHCP durante la preparación de la imagen. [CVADHELP-19892]
- Durante la actualización de una máquina virtual de la versión 1912 LTSR a la versión 1912 LTSR CU2, no se puede iniciar sesión en la máquina con las credenciales de dominio tras el primer reinicio. Sin embargo, sí se puede iniciar sesión correctamente después del reinicio posterior. [CVADHELP-19900]
- Con esta corrección, se asignan nombres únicos a los discos base. [CVADHELP-19938]
- Es posible que Delivery Controller experimente un uso elevado de la CPU. Como resultado, el estado de alimentación de los VDA se muestra como desconocido. [CVADHELP-20061]
- Tras actualizar Delivery Controller a la versión 1912 CU5, es posible que el reinicio programado no funcione correctamente con los VDA que no tienen administración de energía. [CVADHELP-20138]

## Linux Virtual Delivery Agent

La documentación de Linux Virtual Delivery Agent 1912 CU6 no contiene problemas resueltos.

## Profile Management

La [documentación de Profile Management 1912 CU6](#) ofrece información específica acerca de las actualizaciones de esta versión.

## Grabación de sesiones

La documentación de Grabación de sesiones 1912 CU6 no contiene problemas resueltos.

## StoreFront

La [documentación de StoreFront 1912 CU6](#) ofrece información específica acerca de las actualizaciones de esta versión.

## VDA para SO de sesión única

### Teclado

- Es posible que el atajo de teclado Ctrl+Inter no funcione en las sesiones abiertas con la aplicación Citrix Workspace para Linux. [CVADHELP-19043]
- Es posible que un mouse para zurdos con el botón principal configurado en la **izquierda** en el dispositivo del usuario y el VDA no funcione como es debido. [CVADHELP-19444]

### Sesión/Conexión

- Cuando el Reproductor de Windows Media pasa de la pista actual a la pista siguiente de la lista de reproducción, es posible que el audio no se reproduzca al principio de la pista siguiente. El problema se produce si la redirección de Windows Media está habilitada. [CVADHELP-17876]
- Es posible que se cancele el registro de las máquinas debido a un interbloqueo en Broker Agent y que permanezcan sin registrarse. [CVADHELP-18952]
- Al conectar o desconectar un monitor, es posible que la ventana integrada aparezca en una posición incorrecta. [CVADHELP-19168]
- Es posible que se asignen dos agentes VDA en lugar de uno a un solo usuario. [CVADHELP-19700]
- Es posible que los datos de HDX Insights no se actualicen para las sesiones de usuario en el VDA de acceso con Remote PC después de la reconexión. Como consecuencia, Citrix ADM informa de una cantidad de conexiones inferior a la real. [CVADHELP-19762]
- Es posible que no se puedan iniciar sesiones mientras se utiliza el conjunto de cifrado **TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384**. [CVADHELP-19796]
- Al salir de una sesión, es posible que el servidor deje de responder. El problema se produce por el bucle infinito presente en icausbbsys. [CVADHELP-19814]

- Es posible que el servicio de audio de Windows no se inicie automáticamente al instalar Virtual Delivery Agent mediante el parámetro de la línea de comandos `servervdi`. Este mensaje de error aparece en el área de notificaciones:

**The Audio Service is not running.**

[CVADHELP-19823]

- Es posible que el servicio Citrix HDX HTML5 Video Redirection Service (WebSocketService.exe) provoque una pérdida de sesión al usar Microsoft Teams optimizado para Citrix HDX. [CVADHELP-20058]
- Al conectarse de nuevo a una aplicación publicada, es posible que se inicien dos aplicaciones publicadas y que Delivery Controller muestre el estado de la aplicación como Aplicación no ejecutada. [CVADHELP-20476]

### Excepciones del sistema

- Un error en CTXCDF puede provocar que el servicio de proveedores para la extensión Instrumental de administración de Windows (WMIPRVSE.exe) se detenga y genere el ID de evento 5612 en el registro de eventos. [CVADHELP-17425]
- Es posible que el proceso WebSocketService.exe se cierre de forma inesperada y provoque un error en las llamadas de Microsoft Teams con este mensaje de error:

**Still connecting to remote devices. Calling isn't available yet.**

[CVADHELP-17758]

- Es posible que el proceso de PicaVcHost.exe sufra una infracción de acceso y se cierre de forma inesperada. [CVADHELP-18387]
- Es posible que no se puedan iniciar sesiones y que se muestre una pantalla gris. [CVADHELP-19232]

### VDA para SO multisesión

#### Teclado

- Es posible que un mouse para zurdos con el botón principal configurado en la **izquierda** en el dispositivo del usuario y el VDA no funcione como es debido. [CVADHELP-19444]

#### Sesión/Conexión

- Es posible que se cancele el registro de las máquinas debido a un interbloqueo en Broker Agent y que permanezcan sin registrarse. [CVADHELP-18952]

- Al reproducir un vídeo con el Reproductor de Windows Media, es posible que los registros de eventos de canales virtuales personalizados no se muestren en el Visor de eventos. Esto puede ocurrir cuando la directiva de la lista de canales virtuales permitidos está habilitada y el conjunto de valores está vacío. [CVADHELP-19525]
- Es posible que el permiso de TermService en la clave del Registro HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ no se restaure durante la instalación de un VDA en Citrix Virtual Apps and Desktops 1912 CU, lo que provocaría errores en las sesiones. [CVADHELP-19546]
- Es posible que los datos de **HDX Insights** no se actualicen para las sesiones de usuario en el VDA de acceso con Remote PC después de la reconexión. Como consecuencia, Citrix ADM informa de una cantidad de conexiones inferior a la real. [CVADHELP-19762]
- Al salir de una sesión, es posible que el servidor deje de responder. El problema se produce por el bucle infinito presente en icausbbsys. [CVADHELP-19814]
- Al conectarse de nuevo a una aplicación publicada, es posible que se inicien dos aplicaciones publicadas y que Delivery Controller muestre el estado de la aplicación como Aplicación no ejecutada. [CVADHELP-20476]

### Excepciones del sistema

- Un error en CTXCDF puede provocar que el servicio de proveedores para la extensión Instrumental de administración de Windows (WMIPRVSE.exe) se detenga y genere el ID de evento 5612 en el registro de eventos. [CVADHELP-17425]
- Es posible que no se puedan iniciar sesiones y que se muestre una pantalla gris. [CVADHELP-19232]
- Al utilizar la reconexión automática de clientes (ACR) en VDA con SO multisesión, es posible que Citrix Audio Redirection Service se cierre de forma inesperada. [CVADHELP-19694]
- Es posible que los VDA sufran una excepción irre recuperable en picavc.sys o picadm.sys y que se produzca un pantallazo azul. [CVADHELP-19897]

### Componentes de escritorio virtual: Otros

- Es posible que no se puedan iniciar aplicaciones de App-V en máquinas no persistentes si la caché de App-V se redirige a la unidad persistente. [CVADHELP-19125]
- La creación de aplicaciones de App-V mediante el método de administración única en Citrix Studio provoca aplicaciones duplicadas en los paquetes de App-V. Esto ralentiza la enumeración de aplicaciones. El problema se produce después de actualizar la versión CU2 de Citrix Virtual Apps and Desktops 1912 LTSR a CU4. La creación de aplicaciones de App-V mediante el método

de administración única en Citrix Studio provoca aplicaciones duplicadas en los paquetes de App-V. Esto ralentiza la enumeración de aplicaciones. El problema se produce después de actualizar la versión CU2 de Citrix Virtual Apps and Desktops 1912 LTSR a CU4. [CVADHELP-19603]

## Cumulative Update 5 (CU5)

March 10, 2022

Fecha de publicación: 9 de marzo de 2022

### Acerca de esta versión

Citrix Virtual Apps and Desktops 7 1912 LTSR Cumulative Update 5 (CU5) corrige más de 60 problemas notificados desde la publicación de 1912 LTSR CU4.

[1912 LTSR \(información general\)](#)

[1912 LTSR \(funciones e información sobre la actualización de la versión\)](#)

[Problemas resueltos desde Citrix Virtual Apps and Desktops 7 1912 LTSR CU4](#)

[Problemas conocidos en esta versión](#)

[Elementos eliminados y obsoletos](#)

[Fechas de elegibilidad de Subscription Advantage de los productos Citrix](#)

### Descargas

[Citrix Virtual Apps and Desktops 7 1912 LTSR CU5](#)

#### Importante:

Citrix License Administration Console alcanzó el final de su vida útil y el final de su desarrollo en el Servidor de licencias 11.17.2.0\_BUILD\_37000. Utilice [Citrix Licensing Manager](#).

### Nuevas implementaciones

¿Cómo implemento la actualización CU5 desde cero?

Puede configurar un nuevo entorno de Citrix Virtual Apps and Desktops basado en CU5 con el metainstalador de CU5. Antes de ello, le recomendamos que se familiarice con el producto:

Consulte la sección [Citrix Virtual Apps and Desktops 7 1912 LTSR \(versión inicial\)](#) y lea atentamente las secciones [Información técnica general](#), [Instalar y configurar](#) y [Proteger](#) antes de planificar la implementación. Compruebe que la configuración cumple los [requisitos del sistema](#) de todos los componentes.

## Implementaciones existentes

¿Qué actualizo?

CU5 ofrece actualizaciones de componentes base de 1912 LTSR. Recuerde: Citrix recomienda actualizar todos los componentes de LTSR de la implementación a CU5. Por ejemplo: Si Citrix Provisioning forma parte de su implementación LTSR, actualice los componentes de Citrix Provisioning a CU5. Si Citrix Provisioning no forma parte de la implementación, no necesita instalarlo ni actualizarlo.

## Componentes base de Citrix Virtual Apps and Desktops 7 1912 LTSR CU5

Componente base de 1912 LTSR	Versión como se muestra en Programas y características	Notas
VDA de sesión única	1912.0.5000	
VDA multisesión	1912.0.5000	
Delivery Controller	1912.0.5000	
Citrix Studio	1912.0.5000	
Citrix Director	1912.0.5000	
Administración de Directivas de grupo Citrix	7.24.5000	
Extensión del cliente de Directivas de grupo Citrix	7.24.5000	
Citrix StoreFront	1912.0.5000	
Citrix Provisioning	1912.0.25	
Universal Print Server	1912.0.5000	
Grabación de sesiones	1912.0.5000	
Linux VDA	1912.0.5000	Consulte la <a href="#">documentación de Linux VDA</a> para ver las plataformas compatibles.
Profile Management	1912.0.5000	

<b>Componente base de 1912 LTSR</b>	<b>Versión como se muestra en Programas y características</b>	<b>Notas</b>
Servicio de autenticación federada de Citrix	1912.0.5000	
Redirección de contenido de explorador web	15.19.5000	
Citrix Probe Agent	2006	<a href="#">Descargar</a>

### Componentes compatibles de Citrix Virtual Apps and Desktops 7 1912 LTSR CU5

Los siguientes componentes, en las versiones que se indican a continuación, son compatibles con entornos LTSR. Estos componentes no dan derecho a las ventajas de LTSR (ciclo de vida ampliado y actualizaciones acumulativas de correcciones solamente). Citrix puede pedirle que actualice estos componentes a una versión más reciente dentro de sus entornos 1912 LTSR.

<b>Componentes y funciones compatibles</b>	<b>Versión como se muestra en Programas y características</b>
App Layering	21.07.0
Directivas de protección de aplicaciones	1912.0.0
HDX RealTime Optimization Pack	2.9 LTSR CU4
Servidor de licencias	11.17.2.0, compilación 37000
Capa de personalización de usuarios	21.12.2
Reproductor web de grabación de sesiones	1912.0.0
Optimización de Teams	1912.0.0
Autoservicio de restablecimiento de contraseñas	1.1
Windows 10 de 32 bits	Consulte la <a href="#">documentación de la versión inicial</a>
Workspace Environment Management	2112
XenApp y XenDesktop 7.15 LTSR VDA (versión más reciente)*	Solo la actualización acumulativa más reciente

#### **Nota:**

Windows 10 de 32 bits solo es compatible durante 18 meses a partir de la publicación inicial de 1912 LTSR. Windows 10 32 de bits solo es compatible en Windows 10 Enterprise 2019 LTSC.

\* La compatibilidad con VDA de XenApp y XenDesktop 7.15 LTSR en este caso es solo para Windows 7 y Windows 2008 R2. XenApp y XenDesktop 7.15 LTSR dejará de ser compatible a partir de agosto de 2022. La compatibilidad con Citrix para Windows 7 y Windows 2008 R2 finalizará cuando Microsoft finalice el soporte para el sistema operativo o cuando finalice la compatibilidad con XenApp y XenDesktop 7.15 LTSR, lo que ocurra primero. Para obtener más información, consulte la [tabla de productos de Citrix](#).

## **Versiones compatibles de la aplicación Citrix Workspace**

Todas las versiones admitidas de la aplicación Citrix Workspace son compatibles con Citrix Virtual Apps and Desktops 1912 LTSR. Para obtener información sobre el ciclo de vida de la aplicación Citrix Workspace, consulte [Lifecycle Milestones for Citrix Workspace app and Citrix Receiver](#).

Para mayor comodidad, considere la posibilidad de suscribirse al [feed RSS de la aplicación Citrix Workspace](#) para recibir una notificación cuando una nueva versión de la aplicación Citrix Workspace esté disponible.

## **Exclusiones importantes de Citrix Virtual Apps and Desktops 7 1912 LTSR CU5**

Las siguientes funciones, componentes y plataformas no dan derecho a las ventajas y prestaciones del ciclo de vida de 1912 LTSR. Específicamente, se excluyen las ventajas de actualizaciones acumulativas y el ciclo de vida ampliado. Las actualizaciones de los componentes y funciones excluidos están disponibles a través de las versiones publicadas regularmente.

---

### **Componentes y funciones excluidos**

---

AppDisks

AppDNA

Citrix SCOM Management Pack

Framehawk

Personal vDisk

Integración de StoreFront con Citrix Online

---

---

### **Plataformas Windows excluidas\***

---

Windows 2008 de 32 bits (para Universal Print Server)

---

\* Citrix se reserva el derecho a actualizar el soporte que ofrece para las plataformas en función de los hitos de los ciclos de vida de los proveedores externos.

## Datos de análisis de instalación y actualización

Cuando se usa el programa de instalación del producto completo para implementar o actualizar los componentes de XenApp o XenDesktop, se recopila información anónima sobre el proceso de instalación y se guarda en la máquina donde se está realizando la instalación o actualización del componente. Esta información se utiliza para ayudar a Citrix a mejorar la experiencia de instalación de sus clientes.

## Migrar XenApp 6.5

El proceso de migración de XenApp 6.5 permite realizar una transición eficaz y rápida desde una comunidad XenApp 6.5 a un sitio con 1912 LTSR. Esta transición puede resultarle útil en caso de implementaciones que contienen una gran cantidad de aplicaciones y directivas de grupo Citrix, porque reduce el riesgo de que se produzcan errores accidentales al mover manualmente las aplicaciones y las directivas de grupo Citrix al nuevo sitio de XenApp.

Después de instalar los componentes principales de 1912 LTSR y crear un sitio, el proceso de migración sigue estos pasos:

- Ejecute el instalador de 1912 en cada servidor de trabajo de XenApp 6.5. Este instalador actualiza automáticamente el servidor a un nuevo Virtual Delivery Agent para SO de servidor listo para usar en el nuevo sitio.
- Ejecute los cmdlets de exportación de PowerShell en un Controller de XenApp 6.5, que exporta las configuraciones de aplicaciones y directivas de Citrix a archivos XML.
- Si fuera necesario, modifique los archivos XML para seleccionar con exactitud lo que quiere importar al sitio nuevo. Al adaptar los archivos, puede importar las configuraciones de directivas y aplicaciones al sitio de 1912 LTSR por fases: algunas configuraciones ahora y otras más tarde.
- Ejecute los cmdlets de importación de PowerShell en el nuevo Controller de 1912, el cual importa las configuraciones contenidas en los archivos XML al nuevo sitio de XenApp.

Vuelva a configurar el nuevo sitio según sea necesario y, a continuación, haga pruebas en él.

Para obtener más información, consulte [Migrar XenApp 6.x](#).

## Problemas resueltos

April 29, 2022

Se han solucionado estos problemas desde Citrix Virtual Apps and Desktops 7 1912 LTSR CU4:

## Citrix Provisioning

La [documentación de Citrix Provisioning 1912 CU5](#) ofrece información específica acerca de las actualizaciones de esta versión.

## Citrix Director

- Una vez establecida una sesión, el nombre simplificado de la máquina que aparece en la página Detalles de la máquina en Citrix Director se revierte al nombre del grupo de entrega. [CVADHELP-18746]
- Al acceder desde un VDA que tiene el idioma del sistema configurado en español, es posible que Citrix Director muestre texto incorrecto. [CVADHELP-18864]

## Citrix Studio

- Al agregar la dirección del servidor de StoreFront a través de Citrix Studio y al asignarla a un grupo de entrega, el almacén se **desactiva** de forma predeterminada. Como resultado, no se puede acceder al almacén. [CVADHELP-17980]
- El Delivery Controller tarda en responder al agregar, crear o quitar directivas mediante la ficha **Directivas** de Citrix Studio. El tiempo de respuesta habitual es de 10 a 15 minutos. [CVADHELP-18743]

## Delivery Controller

- En un entorno con administración de energía, es posible que las conexiones con los VDA que no se han encendido sigan teniendo intermediación con broker. [CVADHELP-18374]
- Es posible que no se puedan agregar nuevos administradores mediante comandos de PowerShell en Citrix Studio. [CVADHELP-18573]
- Es posible que no se puedan enumerar o iniciar sesiones en Citrix Studio cuando SQL utiliza mucha CPU. Se muestra este mensaje de error:

**Evento 1201: Se ha perdido la conexión entre Citrix Broker Service y la base de datos.**

[CVADHELP-18875]

## **Linux Virtual Delivery Agent**

La [documentación de Linux Virtual Delivery Agent 1912 CU5](#) proporciona información específica acerca de las actualizaciones de esta versión.

## **Profile Management**

La [documentación de Profile Management 1912 CU5](#) ofrece información específica acerca de las actualizaciones de esta versión.

## **Grabación de sesiones**

La documentación de Grabación de sesiones 1912 CU5 no contiene problemas resueltos.

## **StoreFront**

La [documentación de StoreFront 1912 CU5](#) ofrece información específica acerca de las actualizaciones de esta versión.

## **VDA para SO de sesión única**

### **Teclado**

- Al usar una distribución de teclado en ruso en un dispositivo macOS conectado a un VDA con Windows, es posible que las teclas de acceso rápido no funcionen. [CVADHELP-17788]
- En un dispositivo Android conectado a un VDA con la versión 1912 LTSR CU3, al activar un campo de entrada de texto, es posible que el teclado en pantalla no aparezca automáticamente. [CVADHELP-18613]
- Al iniciar sesiones de usuario, es posible que el Editor de métodos de entrada (IME) genérico del cliente no se configure automáticamente. Como resultado, el teclado no se sincroniza automáticamente con el dispositivo de punto final. [CVADHELP-18776]

### **Impresión**

- Cuando se agrega una directiva a la impresora universal genérica, la impresora predeterminada puede cambiar de la impresora principal del cliente a la impresora universal de Citrix genérica. [CVADHELP-18157]

- Es posible que las impresoras de sesión desaparezcan durante la reconexión de la sesión, lo que hace que los VDA sean inaccesibles desde escritorios remotos (RDP). [CVADHELP-19062]

### **Sesión/Conexión**

- La salida de audio de un micrófono puede ser de baja calidad cuando se conecta a través de Citrix Gateway. [CVADHELP-16863]
- Cuando cierra una sesión iniciada desde un escritorio publicado con los VDA alojados en Google Cloud Platform, es posible que la sesión permanezca activa en el VDA y no se marque como desconectada. [CVADHELP-17923]
- Es posible que estos pasos, realizados desde una aplicación de Microsoft Outlook publicada con el IME local habilitado, generen texto aleatorio en la ventana del correo electrónico:
  - Abra la ventana del correo electrónico.
  - Presione la tecla **Esc** para mostrar la ventana **¿Quiere guardar los cambios?** y escriba lo que quiera.
  - Presione la tecla **Esc** para cerrar el cuadro de diálogo.

[CVADHELP-18379]

- Cuando IME de Citrix está habilitado, es posible que ciertas aplicaciones de terceros no respondan y que no se inicien aplicaciones en las sesiones de usuario. El problema se produce por un error en el módulo CtxIme. [CVADHELP-18511]
- Al actualizar la versión 7.15 CU3 de XenApp y XenDesktop del VDA a CU4 o a la versión 1912 LTSR de Citrix Virtual Apps and Desktops, el valor del Registro **LogoffCheckSysModules** de la clave del Registro HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI se restablece a su valor predeterminado. [CVADHELP-19214]

### **Experiencia de usuario**

- Es posible que un mouse para zurdos con el botón principal configurado en la **izquierda** en el dispositivo del usuario y el VDA no funcione como es debido. [CVADHELP-17908]

### **Interfaz de usuario**

- En un entorno de varios monitores, si configura el monitor principal en modo vertical, es posible que las notificaciones de SAS aparezcan giradas 90 grados. [CVADHELP-17779]

## VDA para SO multisesión

### Teclado

- Cuando el Editor de métodos de entrada (IME) japonés está configurado en el **modo de experiencia óptima**, es posible que el texto introducido se duplique. [CVADHELP-18259]
- En un dispositivo Android conectado a un VDA con la versión 1912 LTSR CU3, al activar un campo de entrada de texto, es posible que el teclado en pantalla no aparezca automáticamente. [CVADHELP-18613]

### Impresión

- Cuando se agrega una directiva a la impresora universal genérica, la impresora predeterminada puede cambiar de la impresora principal del cliente a la impresora universal de Citrix genérica. [CVADHELP-18157]
- Es posible que las impresoras de sesión desaparezcan durante la reconexión de la sesión, lo que hace que los VDA sean inaccesibles desde escritorios remotos (RDP). [CVADHELP-19062]

### Sesión/Conexión

- En una instancia publicada de Microsoft Edge o Internet Explorer, es posible que la firma aplicada digitalmente en el explorador web mediante la función de firma no sea claramente visible al iniciar ciertas aplicaciones de terceros.

Para habilitar la opción, establezca la siguiente clave de Registro:

HKEY\_LOCAL\_MACHINE\Software\Citrix\MultiTouch

Nombre: PressureValue

Tipo: REG\_DWORD

Valor: 32000 (decimal)

[CVADHELP-18325]

- Cuando IME de Citrix está habilitado, es posible que ciertas aplicaciones de terceros no respondan y que no se inicien aplicaciones en las sesiones de usuario. El problema se produce por un error en el módulo CtxIme. [CVADHELP-18511]
- Cuando las licencias se agotan en el Servidor de licencias y la función del **período de gracia suplementario** está inhabilitada, es posible que aparezca una pantalla negra congelada con el mensaje de error **Acceso denegado**. [CVADHELP-18712]

- Si se conecta de nuevo a una sesión en la versión 2109 de VDA o una posterior mediante Reconexión automática de clientes, es posible que los dispositivos de audio no se asignen a la sesión. [CVADHELP-18888]
- Al salir de una sesión virtual de Citrix, es posible que se produzca al menos uno de estos problemas:
  - El VDA sigue enumerando la sesión finalizada y el proceso logonui.exe. Se puede forzar el cierre del proceso logonui.exe.
  - La sesión aparece con un nombre de usuario vacío en Citrix Studio.
  - Es posible que no pueda iniciar más sesiones.

[CVADHELP-19182]

### Excepciones del sistema

- Al configurar el proxy BCR con un archivo PAC, la redirección de contenido de explorador Web podría fallar. Como resultado, el proceso HdxBrowserCef.exe se cierra de forma imprevista. [CVADHELP-16463]
- Al iniciar Conexión a Escritorio remoto (mstsc.exe) como una aplicación publicada, es posible que el proceso CredentialUIBroker.exe se cierre inesperadamente. [CVADHELP-18694]
- Es posible que Citrix Stack Control Service (SCService64.exe) se cierre inesperadamente. [CVADHELP-18707]
- Es posible que Microsoft envíe incorrectamente el mensaje **WTS\_REMOTE\_CONNECT** antes de enviar la notificación de conexión **ConnectNotify**. Como resultado, es posible que se produzca al menos uno de estos problemas funcionales:
  - Es posible que las sesiones se cierre de forma inesperada.
  - Es posible que las sesiones no puedan reconectarse.
  - Es posible que el administrador de paquetes RPM se cierre de forma inesperada.

[CVADHELP-18980]

- Al seleccionar la opción Reconexión automática de clientes, es posible que la sesión se cierre forma inesperada. [CVADHELP-19268]

### Interfaz de usuario

- En una sesión de usuario iniciada a través de la aplicación Citrix Workspace, es posible que no pueda ocultar la barra de idioma a pesar de haber establecido la opción **No, ocultar la barra de idioma**. [CVADHELP-18239]

- Es posible que no aparezcan mensajes de estado al iniciar recursos publicados. [CVADHELP-19070]

## Cumulative Update 4 (CU4)

March 10, 2022

Fecha de publicación: 3 de noviembre de 2021

### Acerca de esta versión

Citrix Virtual Apps and Desktops 7 1912 LTSR Cumulative Update 4 (CU4) corrige más de 70 problemas notificados desde la publicación de 1912 LTSR CU3.

[1912 LTSR \(información general\)](#)

[1912 LTSR \(funciones e información sobre la actualización de la versión\)](#)

[Problemas resueltos desde Citrix Virtual Apps and Desktops 7 1912 LTSR CU3](#)

[Problemas conocidos en esta versión](#)

[Elementos eliminados y obsoletos](#)

[Fechas de elegibilidad de Subscription Advantage de los productos Citrix](#)

### Descargas

[Citrix Virtual Apps and Desktops 7 1912 LTSR CU4](#)

#### Importante:

Citrix License Administration Console alcanzó el final de su vida útil y el final del soporte técnico en servidor de licencias 11.16.3.0 compilación 30000. Utilice [Citrix Licensing Manager](#).

### Nuevas implementaciones

¿Cómo implemento la actualización CU4 desde cero?

Puede configurar un nuevo entorno de Citrix Virtual Apps and Desktops basado en CU4 con el metainstalador de CU4. Antes de ello, le recomendamos que se familiarice con el producto:

Consulte la sección [Citrix Virtual Apps and Desktops 7 1912 LTSR \(versión inicial\)](#) y lea atentamente las secciones [Información técnica general](#), [Instalar y configurar](#) y [Proteger](#) antes de planificar la implementación. Compruebe que la configuración cumple los [requisitos del sistema](#) de todos los componentes.

## Implementaciones existentes

¿Qué actualizo?

CU4 ofrece actualizaciones de componentes base de 1912 LTSR. Recuerde: Citrix recomienda actualizar todos los componentes de LTSR de la implementación a CU4. Por ejemplo: Si Citrix Provisioning forma parte de su implementación LTSR, actualice los componentes de Citrix Provisioning a CU4. Si Citrix Provisioning no forma parte de la implementación, no necesita instalarlo ni actualizarlo.

## Componentes base de Citrix Virtual Apps and Desktops 7 1912 LTSR CU4

Componente base de 1912 LTSR	Versión como se muestra en Programas y características	Notas
VDA de sesión única	1912.0.4000	
VDA multisesión	1912.0.4000	
Delivery Controller	1912.0.4000	
Citrix Studio	1912.0.4000	
Citrix Director	1912.0.4000	
Administración de Directivas de grupo Citrix	7.24.4000	
Extensión del cliente de Directivas de grupo Citrix	7.24.4000	
Citrix StoreFront	1912.0.4000	
Citrix Provisioning	1912.0.19	
Universal Print Server	1912.0.4000	
Grabación de sesiones	1912.0.4000	
Linux VDA	1912.0.3000	Consulte la <a href="#">documentación de Linux VDA</a> para ver las plataformas compatibles.
Profile Management	1912.0.4000	

<b>Componente base de 1912 LTSR</b>	<b>Versión como se muestra en Programas y características</b>	<b>Notas</b>
Servicio de autenticación federada de Citrix	1912.0.4000	
Redirección de contenido de explorador web	15.19.4000	
Citrix Probe Agent	2006	<a href="#">Descargar</a>

### Componentes compatibles de Citrix Virtual Apps and Desktops 7 1912 LTSR CU4

Los siguientes componentes, en las versiones que se indican a continuación, son compatibles con entornos LTSR. Estos componentes no dan derecho a las ventajas de LTSR (ciclo de vida ampliado y actualizaciones acumulativas de correcciones solamente). Citrix puede pedirle que actualice estos componentes a una versión más reciente dentro de sus entornos 1912 LTSR.

<b>Componentes y funciones compatibles</b>	<b>Versión como se muestra en Programas y características</b>
App Layering	21.07.0
Directivas de protección de aplicaciones	1912.0.0
HDX RealTime Optimization Pack	2.9 LTSR CU4
Servidor de licencias	11.17.2.0, compilación 36000
Capa de personalización de usuarios	21.02.0
Reproductor web de grabación de sesiones	1912.0.0
Optimización de Teams	1912.0.0
Autoservicio de restablecimiento de contraseñas	1.1
Windows 10 de 32 bits	Consulte la <a href="#">documentación de la versión inicial</a>
Workspace Environment Management	2109
XenApp y XenDesktop 7.15 LTSR VDA (versión más reciente)*	Solo la actualización acumulativa más reciente

#### **Nota:**

Windows 10 de 32 bits solo es compatible durante 18 meses a partir de la publicación inicial de 1912 LTSR. Windows 10 32 de bits solo es compatible en Windows 10 Enterprise 2019 LTSC.

\* La compatibilidad con VDA de XenApp y XenDesktop 7.15 LTSR en este caso es solo para Windows 7 y Windows 2008 R2. XenApp y XenDesktop 7.15 LTSR dejará de ser compatible a partir de agosto de 2022. La compatibilidad con Citrix para Windows 7 y Windows 2008 R2 finalizará cuando Microsoft finalice el soporte para el sistema operativo o cuando finalice la compatibilidad con XenApp y XenDesktop 7.15 LTSR, lo que ocurra primero. Para obtener más información, consulte la [tabla de productos de Citrix](#).

## Versiones compatibles de la aplicación Citrix Workspace

Todas las versiones admitidas de la aplicación Citrix Workspace son compatibles con Citrix Virtual Apps and Desktops 1912 LTSR. Para obtener información sobre el ciclo de vida de la aplicación Citrix Workspace, consulte [Lifecycle Milestones for Citrix Workspace app and Citrix Receiver](#).

Para mayor comodidad, considere la posibilidad de suscribirse al [feed RSS de la aplicación Citrix Workspace](#) para recibir una notificación cuando una nueva versión de la aplicación Citrix Workspace esté disponible.

## Exclusiones importantes de Citrix Virtual Apps and Desktops 7 1912 LTSR CU4

Las siguientes funciones, componentes y plataformas no dan derecho a las ventajas y prestaciones del ciclo de vida de 1912 LTSR. Específicamente, se excluyen las ventajas de actualizaciones acumulativas y el ciclo de vida ampliado. Las actualizaciones de los componentes y funciones excluidos están disponibles a través de las versiones publicadas regularmente.

---

### Componentes y funciones excluidos

---

AppDisks

AppDNA

Citrix SCOM Management Pack

Framehawk

Personal vDisk

Integración de StoreFront con Citrix Online

---

---

### Plataformas Windows excluidas\*

---

Windows 2008 de 32 bits (para Universal Print Server)

---

\* Citrix se reserva el derecho a actualizar el soporte que ofrece para las plataformas en función de los hitos de los ciclos de vida de los proveedores externos.

## Datos de análisis de instalación y actualización

Cuando se usa el programa de instalación del producto completo para implementar o actualizar los componentes de XenApp o XenDesktop, se recopila información anónima sobre el proceso de instalación y se guarda en la máquina donde se está realizando la instalación o actualización del componente. Esta información se utiliza para ayudar a Citrix a mejorar la experiencia de instalación de sus clientes.

## Migrar XenApp 6.5

El proceso de migración de XenApp 6.5 permite realizar una transición eficaz y rápida desde una comunidad XenApp 6.5 a un sitio con 1912 LTSR. Esta transición puede resultarle útil en caso de implementaciones que contienen una gran cantidad de aplicaciones y directivas de grupo Citrix, porque reduce el riesgo de que se produzcan errores accidentales al mover manualmente las aplicaciones y las directivas de grupo Citrix al nuevo sitio de XenApp.

Después de instalar los componentes principales de 1912 LTSR y crear un sitio, el proceso de migración sigue estos pasos:

- Ejecute el instalador de 1912 en cada servidor de trabajo de XenApp 6.5. Este instalador actualiza automáticamente el servidor a un nuevo Virtual Delivery Agent para SO de servidor listo para usar en el nuevo sitio.
- Ejecute los cmdlets de exportación de PowerShell en un Controller de XenApp 6.5, que exporta las configuraciones de aplicaciones y directivas de Citrix a archivos XML.
- Si fuera necesario, modifique los archivos XML para seleccionar con exactitud lo que quiere importar al sitio nuevo. Al adaptar los archivos, puede importar las configuraciones de directivas y aplicaciones al sitio de 1912 LTSR por fases: algunas configuraciones ahora y otras más tarde.
- Ejecute los cmdlets de importación de PowerShell en el nuevo Controller de 1912, el cual importa las configuraciones contenidas en los archivos XML al nuevo sitio de XenApp.

Vuelva a configurar el nuevo sitio según sea necesario y, a continuación, haga pruebas en él.

Para obtener más información, consulte [Migrar XenApp 6.x](#).

## Problemas resueltos

July 8, 2022

Se han solucionado los siguientes problemas desde Citrix Virtual Apps and Desktops 7 1912 LTSR CU3:

### Directiva de Citrix

- Al crear una directiva en un entorno de Citrix Cloud y filtrar mediante la unidad organizativa del dominio A, es posible que el usuario del dominio B no pueda iniciar sesión. El problema se produce al acceder a una aplicación o escritorio publicados. [CVADHELP-17179]

### Citrix Provisioning

La [documentación de Citrix Provisioning 1912 CU4](#) ofrece información específica acerca de las actualizaciones de esta versión.

### Citrix Director

- La instancia local de Citrix Director y la ficha **Supervisor** de Citrix Virtual Apps and Desktops Service podrían mostrar el siguiente mensaje incluso cuando la licencia de RDS funciona según lo previsto.

**La licencia RDS ha excedido su período de gracia.**

[CVADHELP-17469]

- La asignación del VDA a un grupo de entrega y la habilitación del parámetro **VdaDataCollection** en el Delivery Controller podría provocar que el motor de recopilación de datos del VDA se reinicie de forma intermitente. El problema ocurre cuando se actualiza cualquier parámetro de directiva de grupo. [CVADHELP-18361]
- La búsqueda de un usuario seleccionando un escritorio asignado o estático sin sesiones activas puede fallar y mostrarse el siguiente mensaje de error en Citrix Director:

**No se puede obtener las máquinas**

[CVADHELP-18327]

### Citrix Studio

- Al hacer clic en el enlace **Encontrar una solución** del mensaje de error que aparece en Citrix Studio, podría abrirse un enlace incorrecto. [CVADHELP-17800]

## Delivery Controller

- Cuando se interrumpe la licencia, una sesión puede seguir funcionando durante un período de gracia de 30 días. Después de 30 días, el período de gracia finaliza y la conexión falla. [CVADHELP-16487]
- Es posible que la actualización de Citrix Virtual Apps and Desktops a la versión 1912 LTSR no actualice el archivo de configuración Citrix.AzureRmPlugin.dll.config y que la conexión con Microsoft Azure Resource Manager falle. [CVADHELP-16839]
- Es posible que el Delivery Controller no se conecte a la base de datos y que aparezca el siguiente mensaje de error. El error da lugar a problemas de rendimiento.

### **Evento 1201 Se ha perdido la conexión entre Citrix Broker Service y la base de datos.**

Este error se produce cuando se llama a una función de tabla multilínea en SQL, como **DAGet-SessionUidsInCatalogScope** o **DesktopGroupScope**, en un entorno en el que se ejecuta una gran cantidad de sesiones. Por ejemplo, si se están ejecutando 100 000 sesiones y se hacen 100 000 entradas Uid en una sola tabla, el rendimiento se ve afectado y la conexión falla.

[CVADHELP-17021]

- La tabla **MonitorData.[Machine]** presente en la base de datos de supervisión puede incluir entradas duplicadas. [CVADHELP-17025]
- Los intentos de inhabilitar las alertas de Estado del hipervisor en Citrix Director pueden fallar.

Para habilitar la corrección, establezca la siguiente clave de Registro:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\Monitor\Service\Toggles

Nombre: HypervisorMonitoring

Tipo: DWORD

Valor: 00000000

[CVADHELP-17218]

- La prueba del sitio puede fallar si se bloquea la conectividad de red entre los Delivery Controllers de distintas zonas satélite. [CVADHELP-17273]
- Es posible que un administrador de grupos de entrega asignado con un ámbito personalizado no pueda obtener la lista de programaciones de reinicio ni administrarlas. [CVADHELP-17683]
- Es posible que no se puedan actualizar catálogos con nombres que contienen caracteres especiales, como & y \$, cuando la imagen maestra actualizada no se transfiere a los agentes VDA. [CVADHELP-17686]

- Con la funcionalidad de agrupación multisitio configurada y la propiedad “SessionReconnection” establecida en **SameEndPointOnly** en la regla de directiva de autorización, se podría iniciar una nueva sesión en lugar de volver a conectar con la sesión activa. [CVADHELP-17692]
- Al actualizar Citrix Virtual Apps and Desktops a la versión 1912 LTSR y reiniciar XenServer, es posible que las máquinas virtuales se atasquen en el estado de energía Desconocido y no se actualicen en Citrix Studio. [CVADHELP-17750]
- Es posible que una unidad de alojamiento no se agregue en el Delivery Controller si el nombre de dominio completo (FQDN) está escrito en mayúsculas, como HTTPS URL o HTTP URL. [CVADHELP-17862]
- Si se intenta actualizar la contraseña de conexión de host del hipervisor basado en Microsoft System Center Virtual Machine Manager (SCVMM), podría producirse un error de tiempo de espera. [CVADHELP-17909]
- Iniciar o reiniciar el servicio Citrix Monitoring durante una actualización podría provocar un error de conectividad de la base de datos y la pérdida de datos antiguos. Para evitarlo, establezca la retención predeterminada de acuerdo con la edición Platinum (PLT). [CVADHELP-18069]

## Linux Virtual Delivery Agent

La [documentación de Linux Virtual Delivery Agent 1912 CU4](#) proporciona información específica acerca de las actualizaciones de esta versión.

## Metainstalador

- Al instalar o actualizar la versión de un VDA, es posible que se elimine el valor SetDisplayRequiredMode en la clave del Registro HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\Graphics. [CVADHELP-17031]
- La capa de personalización de usuarios no está instalada. [CVADHELP-17672]

## Optimización de Microsoft Teams

- Las llamadas optimizadas de Microsoft Teams pueden fallar y el proceso ctxsvchost.exe puede cerrarse de manera imprevista debido al fallo del módulo CtxTeamsSvc.dll. [CVADHELP-16918]
- Es posible que el servicio HTML5 Video Redirection Service (txHdxWebSocketService) se cierre de forma inesperada. [CVADHELP-17146]
- Cuando se utiliza Microsoft Teams en modo optimizado HDX en un escritorio publicado, es posible que las llamadas de audio se desconecten. [CVADHELP-17341]

- Al intentar unirse a una llamada, es posible que Citrix HDX HTML5 Video Redirection Service (WebSocketService.exe) se cierre de forma inesperada y provoque que falle la llamada. [CVADHELP-17424]

## Profile Management

La [documentación de Profile Management 1912 CU4](#) ofrece información específica acerca de las actualizaciones de esta versión.

## Grabación de sesiones

La [documentación de Grabación de sesiones 1912 CU4](#) ofrece información específica acerca de las actualizaciones de esta versión.

## StoreFront

La [documentación de StoreFront 1912 CU4](#) ofrece información específica acerca de las actualizaciones de esta versión.

## VDA para SO de sesión única

### Redirección de contenido

- Es posible que aparezca un parche negro en la pantalla cuando se utiliza Explorador. El problema ocurre cuando se conecta a dispositivos de punto final con determinados modelos de GPU AMD. [CVADHELP-17057]
- Cuando se utilizan algunas aplicaciones de terceros, Websocketagent.exe puede usar un alto porcentaje de la CPU. El problema se produce cuando la directiva **Redirección de contenido de explorador Web** o **Redirección de vídeo HTML5** está habilitada. [CVADHELP-17067]
- Esta corrección es una mejora de HdxWebProxy para interoperar con sus proxys web Blue Coat. [CVADHELP-18078]

### Teclado

- La detección de MTU en EDT puede calcular una MTU incorrecta cuando las rutas entre el VDA y el cliente son asimétricas. Como resultado, el inicio de la sesión funciona correctamente. Sin embargo, el teclado y el mouse no responden. [CVADHELP-16654]

## Sesión/Conexión

- Los VDA pueden anular su registro intermitentemente cuando IPv6 está habilitado. [CVADHELP-14847]
- Es posible que se cancele el registro de los VDA y que permanezcan así. [CVADHELP-16445]
- Después de iniciar una sesión, el audio que se ejecuta en Microsoft Windows puede mostrar una X roja que no se puede quitar. [CVADHELP-16815]
- La asignación del Portapapeles puede bloquearse cuando se conecta inicialmente desde una sesión de escritorio virtual a un cliente y viceversa. Al desconectar y volver a conectar, la asignación del Portapapeles solo funciona desde la sesión de escritorio virtual al cliente. [CVADHELP-17039]
- Para actualizar el texto personalizado de una marca de agua, cierre la sesión y vuelva a conectarse a la sesión. [CVADHELP-17056]
- Al establecer **PPP** en un valor distinto del 100% en de un VDA, es posible que dicho valor de **PPP** se restablezca al 100%. El problema se produce al intentar bloquear un escritorio. [CVADHELP-17276]
- Con la directiva Multisequencia habilitada, las sesiones iniciadas en dispositivos de punto final Linux podrían desconectarse. El problema ocurre con la versión 1912 LTSR del VDA. [CVADHELP-17301]
- Cuando se utiliza Microsoft Teams en modo optimizado HDX en un escritorio publicado, es posible que las llamadas de audio se desconecten. [CVADHELP-17341]
- Es posible que no se pueda volver a conectar a una sesión con la directiva de capa de personalización de usuarios habilitada. [CVADHELP-17369]
- El uso de la tarjeta gráfica AMD en un escritorio VDI de sesión única podría fallar. [CVADHELP-17757]
- Las licencias de conexión de Citrix se consumen al desconectar sesiones de usuario que se habían conectado a través de un VDA de máquina física. [CVADHELP-17802]
- Al utilizar una GPU NVIDIA, la frecuencia de fotogramas en modo de pantalla completa no puede superar los 60 fps (fotogramas por segundo) incluso después de configurar la pantalla a la frecuencia máxima. [CVADHELP-17904]
- Es posible que la opción de copia de tablas esté inhabilitada o no esté disponible en determinadas aplicaciones de terceros. Para habilitar la opción, establezca la siguiente clave de Registro:

HKEY\_LOCAL\_MACHINE\CurrentControlSet\Control\Citrix\wfshell\virtual Clipboard

Nombre: DisableFileSupport

Tipo: DWORD

Valor: 00000001

[CVADHELP-17986]

- Esta corrección permite registrar la lista de canales virtuales permitidos. Para obtener más información, consulte [Seguridad de los canales virtuales](#). [CVADHELP-18129]

### Tarjetas inteligentes

- El acceso a tarjetas inteligentes con el explorador web Microsoft Edge con **SFRhook** habilitado podría provocar que el proceso msedge.exe se cierre de forma imprevista. [CVADHELP-17956]

### Excepciones del sistema

- Citrix Desktop Service (BrokerAgent.exe) podría generar un gran número de eventos ID 1010 cuando se utiliza la detección de Controller basada en unidad organizativa a través de un túnel VPN de acceso directo. [CVADHELP-16754]
- Es posible que Microsoft Teams no se optimice cuando uno de los procesos de CtxSvcHost.exe se cierra de forma imprevista. El problema se debe al fallo del servicio Citrix HDX Teams Redirection Service. [CVADHELP-16946]
- Citrix Desktop Service (BrokerAgent.exe) podría sufrir una infracción de acceso y cerrarse de forma imprevista. [CVADHELP-17055]
- Es posible que el servicio HTML5 Video Redirection Service (CtxHdxWebSocketService) se cierre de forma inesperada. [CVADHELP-17146]
- Es posible que el proceso wfshell.exe se cierre de forma imprevista y provoque un error al iniciar nuevas aplicaciones desde aplicaciones publicadas. [CVADHELP-17310]
- Es posible que los VDA experimenten una excepción irrecoverable en icausbbsys y muestren una pantalla azul con el código de comprobación de errores 0x3B. [CVADHELP-17339]
- Al intentar unirse a una llamada, es posible que Citrix HDX HTML5 Video Redirection Service (WebSocketService.exe) se cierre de forma inesperada y provoque que falle la llamada. [CVADHELP-17424]
- El proceso winlogon.exe puede cerrarse de manera imprevista. El problema ocurre por un error en el módulo PicaWinlogonHook64.dll. [CVADHELP-17651]
- Es posible que el audio y el vídeo de una conferencia de vídeo optimizada para Microsoft Teams se desconecten y que se cierre el proceso HdxRtcEngine.exe. [CVADHELP-17741]

## VDA para SO multisesión

### Redirección de contenido

- Es posible que aparezca un parche negro en la pantalla cuando se utiliza Explorador. El problema ocurre cuando se conecta a dispositivos de punto final con determinados modelos de GPU AMD. [CVADHELP-17057]
- Esta corrección es una mejora de HdxWebProxy para interoperar con sus proxys web Blue Coat. [CVADHELP-18078]

### Teclado

- La detección de MTU en EDT puede calcular una MTU incorrecta cuando las rutas entre el VDA y el cliente son asimétricas. Como resultado, el inicio de la sesión funciona correctamente. Sin embargo, el teclado y el mouse no responden. [CVADHELP-16654]

### Impresión

- Al utilizar la opción **Guardar impresión como** para imprimir en un archivo en una sesión integrada, es posible que la ventana de impresión no se muestre correctamente. [CVADHELP-16614]

### Sesión/Conexión

- Los VDA pueden anular su registro intermitentemente cuando IPv6 está habilitado. [CVADHELP-14847]
- Es posible que se cancele el registro de los VDA y que permanezcan así. [CVADHELP-16445]
- Al utilizar determinadas aplicaciones de terceros, puede aparecer una pantalla negra cuando la aplicación abre otra ventana. [CVADHELP-16956]
- La asignación del Portapapeles puede bloquearse cuando se conecta inicialmente desde una sesión de escritorio virtual a un cliente y viceversa. Al desconectar y volver a conectar, la asignación del Portapapeles solo funciona desde la sesión de escritorio virtual al cliente. [CVADHELP-17039]
- Si se establece el valor de **HideStatusMessages** en **1** para ocultar la barra de inicio, es posible que la clave del Registro HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System no funcione según lo previsto. [CVADHELP-17138]

- Con la directiva Multisequencia habilitada, las sesiones iniciadas en dispositivos de punto final Linux podrían desconectarse. El problema ocurre con la versión 1912 LTSR del VDA. [CVADHELP-17301]
- Cuando se utiliza Microsoft Teams en modo optimizado HDX en un escritorio publicado, es posible que las llamadas de audio se desconecten. [CVADHELP-17341]
- Es posible que algunas aplicaciones de terceros no respondan en una sesión integrada. [CVADHELP-17309]
- Es posible el inicio de una sesión SSL en Citrix Virtual Apps and Desktops LTSR versión CU1, CU2 o CU3 falle y se muestre el siguiente mensaje de error:

**La sesión “nombre del grupo de entrega” no se inició correctamente debido al código de error 3500. Póngase en contacto con el administrador para obtener más información sobre el error.**

[CVADHELP-17421]

- El controlador de enlazado, CtxUvi, podría descargarse cuando se utilizan contenedores de Docker. [CVADHELP-17614]
- Esta corrección proporciona mejoras a la función Lista de canales virtuales permitidos. Como resultado, solo se pueden abrir los canales virtuales de Citrix en las sesiones de Virtual Apps and Desktops. También puede agregar canales virtuales personalizados a la lista de permitidos mediante la configuración de la directiva **Lista de canales virtuales permitidos**. [CVADHELP-17918]
- Después de actualizar la aplicación Citrix Workspace a la versión 1909 o posterior, es posible que no pueda mover la barra de idioma de manera fluida en una sesión integrada. [CVADHELP-18118]
- Es posible que la opción de copia de tablas esté inhabilitada o no esté disponible en determinadas aplicaciones de terceros. Para habilitar la opción, establezca la siguiente clave de Registro:

HKEY\_LOCAL\_MACHINE\CurrentControlSet\Control\Citrix\wfshell\virtual Clipboard

Nombre: DisableFileSupport

Tipo: DWORD

Valor: 00000001

[CVADHELP-17986]

- Esta corrección permite registrar la lista de canales virtuales permitidos. Para obtener más información, consulte Seguridad de los canales virtuales. [CVADHELP-18129]

## Tarjetas inteligentes

- El acceso a tarjetas inteligentes con el explorador web Microsoft Edge con **SFRhook** habilitado podría provocar que el proceso msedge.exe se cierre de forma imprevista. [CVADHELP-17956]

## Excepciones del sistema

- Citrix Desktop Service (BrokerAgent.exe) podría generar un gran número de eventos ID 1010 cuando se utiliza la detección de Controller basada en unidad organizativa a través de un túnel VPN de acceso directo. [CVADHELP-16754]
- Es posible que Microsoft Teams no se optimice cuando uno de los procesos de CtxSvcHost.exe se cierra de forma imprevista. El problema se debe al fallo del servicio Citrix HDX Teams Redirection Service. [CVADHELP-16946]
- Citrix Desktop Service (BrokerAgent.exe) podría sufrir una infracción de acceso y cerrarse de forma imprevista. [CVADHELP-17055]
- Es posible que el servicio HTML5 Video Redirection Service (CtxHdxWebSocketService) se cierre de forma inesperada. [CVADHELP-17146]
- Es posible que el proceso wfshell.exe se cierre de forma imprevista y provoque un error al iniciar nuevas aplicaciones desde aplicaciones publicadas. [CVADHELP-17310]
- Al intentar unirse a una llamada, es posible que Citrix HDX HTML5 Video Redirection Service (WebSocketService.exe) se cierre de forma inesperada y provoque que falle la llamada. [CVADHELP-17424]
- Al iniciar una aplicación publicada, winlogon.exe podría cerrarse imprevistamente y la sesión del usuario podría desconectarse. [CVADHELP-17602]
- Es posible que las aplicaciones de Windows universal (UWA) publicadas no se inicien con la siguiente excepción:

**System.Runtime.InteropServices.COMException (0x80270134)**

[CVADHELP-18116]

## Cumulative Update 3 (CU3)

November 4, 2021

Fecha de publicación: 12 de mayo de 2021

## Acerca de esta versión

Citrix Virtual Apps and Desktops 7 1912 LTSR Cumulative Update 3 (CU3) corrige más de 80 problemas notificados desde la publicación de 1912 LTSR CU2.

[1912 LTSR \(información general\)](#)

[1912 LTSR \(funciones e información sobre la actualización de la versión\)](#)

[Problemas resueltos desde Citrix Virtual Apps and Desktops 7 1912 LTSR CU2](#)

[Problemas conocidos en esta versión](#)

[Elementos eliminados y obsoletos](#)

[Fechas de elegibilidad de Subscription Advantage de los productos Citrix](#)

## Descargas

[Citrix Virtual Apps and Desktops 7 1912 LTSR CU3](#)

### Importante:

Citrix License Administration Console alcanzó el final de su vida útil y el final del soporte técnico en servidor de licencias 11.16.3.0 compilación 30000. Utilice [Citrix Licensing Manager](#).

## Nuevas implementaciones

¿Cómo implemento la actualización CU3 desde cero?

Puede configurar un nuevo entorno de Citrix Virtual Apps and Desktops basado en CU3 con el metainstalador de CU3. Antes de ello, le recomendamos que se familiarice con el producto:

Consulte la sección [Citrix Virtual Apps and Desktops 7 1912 LTSR \(versión inicial\)](#) y lea atentamente las secciones [Información técnica general](#), [Instalar y configurar](#) y [Proteger](#) antes de planificar la implementación. Compruebe que la configuración cumple los [requisitos del sistema](#) de todos los componentes.

## Implementaciones existentes

¿Qué actualizo?

CU3 ofrece actualizaciones de componentes base de 1912 LTSR. Recuerde: Citrix recomienda actualizar todos los componentes de LTSR de la implementación a CU3. Por ejemplo: Si Citrix Provisioning forma parte de su implementación LTSR, actualice los componentes de Citrix Provisioning a CU3. Si Citrix Provisioning no forma parte de la implementación, no necesita instalarlo ni actualizarlo.

### Componentes base de Citrix Virtual Apps and Desktops 7 1912 LTSR CU3

Componente base de 1912 LTSR	Versión como se muestra en Programas y características	Notas
VDA de sesión única	1912.0.3000	
VDA multisesión	1912.0.3000	
Delivery Controller	1912.0.3000	
Citrix Studio	1912.0.3000	
Citrix Director	1912.0.3000	
Administración de Directivas de grupo Citrix	7.24.3000	
Extensión del cliente de Directivas de grupo Citrix	7.24.3000	
Citrix StoreFront	1912.0.3000	
Citrix Provisioning	1912.0.13	
Universal Print Server	1912.0.3000	
Grabación de sesiones	1912.0.3000	
Linux VDA	1912.0.3000	Consulte la <a href="#">documentación de Linux VDA</a> para ver las plataformas compatibles.
Profile Management	1912.0.3000	
Servicio de autenticación federada de Citrix	1912.0.3000	
Redirección de contenido de explorador web	15.19.3000	
Citrix Probe Agent	2006	<a href="#">Descargas</a>

### Componentes compatibles de Citrix Virtual Apps and Desktops 7 1912 LTSR CU3

Los siguientes componentes, en las versiones que se indican a continuación, son compatibles con entornos LTSR. Estos componentes no dan derecho a las ventajas de LTSR (ciclo de vida ampliado y actualizaciones acumulativas de correcciones solamente). Citrix puede pedirle que actualice estos componentes a una versión más reciente dentro de sus entornos 1912 LTSR.

<b>Componentes y funciones compatibles</b>	<b>Versión como se muestra en Programas y características</b>
App Layering	19.11.0
Directivas de protección de aplicaciones	1912.0.0
HDX RealTime Optimization Pack	2.9 LTSR.
Servidor de licencias	11.16.6.0, compilación 34000
Capa de personalización de usuarios	19.11.0
Reproductor web de grabación de sesiones	1912.0.0
Optimización de Teams	1912.0.0
Autoservicio de restablecimiento de contraseñas	1.1
Windows 10 de 32 bits	
Workspace Environment Management	2003.0.0 y versiones posteriores
XenApp y XenDesktop 7.15 LTSR VDA (versión más reciente)*	Solo la actualización acumulativa más reciente

**Nota:**

Windows 10 de 32 bits solo es compatible durante 18 meses a partir de la publicación inicial de 1912 LTSR. Windows 10 32 de bits solo es compatible en Windows 10 Enterprise 2019 LTSC.

\* La compatibilidad con VDA de XenApp y XenDesktop 7.15 LTSR en este caso es solo para Windows 7 y Windows 2008 R2. XenApp y XenDesktop 7.15 LTSR dejará de ser compatible a partir de agosto de 2022. La compatibilidad con Citrix para Windows 7 y Windows 2008 R2 finalizará cuando Microsoft finalice el soporte para el sistema operativo o cuando finalice la compatibilidad con XenApp y XenDesktop 7.15 LTSR, lo que ocurra primero. Para obtener más información, consulte la [tabla de productos de Citrix](#).

**Versiones compatibles de la aplicación Citrix Workspace**

Todas las versiones admitidas de la aplicación Citrix Workspace son compatibles con Citrix Virtual Apps and Desktops 1912 LTSR. Para obtener información sobre el ciclo de vida de la aplicación Citrix Workspace, consulte [Lifecycle Milestones for Citrix Workspace app and Citrix Receiver](#).

Para mayor comodidad, considere la posibilidad de suscribirse al [feed RSS de la aplicación Citrix Workspace](#) para recibir una notificación cuando una nueva versión de la aplicación Citrix Workspace esté disponible.

## **Exclusiones importantes de Citrix Virtual Apps and Desktops 7 1912 LTSR CU3**

Las siguientes funciones, componentes y plataformas no dan derecho a las ventajas y prestaciones del ciclo de vida de 1912 LTSR. Específicamente, se excluyen las ventajas de actualizaciones acumulativas y el ciclo de vida ampliado. Las actualizaciones de los componentes y funciones excluidos están disponibles a través de las versiones publicadas regularmente.

---

### **Componentes y funciones excluidos**

---

AppDisks

AppDNA

Citrix SCOM Management Pack

Framehawk

Personal vDisk

Integración de StoreFront con Citrix Online

---

---

### **Plataformas Windows excluidas\***

---

Windows 2008 de 32 bits (para Universal Print Server)

---

\* Citrix se reserva el derecho a actualizar el soporte que ofrece para las plataformas en función de los hitos de los ciclos de vida de los proveedores externos.

## **Datos de análisis de instalación y actualización**

Cuando se usa el programa de instalación del producto completo para implementar o actualizar los componentes de XenApp o XenDesktop, se recopila información anónima sobre el proceso de instalación y se guarda en la máquina donde se está realizando la instalación o actualización del componente. Esta información se utiliza para ayudar a Citrix a mejorar la experiencia de instalación de sus clientes.

## **Migrar XenApp 6.5**

El proceso de migración de XenApp 6.5 permite realizar una transición eficaz y rápida desde una comunidad XenApp 6.5 a un sitio con 1912 LTSR. Esta transición puede resultarle útil en caso de implementaciones que contienen una gran cantidad de aplicaciones y directivas de grupo Citrix, porque

reduce el riesgo de que se produzcan errores accidentales al mover manualmente las aplicaciones y las directivas de grupo Citrix al nuevo sitio de XenApp.

Después de instalar los componentes principales de 1912 LTSR y crear un sitio, el proceso de migración sigue estos pasos:

- Ejecute el instalador de 1912 en cada servidor de trabajo de XenApp 6.5. Este instalador actualiza automáticamente el servidor a un nuevo Virtual Delivery Agent para SO de servidor listo para usar en el nuevo sitio.
- Ejecute los cmdlets de exportación de PowerShell en un Controller de XenApp 6.5, que exporta las configuraciones de aplicaciones y directivas de Citrix a archivos XML.
- Si fuera necesario, modifique los archivos XML para seleccionar con exactitud lo que quiere importar al sitio nuevo. Al adaptar los archivos, puede importar las configuraciones de directivas y aplicaciones al sitio de 1912 LTSR por fases: algunas configuraciones ahora y otras más tarde.
- Ejecute los cmdlets de importación de PowerShell en el nuevo Controller de 1912, el cual importa las configuraciones contenidas en los archivos XML al nuevo sitio de XenApp.

Vuelva a configurar el nuevo sitio según sea necesario y, a continuación, haga pruebas en él.

Para obtener más información, consulte [Migrar XenApp 6.x](#).

## Problemas resueltos

September 22, 2021

Se han resuelto estos problemas desde Citrix Virtual Apps and Desktops 7 1912 LTSR CU2:

### Citrix Director

- Después de desinstalar un VDA, es posible que permanezcan los espacios de nombres de Citrix Windows Management Instrumentation (WMI). [CVADHELP-14965]
- Es posible que Citrix Director muestre de forma intermitente esta alerta en el Delivery Controller:

**El `System.ServiceModel.ChannelFactory1communication object _[<object name>_]` no se puede cambiar mientras su estado sea “Abriendo”.**

[CVADHELP-15801]

- En la página **Utilización histórica de máquinas**, puede que no se muestren los datos de la tabla **10 procesos principales**. Aparece este mensaje:

**La recopilación de datos de proceso está inhabilitada en esta máquina. Habilite la directiva de supervisión de procesos para iniciar la recopilación.**

[CVADHELP-15893]

- En la página **Director > Tendencias > Rendimiento de inicio de sesión > Exportar informe**, al generar y exportar un informe, pueden aparecer valores de tiempo de intermediación incorrectos en el informe. El problema se produce con informes en alemán, donde . se reemplaza por ,. [CVADHELP-16097]
- En la página **Director > Filtros > Todas las máquinas**, si selecciona una máquina y realiza operaciones de mantenimiento, es posible que no se conserven las marcas de verificación para las máquinas seleccionadas. [CVADHELP-16469]
- Al extraer datos de proceso de la API de Supervisar, es posible que aparezcan datos no válidos. La hora de creación del proceso (**ProcessCreationDate**) aparece después de la hora de recopilación del proceso (**CollectionDate**) en lugar de aparecer antes. [CVADHELP-17092]

## Directiva de Citrix

- Al actualizar Citrix Group Policy Engine de la versión 1.7 a la versión 1912 LTSR, es posible que no se muestre la directiva **Asignaciones de impresora** en **Directivas de usuario Citrix**. [CVADHELP-15608]

## Citrix Provisioning

La [documentación de Citrix Provisioning 1912 CU3](#) ofrece información específica acerca de las actualizaciones de esta versión.

## Delivery Controller

- Es posible que, al reiniciar un Delivery Controller, se cancele el registro de todos los VDA conectados en varios dominios. [CVADHELP-12840]
- Esta corrección soluciona los problemas de rendimiento que podría experimentar con Delivery Controller (XML Service) en entornos lentos de Active Directory.

Para habilitar la corrección, establezca la siguiente clave de Registro:

HKEY\_LOCAL\_MACHINE\Software\Citrix\DesktopServer

o

HKEY\_LOCAL\_MACHINE\Software\Policies\Citrix\DesktopServer

Nombre: DisableGetPasswordExpiryInfo

Tipo: DWORD

Valor: 1

[CVADHELP-15536]

- Con esta corrección, la máquina de preparación no utiliza el tiempo de caducidad de caché predeterminado (cinco minutos). La corrección ofrece lo siguiente:
  - Reduce el tiempo de caducidad de una máquina en un estado de energía desconocido (un minuto).
  - Reduce el tiempo de caducidad de una máquina de preparación en transición de energía (cinco segundos).
  - Reduce el tiempo de caducidad de una máquina de preparación que no se halla en transición de energía (un minuto).
  - Reduce el tiempo de caducidad de una máquina que no es de preparación en transición de energía (30 segundos).

[CVADHELP-15678]

- Cuando se utiliza PowerShell para realizar una acción de energía, es posible que la acción se procese correctamente, pero se registra como fallida en **Citrix Studio > Registro**. [CVADHELP-15807]
- Cuando se eliminan máquinas o catálogos asociados a una conexión de alojamiento de AWS, es posible que los dispositivos raíz de EBS no se eliminen automáticamente. El problema se produce porque el indicador **DeleteOnTermination** de la imagen base cambia de `$true` a `$false` en los discos creados para esos catálogos durante la creación del catálogo de máquinas. [CVADHELP-16096]
- En un entorno de varias zonas con latencias altas, es posible que no se pueda actualizar la versión 7.15 LTSR CU5 de XenApp y XenDesktop a la versión 1912 CU1 de Citrix Virtual Apps and Desktops y que se muestre esta excepción:

#### **NullReferenceException**

[CVADHELP-16236]

- En un Delivery Controller, puede aparecer frecuentemente el siguiente mensaje de error en **Visor de eventos > Registros de Windows > Aplicación**:

**ID de evento 505: Falló una importación de Citrix Config Sync Service.**

[CVADHELP-16322]

- Es posible que, al iniciar sesión en una sesión RDP sin intermediario con una credencial UPN, se produzca una excepción no detectada. En 1912 LTSR CU2, se introdujo una traducción de

nombres de usuario como UPN. Cuando el nombre de usuario se trunca por al límite impuesto en las estructuras de datos RDS, se genera un nombre de usuario incorrecto, lo que produce la excepción no detectada. [CVADHELP-16510]

- Al iniciar una aplicación alojada en VM y, a continuación, se intenta iniciar una segunda aplicación alojada en VM desde el mismo VDA, es posible que no se pueda iniciar esta segunda aplicación. El problema se produce cuando el catálogo de máquinas utiliza la asignación estática. [CVADHELP-16829]

## **Linux Virtual Delivery Agent**

La [documentación de Linux Virtual Delivery Agent 1912 CU3](#) proporciona información específica acerca de las actualizaciones de esta versión.

## **Metainstalador**

- Al instalar o actualizar la versión de un VDA, es posible que se elimine el valor SetDisplayRequiredMode en la clave del Registro HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\Graphics. [CVADHELP-17031]

## **Profile Management**

La [documentación de Profile Management 1912 CU3](#) ofrece información específica acerca de las actualizaciones de esta versión.

## **Grabación de sesiones**

La [documentación de Grabación de sesiones 1912 CU3](#) ofrece información específica acerca de las actualizaciones de esta versión.

## **StoreFront**

La [documentación de StoreFront 1912 CU3](#) ofrece información específica acerca de las actualizaciones de esta versión.

## VDA para SO de sesión única

### Teclado

- Con la directiva de redirección del portapapeles habilitada, puede que falle el atajo de teclado de la opción **Copiar**, incluida en el menú contextual, para copiar y pegar contenido entre una aplicación publicada y un dispositivo de punto final. El problema se produce con Internet Explorer. [CVADHELP-15647]

### Impresión

- Es posible que no se puedan imprimir archivos PDF desde una sesión iniciada a través de la aplicación Citrix Workspace para Chrome. [CVADHELP-15318]
- Al usar un VDA mediante el acceso con Remote PC para imprimir contenido a través de la aplicación Citrix Workspace para Mac, es posible que se ignoren los ajustes de la impresora. [CVADHELP-15320]
- Es posible que se pierdan los cambios realizados en **Local Settings**, en **Printer Preferences**, cuando no se guardan los cambios en 54 segundos. [CVADHELP-15725]
- Al intentar imprimir un archivo con el Controlador de impresora universal de Citrix (UPD), es posible que aparezcan imágenes incorrectas en el archivo impreso. El problema se produce al actualizar un VDA de la versión 7.15.5000 a la versión 1912.1000 y al habilitar la compresión intensa. [CVADHELP-15813]
- Es posible que las impresoras cliente no se redirijan al conectarse a una sesión HDX alojada. [CVADHELP-16279]
- Al intentar imprimir un archivo PDF desde una sesión iniciada a través de la aplicación Citrix Workspace para HTML5, es posible que el archivo no se imprima correctamente. [CVADHELP-16809]

### Sesión/Conexión

- Después de actualizar un VDA de la versión 7.15.2000 a la versión 1912.2000, es posible que los valores de datos de **EnableReadImageFileExecOptionsExclusionList** desaparezcan de las claves del Registro: HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\CtxHook\ y HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook. [CVADHELP-15090]
- Aunque la directiva de zona horaria de VDA esté configurada para utilizar la zona horaria del lado del servidor, es posible que todavía se use la zona horaria del lado del cliente. [CVADHELP-15395]

- Es posible que las cámaras web integradas de Surface Pro fallen. [CVADHELP-15567]
- Citrix HDX HTML5 Video Redirection Agent Service (WebSocketAgent.exe) puede detenerse intermitentemente. Por eso, las llamadas entrantes no se muestran en Microsoft Teams. Además, el usuario que recibe la llamada no recibe ninguna notificación. [CVADHELP-15611]
- Después de instalar un VDA, al intentar ver la ficha **Private Key** en **Certificate Properties**, es posible que aparezca este mensaje de error:

**One or more of the objects properties are missing or invalid (Faltan al menos una de las propiedades de los objetos o las que hay no son válidas).**

[CVADHELP-15703]

- Al conectar un monitor físico a un Remote PC con GPU física NVIDIA a través de un DisplayPort, es posible que el monitor muestre una pantalla vacía. [CVADHELP-16022]
- Al conectarse desde un dispositivo de punto final táctil a un VDA con la versión 1912, es posible que el teclado en pantalla no funcione. El problema se produce con usuarios no administradores con el Control de cuentas de usuario habilitado en un VDA. [CVADHELP-16045]
- Es posible que se cancele el registro de VDA cuando la sesión de la consola se vuelva a conectar inmediatamente después de que se haya desconectado la sesión de usuario. [CVADHELP-16152]
- Es posible que, al intentar iniciar una sesión de VDA en un equipo portátil que utiliza una tarjeta gráfica Intel UHD, se vea una pantalla gris. [CVADHELP-16519]
- En los VDA de servidor VDI, es posible que el botón de encendido del menú **Inicio** no ofrezca la opción **Desconectar**. [CVADHELP-16595]
- Al usar el IME genérico para Microsoft Windows 10 20H2 con la actualización KB4586853, es posible que la aplicación se cierre de forma inesperada. [CVADHELP-16664]
- Al intentar realizar una captura de pantalla con la herramienta Recortes o al hacer cálculos complejos, como una tabla dinámica, es posible que haya problemas de rendimiento. El problema se produce al establecer el valor de **CursorShapeChangeMinInterval** en 50 en la clave del Registro HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\Graphics. [CVADHELP-16718]
- Con esta corrección, ahora puede establecer diferentes métodos de entrada para cada ventana de aplicación disponible en los parámetros avanzados del teclado. [CVADHELP-16731]
- Cuando se utiliza Acceso con Remote PC en Windows 10 con adaptador de tarjeta gráfica NVIDIA en una configuración “headless”, pueden producirse problemas de reconexión. [CVADHELP-16848]
- Cuando un VDA que no está en inglés se queda inactivo, es posible que aparezca un mensaje de tiempo de espera agotado con código sin sentido. [CVADHELP-16880]

- Esta corrección es una mejora de **HdxWebProxy**. Un componente BCR, en la medida en que el tráfico HTTP que se origina en la superposición, se puede redirigir a través de proxies web configurados para autorizar el tráfico HTTP. [CVADHELP-17044]

### Excepciones del sistema

- Al intentar ver archivos incrustados de Windows Media desde una aplicación web, es posible que Internet Explorer se cierre de forma inesperada. El problema se produce debido al módulo defectuoso, HostMMTransport.dll. [CVADHELP-15598]
- Los VDA podrían sufrir una excepción irre recuperable en wdica.sys y provocar un pantallazo azul. [CVADHELP-16055]
- Si Terminal Services se cierra de manera inesperada, es posible que se cancele el registro de los agentes VDA. El problema ocurre por un error en el módulo RPM.dll. [CVADHELP-16110]
- Es posible que los VDA sufran una excepción irre recuperable y muestren un pantallazo azul durante el acceso remoto. El problema se produce al instalar un VDA en una máquina nueva y al intentar reiniciarla. [CVADHELP-16284]
- Es posible que los VDA sufran una excepción irre recuperable y muestren una pantalla azul con el código de comprobación de errores 0x0000010D (WDF\_VIOLATION). [CVADHELP-16773]

### VDA para SO multisesión

#### Teclado

- Es posible que la asignación de teclado japonés no funcione al conectarse a un dispositivo de punto final que no tenga Windows. [CVADHELP-15273]
- Con la directiva de redirección del portapapeles habilitada, puede que falle el atajo de teclado de la opción **Copiar**, incluida en el menú contextual, para copiar y pegar contenido entre una aplicación publicada y un dispositivo de punto final. El problema se produce con Internet Explorer. [CVADHELP-15647]

#### Impresión

- Es posible que no se puedan imprimir archivos PDF desde una sesión iniciada a través de la aplicación Citrix Workspace para Chrome. [CVADHELP-15318]
- Al usar un VDA mediante el acceso con Remote PC para imprimir contenido a través de la aplicación Citrix Workspace para Mac, es posible que se ignoren los ajustes de la impresora. [CVADHELP-15320]

- Es posible que se pierdan los cambios realizados en **Local Settings**, en **Printer Preferences**, cuando no se guardan los cambios en 54 segundos. [CVADHELP-15725]
- Al intentar imprimir un archivo con el Controlador de impresora universal de Citrix (UPD), es posible que aparezcan imágenes incorrectas en el archivo impreso. El problema se produce al actualizar un VDA de la versión 7.15.5000 a la versión 1912.1000 y al habilitar la **compresión intensa**. [CVADHELP-15813]
- Al intentar imprimir un archivo grande de Microsoft Excel con el Controlador de impresora universal de Citrix (UPD), es posible que la impresión falle durante el proceso **En cola - Imprimiendo**. [CVADHELP-16153]
- Al intentar imprimir un archivo PDF desde una sesión iniciada a través de la aplicación Citrix Workspace para HTML5, es posible que el archivo no se imprima correctamente. [CVADHELP-16809]

## Sesión/Conexión

- En algunos casos, el uso de licencias de productos Citrix que se muestra en Citrix Studio no coincide con el uso de licencias que se muestra en Citrix License Manager. [CVADHELP-14950]
- Después de actualizar un VDA de la versión 7.15.2000 a la versión 1912.2000, es posible que los valores de datos de **EnableReadImageFileExecOptionsExclusionList** desaparezcan de las claves del Registro: HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\CtxHook\ y HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook. [CVADHELP-15090]
- Aunque la directiva de zona horaria de VDA esté configurada para utilizar la zona horaria del lado del servidor, es posible que todavía se use la zona horaria del lado del cliente. [CVADHELP-15395]
- Después de instalar un VDA, al intentar ver la ficha **Private Key** en **Certificate Properties**, es posible que aparezca este mensaje de error:  
**One or more of the objects properties are missing or invalid (Faltan al menos una de las propiedades de los objetos o las que hay no son válidas).**  
[CVADHELP-15703]
- Al volver a conectarse a una sesión, es posible que falle Citrix Audio Redirection Service (CtxAudioSvc). El problema se produce al ejecutar un VDA para un SO multisesión en la versión 2004 de Microsoft Windows 10 o una posterior. [CVADHELP-15804]
- Al conectarse desde un dispositivo de punto final táctil a un VDA con la versión 1912, es posible que el teclado en pantalla no funcione. El problema se produce con usuarios no administradores con el Control de cuentas de usuario habilitado en un VDA. [CVADHELP-16045]

- Puede que se inicie una sesión de XenApp no válida en un VDA para SO de servidor al desconectar y volver a conectar una sesión de escritorio remoto. La sesión no válida permanece abierta hasta que se reinicie el VDA. [CVADHELP-16453]
- Es posible que los cambios en la directiva de marca de agua, como **Incluir nombre de host del VDA** e **Incluir dirección IP del VDA**, no estén en vigor durante la siguiente sesión.

Para habilitar esta corrección, configure esta clave de Registro:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\Graphics\Watermark

Nombre: PolicyInterval

Tipo: DWORD

Valor: El valor que quiera en segundos (por ejemplo, 2 segundos)

[CVADHELP-16485]

- Al aplicar la corrección CVADHELP-12886 y, a continuación, utilizar una herramienta de recortes, es posible que el consumo de memoria aumente a 4 GB, lo que provoca que las sesiones dejen de responder. [CVADHELP-16542]
- Al intentar realizar una captura de pantalla con la herramienta Recortes o al hacer cálculos complejos, como una tabla dinámica, es posible que haya problemas de rendimiento. El problema se produce al establecer el valor de **CursorShapeChangeMinInterval** en 50 en la clave del Registro HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\Graphics. [CVADHELP-16718]
- Con esta corrección, ahora puede establecer diferentes métodos de entrada para cada ventana de aplicación disponible en los parámetros avanzados del teclado. [CVADHELP-16731]
- Al desconectar la sesión inicial iniciada desde Desktop Viewer en un dispositivo, es posible que se omita la función de reconexión rápida, lo que ralentiza la sesión. [CVADHELP-16953]

## Excepciones del sistema

- Con la directiva **Transporte adaptable HDX** habilitada, es posible que Terminal Services no se cierre al finalizar el servicio manualmente. [CVADHELP-15524]
- Al intentar ver archivos incrustados de Windows Media desde una aplicación web, es posible que Internet Explorer se cierre de forma inesperada. El problema se produce debido al módulo defectuoso, HostMMTransport.dll. [CVADHELP-15598]
- Los VDA podrían sufrir una excepción irreparable en wdica.sys y provocar un pantallazo azul. [CVADHELP-16055]
- Si Terminal Services se cierra de manera inesperada, es posible que se cancele el registro de los agentes VDA. El problema ocurre por un error en el módulo RPM.dll. [CVADHELP-16110]

## Componentes de escritorio virtual: Otros

- Es posible que no se pueda iniciar un ejecutable con comillas simples en el nombre del archivo.  
[CVADHELP-16104]

## Cumulative Update 2 (CU2)

September 22, 2021

Fecha de publicación: Noviembre de 2020

### Acerca de esta versión

Citrix Virtual Apps and Desktops 7 1912 LTSR Cumulative Update 2 (CU2) corrige más de 100 problemas notificados desde la publicación de 1912 LTSR CU1.

[1912 LTSR \(información general\)](#)

[1912 LTSR \(funciones e información sobre la actualización de la versión\)](#)

[Problemas resueltos desde Citrix Virtual Apps and Desktops 7 1912 LTSR CU1](#)

[Problemas conocidos en esta versión](#)

[Elementos eliminados y obsoletos](#)

[Fechas de elegibilidad de Subscription Advantage de los productos Citrix](#)

### Descargas

[Citrix Virtual Apps and Desktops 7 1912 LTSR CU2](#)

#### Importante:

Citrix License Administration Console alcanzó el final de su vida útil y el final del soporte técnico en servidor de licencias 11.16.3.0 compilación 30000. Utilice [Citrix Licensing Manager](#).

### Nuevas implementaciones

¿Cómo implemento la actualización CU2 desde cero?

Puede configurar un nuevo entorno de Citrix Virtual Apps and Desktops basado en CU2 con el metainstalador de CU2. Antes de ello, le recomendamos que se familiarice con el producto:

Consulte la sección [Citrix Virtual Apps and Desktops 7 1912 LTSR \(versión inicial\)](#) y lea atentamente las secciones [Información técnica general](#), [Instalar y configurar](#) y [Proteger](#) antes de planificar la implementación. Compruebe que la configuración cumple los [requisitos del sistema](#) de todos los componentes.

## Implementaciones existentes

¿Qué actualizo?

CU2 ofrece actualizaciones de componentes base de 1912 LTSR. Recuerde: Citrix recomienda actualizar todos los componentes de LTSR de la implementación a CU2. Por ejemplo: Si Citrix Provisioning forma parte de su implementación LTSR, actualice los componentes de Citrix Provisioning a CU2. Si Citrix Provisioning no forma parte de la implementación, no necesita instalarlo ni actualizarlo.

## Componentes base de Citrix Virtual Apps and Desktops 7 1912 LTSR CU2

Componente base de 1912 LTSR	Versión como se muestra en Programas y características	Notas
VDA de sesión única	1912.0.2000	
VDA multisesión	1912.0.2000	
Delivery Controller	1912.0.2000	
Citrix Studio	1912.0.2000	
Citrix Director	1912.0.2000	
Administración de Directivas de grupo Citrix	7.24.2000	
Extensión del cliente de Directivas de grupo Citrix	7.24.2000	
Citrix StoreFront	1912.0.2000	
Citrix Provisioning	1912.0.7	
Universal Print Server	1912.0.2000	
Grabación de sesiones	1912.0.2000	
Linux VDA	1912.0.2000	Consulte la <a href="#">documentación de Linux VDA</a> para ver las plataformas compatibles.
Profile Management	1912.0.2000	

<b>Componente base de 1912 LTSR</b>	<b>Versión como se muestra en Programas y características</b>	<b>Notas</b>
Servicio de autenticación federada de Citrix	1912.0.2000	
Redirección de contenido de explorador web	15.19.2000	
Citrix Probe Agent	2006	<a href="#">Descargas</a>

### Componentes compatibles de Citrix Virtual Apps and Desktops 7 1912 LTSR CU2

Los siguientes componentes, en las versiones que se indican a continuación, son compatibles con entornos LTSR. Estos componentes no dan derecho a las ventajas de LTSR (ciclo de vida ampliado y actualizaciones acumulativas de correcciones solamente). Citrix puede pedirle que actualice estos componentes a una versión más reciente dentro de sus entornos 1912 LTSR.

<b>Componentes y funciones compatibles</b>	<b>Versión como se muestra en Programas y características</b>
App Layering	19.11.0
Directivas de protección de aplicaciones	1912.0.0
HDX RealTime Optimization Pack	2.9 LTSR.
Servidor de licencias	11.16.6.0 compilación 32000
Capa de personalización de usuarios	19.11.0
Reproductor web de grabación de sesiones	1912.0.0
Optimización de Teams	1912.0.0
Autoservicio de restablecimiento de contraseñas	1.1
Windows 10 de 32 bits	
Workspace Environment Management	2003.0.0 y versiones posteriores
XenApp y XenDesktop 7.15 LTSR VDA (versión más reciente)*	Solo la actualización acumulativa más reciente

#### **Nota:**

Windows 10 de 32 bits solo es compatible durante 18 meses a partir de la publicación inicial de 1912 LTSR. Windows 10 32 de bits solo es compatible en Windows 10 Enterprise 2019 LTSC.

\* La compatibilidad con VDA de XenApp y XenDesktop 7.15 LTSR en este caso es solo para Windows 7 y Windows 2008 R2. XenApp y XenDesktop 7.15 LTSR dejará de ser compatible a partir de agosto de 2022. La compatibilidad con Citrix para Windows 7 y Windows 2008 R2 finalizará cuando Microsoft finalice el soporte para el sistema operativo o cuando finalice la compatibilidad con XenApp y XenDesktop 7.15 LTSR, lo que ocurra primero. Para obtener más información, consulte la [tabla de productos de Citrix](#).

## Versiones compatibles de la aplicación Citrix Workspace

Todas las versiones admitidas de la aplicación Citrix Workspace son compatibles con Citrix Virtual Apps and Desktops 1912 LTSR. Para obtener información sobre el ciclo de vida de la aplicación Citrix Workspace, consulte [Lifecycle Milestones for Citrix Workspace app and Citrix Receiver](#).

Para mayor comodidad, considere la posibilidad de suscribirse al [feed RSS de la aplicación Citrix Workspace](#) para recibir una notificación cuando una nueva versión de la aplicación Citrix Workspace esté disponible.

## Exclusiones importantes de Citrix Virtual Apps and Desktops 7 1912 LTSR CU2

Las siguientes funciones, componentes y plataformas no dan derecho a las ventajas y prestaciones del ciclo de vida de 1912 LTSR. Específicamente, se excluyen las ventajas de actualizaciones acumulativas y el ciclo de vida ampliado. Las actualizaciones de los componentes y funciones excluidos están disponibles a través de las versiones publicadas regularmente.

---

### Componentes y funciones excluidos

---

AppDisks

AppDNA

Citrix SCOM Management Pack

Framehawk

Personal vDisk

Integración de StoreFront con Citrix Online

---

---

### Plataformas Windows excluidas\*

---

Windows 2008 de 32 bits (para Universal Print Server)

---

\* Citrix se reserva el derecho a actualizar el soporte que ofrece para las plataformas en función de los hitos de los ciclos de vida de los proveedores externos.

## **Datos de análisis de instalación y actualización**

Cuando se usa el programa de instalación del producto completo para implementar o actualizar los componentes de XenApp o XenDesktop, se recopila información anónima sobre el proceso de instalación y se guarda en la máquina donde se está realizando la instalación o actualización del componente. Esta información se utiliza para ayudar a Citrix a mejorar la experiencia de instalación de sus clientes.

## **Migrar XenApp 6.5**

El proceso de migración de XenApp 6.5 permite realizar una transición eficaz y rápida desde una comunidad XenApp 6.5 a un sitio con 1912 LTSR. Esta transición puede resultarle útil en caso de implementaciones que contienen una gran cantidad de aplicaciones y directivas de grupo Citrix, porque reduce el riesgo de que se produzcan errores accidentales al mover manualmente las aplicaciones y las directivas de grupo Citrix al nuevo sitio de XenApp.

Después de instalar los componentes principales de 1912 LTSR y crear un sitio, el proceso de migración sigue estos pasos:

- Ejecute el instalador de 1912 en cada servidor de trabajo de XenApp 6.5. Este instalador actualiza automáticamente el servidor a un nuevo Virtual Delivery Agent para SO de servidor listo para usar en el nuevo sitio.
- Ejecute los cmdlets de exportación de PowerShell en un Controller de XenApp 6.5, que exporta las configuraciones de aplicaciones y directivas de Citrix a archivos XML.
- Si fuera necesario, modifique los archivos XML para seleccionar con exactitud lo que quiere importar al sitio nuevo. Al adaptar los archivos, puede importar las configuraciones de directivas y aplicaciones al sitio de 1912 LTSR por fases: algunas configuraciones ahora y otras más tarde.
- Ejecute los cmdlets de importación de PowerShell en el nuevo Controller de 1912, el cual importa las configuraciones contenidas en los archivos XML al nuevo sitio de XenApp.

Vuelva a configurar el nuevo sitio según sea necesario y, a continuación, haga pruebas en él.

Para obtener más información, consulte [Migrar XenApp 6.x](#).

## **Lista de correcciones presentes en 7.15 LTSR CU7, pero no incluidas en 1912 LTSR CU2**

Si está considerando la posibilidad de llevar a cabo esta actualización desde [7.15 LTSR CU7](#) a 1912 LTSR CU2, tenga en cuenta que un pequeño subconjunto de correcciones que se incluyen en 7.15

LTSR CU7 no están presentes en 1912 LTSR CU2. Si su implementación tiene dependencias en correcciones específicas incluidas en 7.15 LTSR CU7, Citrix recomienda que revise esta lista antes de realizar la actualización.

- CVADHELP-13287
- CVADHELP-13993
- CVADHELP-14249
- CVADHELP-14428
- CVADHELP-14515
- CVADHELP-14640
- CVADHELP-14740
- CVADHELP-14847
- CVADHELP-14865
- CVADHELP-14870
- CVADHELP-14905
- CVADHELP-14935
- CVADHELP-14950
- CVADHELP-14959
- CVADHELP-14965
- CVADHELP-15248
- CVADHELP-15298
- CVADHELP-15326
- CVADHELP-15536
- CVADHELP-15568
- CVADHELP-15572
- CVADHELP-15598
- CVADHELP-15608
- CVADHELP-15628
- CVADHELP-15724
- CVADHELP-15749
- CVADHELP-15792
- CVADHELP-15893
- CVADHELP-16036
- CVADHELP-16096
- CVADHELP-16097
- CVADHELP-16410
- CVADHELP-16453

## Problemas resueltos

June 19, 2023

Se han solucionado los siguientes problemas desde Citrix Virtual Apps and Desktops 7 1912 LTSR CU1:

### Citrix Director

- En Citrix Director, al extraer el informe de un grupo de entrega sin una conexión fallida en la ficha **Fallo**, en **Tendencias**, los detalles se rellenan correctamente. Sin embargo, los detalles de todos los grupos de entrega, incluido el grupo de entrega sin conexiones fallidas, pueden aparecer como si tuvieran conexiones fallidas al exportar el informe. [CVADHELP-14392]
- Cuando intenta configurar un servidor de correo electrónico en un servidor independiente mediante Citrix Director, puede aparecer este mensaje de error:

#### **Servidor de correo electrónico no válido.**

El problema se produce al configurar el servidor de correo electrónico para alertas y notificaciones. [CVADHELP-14648]

- Es posible que Citrix Director no muestre todas las filas de registros. Solo se exportan las 50 primeras entradas al archivo CSV, aunque la página del filtro **Instancias de aplicación** muestre varias instancias de aplicación. [CVADHELP-14783]
- En Citrix Director, al extraer el informe de un grupo de entrega en la ficha **Índice de patrón de carga**, es posible que los detalles aparezcan incorrectamente. El informe muestra los detalles de todos los grupos de entrega, en lugar del grupo de entrega seleccionado. [CVADHELP-14869]
- En Citrix Director, cuando comprueba el uso de máquina para un grupo de entrega seleccionado desde la **consola de Director > Tendencias > Uso de máquina**, el valor aparece como 0 (cero). El problema se produce al seleccionar un grupo de entrega en **Máquinas con SO multisesión**. El problema se produce solo con la columna En uso. [CVADHELP-15136]
- La integración de NetScaler Management and Analytics System (MAS) con Citrix Director puede fallar. Como resultado, el comando `C:\inetpub\wwwroot\Director\bin..\DisplayConfig\HdxInsightPlugin\Hd` falla con la siguiente excepción:  
**No se pudo realizar la operación de inicio de sesión y excepción interna: el servidor remoto devolvió un error: (400) Solicitud incorrecta.**  
[CVADHELP-15219]
- Cuando se remedia una sesión en la versión 1912 LTSR o 1912 LTSR CU1 de VDA, el proceso de Asistencia remota de Microsoft (msra.exe) puede cerrarse inesperadamente. [CVADHELP-15230]

- Puede que se agote el tiempo de la tarea de consolidación de Session Activity (actividad de la sesión), lo que afecta a la experiencia del usuario. [CVADHELP-15305]
- En la ficha **Administración de capacidad > Uso de aplicaciones alojadas**, al ver una tabla que muestra el uso basado en aplicaciones para un grupo de entrega durante un período de tiempo, los datos de uso pueden ser incorrectos. [CVADHELP-15368]

## Directiva de Citrix

- Es posible que la ficha **Directivas > Asignada a** muestre incorrectamente las directivas de Citrix que se asignan a uno o varios grupos de entrega. Por ejemplo, si asigna una directiva a dos grupos de entrega y habilita la asignación solo para uno de ellos. Al ir a la ficha **Asignada a**, se muestran ambos grupos de entrega. Cuando inhabilita la directiva, se anula la asignación. Sin embargo, la ficha **Asignada a** sigue mostrando la directiva como asignada. [CVADHELP-15233]
- Después de actualizar un VDA desde la versión de actualización acumulativa CU 2005 a la versión 2006, el servicio del motor de directivas de grupo (CseEngine.exe) puede cerrarse inesperadamente con el código de excepción 0xc0000409. [CVADHELP-15363]
- En Citrix Studio, cuando intenta crear o modificar una directiva de Citrix, aparece este mensaje de error en la ficha Registro:

### **Error al intentar determinar los detalles del cambio de directiva.**

La directiva se aplica correctamente, pero no se puede saber quién modificó la configuración. El problema se produce después de actualizar Citrix Virtual Apps and Desktops a la versión 1912 LTSR CU1 desde la versión 1912 LTSR. [CVADHELP-15726]

## Citrix Provisioning

La [documentación de Citrix Provisioning 1912 CU2](#) ofrece información específica acerca de las actualizaciones de esta versión.

## Citrix Studio

- Cuando inicia sesión en un escritorio dedicado, puede ocurrir un error de inicio de sesión y el proceso de cierre de sesión puede bloquearse. Citrix Studio muestra la sesión como conectada, pero esa sesión no se puede cerrar hasta que se reinicie manualmente la máquina. [CVADHELP-10932]
- Cuando se ejecuta Studio como aplicación publicada, es posible que deje de responder. [CVADHELP-14207]

- En la página **Asignación de máquinas**, es posible que falten algunas casillas de verificación. El problema se produce si se intenta agregar máquinas a un grupo de entrega o a un catálogo de máquinas que tiene una o más máquinas asignadas por el usuario. [CVADHELP-15684]
- Esta corrección reemplaza los siguientes parámetros de Registro con una directiva de Studio:
  - **Sincronización de la distribución del teclado del cliente y mejora de IME.** Habilita o inhabilita la sincronización dinámica de la distribución del teclado y el editor IME.
  - **Habilitar la asignación de distribución de teclado Unicode.** Habilita o inhabilita la asignación de distribución de teclado Unicode.
  - **Ocultar cuadro de mensaje emergente del botón de distribución del teclado.** Oculta o muestra el mensaje de notificación del botón para cambiar la distribución del teclado.

[CVADHELP-15706]

- Mientras se crea una conexión de alojamiento a Azure, es posible que no se pueda crear la entidad principal de servicio y aparezca el error **ADSTS700016**. [CVADHELP-16219]

## Delivery Controller

- Cuando se genera un informe del servidor de licencias mediante el comando **udadmin**, el informe puede mostrar que se emiten licencias para un mismo dispositivo varias veces. El problema ocurre cuando diferentes dispositivos con ID de hardware correctos se actualizan con nombres duplicados. El problema no afecta al consumo de licencias; solo al informe. [CVADHELP-13763]
- Al actualizar catálogos de máquinas por medio de Machine Creation Services, es posible que la carpeta de disco base anterior no se elimine del **almacenamiento de VMware**. [CVADHELP-14264]
- **MonitorData.** Es posible que la tabla de **[usuario]** presente en la base de datos de supervisión no sincronice los datos con Active Directory. Además, el nombre de usuario, el nombre simplificado y la información de UPN presente en la tabla se vuelven obsoletos. [CVADHELP-14700]
- Es posible que no se inicien algunas aplicaciones. Se bloquean muchas solicitudes de acceso a la tabla **Chb\_State.Sessions**. [CVADHELP-14876]
- Al seleccionar Catálogos de máquinas en el panel de navegación de Studio, es posible que Studio no muestre la lista de catálogos. Aparece este mensaje de error:

### No puede ver ningún catálogo.

El problema se produce porque Studio no puede obtener la lista de objetos mediante el comando **Get-ProvSchemeMasterVMImageHistory** PowerShell. [CVADHELP-15211]

- Puede que no se cree ningún catálogo de Machine Creation Services (MCS) cuando se utiliza VMware vSphere 7.0. [CVADHELP-15237]
- Esta corrección agrega compatibilidad con los tipos de máquinas NV4as\_v4 en Azure. [CVADHELP-15317]
- Con esta corrección, se eliminan las referencias de clave v1 al servicio Director y Monitor. [CVADHELP-15327]
- Después de actualizar un VDA a la versión 1912 LTSR CU1, el nombre de usuario de un usuario que no es de confianza que inicia sesión en la máquina aparece como **Dominio\UPN**, en lugar de **Dominio\Nombre de usuario**. [CVADHELP-15440]
- Con Citrix Analytics for Performance habilitado en Citrix Director, es posible que se produzca una pérdida de memoria en el servicio Monitor. [CVADHELP-15607]
- Se pueden leer los registros individuales de cada máquina cada 20 segundos durante 15 minutos, aunque falte una cuenta de almacenamiento de tablas. Pasado ese tiempo, el estado de energía deja de responder. [CVADHELP-15677]
- Cuando se utiliza Microsoft Azure, puede que no se descarguen las instantáneas. [CVADHELP-15679]
- Con esta corrección, está disponible Microsoft System Center Virtual Machine Manager (SCVMM) 2019 para Machine Creation Services (MCS). [CVADHELP-15779]
- Cambios realizados en el parámetro `DefaultInstall` permiten utilizar Microsoft System Center Configuration Manager (SCCM) para instalar la E/S de Machine Creation Services (MCSIO) en una cuenta del sistema. [CVADHELP-15593]
- Puede que un escritorio no se inicie cuando la acción de energía se envía desde el Delivery Controller. La acción de energía falla con la siguiente excepción:

**System.Runtime.Remoting.RemotingException**

[CVADHELP-15835]

- Esta corrección ofrece las siguientes mejoras:
  - **Proporciona compatibilidad con SSD estándar de Azure.** Al crear un catálogo, los administradores de Citrix Virtual Apps and Desktops pueden seleccionar SSD estándar como tipo de disco para los tipos de catálogo agrupados y persistentes.
  - **Permite Azure para la transferencia segura en Azure Storage.** La opción “Se requiere transferencia segura” mejora la seguridad de las cuentas de almacenamiento porque permite el acceso a las cuentas solo desde conexiones seguras.
  - **Resuelve un problema de almacenamiento en caché del estado de energía.** La sincronización del estado de energía se reduce de 20 a 5 minutos.

- **Permite la eliminación de restricciones a la administración de energía.** Puede encender 1000 máquinas virtuales en 12 minutos. Antes, esa operación tardaba 1 hora.
- Con esta corrección, Azure Resource Manager limita las solicitudes de suscripciones y arrendatarios gracias a una redirección del tráfico basada en límites definidos y adaptada a las necesidades específicas del proveedor.

[CVADHELP-15392]

- El estado de energía de las máquinas virtuales que obtiene Citrix Broker Service puede ser incorrecto, lo que ocasiona errores en el inicio de la sesión. El problema se produce cuando el Controller no puede encender o apagar correctamente las máquinas virtuales. [CVADHELP-15864]
- Cuando administra o enciende y apaga muchas máquinas mediante un plug-in de Microsoft Azure, pueden producirse excepciones de comunicación remota. [CVADHELP-16103]

## Linux VDA

La [documentación de Linux VDA 1912 CU2](#) ofrece información específica acerca de las actualizaciones de esta versión.

## Metainstalador

- Puede producirse una excepción cuando intenta ejecutar el instalador VDAServerSetup\_1912.exe. [CVADHELP-14457]
- Al actualizar un VDA, no se puede inhabilitar la función **Optimizar el rendimiento** en la página **Funciones**. Además, no se pueden habilitar otras funciones en esa página. [CVADHELP-14560]

## Profile Management

La [documentación de Profile Management 1912 CU2](#) ofrece información específica acerca de las actualizaciones de esta versión.

## Grabación de sesiones

La [documentación de Grabación de sesiones 1912 CU2](#) ofrece información específica acerca de las actualizaciones de esta versión.

## StoreFront

La [documentación de StoreFront 1912 CU2](#) ofrece información específica acerca de las actualizaciones de esta versión.

## Problemas de terceros

- Un problema en la versión 1809 de Microsoft Windows 10 puede causar un comportamiento ligeramente errático al usar el lápiz para Surface Pro y Surface Book. [HDX-17649]

## VDA para SO de sesión única

### Instalación, desinstalación y actualización

- Al actualizar la versión de un VDA, es posible que la clave de Registro **MaxVideoMemoryBytes** se revierta a su valor predeterminado. [CVADHELP-13629]

## Teclado

- Cuando presiona la tecla **Windows+ P** para ver la barra lateral de proyección, es posible que todos los monitores conectados muestren un fondo negro hasta que haga clic en la tecla Esc. El problema se produce con el **Paso de clave transparente** habilitado en una sesión integrada. [CVADHELP-14949]
- Para implementaciones de acceso con Remote PC, es posible que la entrada del teclado no funcione en sesiones que se ejecutan en dispositivos que no sean Windows. [CVADHELP-15291]
- Con la tecla F5 configurada como atajo de teclado para la función de **activación del nodo de terminal** en CATIA V5 Digital Mockup (DMU), es posible que, al volver a conectarse a una sesión, se active la función. [CVADHELP-15402]

## Sesión/Conexión

- Cuando inicia sesión en un escritorio dedicado, puede ocurrir un error de inicio de sesión y el proceso de cierre de sesión puede bloquearse. Citrix Studio muestra la sesión como conectada, pero esa sesión no se puede cerrar hasta que se reinicie manualmente la máquina. [CVADHELP-10931]
- Cuando se redirigen varios dispositivos USB a una sesión, es posible que uno de ellos no funcione correctamente. [CVADHELP-12516]

- Cuando se agregan dispositivos de audio a una sesión de usuario, no se puede escuchar sonido de ninguno de los dispositivos, excepto los sonidos de Skype Empresarial. Aparece este mensaje de error:

**Error - no more device slots available - failed to add the device.** (Error - no hay más ranuras de dispositivo disponibles - no se pudo agregar el dispositivo)

El problema ocurre cuando hay más de ocho dispositivos de reproducción o grabación conectados a un dispositivo de punto final. [CVADHELP-12760]

- Al configurar el parámetro **PPP elevado** para utilizar la resolución nativa, en lugar de PPP elevado, es posible que el escalado de PPP entre el VDA y el dispositivo de usuario no coincida. El problema ocurre durante la conexión inicial. [CVADHELP-13205]
- Es posible que el dispositivo de audio predeterminado de una sesión no sea el mismo que el predeterminado de un dispositivo de usuario. En la sesión, el primer dispositivo de la lista de dispositivos de audio se convierte en el predeterminado. [CVADHELP-13324]
- Después de reiniciar un VDA, es posible que la redirección USB cifrada basada en hardware no funcione. [CVADHELP-13336]
- En un entorno de varios monitores, es posible que las aplicaciones no se muestren de forma coherente en el mismo monitor. El problema se produce al cambiar de estación de trabajo. [CVADHELP-13657]
- Cuando utiliza la compresión de vídeo de cámara web de HDX RealTime, es posible que una cámara web muestre una imagen negra en lugar de una imagen en directo. [CVADHELP-13877]
- Algunas secciones de una ventana de aplicación pueden volverse transparentes, lo que hace que la aplicación se ejecute en segundo plano en lugar de en primer plano. El problema se produce en modo integrado. [CVADHELP-13903]
- En un sitio donde la versión 7.15 LTSR Cumulative Update 4 de XenApp y XenDesktop se ejecuta en Microsoft Windows Server 2016, es posible que la sesión de la aplicación deje de responder si se intenta iniciar una aplicación publicada. Aparece este mensaje de error:

**Espere al administrador de sesión local**

[CVADHELP-13967]

- Al iniciar por primera vez una sesión VDI en un monitor 4K, es posible que la sesión disponga de una resolución inferior. Además, puede aparecer un borde gris alrededor de la ventana de sesión. El problema ocurre con los dispositivos que usan ciertas tarjetas gráficas de terceros. [CVADHELP-14401]
- El proceso para gráficos de software de Citrix (Ctxgfx.exe) puede consumir constantemente memoria disponible dentro de una sesión. [CVADHELP-14509]

- Cuando instala VDA 1912 o 7.15 CU5 en una máquina física, Instrumental de administración de Windows (WMI) registra esa máquina como máquina virtual en lugar de como máquina física virtual. Microsoft System Center Configuration Manager (SCCM) registra esa máquina como máquina virtual, en lugar de como máquina física. El problema se produce cuando la directiva de Microsoft **Activar la seguridad basada en la virtualización** se **activa**.

Para habilitar la corrección, establezca la siguiente clave de Registro:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\XdMonitor

Nombre: IsVDARunningOnVM

Tipo: DWORD

Valor: 00000000

[CVADHELP-14597]

- En un VDA, cuando se vuelve a conectar a un cliente ligero de un solo monitor desde un cliente ligero de varios monitores, es posible que el diseño del monitor no se actualice. [CVADHELP-14646]
- Es posible que algunas aplicaciones de análisis de 32 bits de terceros no funcionen en un VDA cuando se redirigen al VDA mediante redirección de USB genérico. El problema ocurre cuando las aplicaciones de análisis del VDA utilizan TWAIN DSM. El problema también puede ocurrir en un VDA de acceso con Remote PC. [CVADHELP-14698]
- Cuando un usuario utiliza Acceso con Remote PC para acceder al PC de oficina, es posible que se vea la sesión remota desde el PC de oficina. Como resultado, se exponen a la vista las actividades de la sesión. [CVADHELP-14893]
- Puede que la optimización para Microsoft Teams no funcione en Microsoft Teams. El problema se produce cuando Citrix HDX no está conectado. [CVADHELP-14967]
- Esta corrección proporciona un temporizador que envía un pequeño datagrama a través de una conexión UDP y así mantiene activa la conexión entre el host y el cliente.

Para habilitar la corrección, cree la clave de Registro de esta manera:

- *En sistemas de 32 bits*

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\Audio

Nombre: KeepAliveTimer

Tipo: DWORD

Valor: Indica el intervalo del tiempo de espera (en segundos) entre los mensajes de mantenimiento de conexión. Si se deja vacío o se establece en 0, no se envían paquetes de mantenimiento de conexión y la función de mantenimiento de conexión no funciona. El valor recomendado es 15.

- *En sistemas de 64 bits*

HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Citrix\Audio

Nombre: KeepAliveTimer

Tipo: DWORD

Valor: Indica el intervalo del tiempo de espera (en segundos) entre los mensajes de mantenimiento de conexión. Si se deja vacío o se establece en 0, no se envían paquetes de mantenimiento de conexión y la función de mantenimiento de conexión no funciona. El valor recomendado es 15.

[CVADHELP-15122]

- Una sesión puede desconectarse al maximizar, minimizar o cambiar el tamaño del escritorio. El problema ocurre en la versión 1912 CU1 de VDA para SO de sesión única con Microsoft Windows 10, versión 1809. [CVADHELP-15200]
- Con el controlador CtxUvi Hooking inhabilitado, es posible que no se generen registros de eventos. El problema se produce cuando los recursos del sistema disponibles son bajos. [CVADHELP-15241]
- Cuando intenta volver a conectarse a una nueva máquina virtual, es posible que aparezca el siguiente mensaje de error de Microsoft .NET Framework:

**Error: Se produjo una excepción no controlada en su aplicación**

[CVADHELP-15267]

- Es posible que los canales virtuales más recientes no se agreguen a la lista interna codificada de canales permitidos. Cuando se habilita la lista de permitidos, los nuevos canales virtuales dejan de funcionar a menos que se agreguen ellos mismos a la lista de permitidos configurada por el usuario. [CVADHELP-15296]
- Con esta corrección, aparece un mensaje de advertencia en la estación de trabajo de un VDA antes de que la sesión se desconecte debido al tiempo de espera por inactividad. [CVADHELP-15319]
- Esta corrección proporciona compatibilidad con una nueva función que permite configurar varias implementaciones de bosque sin habilitar la autenticación NTLM en los VDA. Sin embargo, la función anterior para habilitar la autenticación NTLM se reserva para otras implementaciones sin confianza. Se agregó una entrada de Registro denominada **SupportMultipleForestDdcLookup** para evitar la habilitación no deseada de autenticación NTLM en los VDA. (NTLM es menos seguro que Kerberos.) Se puede utilizar **SupportMultipleForestDdcLookup**, en lugar de la entrada **SupportMultipleForest**. Puede seguir utilizando **SupportMultipleForest** para la compatibilidad con versiones anteriores. La clave de Registro **SupportMultipleForestDdcLookup** determina cómo los VDA realizan las búsquedas de los

Controllers. Para obtener más información, consulte [Implementación en un entorno de Active Directory de varios bosques](#). [CVADHELP-15467]

- Cuando un VDA intenta registrarse en un Delivery Controller, el agente de broker realiza una búsqueda de DNS inicial en el dominio local. Esta búsqueda garantiza que se pueda establecer conexión con el Delivery Controller. Cuando se produce un error en la búsqueda de DNS, el agente de broker recurre a consultas de arriba a abajo en Active Directory, realizando repetidamente búsquedas en todos los dominios. Si la dirección del Delivery Controller no es válida (por ejemplo, el administrador escribió el FQDN incorrectamente al instalar el VDA), las operaciones de consulta pueden provocar resultados similares a DDoS (denegación de servicio distribuido) en el controlador de dominio. Para obtener más información, consulte [Búsqueda del Controller durante el registro de VDA](#). [CVADHELP-15484]
- Con la directiva Modo de gráficos antiguo habilitada, puede aparecer una pantalla gris al iniciar una sesión. Este problema se produce con la versión 7.15.6000 de VDA. [CVADHELP-15841]
- Con esta corrección, Hook WTS se habilita de forma predeterminada cuando se establece el indicador en 0x80000000. [CVADHELP-15929]
- Pueden darse los siguientes problemas con Microsoft Teams:
  - Cuando se vuelve a conectar a una sesión, es posible que el proceso HdxTeams.exe no se inicie. El problema se produce en un VDA con Microsoft Windows Server.
  - Es posible que Citrix HDX Teams Redirection Service (TeamsSvc) no obtenga el ID de la sesión de usuario. Como resultado, no se actualiza la clave de Registro de redirección para Microsoft Teams.
  - Al volver a conectarse a una sesión, es posible que Citrix HDX Teams Redirection Service (TeamsSvc) se cierre inesperadamente.

[CVADHELP-16213]

### Tarjetas inteligentes

- Con esta corrección, puede rastrear la cantidad de veces que se ha insertado o retirado una tarjeta inteligente de un lector mediante la función **SCardGetStatusChange**. [CVADHELP-15463]

### Excepciones del sistema

- Es posible que Citrix Audio Redirection Service (CtxAudioSvc) se cierre de manera inesperada con un ID de evento 1000 y un código de excepción 0x0c000005. El problema se debe a un error en el módulo CtxVorbisDmo64.dll. [CVADHELP-14898]
- Es posible que el proceso PicaShell.exe se cierre de manera inesperada cuando hay daños en el montón en la DLL del canal virtual del portapapeles. [CVADHELP-14945]

- El complemento del explorador Internet Explorer (Citrix HDXJsInjector) necesario para la redirección de contenido puede provocar un error de página web cuando se utilizan las herramientas del desarrollador. InjectorScript.js experimenta de forma intermitente una excepción en tiempo de ejecución al acceder al encabezado de documento HTML. Aparece este mensaje de error:

**Error: Unable to get property 'appendChild' of undefined or null reference.**

[CVADHELP-14960]

- Los VDA pueden experimentar una excepción irrecuperable en tdica.sys y mostrar una pantalla azul con el código de comprobación de errores 0x1000007e. El problema se produce cuando inicia una sesión a través de la aplicación Citrix Workspace para HTML5. [CVADHELP-15220]

### Experiencia de usuario

- Cuando ciertas aplicaciones de terceros se ejecutan dentro de una sesión de usuario, es posible que el puntero del mouse cambie a un círculo giratorio. El problema se produce cuando arrastra un objeto en la sesión o realiza una operación de zoom. [CVADHELP-14247]

### VDA para SO multisesión

#### Teclado

- Cuando presiona la tecla **Windows+ P** para ver la barra lateral de proyección, es posible que todos los monitores conectados muestren un fondo negro hasta que haga clic en la tecla Esc. El problema se produce con el **Paso de clave transparente** habilitado en una sesión integrada. [CVADHELP-14949]

#### Sesión/Conexión

- Cuando se redirigen varios dispositivos USB a una sesión, es posible que uno de ellos no funcione correctamente. [CVADHELP-12516]
- Al intentar resaltar texto en una sesión de usuario, es posible que haya problemas de rendimiento. El problema ocurre cuando se ejecuta Microsoft Outlook versión 2016 en un escritorio publicado.

Para habilitar la corrección, establezca la siguiente clave de Registro:

Ruta: HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\Graphics

Nombre: CursorShapeChangeMinInterval

Tipo: DWORD

Valor: Valores posibles: 10 a 100. Valor recomendado: 50. El valor predeterminado es 0, lo que significa inhabilitado.

[CVADHELP-12886]

- Después de reiniciar un VDA, es posible que la redirección USB cifrada basada en hardware no funcione. [CVADHELP-13336]
- En un entorno de varios monitores, es posible que las aplicaciones no se muestren de forma coherente en el mismo monitor. El problema se produce al cambiar de estación de trabajo. [CVADHELP-13657]
- Cuando utiliza la compresión de vídeo de cámara web de HDX RealTime, es posible que una cámara web muestre una imagen negra en lugar de una imagen en directo. [CVADHELP-13877]
- Algunas secciones de una ventana de aplicación pueden volverse transparentes, lo que hace que la aplicación se ejecute en segundo plano en lugar de en primer plano. El problema se produce en modo integrado. [CVADHELP-13903]
- En un sitio donde la versión 7.15 LTSR Cumulative Update 4 de XenApp y XenDesktop se ejecuta en Microsoft Windows Server 2016, es posible que la sesión de la aplicación deje de responder si se intenta iniciar una aplicación publicada. Aparece este mensaje de error:

**Espere al administrador de sesión local**

[CVADHELP-13967]

- El proceso para gráficos de software de Citrix (Ctxgfx.exe) puede consumir constantemente memoria disponible dentro de una sesión. [CVADHELP-14509]
- Cuando se intenta cargar un archivo (CRX, EXE o ZIP) a través de una sesión de la aplicación Citrix Workspace para HTML5, la fiabilidad de la sesión puede provocar que la sesión se desconecte. [CVADHELP-14513]
- Después de que un VDA informe de una carga completa debido a un uso de memoria elevado, el valor del índice de carga puede permanecer en 10 000, incluso si el uso de memoria desciende a un nivel bajo. [CVADHELP-14563]
- El proceso winlogon.exe de Microsoft Windows puede cerrarse de manera imprevista. El problema ocurre al cerrar una sesión integrada iniciada a través de un servidor. El problema se debe a un error en el módulo icagfxstack.dll. [CVADHELP-14579]
- Al bloquear una sesión integrada, es posible que la ventana de inicio de sesión cubra toda la pantalla, independientemente del tamaño de la ventana de sesión. Como consecuencia, no se puede acceder al escritorio del dispositivo de punto final ni a otras aplicaciones. [CVADHELP-14589]

- Es posible que algunas aplicaciones de análisis de 32 bits de terceros no funcionen en un VDA cuando se redirigen al VDA mediante redirección de USB genérico. El problema ocurre cuando las aplicaciones de análisis del VDA utilizan TWAIN DSM. El problema también puede ocurrir en un VDA de acceso con Remote PC. [CVADHELP-14698]
- Esta corrección soluciona una vulnerabilidad de seguridad en un componente subyacente. Para obtener más información, consulte el artículo [CTX285059](#) de Knowledge Center. [CVADHELP-14755]
- Con la directiva **Permite que se ejecute la zona de pruebas de audio**, es posible que el audio no funcione en Google Chrome que se abra a través de Citrix Virtual Apps and Desktops. [CVADHELP-14784]
- Puede que la optimización para Microsoft Teams no funcione en Microsoft Teams. El problema se produce cuando Citrix HDX no está conectado. [CVADHELP-14967]
- Esta corrección proporciona un temporizador que envía un pequeño datagrama a través de una conexión UDP y así mantiene activa la conexión entre el host y el cliente.

Para habilitar la corrección, cree la clave de Registro de esta manera:

- *En sistemas de 32 bits*

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\Audio

Nombre: KeepAliveTimer

Tipo: DWORD

Valor: Indica el intervalo del tiempo de espera (en segundos) entre los mensajes de mantenimiento de conexión. Si se deja vacío o se establece en 0, no se envían paquetes de mantenimiento de conexión y la función de mantenimiento de conexión no funciona. El valor recomendado es 15.

- *En sistemas de 64 bits*

HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Citrix\Audio

Nombre: KeepAliveTimer

Tipo: DWORD

Valor: Indica el intervalo del tiempo de espera (en segundos) entre los mensajes de mantenimiento de conexión. Si se deja vacío o se establece en 0, no se envían paquetes de mantenimiento de conexión y la función de mantenimiento de conexión no funciona. El valor recomendado es 15.

[CVADHELP-15122]

- Con el controlador CtxUvi Hooking inhabilitado, es posible que no se generen registros de eventos. El problema se produce cuando los recursos del sistema disponibles son bajos. [CVADHELP-15241]
- Cuando intenta volver a conectarse a una nueva máquina virtual, es posible que aparezca el siguiente mensaje de error de Microsoft .NET Framework:

**Error: Se produjo una excepción no controlada en su aplicación**

[CVADHELP-15267]

- Es posible que los canales virtuales más recientes no se agreguen a la lista interna codificada de canales permitidos. Cuando se habilita la lista de permitidos, los nuevos canales virtuales dejan de funcionar a menos que se agreguen ellos mismos a la lista de permitidos configurada por el usuario. [CVADHELP-15296]
- Cuando se intenta cambiar a una ventana desde la vista previa de la barra de tareas, esa ventana puede tardar mucho tiempo en abrirse. [CVADHELP-15422]
- Esta corrección proporciona compatibilidad con una nueva función que permite configurar varias implementaciones de bosque sin habilitar la autenticación NTLM en los VDA. Sin embargo, la función anterior para habilitar la autenticación NTLM se reserva para otras implementaciones sin confianza. Se agregó una entrada de Registro denominada **SupportMultipleForestDdcLookup** para evitar la habilitación no deseada de autenticación NTLM en los VDA. (NTLM es menos seguro que Kerberos.) Se puede utilizar **SupportMultipleForestDdcLookup**, en lugar de la entrada **SupportMultipleForest**. Puede seguir utilizando **SupportMultipleForest** para la compatibilidad con versiones anteriores. La clave de Registro **SupportMultipleForestDdcLookup** determina cómo los VDA realizan las búsquedas de los Controllers. Para obtener más información, consulte [Implementación en un entorno de Active Directory de varios bosques](#). [CVADHELP-15467]
- Cuando un VDA intenta registrarse en un Delivery Controller, el agente de broker realiza una búsqueda de DNS inicial en el dominio local. Esta búsqueda garantiza que se pueda establecer conexión con el Delivery Controller. Cuando se produce un error en la búsqueda de DNS, el agente de broker recurre a consultas de arriba a abajo en Active Directory, realizando repetidamente búsquedas en todos los dominios. Si la dirección del Delivery Controller no es válida (por ejemplo, el administrador escribió el FQDN incorrectamente al instalar el VDA), las operaciones de consulta pueden provocar resultados similares a DDoS (denegación de servicio distribuido) en el controlador de dominio. [CVADHELP-15484]
- Con esta corrección, Hook WTS se habilita de forma predeterminada cuando se establece el indicador en 0x80000000. [CVADHELP-15929]

## Tarjetas inteligentes

- Con esta corrección, puede rastrear la cantidad de veces que se ha insertado o retirado una tarjeta inteligente de un lector mediante la función **SCardGetStatusChange**. [CVADHELP-15463]

## Excepciones del sistema

- Es posible que el proceso host de servicios (svchost.exe) que aloja el servicio de audio de Windows se cierre inesperadamente dentro de una sesión de usuario. El problema se produce debido a una fuga de memoria. [CVADHELP-13687]
- Es posible que el proceso Service Host (svchost.exe) del proceso wfshell.exe sufra una infracción de acceso y se cierre de forma imprevista. El problema ocurre por un error en el módulo icaendpoint.dll. [CVADHELP-14276]
- Los VDA pueden experimentar una excepción irrecoverable y provocar un pantallazo azul en picadm.sys con el código de comprobación de errores 0x22. [CVADHELP-14332]
- El proceso wfshell.exe puede cerrarse inesperadamente. [CVADHELP-14414]
- En un dispositivo con más de nueve monitores, los intentos de iniciar una sesión de usuario pueden fallar con una excepción irrecoverable y provocar un pantallazo azul con el código de comprobación de errores 0x3B. [CVADHELP-14775]
- Es posible que Citrix Audio Redirection Service (CtxAudioSvc) se cierre de manera inesperada con un ID de evento 1000 y un código de excepción 0x0c000005. El problema se debe a un error en el módulo CtxVorbisDmo64.dll. [CVADHELP-14898]
- Es posible que el proceso PicaShell.exe se cierre de manera inesperada cuando hay daños en el montón en la DLL del canal virtual del portapapeles. [CVADHELP-14945]
- El complemento del explorador Internet Explorer (Citrix HDXJsInjector) necesario para la redirección de contenido puede provocar un error de página web cuando se utilizan las herramientas del desarrollador. InjectorScript.js experimenta de forma intermitente una excepción en tiempo de ejecución al acceder al encabezado de documento HTML. Aparece este mensaje de error:

**Error: Unable to get property 'appendChild' of undefined or null reference.**

[CVADHELP-14960]

- Los VDA pueden experimentar una excepción irrecoverable en tdica.sys y mostrar una pantalla azul con el código de comprobación de errores 0x1000007e. El problema se produce cuando inicia una sesión a través de la aplicación Citrix Workspace para HTML5. [CVADHELP-15220]

- Cuando intenta volver a conectarse a una sesión TCP habilitada para varios puertos iniciada desde la aplicación Citrix Workspace para Linux, es posible que el VDA se cierre inesperadamente. [CVADHELP-15674]

## Componentes de escritorio virtual: Otros

- Al iniciar una aplicación de App-V mediante un acceso directo que se encuentre fuera del paquete de la aplicación, es posible que se agregue el argumento **appve** a la línea de comandos. Este argumento **appve** es innecesario. [CVADHELP-14369]
- Es posible que no se inicie una aplicación App-V desde un acceso directo ubicado en la carpeta **AppData** . [CVADHELP-14691]
- Esta corrección soluciona una vulnerabilidad de seguridad en un componente subyacente. Para obtener más información, consulte el artículo [CTX285059](#) de Knowledge Center. [CVADHELP-14989]
- Si crea aplicaciones App-V mediante el método de administración única en Citrix Studio, puede que la enumeración de aplicaciones sea lenta. El problema se produce cuando hay presentes aplicaciones duplicadas en los paquetes de App-V. [CVADHELP-15427]
- Esta corrección soluciona una vulnerabilidad de seguridad en un componente subyacente. Para obtener más información, consulte el artículo [CTX285059](#) de Knowledge Center. [CVADHELP-15612]

## Cumulative Update 1 (CU1)

September 22, 2021

Fecha de publicación: 7 de mayo de 2020

### Acerca de esta versión

Citrix Virtual Apps and Desktops 7 1912 LTSR Cumulative Update 1 (CU1) corrige más de 70 problemas notificados desde la publicación de la versión inicial de 1912 LTSR.

[1912 LTSR \(información general\)](#)

[1912 LTSR \(funciones e información sobre la actualización de la versión\)](#)

[Problemas resueltos desde Citrix Virtual Apps and Desktops 7 1912 LTSR \(versión inicial\)](#)

[Problemas conocidos en esta versión](#)

[Elementos eliminados y obsoletos](#)

[Fechas de elegibilidad de Subscription Advantage de los productos Citrix](#)

## Descargas

[Citrix Virtual Apps and Desktops 7 1912 LTSR CU1](#)

### Importante:

Esta versión presenta cambios en la instalación y actualización de StoreFront. En versiones anteriores, al hacer clic en el icono **Introducción** de la página principal del instalador del producto completo, la página **Componentes principales** incluía StoreFront. Se puede seleccionar StoreFront y otros componentes principales para instalarlos en la misma máquina.

A partir de esta versión, la página **Componentes principales** ya no contiene la casilla de StoreFront. Para instalar o actualizar una versión de StoreFront, haga clic en **Citrix StoreFront** en el panel **Ampliar implementación** de la página principal. Esto inicia `CitrixStoreFront-x64.exe` desde los medios de instalación.

En el comando `XenDesktopServerSetup.exe`, ya no se puede especificar `/components storefront`. Si lo hace, el comando falla. Para instalar StoreFront desde la línea de comandos, ejecute `CitrixStoreFront-x64.exe`, que está disponible en la carpeta `x64` de los medios de instalación de Citrix Virtual Apps and Desktops.

## Nuevas implementaciones

¿Cómo implemento la actualización CU1 desde cero?

Puede configurar un nuevo entorno de Citrix Virtual Apps and Desktops basado en CU1 con el metainstalador de CU1. Antes de ello, le recomendamos que se familiarice con el producto:

Consulte la sección [Citrix Virtual Apps and Desktops 7 1912 LTSR \(versión inicial\)](#) y lea atentamente las secciones [Información técnica general](#), [Instalar y configurar](#) y [Proteger](#) antes de planificar la implementación. Compruebe que la configuración cumple los [requisitos del sistema](#) de todos los componentes.

## Implementaciones existentes

¿Qué actualizo?

CU1 ofrece actualizaciones de 15 componentes base de 1912 LTSR. Recuerde: Citrix recomienda actualizar todos los componentes de LTSR de la implementación a CU1. Por ejemplo: Si Citrix Provisioning

forma parte de su implementación LTSR, actualice los componentes de Citrix Provisioning a CU1. Si Citrix Provisioning no forma parte de la implementación, no necesita instalarlo ni actualizarlo.

### Componentes base de Citrix Virtual Apps and Desktops 7 1912 LTSR CU1

Componente base de 1912 LTSR	Versión como se muestra en Programas y características	Notas
VDA de sesión única	1912.0.1000	
VDA multisesión	1912.0.1000	
Delivery Controller	1912.0.1000	
Citrix Studio	1912.0.1000	
Citrix Director	1912.0.1000	
Administración de Directivas de grupo Citrix	7.24.1000	
Extensión del cliente de Directivas de grupo Citrix	7.24.1000	
Citrix StoreFront	1912.0.1000	
Citrix Provisioning	1912.0.1	
Universal Print Server	1912.0.1000	
Grabación de sesiones	1912.0.1000	
Linux VDA	1912.0.1000	Consulte la <a href="#">documentación de Linux VDA</a> para ver las plataformas compatibles.
Profile Management	1912.0.1000	
Servicio de autenticación federada de Citrix	1912.0.1000	
Redirección de contenido de explorador web	15.19.1000	

### Componentes compatibles de Citrix Virtual Apps and Desktops 7 1912 LTSR CU1

Los siguientes componentes, en las versiones que se indican a continuación, son compatibles con entornos LTSR. Estos componentes no dan derecho a las ventajas de LTSR (ciclo de vida ampliado y actualizaciones acumulativas de correcciones solamente). Citrix puede pedirle que actualice estos componentes a una versión más reciente dentro de sus entornos 1912 LTSR.

<b>Componentes y funciones compatibles</b>	<b>Versión como se muestra en Programas y características</b>
App Layering	19.11.0
Directivas de protección de aplicaciones	1912.0.0
HDX RealTime Optimization Pack	2.9 LTSR.
Servidor de licencias	11.16.3.0, compilación 30000
Capa de personalización de usuarios	19.11.0
Reproductor web de grabación de sesiones	1912.0.0
Optimización de Teams	1912.0.0
Autoservicio de restablecimiento de contraseñas	1.1
Windows 10 de 32 bits	
Workspace Environment Management	2003.0.0 y versiones posteriores
XenApp y XenDesktop 7.15 LTSR VDA (versión más reciente)*	Solo la actualización acumulativa más reciente

**Nota:**

Windows 10 de 32 bits solo es compatible durante 18 meses a partir de la publicación inicial de 1912 LTSR. Windows 10 32 de bits solo es compatible en Windows 10 Enterprise 2019 LTSC.

\* La compatibilidad con VDA de XenApp y XenDesktop 7.15 LTSR en este caso es solo para Windows 7 y Windows 2008 R2. XenApp y XenDesktop 7.15 LTSR dejará de ser compatible a partir de agosto de 2022. La compatibilidad con Citrix para Windows 7 y Windows 2008 R2 finalizará cuando Microsoft finalice el soporte para el sistema operativo o cuando finalice la compatibilidad con XenApp y XenDesktop 7.15 LTSR, lo que ocurra primero. Para obtener más información, consulte la [tabla de productos de Citrix](#).

**Versiones compatibles de la aplicación Citrix Workspace**

Todas las versiones admitidas de la aplicación Citrix Workspace son compatibles con Citrix Virtual Apps and Desktops 1912 LTSR. Para obtener información sobre el ciclo de vida de la aplicación Citrix Workspace, consulte [Lifecycle Milestones for Citrix Workspace app and Citrix Receiver](#).

Para mayor comodidad, considere la posibilidad de suscribirse al [feed RSS de la aplicación Citrix Workspace](#) para recibir una notificación cuando una nueva versión de la aplicación Citrix Workspace esté disponible.

## **Exclusiones importantes de Citrix Virtual Apps and Desktops 7 1912 LTSR CU1**

Las siguientes funciones, componentes y plataformas no dan derecho a las ventajas y prestaciones del ciclo de vida de 1912 LTSR. Específicamente, se excluyen las ventajas de actualizaciones acumulativas y el ciclo de vida ampliado. Las actualizaciones de los componentes y funciones excluidos están disponibles a través de las versiones publicadas regularmente.

---

### **Componentes y funciones excluidos**

---

AppDisks

AppDNA

Citrix SCOM Management Pack

Framehawk

Personal vDisk

Integración de StoreFront con Citrix Online

---

---

### **Plataformas Windows excluidas\***

---

Windows 2008 de 32 bits (para Universal Print Server)

---

\* Citrix se reserva el derecho a actualizar el soporte que ofrece para las plataformas en función de los hitos de los ciclos de vida de los proveedores externos.

## **Datos de análisis de instalación y actualización**

Cuando se usa el programa de instalación del producto completo para implementar o actualizar los componentes de XenApp o XenDesktop, se recopila información anónima sobre el proceso de instalación y se guarda en la máquina donde se está realizando la instalación o actualización del componente. Esta información se utiliza para ayudar a Citrix a mejorar la experiencia de instalación de sus clientes.

## **Migrar XenApp 6.5**

El proceso de migración de XenApp 6.5 permite realizar una transición eficaz y rápida desde una comunidad XenApp 6.5 a un sitio con 1912 LTSR. Esta transición puede resultarle útil en caso de implementaciones que contienen una gran cantidad de aplicaciones y directivas de grupo Citrix, porque

reduce el riesgo de que se produzcan errores accidentales al mover manualmente las aplicaciones y las directivas de grupo Citrix al nuevo sitio de XenApp.

Después de instalar los componentes principales de 1912 LTSR y crear un sitio, el proceso de migración sigue estos pasos:

- Ejecute el instalador de 1912 en cada servidor de trabajo de XenApp 6.5. Este instalador actualiza automáticamente el servidor a un nuevo Virtual Delivery Agent para SO de servidor listo para usar en el nuevo sitio.
- Ejecute los cmdlets de exportación de PowerShell en un Controller de XenApp 6.5, que exporta las configuraciones de aplicaciones y directivas de Citrix a archivos XML.
- Si fuera necesario, modifique los archivos XML para seleccionar con exactitud lo que quiere importar al sitio nuevo. Al adaptar los archivos, puede importar las configuraciones de directivas y aplicaciones al sitio de 1912 LTSR por fases: algunas configuraciones ahora y otras más tarde.
- Ejecute los cmdlets de importación de PowerShell en el nuevo Controller de 1912, el cual importa las configuraciones contenidas en los archivos XML al nuevo sitio de XenApp.

Vuelva a configurar el nuevo sitio según sea necesario y, a continuación, haga pruebas en él.

Para obtener más información, consulte [Migrar XenApp 6.x](#).

## Problemas resueltos

September 22, 2021

Se han solucionado los siguientes problemas desde Citrix Virtual Apps and Desktops 7 1912 LTSR (versión inicial):

### Citrix Director

- Cuando un Delivery Controller está apagado, Citrix Director muestra su estado incorrectamente. Como consecuencia, aparecen alertas falsas en la ficha *Infraestructura* de Citrix Director. [CVADHELP-13835]

### Directiva de Citrix

- Los servidores pueden desconectarse y dejar de responder, a menos que reinicie Group Policy Engine Service (CseEngine.exe). [CVADHELP-12987]

## Citrix Provisioning

La [documentación de Citrix Provisioning 1912 CU1](#) ofrece información específica acerca de las actualizaciones de esta versión.

## Citrix Studio

- Al actualizar Citrix Studio de la versión 7.6 a la versión 7.15, es posible que aumente el tiempo que se tarda en abrir algunos asistentes (como Catálogo de máquinas y Grupo de entrega). [CVADHELP-13267]
- Al agregar paquetes de App-V a Citrix Studio, algunos paquetes pueden mostrar iconos predeterminados en lugar de iconos personalizados. [CVADHELP-13338]

## Delivery Controller

- Es posible que algunas aplicaciones publicadas provoquen un error en la enumeración de aplicaciones. El problema se produce cuando el icono de una aplicación dañada está presente en un archivo EXE. [CVADHELP-13133]
- Una vez finalizado el horario de verano para el año 2019 y con la programación de reinicio configurada, ocurrió un reinicio programado imprevisto solo para el grupo de entrega. [CVADHELP-13486]
- Al agregar administradores de otros dominios a Citrix Studio, es posible que Studio muestre el siguiente mensaje de error:

**Error: No se pudo validar la ubicación de Central Configuration Service.**

**No tiene permisos suficientes para administrar el sitio mediante Studio, o bien hay un problema con Delegated Administration Service.**

El problema se produce si no se puede contactar con un controlador de dominio de uno de los dominios. [CVADHELP-13651]

- Con esta corrección, Machine Creation Services (MCS) ofrece las siguientes funciones nuevas de Citrix Hypervisor: arranque con UEFI para invitados y arranque seguro. [CVADHELP-14210]
- En Citrix Hypervisor, es posible que no se pueda agregar máquinas a un catálogo existente de Machine Creation Services (MCS). [CVADHELP-14212]

## Servicio de autenticación federada

- En las propiedades de la plantilla de certificado Citrix\_SmartCardLogon, la descripción de la extensión Uso de clave debe contener solo “Firma digital” y “Cifrado de clave”, pero muestra otros

elementos adicionales. Sin embargo, los certificados emitidos con esta plantilla son correctos.  
[CVADHELP-14040]

## **Linux Virtual Delivery Agent**

La [documentación de Linux Virtual Delivery Agent 1912 CU1](#) proporciona información específica acerca de las actualizaciones de esta versión.

## **Metainstalador**

- Al intentar iniciar un escritorio, es posible que aparezca una pantalla gris. El problema se produce después de actualizar la versión 7.6 LTSR Cumulative Update de un VDA a la versión 1912. [CVADHELP-13969]

## **Profile Management**

La [documentación de Profile Management 1912 CU1](#) ofrece información específica acerca de las actualizaciones de esta versión.

## **Grabación de sesiones**

La [documentación de Grabación de sesiones 1912 CU1](#) ofrece información específica acerca de las actualizaciones de esta versión.

## **StoreFront**

La [documentación de StoreFront 1912 CU1](#) ofrece información específica acerca de las actualizaciones de esta versión.

## **Universal Print Server**

### **Ciente**

- Al intentar iniciar una aplicación, es posible que Citrix Print Manager Service (CpSvc.exe) se cierre de forma inesperada. [CVADHELP-13945]
- Es posible que el servicio Print Spooler se cierre de forma inesperada. [CVADHELP-13954]

## Servidor

- Debido a una infracción de acceso, Universal Print Server (UPServer.exe) puede cerrarse de forma inesperada. [CVADHELP-10627]

## VDA para SO de sesión única

### Instalación, desinstalación y actualización

- Al actualizar la versión de un VDA, es posible que la clave del Registro `MaxVideoMemoryBytes` se revierta a su valor predeterminado. [CVADHELP-13629]

## Impresión

- Al intentar iniciar una aplicación, es posible que Citrix Print Manager Service (CpSvc.exe) se cierre de forma inesperada. [CVADHELP-13945]
- Es posible que las impresoras PDF creadas automáticamente no se eliminen. El problema se produce si se crean en `HKEY_LOCAL_MACHINE\SOFTWARE` en lugar de `HKEY_CURRENT_CONFIG`. [CVADHELP-14280]

## Sesión/Conexión

- Cuando el Reproductor de Windows Media pasa de la pista actual a la pista siguiente de la lista de reproducción, es posible que el audio no se reproduzca al principio de la pista siguiente. El problema se produce si la redirección de Windows Media está habilitada. [CVADHELP-11639]
- Al volver a conectarse a una sesión activa en otra máquina, es posible que falten impresoras redirigidas y unidades de cliente. El problema se produce al pasar de una máquina a otra sin bloquear o desconectar la sesión activa de usuario. [CVADHELP-13035]
- Es posible que la lectura de datos de una unidad de cliente tarde mucho tiempo después de cambiar el valor de la siguiente clave del Registro a 1 en un VDA:

Para habilitar la corrección, cree la siguiente clave de Registro:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd`

Nombre: `PacketIntegrityChecks`

Tipo: `DWORD`

Valor: `1`

[CVADHELP-13063]

- Es posible que no se pueda iniciar una sesión en un VDA al utilizar algunos analizadores de vulnerabilidades de terceros. [CVADHELP-13306]
- Es posible que fallen los intentos de reconectarse a sesiones, con el siguiente mensaje de error:  
**No se puede iniciar el escritorio.**  
[CVADHELP-13320]
- Al intentar cambiar el tamaño de la ventana de un escritorio publicado, es posible que la codificación por hardware no esté habilitada. [CVADHELP-13818]
- Es posible que un VDA deje de responder después del reinicio. El problema se produce cuando un software de seguridad, como Symantec SEP, aplica análisis de seguridad. [CVADHELP-13832]
- Con la directiva **Visualización automática del teclado** habilitada, al hacer clic en el cuadro **Buscar en Google**, es posible que el teclado no aparezca automáticamente. El problema se produce cuando se ejecuta una sesión en los exploradores Internet Explorer, Firefox o Chrome. [CVADHELP-14065]
- Al hacer clic con el botón secundario en el icono de usuario del menú Inicio, el menú contextual no muestra las opciones **Apagar** ni **Cerrar sesión**. En su lugar, el menú contextual muestra las mismas opciones que el menú contextual que aparece después de hacer clic con el botón secundario en un icono. [CVADHELP-14149]
- Con la directiva de zona horaria establecida en **Usar la hora local del cliente**, es posible que la zona horaria se redirija incorrectamente al iniciar una sesión a través de la aplicación Citrix Workspace para HTML5. Por ejemplo, la hora se establece en **UTC+01:00** en lugar de **UTC+00:00**. Como resultado, el parámetro **Ajustar el reloj automáticamente al horario de verano** se desactiva en lugar de activarse. [CVADHELP-14471]
- En un caso de doble salto, puede que un solo usuario consuma dos licencias de usuario simultáneo (CCU) de Citrix. El doble salto es cuando un usuario inicia la sesión HDX dentro de otra sesión HDX (por ejemplo, cuando se inicia una aplicación publicada en una sesión de escritorio virtual). [CVADHELP-14409]
- Al intentar mover objetos pequeños en la pantalla, es posible que se dañe un único píxel. El problema se produce cuando la directiva **Calidad visual** se establece en **Gradual sin pérdida**. [CVADFIX-8214]

### Tarjetas inteligentes

- Después de configurar la autenticación con tarjeta inteligente en Windows 10, es posible que la autenticación PassThrough con tarjeta inteligente falle si inicia un escritorio en una sesión de usuario. El problema se produce al iniciar un escritorio desde un cliente ligero. [CVADHELP-11757]

- Cuando utiliza una tarjeta inteligente rápida para conectarse a una sesión, el símbolo del PIN puede aparecer dos veces. [CVADHELP-12949]

### Excepciones del sistema

- La redirección USB puede provocar que los VDA experimenten una excepción irreparable y muestren una pantalla azul con el código de comprobación de errores **SYSTEM\_THREAD\_EXCEPTION\_NOT\_HANDLED (7e)**. Además, es posible que la redirección USB global no se desbloquee, con lo que se bloquearán otras redirecciones. [CVADHELP-9237]
- Los VDA pueden experimentar una excepción irreparable en ctxdvcs.sys y mostrar una pantalla azul con el código de comprobación de errores 0xc0000409. [CVADHELP-13102]
- Una aplicación que utilice el marco de trabajo Electron podría cerrarse inesperadamente con el siguiente mensaje de error:

**{EXCEPCIÓN} Instrucción ilegal Se ha intentado ejecutar una instrucción ilegal.**

[CVADHELP-13440]

- Los VDA pueden experimentar una excepción irreparable y provocar un pantallazo azul en picadm.sys con el código de comprobación de errores 0x22. [CVADHELP-14431]

### Experiencia de usuario

- Es posible que las sesiones de escritorio muestren artefactos que oscurecen el contenido de la pantalla y otras partes de la pantalla. [CVADHELP-13301]

### Interfaz de usuario

- Es posible que falte la ficha **Dispositivos** en la ventana **Citrix Workspace: Preferencias (barra de herramientas de Desktop Viewer > Preferencias)**. El problema se produce con un escritorio de VDI que se ejecuta en Microsoft Windows Server a través de un conmutador VDI de servidor. [CVADHELP-14158]

### VDA para SO multisesión

#### Redirección de contenido

- Al configurar la directiva de redirección de contenido de explorador web en los modos **Obtención en servidor** y **Generación en cliente**, se redirige el tráfico únicamente a través de un proxy web configurado estáticamente. [CVADHELP-14134]

## Impresión

- Es posible que no se pueda imprimir documentos en una bandeja de impresora de salida diferente. El trabajo de impresión utiliza la bandeja predeterminada para imprimir documentos aunque elija otra bandeja en el cuadro de diálogo Imprimir. [CVADHELP-13492]
- Al intentar iniciar una aplicación, es posible que Citrix Print Manager Service (CpSvc.exe) se cierre de forma inesperada. [CVADHELP-13945]
- Es posible que las impresoras PDF creadas automáticamente no se eliminen. El problema se produce si se crean en HKEY\_LOCAL\_MACHINE\SOFTWARE en lugar de HKEY\_CURRENT\_CONFIG. [CVADHELP-14280]

## Sesión/Conexión

- Cuando el Reproductor de Windows Media pasa de la pista actual a la pista siguiente de la lista de reproducción, es posible que el audio no se reproduzca al principio de la pista siguiente. El problema se produce si la redirección de Windows Media está habilitada. [CVADHELP-11639]
- Al iniciar una aplicación publicada en un VDA multisesión, es posible que no se ejecute la clave del Registro RunOnce de Windows. [CVADHELP-11991]
- Es posible que no se inicien algunas aplicaciones. En consecuencia, no se pueden encontrar los detalles de la sesión en el **Administrador de tareas**, y aparece el siguiente estado de aplicación en Citrix Studio: **Aplicación no ejecutada**. Cuando se produce este problema, es posible que el VDA vuelva a registrarse, tras lo cual aparece el siguiente mensaje de error:

### **ID de evento 1048: Error de WCF o rechazo del broker**

[CVADHELP-12856]

- Es posible que la lectura de datos de una unidad de cliente tarde mucho tiempo después de cambiar el valor de la siguiente clave del Registro a 1 en un VDA:

Para habilitar la corrección, cree la siguiente clave de Registro:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd

Nombre: PacketIntegrityChecks

Tipo: DWORD

Valor: 1

[CVADHELP-13063]

- Es posible que fallen los intentos de reconectarse a sesiones, con el siguiente mensaje de error:  
**No se puede iniciar el escritorio.**

[CVADHELP-13320]

- Cuando intente reconectarse a una sesión, es posible que el escritorio no se cargue y que aparezca una ventana gris. El problema ocurre con la versión 1909 de VDA cuando se ejecuta en Microsoft Windows Server 2019. [CVADHELP-13376]
- Es posible que un VDA deje de responder después del reinicio. El problema se produce cuando un software de seguridad, como Symantec SEP, aplica análisis de seguridad. [CVADHELP-13832]
- Es posible que algunas sesiones de usuario se cierren de forma inesperada. El problema se produce con usuarios no autenticados (anónimos) cuando estos inician una segunda aplicación en modo de ventana. [CVADHELP-13917]
- Después de actualizar un VDA a la versión 1909.1, algunas aplicaciones de terceros, como [RemoteScan](#), pueden no escanear un documento y dejar de responder. El problema ocurre por un error en el módulo twnhook.dll. [CVADHELP-13937]
- Es posible que el teclado virtual no aparezca automáticamente dentro de una aplicación publicada. [CVADHELP-14012]
- Al intentar volver a configurar la versión 1912 del VDA para utilizar un puerto de VDA personalizado desde la línea de comandos, es posible que aparezca este mensaje de error:

**No se pudo completar el proceso...No se puede encontrar el archivo ICA de configuración ...IcaConfigConsole.exe.**

[CVADHELP-14052]

- Con la directiva **Visualización automática del teclado** habilitada, al hacer clic en el cuadro **Buscar en Google**, es posible que el teclado no aparezca automáticamente. El problema se produce cuando se ejecuta una sesión en los exploradores Internet Explorer, Firefox o Chrome. [CVADHELP-14065]
- Esta corrección presenta una configuración de directiva que modifica los canales virtuales mediante ICA multisección a través de una directiva de Citrix en lugar de hacerlo a través de una clave del Registro. [CVADHELP-14136]
- Si conecta un micrófono USB a un dispositivo de usuario e inicia una sesión, es posible que el micrófono USB no se redirija. El dispositivo USB se muestra como **Optimizado, Restringido por directiva**. [CVADHELP-14301]
- En un caso de doble salto, puede que un solo usuario consuma dos licencias de usuario simultáneo (CCU) de Citrix. El doble salto es cuando un usuario inicia la sesión HDX dentro de otra sesión HDX (por ejemplo, cuando se inicia una aplicación publicada en una sesión de escritorio virtual). [CVADHELP-14409]
- Al intentar mover objetos pequeños en la pantalla, es posible que se dañe un único píxel. El problema se produce cuando la directiva **Calidad visual** se establece en **Gradual sin pérdida**.

[CVADFIX-8214]

### Tarjetas inteligentes

- Cuando utiliza una tarjeta inteligente rápida para conectarse a una sesión, el símbolo del PIN puede aparecer dos veces. [CVADHELP-12949]

### Excepciones del sistema

- La redirección USB puede provocar que los VDA experimenten una excepción irreparable y muestren una pantalla azul con el código de comprobación de errores **SYSTEM\_THREAD\_EXCEPTION\_NOT\_HANDLED (7e)**. Además, es posible que la redirección USB global no se desbloquee, con lo que se bloquearán otras redirecciones. [CVADHELP-9237]
- Los VDA pueden experimentar una excepción irreparable en ctxdvcs.sys y mostrar una pantalla azul con el código de comprobación de errores 0xc0000409. [CVADHELP-13102]
- Una aplicación que utilice el marco de trabajo Electron podría cerrarse inesperadamente con el siguiente mensaje de error:

**{EXCEPCIÓN} Instrucción ilegal Se ha intentado ejecutar una instrucción ilegal.**

[CVADHELP-13440]

- Los VDA pueden experimentar una excepción irreparable y provocar un pantallazo azul en picadm.sys con el código de comprobación de errores 0x22. [CVADHELP-14431]

### Experiencia de usuario

- Es posible que las sesiones de escritorio muestren artefactos que oscurecen el contenido de la pantalla y otras partes de la pantalla. [CVADHELP-13301]

### Interfaz de usuario

- Al mover una ventana integrada, es posible que el contenido gráfico de la aplicación correspondiente se vea distorsionado. El problema se produce al mover algunas partes de la ventana fuera del área del escritorio. [CVADHELP-14209]

## Componentes de escritorio virtual: Otros

- Al iniciar una aplicación de App-V desde un VDA que aloja muchas aplicaciones de App-V, es posible que el VDA anule su registro. El problema se produce cuando tarda mucho en procesar los archivos de directiva asociados. [CVADHELP-12592]
- Al abrir un archivo con la aplicación de App-V publicada asociada, la aplicación se abre. Sin embargo, el archivo no se abre en la aplicación asociada. [CVADHELP-13971]

## 1912 LTSR (versión inicial)

May 5, 2023

### Acerca de esta versión

El programa Long Term Service Release (LTSR o Servicio a largo plazo) de Citrix Virtual Apps and Desktops ofrece estabilidad y funcionalidad a largo plazo para las versiones de Citrix Virtual Apps and Desktops.

Los LTSR están disponibles actualmente para Citrix Virtual Apps and Desktops 7 1912 (esta versión) y para las versiones de XenApp y XenDesktop [7.6](#) y [7.15](#). Si es nuevo en el programa LTSR, puede instalar Citrix Virtual Apps and Desktops 7 1912 desde cero. Si ya participa en uno de los LTSR anteriores, puede actualizar desde allí, incluso desde cualquier actualización acumulativa (CU). Para obtener información adicional acerca de las rutas de actualización admitidas, consulte la [Guía sobre la actualización de versiones](#).

Además, Citrix recomienda usar versiones específicas de la [aplicación Citrix Workspace y de otros componentes](#). Aunque no es necesario para la conformidad con LTSR, la actualización de esos componentes a las versiones más recientes facilita el mantenimiento y la disponibilidad de revisiones y correcciones de problemas en la implementación.

Para obtener información general sobre las funciones de Citrix Virtual Apps and Desktops 7 1912 que se han agregado desde versiones anteriores, consulte la tabla [Resumen comparativo de funciones de Citrix Virtual Apps and Desktops](#).

Esta versión de Citrix Virtual Apps and Desktops incluye nuevas versiones de Virtual Delivery Agent (VDA) para Windows y nuevas versiones de varios componentes principales. Puede hacer lo siguiente:

- **Instalar o actualizar un sitio**

Use el archivo ISO para que esta versión instale o actualice los VDA y los componentes principales. Instalar o actualizar a la última versión permite utilizar todas las funciones más recientes.

- **Instalar o actualizar VDA en un sitio existente**

Si ya tiene una implementación, puede usar varias de las funciones de HDX más recientes sin tener que actualizar los componentes principales. Para ello, instale VDA recientes o actualícelos a la versión nueva. A menudo, puede interesarle actualizar solo los agentes VDA para probar mejoras en un entorno independiente del entorno de producción.

Después de actualizar los agentes VDA a esta versión (desde 7.9 o posterior), no es necesario actualizar el nivel funcional del catálogo de máquinas. El valor **7.9 (o uno posterior)** sigue siendo el nivel funcional predeterminado y es válido para esta versión. Para obtener más información, consulte [Niveles funcionales y versiones de VDA](#).

Para obtener instrucciones:

- Si va a crear un sitio nuevo, siga la secuencia de tareas indicada en [Instalar y configurar](#).
- Si va a actualizar un sitio, consulte [Actualizar la versión de una implementación](#).

## Citrix Virtual Apps and Desktops 7 1912 LTSR

### Aviso importante sobre la actualización de los agentes VDA

Si el componente Personal vDisk (PvD) se ha instalado alguna vez en un VDA, dicho VDA no se puede actualizar a la versión 1912 LTSR ni a ninguna posterior. Para utilizar el nuevo VDA, debe desinstalar el VDA actual y, a continuación, instalar el nuevo

Este paso debe seguirse incluso si se ha instalado PvD, pero nunca se ha utilizado.

**Averigüe si le afecta** Cómo podría haberse instalado PvD en versiones anteriores:

- En la interfaz gráfica del instalador de VDA, PvD era una opción en la página **Componentes adicionales**. La versión 7.15 LTSR y las 7.x anteriores habilitaban esta opción de forma predeterminada. Por lo tanto, si aceptó los valores predeterminados (o habilitó explícitamente la opción en cualquier versión), PvD se ha instalado.
- En la línea de comandos, la opción `/baseimage` instaló PvD. Si especificó esta opción o utilizó un script que contenía esta opción, PvD se ha instalado.

Si no sabe si el VDA tiene PvD instalado, ejecute el instalador del nuevo VDA (1912 LTSR o una versión posterior) en la máquina o en la imagen.

- Si PvD está instalado, aparece un mensaje que indica que hay un componente incompatible.

- Para la interfaz gráfica, haga clic en **Cancelar** en la página que contiene el mensaje y, a continuación, confirme que quiere cerrar el instalador.
- Desde la CLI, el comando simplemente falla con el mensaje indicado.
- Si PvD no está instalado, la actualización continúa.

**Qué se debe hacer** Si el VDA no tiene PvD instalado, siga el procedimiento de actualización habitual.

Si el VDA tiene PvD instalado:

1. Desinstale el VDA actual. Para obtener más información, consulte [Eliminación de componentes](#).
2. Instale el nuevo VDA.

Si quiere continuar mediante PvD en sus máquinas con Windows 7 o Windows 10 (1607 y versiones anteriores, sin actualizaciones), VDA 7.15 LTSR es la última versión compatible.

### **Instalación y actualización: Nuevo componente de capa de personalización de usuarios en los VDA de sesión única**

Al instalar o actualizar la versión de un VDA de sesión única, puede incluir el componente de la capa de personalización de usuarios. Esta función cuenta con la tecnología de Citrix App Layering. En máquinas no persistentes, la función conserva en todas las sesiones los datos de los usuarios y las aplicaciones instaladas localmente.

Esta función reemplaza los discos Personal vDisk, que han sido retirados. Si va a actualizar un VDA que tuvo PvD instalado, consulte [Aviso importante sobre la actualización de los agentes VDA](#).

Para obtener información detallada sobre la nueva función, consulte la documentación de [Capa de personalización de usuarios](#). Para obtener directrices de instalación de VDA, consulte [Instalar agentes VDA](#).

### **Instalación y actualización: Requisito previo del runtime de Microsoft Visual C++ 2017**

Al instalar un Delivery Controller o Windows VDA, el runtime de Microsoft Visual C++ 2017 se instala automáticamente si no está instalado (o una versión posterior compatible). Esta es una versión más reciente del runtime de Visual C++ que la instalada en las versiones anteriores de Citrix Virtual Apps and Desktops.

### **Instalación y actualización: Versión de SQL Server Express**

Al instalar el primer Delivery Controller, puede elegir que Citrix instale Microsoft SQL Server Express en la misma máquina para utilizarlo como base de datos del sitio. A partir de esta versión, para las nuevas

instalaciones, instalamos SQL Server Express 2017 con Cumulative Update 16. Esta es una versión más reciente que las versiones anteriores de Citrix Virtual Apps and Desktops. Para la actualización de versiones, no actualizamos ninguna versión de SQL Server Express que ya esté instalada.

Al instalar un Controller, Microsoft SQL Server Express LocalDB se instala automáticamente para usarlo con la caché de host local (esta instalación es independiente de la instancia de SQL Server Express utilizada para la base de datos del sitio). Para una nueva instalación, instalamos SQL Server Express LocalDB 2017 con Cumulative Update 16. Esta es una versión más reciente que las versiones anteriores de Citrix Virtual Apps and Desktops. Para la actualización de versiones, no actualizamos ninguna versión de SQL Server Express LocalDB que ya esté instalada.

### **Instalación y actualización: Versiones compatibles de Windows 10 para VDA**

Esta versión es compatible con sistemas operativos Windows 10 de 32 bits (x86) y 64 bits (x64). Windows 10 de 32 bits solo es compatible durante 18 meses a partir de la publicación inicial de 1912 LTSR. Windows 10 32 de bits solo es compatible en Windows 10 Enterprise 2019 LTSC. Para máquinas con Windows 10, Citrix recomienda usar 64 bits (x64).

### **Instalación y actualización: Evitar la comprobación de reinicio pendiente**

Al instalar o actualizar componentes principales, el instalador se detiene si detecta que hay un reinicio pendiente de una instalación anterior de Windows en la máquina. Ahora, cuando utilice la interfaz de línea de comandos, puede impedir la comprobación de reinicios pendientes. Para ello, incluya la opción `/no_pending_reboot_check` en el comando. Para obtener más información, consulte [Durante la instalación de un componente](#).

### **VDA y catálogos de máquinas: Cambios en los nombres de los sistemas operativos**

Los nombres de los sistemas operativos de los VDA y de los catálogos de máquinas han cambiado.

- **SO multisesión** (antes llamado SO de servidor): El catálogo de máquinas con SO multisesión proporciona escritorios alojados compartidos para una distribución a gran escala de máquinas con SO Windows multisesión o con SO Linux estandarizadas.
- **SO de sesión única** (anteriormente SO de escritorio): El catálogo de máquinas con SO de sesión única proporciona escritorios VDI, opción idónea para varios usuarios.

### **Número de versión del componente: Cambiar al valor local**

En un número de versión de producto y componente (*YYMM.c.m.b*), el valor de *c* es **0** para una versión local. Por ejemplo, en **Aplicaciones y funciones**, esta versión aparece como 1912.0.0.*número de com-*

*pilación.*

En versiones locales anteriores y en versiones de Citrix Cloud, el valor de *c* es **1**.

Para obtener más información, consulte [Números de versión de productos y componentes](#).

## **Citrix Studio**

### **Compatibilidad con aprovisionamiento de máquinas Linux en Amazon Web Services**

Citrix Studio ahora admite el uso de Machine Creation Services (MCS) para aprovisionar máquinas Linux en Amazon Web Services (AWS). Para obtener más información, consulte [Usar MCS para crear máquinas virtuales Linux](#).

## **Agentes Virtual Delivery Agent (VDA) 1912**

La versión 1912 de VDA para SO multisesión y VDA para SO de sesión única presenta las siguientes mejoras (además de los elementos de instalación y actualización de VDA mencionados anteriormente en este artículo):

### **Nota:**

Aunque el número de versión de VDA indica “Citrix Virtual Apps and Desktops 7 1912 LTSR”, los VDA son compatibles con las implementaciones de LTSR y CR.

## **Protección de la autoridad de seguridad local (LSA)**

Ahora admitimos el uso de la protección Local Security Authority (LSA) en un SO multisesión de servidor y un SO de sesión única de escritorio para la autenticación estándar, la autenticación del Servicio de autenticación federada (FAS) y la autenticación con tarjeta inteligente. Para obtener más información acerca de la protección LSA, consulte el artículo de Microsoft [Configuring Additional LSA Protection](#).

## **Protección de aplicaciones**

Esta versión presenta una función adicional que mejora la seguridad al usar la aplicación Citrix Workspace mediante nuevas directivas que ofrecen prestaciones para protegerse del registro de claves y de capturas de pantalla en las sesiones. Las nuevas directivas, junto con la aplicación Citrix Workspace 1912 o versiones posteriores para Windows, pueden ayudar a proteger los datos de registradores de claves y capturadores de pantalla. Para obtener más información, consulte [Protección de aplicaciones](#).

## Citrix Licensing 11.16.3.0 Build 29000

Citrix Licensing 11.16.3.0 compilación 29000 contiene [funciones nuevas](#), así como [problemas resueltos](#) y [problemas conocidos](#).

## Versión 1912 del Servicio de autenticación federada de Citrix

La versión 1912 del Servicio de autenticación federada (FAS) de Citrix contiene [nuevas funciones](#).

## Más información

- Compruebe la sección [Elementos retirados](#) por si hay cambios en las versiones que se anuncian y se eliminan.
- Para obtener información sobre los cambios efectuados en 2018 en nombres de producto y números de versión, consulte [Nuevos nombres y números](#).

## Componentes base

---

### Componente base de 1912

LTSR	Versión	Notas
VDA de sesión única	1912.0	
VDA multisesión	1912.0	
Delivery Controller	1912.0.0	
Citrix Studio	7.24.0	
Citrix Director	7.24.0	
Experiencia de administración de Directivas de grupo	7.24.0	
StoreFront	19.12.0.0	
Provisioning Services	1912	
Universal Print Server	7.24.0	
Grabación de sesiones	1912.0.0	
Linux VDA	1912.0.0	Consulte la <a href="#">documentación de Linux VDA</a> para ver las plataformas compatibles.
Profile Management	1912.0.0	

**Componente base de 1912**

<b>LTSR</b>	<b>Versión</b>	<b>Notas</b>
Servicio de autenticación federada	7.24.0	
Redirección de contenido del explorador web	15.19.0	

**Componentes compatibles**

Los siguientes componentes, en las versiones que se indican a continuación, son compatibles con entornos LTSR. Estos componentes no dan derecho a las ventajas de LTSR (ciclo de vida ampliado y actualizaciones acumulativas de correcciones solamente). Citrix puede pedirle que actualice estos componentes a una versión más reciente dentro de sus entornos 1912 LTSR.

<b>Componentes y funciones compatibles</b>	<b>Versión</b>
App Layering	19.11.0
Directivas de protección de aplicaciones	1912.0.0
HDX RealTime Optimization Pack	2.8
Servidor de licencias	11.16.3.0, compilación 29000
Capa de personalización de usuarios	19.11.0
Reproductor web de grabación de sesiones	1912.0.0
Optimización de Teams	1912.0.0
Autoservicio de restablecimiento de contraseñas	1.1
Windows 10 de 32 bits	
Workspace Environment Management	1912.0.0
XenApp y XenDesktop 7.15 LTSR VDA (versión más reciente)*	Solo la actualización acumulativa más reciente

**Nota:**

Windows 10 de 32 bits solo es compatible durante 18 meses a partir de la publicación inicial de 1912 LTSR. Windows 10 32 de bits solo es compatible en Windows 10 Enterprise 2019 LTSC.

\* La compatibilidad con VDA de XenApp y XenDesktop 7.15 LTSR en este caso es solo para Windows 7 y Windows 2008 R2. XenApp y XenDesktop 7.15 LTSR dejará de ser compatible a partir

de agosto de 2022. La compatibilidad con Citrix para Windows 7 y Windows 2008 R2 finalizará cuando Microsoft finalice el soporte para el sistema operativo o cuando finalice la compatibilidad con XenApp y XenDesktop 7.15 LTSR, lo que ocurra primero. Para obtener más información, consulte la [tabla de productos de Citrix](#).

### **Versiones compatibles de la aplicación Citrix Workspace**

Todas las versiones admitidas de la aplicación Citrix Workspace son compatibles con Citrix Virtual Apps and Desktops 1912 LTSR. Para obtener información sobre el ciclo de vida de la aplicación Citrix Workspace, consulte [Lifecycle Milestones for Citrix Workspace app and Citrix Receiver](#).

Para mayor comodidad, considere la posibilidad de suscribirse al [feed RSS de la aplicación Citrix Workspace](#) para recibir una notificación cuando una nueva versión de la aplicación Citrix Workspace esté disponible.

### **Exclusiones destacables**

Las siguientes funciones, componentes y plataformas no dan derecho a las ventajas y prestaciones del ciclo de vida de 1912 LTSR. Específicamente, se excluyen las ventajas de actualizaciones acumulativas y el ciclo de vida ampliado. Las actualizaciones de los componentes y funciones excluidos están disponibles a través de las versiones publicadas regularmente.

---

#### **Componentes y funciones excluidos**

---

AppDisks

AppDNA

Citrix SCOM Management Pack

Framehawk

Personal vDisk

Integración de StoreFront con Citrix Online

---

---

#### **Plataformas Windows excluidas\***

---

Windows 2008 de 32 bits (para Universal Print Server)

---

\* Citrix se reserva el derecho a actualizar el soporte que ofrece para las plataformas en función de los hitos de los ciclos de vida de los proveedores externos.

## Datos de análisis de instalación y actualización

Cuando se usa el programa de instalación del producto completo para implementar o actualizar los componentes de XenApp o XenDesktop, se recopila información anónima sobre el proceso de instalación y se guarda en la máquina donde se está realizando la instalación o actualización del componente. Esta información se utiliza para ayudar a Citrix a mejorar la experiencia de instalación de sus clientes.

## Migrar XenApp 6.5

El proceso de migración de XenApp 6.5 permite realizar una transición eficaz y rápida desde una comunidad XenApp 6.5 a un sitio con 1912 LTSR. Esta transición puede resultarle útil en caso de implementaciones que contienen una gran cantidad de aplicaciones y directivas de grupo Citrix, porque reduce el riesgo de que se produzcan errores accidentales al mover manualmente las aplicaciones y las directivas de grupo Citrix al nuevo sitio de XenApp.

Después de instalar los componentes principales de XenApp 1912 LTSR y crear un sitio, el proceso de migración sigue estos pasos:

- Ejecute el instalador de 1912 en cada servidor de trabajo de XenApp 6.5. Este instalador actualiza automáticamente el servidor a un nuevo Virtual Delivery Agent para SO de servidor listo para usar en el nuevo sitio.
- Ejecute los cmdlets de exportación de PowerShell en un Controller de XenApp 6.5, que exporta las configuraciones de aplicaciones y directivas de Citrix a archivos XML.
- Si fuera necesario, modifique los archivos XML para seleccionar con exactitud lo que quiere importar al sitio nuevo. Al adaptar los archivos, puede importar las configuraciones de directivas y aplicaciones al sitio de 1912 LTSR por fases: algunas configuraciones ahora y otras más tarde.
- Ejecute los cmdlets de importación de PowerShell en el nuevo Controller de 1912, el cual importa las configuraciones contenidas en los archivos XML al nuevo sitio de XenApp.

Vuelva a configurar el nuevo sitio según sea necesario y, a continuación, haga pruebas en él.

Para obtener más información, consulte [Migrar XenApp 6.x](#).

## Problemas resueltos

April 19, 2024

Se han solucionado los siguientes problemas desde Citrix Virtual Apps and Desktops 7 1909:

## Citrix Studio

- Es posible que Citrix Studio muestre incorrectamente los iconos de algunas aplicaciones detectadas al agregar aplicaciones del menú Inicio. El problema se produce con las aplicaciones integradas de Windows en la versión 1903 de Windows 10. Como solución temporal, seleccione la aplicación, haga clic en **Propiedades**, haga clic en **Cambiar** en la página Entrega y, a continuación, seleccione un icono pertinente para esa aplicación. [BRK-4430]

## Citrix Provisioning

La [documentación de Citrix Provisioning 1912](#) ofrece información específica acerca de las actualizaciones de esta versión.

## Delivery Controller

- Es posible que no se pueda detener Citrix Broker Service. [CVADHELP-12715]
- En entornos de VMware vSAN 6.7, es posible que no se puedan eliminar máquinas virtuales creadas por Machine Creation Services (MCS) porque se quitó la imagen base del disco. Esta imagen se comparte entre varias máquinas virtuales. Este problema se produce cuando el archivo VMDK contiene el indicador `dbb.deletable=false`. [CVADHELP-13127]
- Si intenta crear un catálogo de máquinas mediante Machine Creation Services (MCS) en un entorno de VMware, no se puede crear el catálogo y aparece el siguiente mensaje de error:

### **FailedToCreateImagePreparationVm**

[CVADHELP-13143]

- Es posible que no se pueda crear o actualizar los catálogos de Machine Creation Services (MCS) en Microsoft Azure, tras lo que aparece el siguiente mensaje de error:

### **Error, exception of type: “System.OutOfMemoryException”**

[CVADHELP-13146]

## HDX RealTime Optimization Pack

La [documentación de HDX RealTime Optimization Pack 1912](#) proporciona información específica acerca de las actualizaciones de esta versión.

## Licencias

La [documentación de Licensing 1912](#) ofrece información específica acerca de las actualizaciones de esta versión.

## Linux VDA

La [documentación de Linux VDA 1912](#) ofrece información específica acerca de las actualizaciones de esta versión.

## Profile Management

La [documentación de Profile Management 1912](#) ofrece información específica acerca de las actualizaciones de esta versión.

## StoreFront

La [documentación de StoreFront 1912](#) ofrece información específica acerca de las actualizaciones de esta versión.

## VDA para SO de sesión única

### Impresión

- En un VDA para SO de escritorio, es posible que no se pueda imprimir archivos con una impresora cliente asignada. El problema se produce cuando el VDA está instalado en la versión 1903 de Windows 10. [CVADHELP-13357]
- Con las fuentes no predeterminadas (por ejemplo, la fuente de código de barras CCode390) instaladas en la versión 7.18 de VDA o en una posterior, es posible que haya problemas de impresión al actualizar la versión 7.17 de XenApp y XenDesktop a la versión 7.18 o a una posterior. Como consecuencia, es posible que la fuente de código de barras no se imprima al imprimir documentos desde una sesión. [CVADHELP-12454]

### Sesión/Conexión

- Al reproducir audio en una sesión de usuario, es posible que oiga un golpeteo. [CVADHELP-11241]

- En Citrix Receiver para Windows, es posible que escuche ruidos intermitentes al reproducir audio. [CVADHELP-11440]
- En algunos dispositivos de usuario, es posible que se tarde mucho tiempo en iniciar una segunda aplicación si establece las tarjetas gráficas en Sí. [CVADHELP-12387]
- Es posible que la función de cámara web optimizada de las aplicaciones de vídeo basadas en Media Foundation no funcione para algunas API. [CVADHELP-12427]
- Al cambiar los efectos visuales dentro de una sesión de usuario, es posible que el valor `UserPreferencesMask` de la clave del Registro `HKEY_CURRENT_USER\Control Panel\Desktop` no se actualice al nuevo valor.

Para habilitar la corrección, cree la siguiente clave de Registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\Applnit_DLLs\UI Tweak\SystemPropertiesComputerNa`

Nombre: `HookProcess`

Tipo: `REG_DWORD`

Datos: 1

[CVADHELP-12796]

- Los intentos de copiar texto de una aplicación publicada a un dispositivo de punto final pueden fallar cuando se usa la aplicación Citrix Workspace 1902 para Windows o posterior. [CVADHELP-12945]
- Una infracción de acceso puede provocar que el proceso `wfshell.exe` se cierre de forma inesperada. Como resultado, se produce un error al intentar iniciar una aplicación. [CVADHELP-13032]

## Excepciones del sistema

- Al intentar exportar clips de vídeo en un VDA para SO de escritorio, es posible que ciertas aplicaciones de terceros se cierren inesperadamente. [CVADHELP-11303]
- Es posible que los servidores sufran una excepción irrecuperable en `tdica.sys` y provoquen un pantallazo azul con el código de comprobación de errores **SYSTEM\_THREAD\_EXCEPTION\_NOT\_HANDLED (7e)**.  
[CVADHELP-12611]
- Es posible que el proceso `wfshell.exe` se cierre de forma inesperada en un VDA. [CVADHELP-12819]
- Es posible que las aplicaciones no se inicien cuando el proceso `wfshell.exe` se cierra de forma inesperada. El problema tiene lugar por un error en el módulo `cmpcom.dll`. [CVADHELP-13089]

## VDA para SO multisesión

### Impresión

- Con las fuentes no predeterminadas (por ejemplo, la fuente de código de barras CCode390) instaladas en la versión 7.18 de VDA o en una posterior, es posible que haya problemas de impresión al actualizar la versión 7.17 de XenApp y XenDesktop a la versión 7.18 o a una posterior. Como consecuencia, es posible que la fuente de código de barras no se imprima al imprimir documentos desde una sesión. [CVADHELP-12454]

### Sesión/Conexión

- Al escuchar audio con la calidad de audio establecida en Alta, es posible que escuche un golpeo o un ruido crepitante. El problema se produce cuando se pause el audio durante unos segundos y, luego, se reanuda. [CVADHELP-10657]
- En algunos dispositivos de usuario, es posible que se tarde mucho tiempo en iniciar una segunda aplicación si establece las tarjetas gráficas en Sí. [CVADHELP-12387]
- Es posible que la función de cámara web optimizada de las aplicaciones de vídeo basadas en Media Foundation no funcione para algunas API. [CVADHELP-12427]
- Al cambiar los efectos visuales dentro de una sesión de usuario, es posible que el valor User-PreferencesMask de la clave del Registro HKEY\_CURRENT\_USER\Control Panel\Desktop no se actualice al nuevo valor.

Para habilitar la corrección, cree la siguiente clave de Registro:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\CtxHook\ApplInit\_DLLs\UITweak\SystemPropertiesComputerName

Nombre: HookProcess

Tipo: REG\_DWORD

Datos: 1

[CVADHELP-12796]

- Los intentos de copiar texto de una aplicación publicada a un dispositivo de punto final pueden fallar cuando se usa la aplicación Citrix Workspace 1902 para Windows o posterior. [CVADHELP-12945]
- Una infracción de acceso puede provocar que el proceso wfshell.exe se cierre de forma inesperada. Como resultado, se produce un error al intentar iniciar una aplicación. [CVADHELP-13032]

## Excepciones del sistema

- Es posible que Microsoft Internet Explorer se cierre de forma inesperada. El problema ocurre por un error en el módulo icaendpoint.dll. [CVADHELP-12171]
- Es posible que los servidores sufran una excepción irrecuperable en tdica.sys y provoquen un pantallazo azul con el código de comprobación de errores **SYSTEM\_THREAD\_EXCEPTION\_NOT\_HANDLED (7e)**. [CVADHELP-12611]
- Es posible que el proceso wfshell.exe se cierre de forma inesperada en un VDA. [CVADHELP-12819]
- Es posible que las aplicaciones no se inicien cuando el proceso wfshell.exe se cierra de forma inesperada. El problema tiene lugar por un error en el módulo cmpcom.dll. [CVADHELP-13089]

## Experiencia de usuario

- Al hacer clic en el control de volumen de la barra de tareas con el botón principal del mouse, es posible que el control de volumen no se abra. El problema se produce en una versión no inglesa del sistema operativo Microsoft Windows. [CVADHELP-10739]

## Problemas conocidos

May 24, 2024

## Notas

- Los problemas conocidos que se describen en las secciones de la [versión inicial](#), [CU1](#), [CU2](#), [CU3](#), [CU4](#), [CU5](#), [CU6](#), [CU7](#) y [CU8](#) de 1912 de este artículo siguen estando presentes en CU9, a menos que estén incluidos en la lista de [problemas resueltos](#).
- Si un problema conocido tiene una solución temporal, esta se proporciona después de la descripción del problema.
- La siguiente advertencia se aplica a cualquier solución temporal que sugiera cambiar una entrada del Registro:

### Advertencia:

Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados

de la utilización inadecuada del Editor del Registro puedan resolverse. Si usa el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

### Problemas conocidos en la versión 1912 CU9

- No puede instalar un VDA en Windows 2012 R2 con la aplicación Citrix Workspace durante la instalación o actualización de un VDA.

**Solución alternativa:** excluya la aplicación Citrix Workspace durante la instalación o actualización de un VDA. Consulte los [Requisitos del sistema para la aplicación Citrix Workspace](#) antes de implementar el VDA.

[LCM-14080]

- Cuando se instala CVAD LTSR 1912 CU9 mediante el método de instalación por línea de comandos y se introducen comandos en el símbolo del sistema, pasa una nueva línea e inicia la instalación silenciosa. No obstante, una vez finalizada la instalación, no recibirá ningún mensaje para indicar que la instalación se ha completado. [LCM-14108]

### Problemas conocidos en la versión 1912 CU8

- Si instala Windows, IIS y Citrix Director en unidades distintas de C:\ y actualiza Citrix Director a la versión 1912 LTSR CU8, es posible que el icono de Citrix Director aparezca en blanco. Sin embargo, puede hacer clic en el icono para iniciar Citrix Director.

Puede usar la siguiente solución temporal para que el icono se muestre correctamente.

1. Abra la línea de comandos y ejecute el comando `echo %systemdrive%`.
2. Copia la salida del comando.
3. Haga clic con el botón secundario en el icono de Citrix Director > Más > Abrir ubicación de archivo.
4. Abra Bloc de notas y arrastre el icono desde el explorador de archivos al Bloc de notas.
5. En el contenido, sustituya "C:" por la salida copiada en el paso 2 y guarde.
6. El icono de Citrix Director ahora se mostrará correctamente.

[DIR-21012]

### Problemas conocidos en la versión 1912 CU7

- Es posible que se produzca un error al intentar instalar la aplicación Citrix Workspace en Windows Server 2012 R2. Para obtener más información, consulte el artículo [CTX477888](#) de Knowledge Center. [LCM-12342]

- Es posible que no se pueda instalar la aplicación Citrix Workspace junto con la instalación del VDA si no hay acceso a Internet. Como solución temporal, debe omitir la instalación de la aplicación Citrix Workspace o instalar Microsoft WebView (que es un requisito previo para la aplicación Citrix Workspace) antes de instalar el VDA. [LCM-12992]

### **Problemas conocidos en la versión 1912 CU6**

- Microsoft ya no admite la creación de máquinas virtuales con discos no administrados en Azure. Sin embargo, se pueden usar plantillas maestras creadas anteriormente con discos no administrados. [LCM-10287]
- El parámetro de instalación de la línea de comandos, / `IGNORE_DB_CHECK_FAILURE`, no se admite en las actualizaciones CU de LTSR 1912. [LCM-11958]
- Es posible que se produzca un error al intentar instalar la aplicación Citrix Workspace en Windows Server 2012 R2. Para obtener más información, consulte el artículo [CTX477888](#) de Knowledge Center. [LCM-12342]
- Es posible que no se pueda instalar la aplicación Citrix Workspace junto con la instalación del VDA si no hay acceso a Internet. Como solución temporal, debe omitir la instalación de la aplicación Citrix Workspace o instalar Microsoft WebView (que es un requisito previo para la aplicación Citrix Workspace) antes de instalar el VDA. [LCM-12992]
- Es posible que la función Lista de canales virtuales permitidos no funcione en Microsoft Teams. [CVADHELP-21287]

### **Problemas conocidos en la versión 1912 CU5**

- Es posible que no se puedan crear conexiones de host con Azure en Citrix Studio debido a una excepción. El problema se produce por los cambios de Microsoft realizados en Azure. Hay una corrección privada disponible en [CTX457802](#). [CVADHELP-18741]
- Cuando se usa esta versión de VDA, las directivas de Citrix aplicadas a una máquina por unidad organizativa a veces no pueden aplicarse. [CVADHELP-19826]
- Tras actualizar Delivery Controller a la versión 1912 CU5, es posible que el reinicio programado no funcione correctamente con los VDA que no tienen administración de energía. [CVADHELP-20138]
- Es posible que la función Lista de canales virtuales permitidos no funcione en Microsoft Teams. [CVADHELP-21287]

### Problemas conocidos en la versión 1912 CU4

- Cuando se usa esta versión de VDA, las directivas de Citrix aplicadas a una máquina por unidad organizativa a veces no pueden aplicarse. [CVADHELP-19826]
- Es posible que no se puedan crear conexiones de host con Azure en Citrix Studio debido a una excepción. El problema se produce por los cambios de Microsoft realizados en Azure. Hay una corrección privada disponible en [CTX457802](#). [CVADHELP-18741]
- Al salir de una sesión virtual de Citrix, es posible que se produzca al menos uno de estos problemas:
  - El VDA sigue enumerando la sesión finalizada y el proceso logonui.exe. Se puede forzar el cierre del proceso logonui.exe.
  - La sesión aparece con un nombre de usuario vacío en Citrix Studio.
  - Es posible que no pueda iniciar más sesiones.

Hay una corrección privada disponible en [CTX340125](#).

[CVADHELP-19182]

- Es posible que la función Lista de canales virtuales permitidos no funcione en Microsoft Teams. [CVADHELP-21287]

### Problemas conocidos en la versión 1912 CU3

- Al intentar actualizar la opción CEIP de licencias mediante el cmdlet `Set-LicCEIPOption`, la operación falla con un “error de comunicación”. Como solución temporal, la opción CEIP se puede habilitar a través de Citrix Licensing Manager. Para obtener más información, consulte el artículo [CTX220679](#) de Knowledge Center. [LCM-9169]
- Es posible que no se puedan crear conexiones de host con Azure en Citrix Studio debido a una excepción. El problema se produce por los cambios de Microsoft realizados en Azure. Hay una corrección privada disponible en [CTX457802](#). [CVADHELP-18741]
- Es posible que la función Lista de canales virtuales permitidos no funcione en Microsoft Teams. [CVADHELP-21287]

### Problemas conocidos en la versión 1912 CU2

- Es posible que no pueda configurar el sitio local con Citrix Analytics for Performance de Director si el Delivery Controller usa una versión de Microsoft .NET Framework anterior a 4.8. Como solución temporal, actualice la versión de .NET Framework del Delivery Controller a 4.8. [LCM-9255]

- Es posible que, al iniciar sesión en una sesión RDP sin intermediario con una credencial UPN, se produzca una excepción no detectada. En 1912 LTSR CU2, se introdujo una traducción de nombres de usuario como UPN. Cuando el nombre de usuario se trunca por al límite impuesto en las estructuras de datos RDS, se genera un nombre de usuario incorrecto, lo que produce la excepción no detectada. [CVADHELP-16510]
- Si la versión de .NET Framework no es al menos 4.7.2 tras la actualización a 1912 LTSR CU2, Azure Resource Manager falla. [CVADHELP-16533]
- Es posible que no se puedan crear conexiones de host con Azure en Citrix Studio debido a una excepción. El problema se produce por los cambios de Microsoft realizados en Azure. Hay una corrección privada disponible en [CTX457802](#). [CVADHELP-18741]
- Es posible que Citrix Director no enumere la información de directivas. El problema ocurre cuando se utiliza una versión anterior de Director para ver los detalles de sesión asociados a un VDA 1912 LTSR CU2. Como solución temporal, siga los pasos mencionados en la secuencia de actualización de versión. [LCM-8201]
- Puede que fallen algunas operaciones de archivos, ejecutadas en una sesión de aplicación publicada o escritorio publicado, enviadas a una unidad de cliente asignada y aparezca el mensaje de error “permiso denegado”. Puede que los usuarios también vean el error “Archivo en uso” en la máquina cliente local. Para obtener más información, consulte el artículo [CTX285248](#) de Knowledge Center. [HDX-26969]

## Problemas conocidos en la versión 1912 CU1

Además de los problemas conocidos en la versión inicial de 1912 LTSR, CU1 contiene los siguientes problemas conocidos nuevos:

### Citrix Provisioning

- Cuando intenta revertir la versión de un dispositivo de destino de Citrix Provisioning desde 1912 LTSR o 1912 LTSR CU1, puede aparecer el siguiente mensaje:

#### **La instalación falló.**

Como solución temporal, desinstale la versión 1912 LTSR o 1912 LTSR CU1 y, a continuación, vuelva a instalar la versión anterior. [LCM-7341]

- Al actualizar un servidor de Provisioning desde la versión 7.15 de la CU 5 a la versión 1912, puede aparecer un mensaje de advertencia dos veces. Este mensaje aparece debido a una dependencia en el instalador de CDF (un componente independiente de Citrix Virtual Apps and Desktops) durante la instalación de Citrix Provisioning. El instalador de Provisioning no puede suprimir el

mensaje de reinicio creado por el instalador de CDF. Por eso, el mensaje de reinicio aparece dos veces. [LCM-7594]

## General

- Es posible que no se puedan crear conexiones de host con Azure en Citrix Studio debido a una excepción. El problema se produce por los cambios de Microsoft realizados en Azure. Hay una corrección privada disponible en [CTX457802](#). [CVADHELP-18741]

## Visualización de registros

- Después de ejecutar un cmdlet `BrokerHostingPowerAction` de PowerShell, la pantalla de **registro** de Studio indica que el cmdlet falló, aunque este haya finalizado correctamente. Como solución temporal, compruebe el resultado en el host. [BRK-7002]

## Redirección de contenido

- Con la redirección de contenido del explorador habilitada, pueden fallar los intentos de abrir una nueva ficha haciendo clic con el botón secundario en un hipervínculo en Chrome. Como solución temporal, seleccione `Always allow pop-ups and redirects` en el mensaje `Pop-ups blocked`. [LCM-7480]

## Instalación y actualización

- Con la protección de aplicaciones habilitada, es posible que la tabla de funciones de protección de aplicaciones importadas se elimine al actualizar de la versión 1912 a la versión 1912 LTSR CU1. Además, es posible que se pierda la actualización de la función de StoreFront. Como solución temporal, siga estos pasos:
  1. En un Controller CU1 actualizado, vuelva a importar la tabla de funciones xml disponible con la descarga de CU1.
  2. En el servidor de StoreFront, vuelva a habilitar la función de protección de aplicaciones.

[LCM-7872]

## Problemas conocidos en la versión inicial de 1912

### Instalación y actualización

- Si ya tiene instalado la versión 19061022052 de Universal Print Server (UPS), la actualización de UPS con el metainstallador 1906.2 no agrega ninguna nueva funcionalidad de UPS. Después de la actualización, solamente el número de versión de Universal Print Server, en Programas y características, pasa a ser 19062022068. [HDX-20674]
- Al ejecutar el metainstallador de Citrix Virtual Apps and Desktops, en la página Diagnósticos, si hace clic en **Conectar** sin antes seleccionar **Recopilar información de diagnóstico**, al cerrar el cuadro de diálogo Conectar con Citrix Insight Services, el botón **Siguiente** aparece inhabilitado y no se puede pasar a la página siguiente. Para volver a habilitar el botón **Siguiente**, seleccione y desmarque inmediatamente **Recopilar información de diagnóstico**. [XAXDINST-572]
- Si actualiza la versión de Studio desde XenApp y XenDesktop 7.15 LTSR (7.15 Studio) a Citrix Virtual Apps and Desktops 7 1912 LTSR (1912 Studio) y, a continuación, desinstala 1912 Studio y vuelve a instalar 7.15 Studio, Studio no puede iniciarse y muestra el error “No se puede cargar el complemento de Windows PowerShell PvsPsSnapIn. Se ha producido un error en Studio”. Para resolver este problema, antes de reinstalar 7.15 Studio, elimine manualmente PvsPsSnapIn.dll de `C:\Program Files\Citrix\PowerShell SDK`. [XAXDINST-610]
- Si solicita una lista de opciones válidas para el comando `XenDesktopServerSetup.exe`, aparece la opción `/no_webstudio`. Esta opción es solo para uso interno. No la utilice. [STUD-9701]

### Instalación de VDA

- Después de instalar un VDA y antes de reiniciar la máquina, aparece un mensaje de error de Citrix Files: “.NET Framework incompatible. Apagando. Instale uno de los KB enumerados en esta página de Problemas conocidos para resolver...” Como solución temporal, antes de la instalación del VDA, instale KB4054856 en `NDP471-KB4033342-x86-x64-ALL-ENU.exe`. [LCM-7563]

### General

- Cuando MCS crea máquinas no persistentes en AWS, el indicador `DeleteOnTermination` se establece en `True`. Sin embargo, durante el ciclo de energía, MCS recrea volúmenes EBS y los cambia por el anterior, lo que cambia el indicador `DeleteOnTermination` a `False`. [PMCS-4953]
- En Citrix Hypervisor, después de instalar un nuevo VDA, Citrix Desktop Service establece erróneamente el valor del Registro de XenTools en UTC. El servicio no verifica la hora del sistema,

lo que provoca un error de conexión que pone máquinas existentes en un estado no registrado. Este problema es temporal. El VDA corrige la hora del sistema cuando se sincroniza desde varios orígenes. La corrección actual establece el valor del Registro de XenTools en UTC solamente si la zona horaria del sistema operativo es UTC, lo que provoca que no coincidan. [PMCS-5425]

- Si utiliza el hipervisor para eliminar una máquina virtual provisionada con Citrix Virtual Apps and Desktops, es posible que no pueda agregar la máquina al catálogo porque el disco base también se elimina como parte del proceso de eliminación de la máquina virtual. [PMCS-8591]
- El uso de plantillas para provisionar catálogos se considera una función experimental. Al utilizar este método, es posible que la preparación de la máquina virtual falle. Como consecuencia, el catálogo no se puede publicar con la plantilla. [PMCS-602]
- Si intenta agregar una aplicación protegida a sus **Favoritos**, es posible que aparezca este mensaje: “Sus aplicaciones no están disponibles en este momento...” Al hacer clic en **Aceptar**, aparece el mensaje “No se puede agregar la aplicación”. Después de cambiar a la pantalla **Favoritos**, la aplicación protegida aparece allí, pero no puede quitarla de **Favoritos**. [WSP-5497]
- Cada vez que se carga un archivo comprimido mediante la aplicación Citrix Workspace para HTML5 en una capa SSL de extremo a extremo con los exploradores Chrome o Safari, es posible que se inicie la fiabilidad de la sesión y que, finalmente, se cree una sesión inoperante. Para solucionar este problema, vuelva a iniciar la sesión. Para volver a habilitar la transferencia de archivos, cierre la sesión en curso. [HDX-22106]
- Después de instalar el complemento de la aplicación web de Skype Empresarial, puede que las cámaras web no se enumeren y las páginas de reuniones en Firefox no se actualicen automáticamente. [HDX-13288]
- Al actualizar el VDA a la versión 1906, se instala automáticamente el nuevo controlador de E/S de MCS si no se ha instalado previamente. En consecuencia, los dispositivos de destino no se pueden arrancar en modo de solo lectura. Citrix recomienda no instalar la funcionalidad de E/S MCS actualizada y Citrix Provisioning en el mismo entorno Windows. [PVS-4151]
- Cuando se inicia una aplicación desde StoreFront, es posible que no se inicie en primer plano, o bien está en primer plano, pero no tiene el foco. Como solución temporal, haga clic en el icono de la aplicación situado en la barra de tareas para traerla al primer plano o en la pantalla de la aplicación para situar el foco en ella. [HDX-10126]
- Cuando se conecta a una nueva sesión, se desconecta y luego se vuelve a conectar a la misma sesión, es posible que los iconos de su escritorio parpadeen. Como solución temporal, restablezca el perfil de usuario, cierre sesión y vuelva a iniciar sesión. [HDX-15926, UPM-1362]
- Cuando se usa Windows 10 1809 LTSC, las dependencias VCLibs no se instalan. [HDX-16754]
- Es posible que el cuadro combinado no se muestre correctamente si el usuario selecciona un

cuadro combinado que ya está enfocado en el host. Como solución alternativa, seleccione otro elemento de la interfaz de usuario y, a continuación, seleccione el cuadro combinado. [HDX-21671]

- Cuando intente reconectarse a una sesión, es posible que el escritorio no se cargue y que aparezca una ventana gris. El problema ocurre con la versión 1909 de VDA cuando se ejecuta en Microsoft Windows Server 2019. [HDX-21804]
- Ha habilitado el acceso a aplicaciones locales. Si inicia una sesión en VDA con Windows 2012 R2, desconecta y vuelve a conectar la sesión y, a continuación, inicia una aplicación local y la maximiza, es posible que la barra de tareas del VDA corte la aplicación. [HDX-21913]
- Al configurar las direcciones IPv4 e IPv6 en la red, es posible que no se pueda acceder a los recursos de un grupo de entrega cuando este utiliza una regla de directiva de acceso de brokers configurada para permitir únicamente el filtrado de direcciones IPv4. Para asegurarse de que todos los filtros de recursos se comportan de la manera prevista, configure la regla de la directiva de acceso de brokers para que incluya direcciones IPv4 e IPv6 del cliente. [WADA-7776]

Por ejemplo, para establecer reglas que permitan direcciones IPv4 e IPv6 mediante el acceso “directo a StoreFront” y “de Citrix Gateway”, utilice PowerShell así:

```
1 Set-BrokerAccessPolicyRule -Name "Apps_Direct" -
   IncludedClientIPFilterEnabled $True -IncludedClientIPs @(
   "10.0.0.1", "2001::3")
2 Set-BrokerAccessPolicyRule -Name "Apps_AG" -
   IncludedClientIPFilterEnabled $True -IncludedClientIPs @(
   "10.0.0.1", "2001::3")
```

Para confirmar una regla, use PowerShell así:

```
1 Get-BrokerAccessPolicyRule -Name "\"Apps\_Direct\"" | Select Name,
   IncludedClientIPFilterEnabled, IncludedClientIPs
```

Esto devuelve lo siguiente cuando la regla se configura correctamente para las direcciones IPv4 e IPv6:

```
1 Name          IncludedClientIPFilterEnabled IncludedClientIPs
2 --          -----
3 Apps_Direct          True {
4 10.0.0.1/32, 2001::3/128 }
```

- Cuando las aplicaciones de Microsoft Office 365 compilación 16.0.7967 y versiones posteriores se publican como aplicaciones desde un host Windows Server 2019, se produce un error en la activación de la licencia de Office. Citrix está trabajando con Microsoft para abordar esta limitación de Microsoft. La solución temporal disponible es instalar VDA de Windows Server 2016, que no tienen el componente Web Authentication Manager, que no tiene el comportamiento esperado. [LCM-7637]

- Citrix Virtual Apps and Desktops no admite los administradores delegados de System Center Virtual Machine Manager (SCVMM) con acceso a varios grupos de hosts de nivel superior (sin raíz) y nombres de grupos de hosts duplicados. Aparece este mensaje de error al agregar una conexión de alojamiento de SCVMM mediante la cuenta de administrador delegado:

**Error inesperado. Contactar con Citrix Support**

[CVADHELP-10669]

- Es posible que no se puedan crear conexiones de host con Azure en Citrix Studio debido a una excepción. El problema se produce por los cambios de Microsoft realizados en Azure. Hay una corrección privada disponible en [CTX457802](#). [CVADHELP-18741]

## Studio

- En algunos casos, el estado de energía de la máquina virtual aparece como desconocido aunque aparezca registrada. Para resolver este problema, modifique el valor `HostTime` de la clave del Registro para inhabilitar la sincronización horaria con el host:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XenTools\HostTime="Local"
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\XenTools\HostTime="Local"
```

### Sugerencia:

El valor predeterminado es `HostTime="UTC"`. Cambie este valor a algo que no sea UTC, como, por ejemplo, `Local`. Este cambio inhabilita la sincronización horaria con el host. [BRK-4187]

## Director

- El enlace **Consola** de Citrix Director > Detalles de la máquina no inicia la consola de la máquina en los exploradores web Microsoft Edge 44 y Firefox 68 ESR. [DIR-8160]
- Si ha actualizado Director a la versión 7 1903 o a una posterior desde cualquier versión anterior y no ha desactivado la caché del explorador (la casilla de verificación “Inhabilitar caché” está desmarcada), los informes personalizados creados previamente se pierden y Director muestra un “Error inesperado del servidor” en la ficha Informes personalizados. Las diferencias en el diseño de la interfaz de usuario entre las versiones anteriores y actuales de Director pueden causar este problema. Inhabilite la caché y fuerce una actualización para ver informes personalizados antiguos y, así, crear y ver nuevos informes personalizados. [DIR-7634]

## Gráficos

- Establecer la directiva **Ver contenido de las ventanas al arrastrar** en **Prohibido** no funciona en ESXi ni en Hyper-V. [HDX-22002]
- Si inicia una vista previa de vídeo con una aplicación de cámara web de 64 bits con compresión Theora, es posible que la sesión se bloquee. [HDX-21443]
- La aplicación universal Skype de Windows (UWA) se inicia con un fondo negro. En algunos casos, este fondo ocupa toda la pantalla del cliente. [HDX-22088]
- En ocasiones, es posible que una aplicación se inicie en segundo plano mientras que el foco se encuentra en otra aplicación. Como resultado, se pierde el orden de las ventanas locales. [HDX-21569]
- La consola de XenCenter puede mostrar una pantalla vacía después de desconectar una sesión de XenDesktop. Como solución temporal, envíe CTRL + ALT + SUPR a la consola de XenCenter para que aparezca la pantalla de la consola. [HDX-17261]
- Es posible que los PPP no se correspondan durante una sesión que se ejecuta en un SO multitensión Windows 2016 o 2019 cuando se cambian los PPP en el cliente y se vuelve a conectar la sesión. Como solución alternativa, cambie el tamaño de la ventana de la sesión para que coincida con los PPP. [HDX-17313]
- Estos problemas corresponden a la codificación por hardware de ADM. [HDX-20476]:

- Es posible que se produzca una pixelación al usar la aplicación Citrix Workspace para Windows. Como solución temporal, cree el siguiente parámetro del Registro en el cliente que tenga instalada la aplicación Citrix Workspace para Windows:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\GfxRe  
(32-bit)

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced  
(64-bit)

Nombre: MaxNumRefFrames

Tipo: DWORD

Valor: 5

- Es posible que no vea un rendimiento óptimo al usar la resolución 4K. Este problema reduce la velocidad de fotogramas a solamente 7-10 fotogramas por segundo. Además, el tiempo de codificación aumenta.
- Es posible que los vídeos vayan a trompicones durante los primeros 2-5 segundos cuando se utiliza el modo de gráficos Selective H.264. El SDK de RapidFire no está diseñado para este caso de uso.

## Impresión

- Las impresoras de Universal Print Server seleccionadas en el escritorio virtual no aparecen en la ventana **Dispositivos e impresoras** del Panel de control de Windows. No obstante, cuando los usuarios trabajan en las aplicaciones, pueden imprimir con esas impresoras. Este problema se produce solamente en plataformas Windows Server 2012, Windows 10 y Windows 8. Para obtener más información, consulte [CTX213540](#). [HDX-5043, 335153]
- Puede que la impresora predeterminada no se marque correctamente en la ventana del diálogo de impresión. Este problema no afecta los trabajos de impresión enviados a la impresora predeterminada. [HDX-12755]

## Machine Creation Services

- En entornos de AWS, iniciar y cerrar instancias de trabajador de volumen no quita sus interfaces de red asociadas. Para resolver este problema, elimine manualmente las interfaces de red con las condiciones en este estado: `Available && Description: "XD NIC"&& tag: "XdConfig : XdProvisioned=true"`. [PMCS-20775]

## App-V

- Las aplicaciones de App-V pueden no iniciarse si se publican más de 100 aplicaciones en un único grupo de entrega. Para aumentar este límite, utilice la propiedad `MaxReceivedMessage-Size` en el elemento vinculante adecuado para aumentar el tamaño del mensaje Max Receivable. Puede hacerlo durante la configuración del Delivery Controller y/o del agente del broker en el VDA. [APPV-11]

## Problemas de terceros

- Chrome admite la automatización de interfaz de usuario solamente para barras de herramientas, fichas, menús y botones de una página web. Debido a este problema de Chrome, es posible que la función de visualización automática del teclado no funcione en un explorador Chrome en dispositivos táctiles. Como solución temporal, ejecute `chrome --force-renderer-accessibility` o abra una ficha nueva del explorador, escriba `chrome://accessibility` y habilite la compatibilidad con **API de accesibilidad nativa** para páginas específicas o para todas las páginas. Además, cuando publique una aplicación integrada, puede publicar Chrome con el conmutador `--force-renderer-accessibility`. [HDX-20858]
- Un problema en la versión 1809 de Microsoft Windows 10 puede causar un comportamiento ligeramente errático al usar el lápiz para Surface Pro y Surface Book. [HDX-17649]

- Es posible que un VDA que se ejecute en Azure se bloquee al utilizar Enlightened Data Transport (EDT), lo que requeriría una reconexión a la sesión. Como solución temporal, establezca `edtMSS` en 1350 y `OutbufLength` en 1350 en los entornos de Azure. Para obtener más información, consulte [CTX231821](#). [HDX-12913]
- En la redirección de contenido del explorador, después de iniciar un vídeo de YouTube con el reproductor de vídeos HTML5 de YouTube, el modo de pantalla completa puede no funcionar. Aunque haga clic en el icono situado en la esquina inferior derecha del vídeo, el vídeo no cambia de tamaño, dejando el fondo negro en toda el área de la página. Como solución temporal, haga clic en el botón de pantalla completa y, a continuación, seleccione el modo de pantalla completa. [HDX-11294]

## Elementos retirados

October 9, 2023

Los siguientes anuncios tienen por objeto avisarle por adelantado acerca de las plataformas, los productos y las funciones de Citrix que se están retirando progresivamente, de modo que pueda tomar a tiempo las decisiones empresariales pertinentes. Citrix examina el uso que hacen los clientes de una función que está por retirar y los comentarios que tengan sobre la eliminación de la función para determinar cuándo retirarla. Estos anuncios están sujetos a cambios en las versiones posteriores y es posible que no contengan todas las funciones o funciones retiradas. Para obtener información detallada sobre el ciclo de vida útil de los productos, consulte el artículo [Product Lifecycle Support Policy](#). Para obtener información sobre la opción de servicio Long Term Service Release (LTSR), consulte <https://support.citrix.com/article/CTX205549>.

## Elementos eliminados y obsoletos

En la siguiente tabla, se muestran las plataformas, las funciones y los productos Citrix que se han retirado o eliminado.

Los elementos *obsoletos* no se eliminan inmediatamente. Citrix sigue ofreciéndolos en esta versión Long Term Service Release de Citrix Virtual Apps and Desktops 7 1912, pero se eliminarán en una versión futura.

Los elementos *eliminados* se quitan (o ya no se ofrecen o se desarrollan) en Citrix Virtual Apps and Desktops. Las fechas en **negrita** indican cambios en esta versión.

<b>Elemento</b>	<b>Retirada anunciada en</b>	<b>Eliminado en</b>	<b>Alternativa</b>
Compatibilidad con el formato SDP de WebRTC (Plan B)	2308	—	Actualice la aplicación Citrix Workspace a una versión compatible.
Compatibilidad con el modo de ventana única en la optimización de Microsoft Teams	2308	—	Actualice la aplicación Citrix Workspace a una versión que admita el modo multiventana. Para obtener más información, consulte <a href="#">Tabla de funciones y compatibilidad de versiones</a> .
Importar dispositivos de destino de Citrix Provisioning a catálogos de Citrix Virtual Apps and Desktops para su administración	1912 LTSR	-	Utilice el asistente para exportar dispositivos de Citrix Provisioning.
Compatibilidad con el explorador de StoreFront para la versión antigua de Microsoft Edge	1912 LTSR CU2	<b>1912 LTSR CU3</b>	Actualice la versión a Microsoft Edge (basado en Chromium).
Citrix License Administration Console (última vez incluida en Windows License Server, versión 11.16.3, build 30000, y eliminada en Windows License Server, versión 11.16.6, build 31000).	1912 LTSR CU2	1912 LTSR CU2	Utilice Citrix Licensing Manager.

Elemento	Retirada anunciada en	Eliminado en	Alternativa
Citrix SCOM Management Packs para XenApp y XenDesktop, Provisioning Services y StoreFront. Para ver las versiones de productos que se pueden supervisar, consulte la <a href="#">documentación de Citrix SCOM Management Pack</a> .	<b>1912†</b>		Utilice Director para supervisar y administrar la implementación. Para obtener más información sobre el fin de vida de SCOM y sus alternativas, consulte <a href="https://support.citrix.com/article/CTX266943">https://support.citrix.com/article/CTX266943</a> .
Compatibilidad con versiones de Microsoft .NET Framework anteriores a la versión 4.8 para los VDA y los componentes principales del servidor. Incluye Delivery Controller, Studio, Director y StoreFront.	<b>1912</b>		Actualice a .NET Framework 4.8.
VDA en Windows Server 2012 R2.	<b>1912</b>		Instale los VDA en un sistema operativo compatible.
Componente de migración de aplicaciones de AppDNA de la edición Premium de Citrix Virtual Apps and Desktops.	1909		

<b>Elemento</b>	<b>Retirada anunciada en</b>	<b>Eliminado en</b>	<b>Alternativa</b>
Instalación de Studio en máquinas de 32 bits (x86).	1909		Realice la instalación en un sistema operativo x64 compatible.
Funcionalidad del enlace de Excel en aplicaciones integradas. Esto se utilizó para crear iconos independientes de la barra de tareas para cada libro de Microsoft Excel 2010.	1909	1909	
Componentes principales de servidor en Windows Server 2012 R2 (incluidos los Service Packs). Incluye: Delivery Controller, Studio y Director.	1906		Instale en un sistema operativo compatible más reciente.
Compatibilidad con bases de datos de configuración de sitios, registro de configuraciones y supervisión en las versiones 2008 R2, 2012 y 2014 de Microsoft SQL Server (incluidos todos los Service Packs y ediciones).	1906		Instale bases de datos en una versión compatible de Microsoft SQL Server.

<b>Elemento</b>	<b>Retirada anunciada en</b>	<b>Eliminado en</b>	<b>Alternativa</b>
Compatibilidad con VDA en Windows 10 en plataformas x86.	1906	1909*	Instale los VDA en un sistema operativo x64 compatible. <b>Esta función sigue ofreciéndose en Citrix Virtual Apps and Desktops 7 1912 LTSR.</b>
Eliminación de Citrix Smart Tools Agent de los medios de instalación de Citrix Virtual Apps and Desktops.	1903	1906	
Eliminación de las opciones de Delivery Controller para los siguientes productos de StoreFront que han alcanzado el final de su ciclo de vida: VDI-in-a-Box y XenMobile (9.0 y versiones anteriores).	1903	1903	
Compatibilidad con Linux VDA en Red Hat Enterprise Linux/CentOS 7.5.	1903	1903	Instale Linux VDA en una versión posterior de Red Hat Enterprise Linux.
Acceso a escritorios en sitios de Desktop Appliance para usuarios de StoreFront	1811	<b>1912</b>	Use <a href="#">Desktop Lock</a> para casos de uso que no pertenezcan a ningún dominio.
Compatibilidad con la tecnología de pantalla remota Framehawk	1811	1903	Utilice <a href="#">Thinwire</a> con el <a href="#">transporte adaptable</a> habilitado.

<b>Elemento</b>	<b>Retirada anunciada en</b>	<b>Eliminado en</b>	<b>Alternativa</b>
Disponibilidad de Citrix Smart Scale en todas las versiones de Citrix Virtual Apps and Desktops (y con XenApp y XenDesktop). Esta función alcanzará el ciclo Fin de vida el 31 de mayo de 2019.	1808	1906	Considere la posibilidad de utilizar <a href="#">Virtual Apps and Desktops Service</a> en Citrix Cloud para mejorar la funcionalidad de administración de energía.
Citrix StoreFront, Citrix VDA, Citrix Studio, Citrix Director y Citrix Delivery Controller son compatibles con las versiones de Microsoft .NET Framework 4.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 y 4.7.	7.18	1808	Actualice a .NET Framework 4.7.1 o una posterior. (El instalador instala automáticamente .NET Framework 4.7.1 si aún no está instalado.)
Compatibilidad con Linux VDA en Red Hat Enterprise Linux 7.3.	7.18	1808	Instale Linux VDA en una versión posterior de Red Hat Enterprise Linux.
Compatibilidad de StoreFront con los protocolos TLS 1.0 y TLS 1.1 entre Citrix Virtual Apps and Desktops (antes XenApp y XenDesktop), Citrix Receiver y Workspace Hub.	7.17		Actualice los Citrix Receiver a una aplicación Citrix Workspace que admita el protocolo TLS 1.2. Para obtener más información sobre la aplicación Citrix Workspace, consulte <a href="https://docs.citrix.com/es-es/citrix-workspace-app">https://docs.citrix.com/es-es/citrix-workspace-app</a> .

<b>Elemento</b>	<b>Retirada anunciada</b>		<b>Alternativa</b>
	<b>en</b>	<b>Eliminado en</b>	
Compatibilidad de VDA con la configuración de directiva “Instalación automática de controladores de impresora”.	7.16	7.16	Ninguno. Configuración de directiva que se admitía solo para agentes VDA en sistemas operativos anteriores (Windows 7, Windows Server 2012 R2 y versiones anteriores).
Compatibilidad de Linux VDA con SUSE Linux Enterprise Server 11 Service Pack 4.	7.16	7.16	Instale Linux VDA en una versión compatible de SUSE.
Compatibilidad del controlador WDDM de Citrix con los VDA.	7.16	7.16	El controlador WDDM de Citrix ya no se instala con los agentes VDA.
Mobility SDK / Mobile SDK (del antiguo Citrix Labs)	7.16		Reemplazado por configuraciones de directiva para la experiencia móvil y por una experiencia nativa para aplicaciones o escritorios alojados.

Elemento	Retirada anunciada		Alternativa
	en	Eliminado en	
Agentes VDA en Windows 10 versión 1511 (Threshold 2) y versiones anteriores de SO de sesión única Windows, incluido Windows 8.x y Windows 7 (consulte <a href="https://www.citrix.com/blogs/2018/01/08/the-citrix-strategy-for-windows-7-virtual-desktop-users/">https://www.citrix.com/blogs/2018/01/08/the-citrix-strategy-for-windows-7-virtual-desktop-users/</a> ).	7.15 LTSR (y 7.12)	7.16	Instale agentes VDA de SO de sesión única en Windows 10 versión mínima 1607 (Redstone 1) o una versión más reciente de Canal semianual. Si utiliza LTSB 1607, se recomienda un VDA 7.15. Consulte <a href="#">CTX224843</a> .
Agentes VDA en Windows Server 2008 R2 y Windows Server 2012 (incluidos los Service Packs).	7.15 LTSR (y 7.12)	7.16	Instale los VDA en un sistema operativo compatible.
Redirección de composición del escritorio (anteriormente conocida como DirectX Command Remoting o DCR)	7.15 LTSR	7.16	Use <a href="#">Thinwire</a> .
Experiencia clásica en Citrix Receiver para Web (interfaz de usuario “burbujas verdes”).	7.15 LTSR (y StoreFront 3.12)	1903	<a href="#">Experiencia unificada de Citrix Receiver para Web</a> .

<b>Elemento</b>	<b>Retirada anunciada en</b>	<b>Eliminado en</b>	<b>Alternativa</b>
Componentes principales en Windows Server 2012 y Windows Server 2008 R2 (incluidos los Service Packs). Incluye: Delivery Controller, Studio, Director, StoreFront, License Server y Universal Print Server.	7.15 LTSR	7.18	Instale los componentes en un sistema operativo compatible.
Función Autoservicio de restablecimiento de contraseñas en Windows Server 2012 y Windows Server 2008 R2 (incluidos los Service Packs).	7.15 LTSR	7.18	Instale en un sistema operativo compatible más reciente.
Studio en Windows 7, Windows 8 y Windows 8.1 (incluidos los Service Packs).	7.15 LTSR	7.18	Instale Studio en un sistema operativo compatible.
Redirección de Flash	7.15 LTSR	<b>1912</b>	Cree contenido de vídeo (por ejemplo, un vídeo HTML5). Use la redirección de vídeo HTML5 para el contenido administrado, y la redirección de contenido del explorador web para sitios web públicos. Para obtener más información, consulte <a href="#">Fin de vida para la redirección de Flash</a> .

<b>Elemento</b>	<b>Retirada anunciada en</b>	<b>Eliminado en</b>	<b>Alternativa</b>
Integrar Citrix Online (producto de la familia GoTo) en StoreFront	7.14 (y StoreFront 3.11)	StoreFront 3.12	
Ya no se crea la cuenta de usuario CtxAppVCOMAdmin. Esta cuenta se creaba durante la instalación del VDA y se agregaba al grupo de administradores locales presente en la máquina del VDA. También se ha eliminado el mecanismo “COM” subyacente.	7.14	7.14	El servicio CtxAppVService de Windows cumple la misma función. Se instala y se configura automáticamente, por lo que no requiere la interacción del usuario.
Compatibilidad con el componente UpsServer (Universal Print Server) en Windows Server 2008 de 32 bits	7.14	7.14	Instale en un sistema operativo compatible más reciente.
StoreFront y Receiver para Web en Internet Explorer 8	7.13	7.13	
En la instalación de un VDA desde la línea de comandos, la opción /no_appv para impedir la instalación de componentes de App-V de Citrix.	7.13	7.13	Utilice la opción de línea de comandos: /exclude “Citrix Personalization for App-V –VDA”.

Elemento	Retirada anunciada		Alternativa
	en	Eliminado en	
El instalador del producto completo ya no instala el complemento Citrix.Common.Commands en nuevas instalaciones y lo elimina automáticamente al actualizar instalaciones existentes.	7.13	7.13	Algunos comandos de PowerShell que suministraba el complemento Citrix.Common.Commands siguen estando disponibles en XenApp 6.5 SDK.
La funcionalidad parcial para manipular datos de iconos, proporcionada por los cmdlets *-CtxIcon.	7.13	7.13	Ahora la proporcionan los cmdlets *-BrokerIcon en el servicio Broker.
Modo antiguo de Thinwire	7.12	7.16	Use <a href="#">Thinwire</a> . Si aún utiliza el modo antiguo de Thinwire en Windows Server 2008 R2, migre a Windows Server 2012 R2 o Windows Server 2016 y use Thinwire.
Actualizaciones locales desde StoreFront 2.0, 2.1, 2.5 y 2.5.2.	7.13	7.16	Debe actualizar desde una de estas versiones a una versión posterior compatible y, a continuación, actualizar a XenApp y XenDesktop 7.16.

<b>Elemento</b>	<b>Retirada anunciada en</b>	<b>Eliminado en</b>	<b>Alternativa</b>
Actualizaciones locales desde XenDesktop 5.6 o 5.6 FP1.	7.12	7.16	Debe migrar su implementación de XenDesktop 5.6 o 5.6 FP1 a la versión actual de XenDesktop. Para ello, actualice a XenDesktop 7.6 LTSR (con la actualización CU más reciente) y, a continuación, actualice a la versión más reciente o la versión LTSR de Citrix Virtual Desktops (antes XenDesktop).
Instalación de Delivery Controller, Director, StoreFront o License Server en máquinas de 32 bits (x86).	7.12	7.16	Realice la instalación en un sistema operativo x64 compatible.
Concesión de conexiones XenDesktop 5.6 en Windows XP. No se admiten instalaciones de VDA en Windows XP.	7.12	7.16	Use <a href="#">Caché de host local</a> .
Conexiones a CloudPlatform.	7.12	7.16	Instale los VDA en un sistema operativo compatible.
Conexiones Azure Classic (también conocido como Administración de servicios de Azure).	7.12		Use un hipervisor o servicio de nube compatibles. Use Azure Resource Manager.

Elemento	Retirada anunciada		Alternativa
	en	Eliminado en	
Funcionalidad de AppDisks (y la integración de AppDNA en Studio, que la admite)*	7.13	2003	Consulte “Citrix App Layering”.
Funcionalidad Personal vDisk*	7.13	2006	Utilice la tecnología de <a href="#">capa de personalización de usuarios</a> o <a href="#">capa de usuarios de Citrix App Layering</a> .

† **Importante:** A partir de junio de 2020, deberá eliminar cualquier SCOM Management Pack de su sitio Citrix Virtual Apps and Desktops 7 1912 LTSR para mantener la funcionalidad y las ventajas de LTSR.

\* La opción de servicio Long Term Service Release (LTSR) no cubre esta función.

## Requisitos del sistema

June 27, 2024

### Introducción

Los requisitos del sistema descritos en este documento son válidos en el momento de la publicación de la presente versión de producto. Las actualizaciones se realizan periódicamente. Aquellos componentes de los requisitos del sistema que no se incluyen aquí (por ejemplo, sistemas host, la aplicación Citrix Workspace y Citrix Provisioning) se describen en su documentación respectiva.

Consulte el artículo [Antes de instalar](#) para prepararse.

A menos que se indique lo contrario, el instalador de componentes implementa automáticamente los requisitos previos de software (por ejemplo, los paquetes .NET y C++) si no se han detectado las versiones correspondientes en la máquina. Los medios de instalación de Citrix también contienen algunos de estos programas de requisitos previos.

Los medios de instalación contienen varios componentes de terceros. Antes de usar el software de Citrix, busque actualizaciones para los componentes de terceros e instálelas.

Para obtener información sobre la globalización, consulte el artículo [CTX119253](#) de Knowledge Center.

Para las funciones y los componentes que se pueden instalar en servidores Windows, no se admiten las instalaciones Nano Server a menos que se indique. Server Core solo se admite en Controllers y Director.

### Requisitos de hardware

Los valores de la memoria RAM y el espacio en disco son adicionales a los requisitos de la imagen del producto, el sistema operativo y otro software en la máquina. El rendimiento varía según la configuración. La configuración incluye las funciones que utilice y la cantidad de usuarios, entre otros factores. Utilizar solo lo mínimo puede derivar en un rendimiento lento.

En la siguiente tabla, se muestran los requisitos mínimos para los componentes principales.

---

Componente	Mínimo
Todos los componentes principales en un servidor, solo para un entorno de evaluación, no una implementación de producción.	5 GB de RAM
Todos los componentes principales en un servidor, para una implementación de prueba o un entorno de producción pequeño.	12 GB de RAM
Delivery Controller (se necesita más espacio en disco para la Caché de host local).	5 GB de RAM, 800 MB de disco duro, base de datos; consulte <a href="#">Guía de tamaño</a> .
Studio	1 GB de RAM, 100 MB de disco duro
Director	2 GB de RAM, 200 MB de disco duro
StoreFront	2 GB de RAM; consulte la <a href="#">documentación de StoreFront</a> para conocer las recomendaciones de disco.
Servidor de licencias	2 GB de RAM; consulte la <a href="#">documentación sobre licencias</a> para conocer las recomendaciones de disco.

---

## Tamaño de las máquinas virtuales que entregan escritorios y aplicaciones

No se pueden ofrecer recomendaciones concretas debido a la naturaleza dinámica y compleja del hardware existente en el mercado, además de que cada implementación tiene necesidades únicas. Por lo general, el tamaño de una máquina virtual de Citrix Virtual Apps se calcula en función del hardware y no se tienen en cuenta las cargas de trabajo de usuarios (una excepción es la RAM; se necesita más RAM para aplicaciones que consumen más).

Para obtener más información:

- [Citrix Tech Zone](#) contiene directrices sobre el tamaño de los VDA.
- [La escalabilidad de un solo servidor para Citrix Virtual Apps and Desktops](#) analiza cuántos usuarios o máquinas virtuales puede contener un único host físico.

## Runtime de Microsoft Visual C++ 2017

Instalar el runtime de Microsoft Visual C++ 2017 en una máquina que tiene instalado el runtime de 2015 puede provocar la eliminación automática del runtime de 2015. Esta acción funciona tal y como está diseñada.

Si ya ha instalado componentes de Citrix que instalan automáticamente el runtime de Visual C++ 2015, dichos componentes siguen funcionando correctamente con la versión de Visual C++ 2017.

Para obtener más información, consulte el artículo de Microsoft <https://developercommunity.visualstudio.com/content/problem/332815/visual-c-redistributable-2017-install-removes-visu.html>.

## Delivery Controller

Sistemas operativos compatibles:

- Windows Server 2019, ediciones Standard y Datacenter, y con la opción Server Core
- Windows Server 2016, ediciones Standard y Datacenter, y con opción Server Core
- Windows Server 2012 R2, ediciones Standard y Datacenter, y Server Core para Windows Server 2012 R2

Requisitos:

- Microsoft .NET Framework 4.7.1 (o una versión posterior) se instala automáticamente si no está instalado.
- Windows PowerShell 3.0 o una versión posterior.
- Runtime de Microsoft Visual C++ 2017, de 32 bits y 64 bits.

## Bases de datos

Versiones compatibles de Microsoft SQL Server para la configuración del sitio, el registro de configuración y la base de datos de supervisión:

- SQL Server 2019, ediciones Express, Standard y Enterprise.
- SQL Server 2017, ediciones Express, Standard y Enterprise.
  - Para instalaciones nuevas: De forma predeterminada, si no se detecta una instalación de SQL Server compatible existente, SQL Server Express 2017 con Cumulative Update 16 se instala al instalar el Controller.
  - Para la actualización de versiones, no se actualiza ninguna versión existente de SQL Server Express.
- SQL Server 2016 SP1 hasta SP3, ediciones Express, Standard y Enterprise.
- SQL Server 2014 desde SP1 hasta SP3, ediciones Express, Standard y Enterprise.
- SQL Server 2012 hasta SP4, ediciones Express, Standard y Enterprise.
- SQL Server 2008 R2 SP2 y SP3, ediciones Express, Standard, Enterprise y Datacenter.

Se admiten las siguientes soluciones de alta disponibilidad de base de datos (excepto SQL Server Express, que solo admite el modo autónomo):

- Instancias en clúster de conmutación por error de AlwaysOn de SQL Server
- Grupos de disponibilidad AlwaysOn de SQL Server (incluidos los grupos de disponibilidad básica)
- Crear reflejo de la base de datos de SQL Server

Se requiere la autenticación de Windows para las conexiones entre el Controller y la base de datos de SQL Server del sitio.

Al instalar un Controller, Microsoft SQL Server Express LocalDB 2017 con Cumulative Update 16 se instala para usarlo con la función Caché de host local. Esta instalación es independiente de la instalación predeterminada de SQL Server Express para la base de datos del sitio (Al actualizar la versión de un Controller, la versión existente de Microsoft SQL Server Express LocalDB no se actualiza. Si desea actualizar la versión LocalDB, siga las instrucciones de [Acciones de base de datos](#)).

Para obtener más información, consulte estos artículos:

- [Bases de datos](#)
- En el artículo [CTX114501](#) de Knowledge Center se indican las bases de datos compatibles más recientes.
- [Guía sobre tamaños de bases de datos](#)
- [Caché de host local](#)

## Citrix Studio

Sistemas operativos compatibles:

- Windows Server 2019, Standard y Datacenter Edition
- Windows Server 2016, Standard y Datacenter Edition
- Windows Server 2012 R2, Standard y Datacenter Edition
- Windows 10

Requisitos:

- Microsoft .NET Framework 4.7.1 (o una versión posterior) se instala automáticamente si no está instalado.
- Microsoft Management Console 3.0 (se incluye con todos los sistemas operativos compatibles)
- Windows PowerShell 3.0 o una versión posterior.

## Citrix Director

Sistemas operativos compatibles:

- Windows Server 2019, ediciones Standard y Datacenter, y con la opción Server Core
- Windows Server 2016, ediciones Standard y Datacenter, y con opción Server Core
- Windows Server 2012 R2, ediciones Standard y Datacenter, y Server Core para Windows Server 2012 R2

Requisitos:

- Microsoft .NET Framework 4.7.1 (o una versión posterior) se instala automáticamente si no está instalado.
- Microsoft Internet Information Services (IIS) 7.0 y ASP .NET 2.0. Asegúrese de que el rol de servidor IIS tiene instalado el servicio de rol de contenido estático. Si este software aún no está instalado, se le solicitará que introduzca los medios de instalación de Windows Server. En ese momento, el software se instalará.

Nota:

Para ver los registros de eventos en máquinas en las que está instalado Citrix Director, debe instalar Microsoft .NET Framework 2.0.

## Citrix User Profile Manager

- Asegúrese de que Citrix User Profile Manager y Citrix User Profile Manager WMI Plug-in estén instalados en el VDA (página **Componentes adicionales** del asistente de instalación). Citrix Profile Management Service debe estar ejecutándose para ver los detalles del perfil de usuario en Director.

Requisitos de integración de System Center Operations Manager (SCOM):

- Windows Server 2012 R2
- System Center 2012 R2 Operations Manager

Exploradores compatibles para ver Director:

- Internet Explorer 11 (Solo puede usar Internet Explorer 10 en máquinas Windows Server 2012 R2.) Internet Explorer no admite el modo de compatibilidad. Utilice la configuración recomendada del explorador para acceder a Director. Al instalar Internet Explorer, acepte el valor predeterminado para usar la configuración de compatibilidad y seguridad recomendada. Si ya instaló el explorador web y optó por no usar la configuración recomendada, vaya a **Herramientas > Opciones de Internet > Avanzadas > Restablecer** y siga las instrucciones.
- Microsoft Edge
- Firefox ESR (Extended Support Release; versión de asistencia extendida).
- Chrome

La mejor resolución de pantalla recomendada para ver Director es de 1366 x 1024.

## **Virtual Delivery Agent (VDA) para SO de sesión única**

Sistemas operativos compatibles:

- Windows 10 (solo x64), versión mínima: 1607.
  - Para obtener información sobre las ediciones admitidas, consulte el artículo [CTX224843](#) de Knowledge Center.
  - Para ver los problemas conocidos de Citrix con la versión 1709, consulte el artículo [CTX229052](#) de Knowledge Center.

Requisitos:

- Microsoft .NET Framework 4.7.1 (o una versión posterior) se instala automáticamente si no está instalado.
- Runtime de Microsoft Visual C++ 2017, de 32 bits y 64 bits.

El acceso con Remote PC usa este VDA, que se instala en equipos físicos de oficina. Este VDA admite el arranque seguro (Secure Boot) para el acceso con Remote PC de Citrix Virtual Desktops en Windows 10.

Algunas funciones de aceleración multimedia (como la Redirección de HDX MediaStream para Windows Media) requieren que Microsoft Media Foundation esté instalado en la máquina donde quiere instalar el VDA. Si la máquina no tiene instalado Media Foundation, la función unciones de aceleración multimedia no se instala y no funciona. No quite Media Foundation de la máquina después de instalar el software de Citrix. De lo contrario, los usuarios no pueden iniciar sesión en la máquina. En la

mayoría de las ediciones Windows de SO de sesión única compatibles, la compatibilidad con Media Foundation ya está instalada y no se puede quitar. Sin embargo, las ediciones N no incluyen ciertas tecnologías relacionadas con elementos multimedia, pero se puede obtener el software de Microsoft o de un tercero. Para obtener más información, consulte [Antes de instalar](#).

Para obtener más información acerca de Linux VDA, consulte los artículos de [Linux Virtual Delivery Agent](#).

Para usar la función VDI de servidor, puede usar la interfaz de línea de comandos para instalar un VDA para SO de sesión única en una máquina de Windows Server 2019 o Windows Server 2016. Consulte [VDI de servidor](#) para obtener instrucciones.

Para obtener información sobre cómo instalar un VDA en una máquina con Windows 7, consulte [Sistemas operativos anteriores](#).

## Virtual Delivery Agent (VDA) para SO multisesión

Sistemas operativos compatibles:

- Windows Server 2019, Standard y Datacenter Edition
- Windows Server 2016, Standard y Datacenter Edition
- Windows Server 2012 R2, Standard y Datacenter Edition

El instalador implementa automáticamente estos requisitos, que también están disponibles en las carpetas **Support** de los medios de instalación de Citrix:

- Microsoft .NET Framework 4.7.1 (o una versión posterior) se instala automáticamente si no está instalado.
- Runtime de Microsoft Visual C++ 2017, de 32 bits y 64 bits.

El instalador automáticamente instala y habilita los servicios de rol de los Servicios de Escritorio remoto si aún no están instalados y habilitados.

Algunas funciones de aceleración multimedia (como la Redirección de HDX MediaStream para Windows Media) requieren que Microsoft Media Foundation esté instalado en la máquina donde quiere instalar el VDA. Si la máquina no tiene instalado Media Foundation, las funciones de aceleración multimedia no se instalaron y no funcionan. No quite Media Foundation de la máquina después de instalar el software de Citrix; de lo contrario, los usuarios no podrán iniciar sesión en ella. En la mayoría de las versiones de Windows Server, la función Media Foundation se instala a través del Administrador del servidor. Para obtener más información, consulte [Antes de instalar](#).

Si Media Foundation no está presente en el VDA, estas funciones multimedia no funcionarán:

- Redirección de Windows Media
- Redirección de vídeo HTML5

- Redirección de cámaras web de HDX RealTime

Para obtener más información acerca de Linux VDA, consulte los artículos de [Linux Virtual Delivery Agent](#).

Para obtener información sobre cómo instalar un VDA en un sistema operativo Windows que ya no es compatible, consulte [Sistemas operativos anteriores](#).

## Hosts o recursos de virtualización

Se admiten los siguientes recursos de host/virtualización (ordenados alfabéticamente). Donde corresponda, se admiten las siguientes versiones *superior.inferior*, incluidas las actualizaciones de esas versiones. El artículo [CTX131239](#) de Knowledge Center contiene la información sobre versiones recientes, además de enlaces a los problemas conocidos.

Algunas funciones no están disponibles en todas las plataformas host ni en todas las versiones. Consulte la documentación sobre las funciones en cuestión para obtener más información.

La función Wake on LAN del acceso con Remote PC requiere Microsoft System Center Configuration Manager, mínimo 2012.

- **Amazon Web Services (AWS)**

- Puede aprovisionar aplicaciones y escritorios en sistemas operativos Windows de sesión única y multisesión compatibles.
- Citrix admite Amazon Relational Database Service (RDS). Para obtener información adicional, consulte [Citrix Ready Marketplace](#) y [Citrix y AWS](#).

- **Citrix Hypervisor (anteriormente, XenServer)**

[CTX131239](#) contiene información sobre la versión actual, además de enlaces a los problemas conocidos.

Para obtener más información, consulte [Entornos de virtualización de Citrix Hypervisor](#).

- **CloudPlatform (retirado)**

- **Microsoft Azure Classic (retirado)**

- **Microsoft Azure Resource Manager**

Para obtener información, consulte [Entornos de virtualización para Azure Resource Manager](#).

- **Microsoft System Center Virtual Machine Manager**

Incluye cualquier versión de Hyper-V que se pueda registrar en las versiones compatibles de System Center Virtual Machine Manager.

[CTX131239](#) contiene información sobre la versión actual, además de enlaces a los problemas conocidos.

Para obtener más información, consulte [Entornos de virtualización de Microsoft System Center Virtual Machine Manager](#).

- **Nutanix Acropolis**

[CTX131239](#) contiene información sobre la versión actual, además de enlaces a los problemas conocidos.

Para obtener más información, consulte [Entornos de virtualización de Nutanix](#).

- **VMware vSphere (vCenter + ESXi)**

No se admite la operación “Linked Mode” de vSphere vCenter.

[CTX131239](#) contiene información sobre la versión actual, además de enlaces a los problemas conocidos.

Para obtener más información, consulte [Entornos de virtualización de VMware](#).

## **Niveles funcionales de Active Directory**

Se admiten los siguientes niveles funcionales de bosque y dominio de Active Directory:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008

## **HDX**

### **Audio**

Se admite el audio UDP para ICA de multisección en la aplicación Citrix Workspace para Windows y la aplicación Citrix Workspace para Linux 13.

La eliminación de eco se admite en la aplicación Citrix Workspace para Windows.

Consulte lo que se admite y los requisitos necesarios para la función HDX. Para obtener más información sobre las funciones HDX y las aplicaciones Citrix Workspace, consulte la [Tabla de funciones](#).

## HDX y la entrega de Windows Media

Se admiten los siguientes clientes para la obtención de contenido de Windows Media del lado del cliente, la redirección de Windows Media y la transcodificación multimedia en tiempo real de Windows Media: la aplicación Citrix Workspace para Windows, la aplicación Citrix Workspace para iOS y la aplicación Citrix Workspace para Linux.

Para obtener el contenido Windows Media del lado del cliente en los dispositivos Windows 8, establezca Citrix Multimedia Redirector como el programa predeterminado. Para ello, en **Panel de control > Programas > Programas predeterminados > Establecer programas predeterminados**, seleccione **Citrix Multimedia Redirector** y haga clic en **Establecer este programa como predeterminado** o **Elegir opciones predeterminadas para este programa**. Para la transcodificación por GPU, se necesita una GPU NVIDIA preparada para CUDA con capacidad de cálculo 1.1 o posterior; consulte <https://developer.nvidia.com/cuda/cuda-gpus>.

## HDX 3D Pro

El VDA para SO de sesión única de Windows detecta la presencia de hardware de GPU en tiempo de ejecución.

La máquina física o virtual que aloja la aplicación puede usar GPU PassThrough o GPU virtual (vGPU):

- GPU PassThrough está disponible con Citrix XenServer, Nutanix AHV, VMware vSphere y VMware ESX, donde se le denomina aceleración de gráficos directa virtual (virtual Direct Graphics Acceleration, vDGA). GPU PassThrough también está disponible con Microsoft Hyper-V en Windows Server 2016, donde se conoce como asignación de dispositivos diferenciados (Discrete Device Assignment, DDA).
- vGPU está disponible con Citrix Hypervisor, Nutanix AHV y VMware vSphere; consulte <https://www.citrix.com/products/xenapp-xendesktop/hdx-3d-pro.html>. HDX 3D Pro también se admite con instancias Cloud en la serie NV de Microsoft Azure y las ofertas de Amazon EC2 G3.

Citrix recomienda que el equipo host tenga, como mínimo, 4 GB de RAM y cuatro CPU virtuales con una velocidad de reloj de 2,3 GHz o más.

Unidad de procesamiento de gráficos (GPU):

- Para la compresión basada en CPU (incluida la compresión sin pérdida), HDX 3D Pro admite cualquier adaptador de pantalla en el equipo host que sea compatible con la aplicación que se entrega.
- Para la aceleración de gráficos virtualizados mediante NVIDIA GRID API, HDX 3D Pro puede utilizarse con tarjetas NVIDIA GRID compatibles (consulte [NVIDIA GRID](#)). NVIDIA GRID ofrece una

alta velocidad de fotogramas, lo que resulta en una experiencia de usuario altamente interactiva.

- La aceleración de gráficos virtualizados se admite en la familia de procesadores Intel Xeon E3 de la plataforma de gráficos para el centro de datos. Para obtener más información, consulte <https://www.citrix.com/intel> y <https://www.intel.com/content/www/us/en/servers/data-center-graphics.html>.
- La aceleración de gráficos virtualizados se admite con AMD RapidFire en las tarjetas de servidor de la serie S FirePro de AMD. Consulte [AMD Virtualization Solution](#).

Dispositivo del usuario:

- HDX 3D Pro admite todas las resoluciones de monitor que admite la GPU en el equipo host. Para alcanzar un rendimiento óptimo con las especificaciones mínimas sugeridas para dispositivos de usuario y GPU, Citrix recomienda utilizar una resolución máxima de 1920 x 1200 píxeles en conexiones LAN, y de 1280 x 1024 píxeles en conexiones WAN.
- Citrix también recomienda que la especificación de los dispositivos de usuario tenga, como mínimo, 1 GB de RAM y una CPU con una velocidad de reloj de 1,6 GHz o más. El uso del códec predeterminado de compresión profunda, necesario en conexiones con poco ancho de banda, requiere una CPU más eficaz a menos que la descodificación se realice en hardware. Para alcanzar un rendimiento óptimo, Citrix recomienda que los dispositivos de usuario tengan 2 GB de RAM y una CPU de doble núcleo, como mínimo, con una velocidad de reloj de 3 GHz o más.
- Para el acceso multimonitor, Citrix recomienda dispositivos de usuario con unidades CPU de cuatro núcleos.
- Los dispositivos de usuario no necesitan una GPU para acceder a los escritorios o aplicaciones entregados con HDX 3D Pro.
- La aplicación Citrix Workspace debe estar instalada.

Para obtener más información, consulte los [artículos de HDX 3D Pro](#) y [www.citrix.com/xenapp/3d](http://www.citrix.com/xenapp/3d).

## Universal Print Server

El servidor de impresión universal (Universal Print Server) consta de componentes de cliente y de servidor. El componente UpsClient va incluido en la instalación del VDA. Debe instalar el componente UpsServer en cada servidor de impresión donde residen las impresoras compartidas que se quieren aprovisionar con Citrix Universal Print Driver en las sesiones de usuario.

El componente UpsServer se admite en:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Requisitos:

- Runtimes de Microsoft Visual C++ 2017, x86 y x64
- Microsoft .NET Framework 4.7.1 (mínimo)

En caso de VDA para SO multisesión, la autenticación de usuario durante las operaciones de impresión requiere que el servidor Universal Print Server esté unido al mismo dominio que el VDA.

Los paquetes de componentes de cliente y de servidor independientes también están disponibles para la descarga.

Para obtener más información, consulte [Aprovisionar impresoras](#).

## Otros

Solo se admite Citrix License Server 11.16 y versiones posteriores. Para obtener más información, consulte [Licencias](#).

Cuando se utiliza Citrix Provisioning (anteriormente Provisioning Services) con esta versión, la versión 7.x está cubierta por el ciclo de vida de XenApp 7.x/XenDesktop 7.x y el ciclo de vida de Citrix Virtual Apps and Desktops. Consulte la [Tabla de productos](#) para obtener más información sobre la compatibilidad de versiones.

Para ver las versiones de StoreFront compatibles, consulte los [requisitos del sistema para StoreFront](#).

La Consola de administración de directivas de grupo (GPMC) de Microsoft es necesaria si quiere almacenar la información sobre directivas de Citrix en Active Directory, en lugar de la base de datos de configuración del sitio. Si instala `CitrixGroupPolicyManagement_x64.msi` por separado (por ejemplo, en una máquina que no tiene instalado un componente principal de Citrix Virtual Apps and Desktops), esa máquina debe tener instalado el runtime de Visual Studio 2015. Para obtener más información, consulte la documentación de Microsoft.

Si quiere modificar los GPO de dominio mediante GPMC, habilite la función Administración de directivas de grupo (en Windows Server Manager) en todas las máquinas que contengan Delivery Controllers.

Se admiten varias NIC.

De forma predeterminada, no se instala la aplicación Citrix Workspace para Windows al instalar un VDA actual. Para obtener más información, consulte la documentación más reciente de la aplicación [Citrix Workspace para Windows](#).

Consulte [App-V](#) para conocer las versiones compatibles de Microsoft App-V.

Consulte [Acceso a aplicaciones locales](#) para obtener información acerca del explorador admitido para esa funcionalidad.

Resoluciones mixtas con varios monitores. No se admiten PPP diferentes de un monitor a otro en entornos de Citrix Virtual Apps and Desktops. Puede verificar los PPP (ajuste de escala en %) desde el **Panel de control de Windows > Opciones de pantalla**. Si utiliza un dispositivo cliente con Windows 8.1 o Windows 10, habilite la opción **Dejarme elegir un nivel de ajuste de escala para todas mis pantallas** del **Panel de control de Windows > Opciones de pantalla** para configurar los monitores adecuadamente. Para obtener más información, consulte [CTX201696](#).

Esta versión de Citrix Virtual Apps and Desktops no es compatible con AppDNA 7.8 ni AppDNA 7.9. Citrix recomienda usar la versión actual de AppDNA.

## Información técnica general

June 27, 2024

Citrix Virtual Apps and Desktops son soluciones de virtualización que proporcionan a los equipos de TI control sobre máquinas virtuales, aplicaciones, licencias y seguridad, al tiempo que permiten un acceso desde cualquier lugar y cualquier dispositivo.

Citrix Virtual Apps and Desktops permiten:

- Los usuarios finales pueden ejecutar aplicaciones y escritorios independientemente de la interfaz y el sistema operativo del dispositivo que estén utilizando.
- Los administradores pueden administrar la red y controlar el acceso desde dispositivos seleccionados o desde todos los dispositivos.
- Los administradores pueden administrar toda la red desde un único centro de datos.

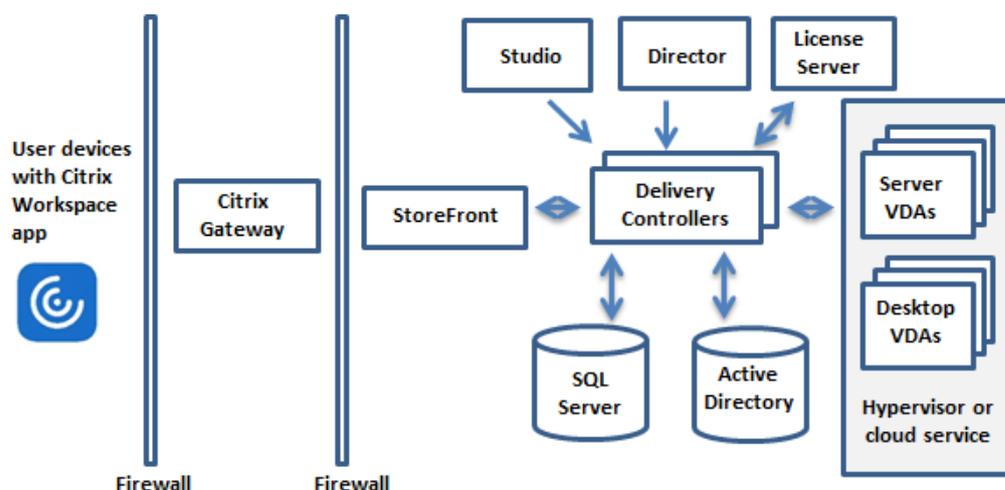
Citrix Virtual Apps and Desktops comparten una arquitectura unificada llamada FlexCast Management Architecture (FMA). Las funciones principales de la arquitectura FMA son el aprovisionamiento integrado y la capacidad de ejecutar distintas versiones de Citrix Virtual Apps o Citrix Virtual Desktops desde un único sitio.

[Puede obtener información sobre los cambios en los nombres de producto aquí.](#)

### Componentes principales

Este artículo es de gran ayuda si acaba de comenzar a utilizar Citrix Virtual Apps and Desktops. Si tiene una comunidad de XenApp 6.x o una versión anterior, o un sitio de XenDesktop 5.6 o una versión anterior, también debería consultar [Cambios en 7.x](#).

En esta imagen, se muestran los componentes principales de una implementación típica, que se denomina “sitio”.



## Delivery Controller

El Delivery Controller es el componente de administración central de un sitio. Cada sitio tiene uno o varios Delivery Controllers. Se instala en al menos un servidor del centro de datos. Para la fiabilidad y la disponibilidad del sitio, los Controllers deben instalarse en más de un servidor. Si la implementación incluye un hipervisor o un servicio de nube, los servicios de Controller se comunican con él para distribuir aplicaciones y escritorios, autenticar y administrar el acceso de los usuarios, actuar como intermediario en las conexiones entre los usuarios y sus aplicaciones y escritorios, optimizar y equilibrar las conexiones de los usuarios.

Broker Service del Controller realiza un rastreo de los usuarios que han iniciado sesión, dónde lo han hecho y qué recursos tienen, y si los usuarios necesitan reconectarse a aplicaciones existentes. Broker Service ejecuta cmdlets de PowerShell y se comunica con el Broker Agent en el VDA a través del puerto TCP 80. No tiene la opción de usar el puerto TCP 443.

Monitor Service recopila datos históricos y los coloca en la base de datos de supervisión. Este servicio utiliza el puerto TCP 80 o 443.

Los datos de los servicios del Controller se almacenan en la base de datos del sitio.

El Controller administra el estado de los escritorios, iniciándolos y deteniéndolos, según la demanda existente y la configuración administrativa. En algunas ediciones, el Controller permite instalar Profile Management para administrar los parámetros de personalización de los usuarios en entornos virtualizados o físicos de Windows.

## Base de datos

Se necesita al menos una base de datos Microsoft SQL Server en cada sitio para almacenar la información de configuración y sesiones. Esta base de datos almacena los datos recopilados y administrados

por los distintos servicios que conforman el Controller. Instale la base de datos en su centro de datos y asegúrese de que haya una conexión persistente con el Controller.

El sitio también usa una base de datos de registros de configuración y una base de datos de supervisión. De forma predeterminada, estas bases de datos se instalan en la misma ubicación que la base de datos del sitio; este aspecto se puede modificar.

### **Virtual Delivery Agent (VDA)**

El VDA se instala en cada máquina física o virtual del sitio que quiera poner a disposición de los usuarios. Esas máquinas entregan aplicaciones o escritorios. Permite que la máquina se registre en el Controller, que, a su vez, permite que la máquina y sus recursos alojados estén disponibles para los usuarios. Los VDA establecen y administran la conexión entre la máquina y el dispositivo del usuario. Los VDA también verifican que haya una licencia de Citrix disponible para el usuario o la sesión, y aplican las directivas que se hayan configurado para la sesión.

El VDA comunica la información de la sesión al Broker Service en el Controller a través del Broker Agent incluido en el VDA. El agente de broker aloja varios plugins y recopila datos en tiempo real. Se comunica con el Controller a través del puerto TCP 80.

La palabra “VDA” se utiliza a menudo para hacer referencia tanto al agente en sí como a la máquina donde está instalado.

Hay VDA disponibles para sistemas operativos Windows de sesión única y multisesión. Los VDA para sistemas operativos multisesión Windows permiten que varios usuarios se conecten al servidor al mismo tiempo. Los VDA para SO de sesión única Windows permiten la conexión de un solo usuario al escritorio en un momento dado. Los agentes VDA para Linux también están disponibles.

### **Citrix StoreFront**

StoreFront autentica a los usuarios y administra almacenes de escritorios y aplicaciones a los que acceden los usuarios. Puede alojar el almacén de las aplicaciones de su empresa, lo que da a los usuarios acceso cada vez que quieran a los escritorios y las aplicaciones que quiera poner a su disposición. También realiza un rastreo de las suscripciones de aplicaciones que tengan los usuarios, los nombres de los accesos directos y otros datos. Gracias a ello, los usuarios tienen una experiencia similar, aunque utilicen varios dispositivos.

### **Aplicación Citrix Workspace**

Se instala en los dispositivos de usuario y otros dispositivos de punto final (por ejemplo, escritorios virtuales). La aplicación Citrix Workspace da a los usuarios un acceso rápido, seguro y de autoservicio a los documentos, las aplicaciones y los escritorios. La aplicación Citrix Workspace también

ofrece acceso a demanda a aplicaciones Windows, web y de Software como servicio (SaaS). Para los dispositivos donde no se puede instalar el software de la aplicación Citrix Workspace específico del dispositivo, la aplicación Citrix Workspace para HTML5 ofrece una conexión a través de un explorador web compatible con HTML5.

### **Citrix Studio**

Studio es la consola de administración desde la que configurar y administrar la implementación de Citrix Virtual Apps and Desktops. Studio elimina la necesidad de consolas de administración independientes para administrar la entrega de aplicaciones y escritorios. Studio incluye asistentes que le guían para la configuración del entorno, la creación de cargas de trabajo para alojar escritorios y aplicaciones, y la asignación de éstos a los usuarios. También puede usar Studio para asignar licencias de Citrix y realizar un rastreo de estas en el sitio.

La información mostrada en Studio se obtiene del Broker Service que hay en el Controller; se comunica a través del puerto TCP 80.

### **Citrix Director**

Director es una herramienta web que permite a los equipos de asistencia técnica y TI supervisar un entorno, solucionar problemas antes de que se agraven, y realizar tareas de asistencia para los usuarios finales. Puede utilizar una implementación de Director para conectarse y supervisar varios sitios de Citrix Virtual Apps o de Citrix Virtual Desktops.

Director muestra:

- Datos de sesión en tiempo real procedentes del Broker Service en el Controller, que incluye datos que el Broker Service obtiene del Broker Agent en el VDA.
- Datos históricos de los sitios, procedentes de Monitor Service en el Controller.

Director utiliza los datos heurísticos y de rendimiento de ICA, capturados por el dispositivo Citrix Gateway, para generar un análisis a partir de los datos y luego presentarlo a los administradores.

También puede ver sesiones de usuario e interactuar con ellas mediante Director mediante la Asistencia remota de Windows.

### **Citrix License Server**

El Servidor de licencias administra las licencias de los productos Citrix. Se comunica con el Controller para administrar las licencias para cada sesión de usuario, y con Studio, para asignar los archivos de licencias. Un sitio debe tener al menos un servidor de licencias para almacenar y administrar los archivos de licencias.

## Hipervisor o servicio de nube

El servicio de nube o hipervisor aloja las máquinas virtuales del sitio. Estas pueden ser las máquinas virtuales que se usen para alojar aplicaciones y escritorios, así como las máquinas virtuales que se usen para alojar los componentes de Citrix Virtual Apps and Desktops. Un hipervisor se instala en un host dedicado enteramente a ejecutar el hipervisor y alojar máquinas virtuales.

Citrix Virtual Apps and Desktops admiten varios hipervisores y servicios de nube.

Aunque muchas implementaciones requieren un hipervisor, no lo necesita para proporcionar acceso con Remote PC. Tampoco necesita un hipervisor cuando usa Provisioning Services (PVS) para aprovisionar las máquinas virtuales.

Para obtener más información, consulte:

- [Puertos de red.](#)
- [Bases de datos.](#)
- Servicios Windows en los componentes de Citrix Virtual Apps and Desktops: [Configurar derechos de usuario.](#)
- Hipervisores y servicios de nube compatibles: [Requisitos del sistema.](#)

## Componentes adicionales

Los siguientes componentes adicionales, no incluidos en la imagen anterior, también pueden incluirse en las implementaciones de Citrix Virtual Apps and Desktops. Para obtener más información, consulte la documentación correspondiente.

### Citrix Provisioning

Citrix Provisioning (anteriormente conocido como Provisioning Services) es un componente opcional que está disponible con algunas ediciones. Proporciona una alternativa a MCS para aprovisionar las máquinas virtuales. Mientras que MCS crea copias de una imagen maestra, Provisioning Services distribuye la imagen maestra por streaming a los dispositivos de usuario. Provisioning Services no requiere un hipervisor para hacerlo, por lo tanto, se puede usar para alojar máquinas físicas. Provisioning Services se comunica con el Controller para proporcionar recursos a los usuarios.

### Citrix Gateway

Cuando los usuarios se conectan desde fuera del firewall de la empresa, Citrix Virtual Apps and Desktops pueden usar la tecnología de Citrix Gateway (antes llamado Access Gateway y NetScaler Gateway) para proteger esas conexiones con TLS. El dispositivo virtual Citrix Gateway o VPX es un dispositivo de

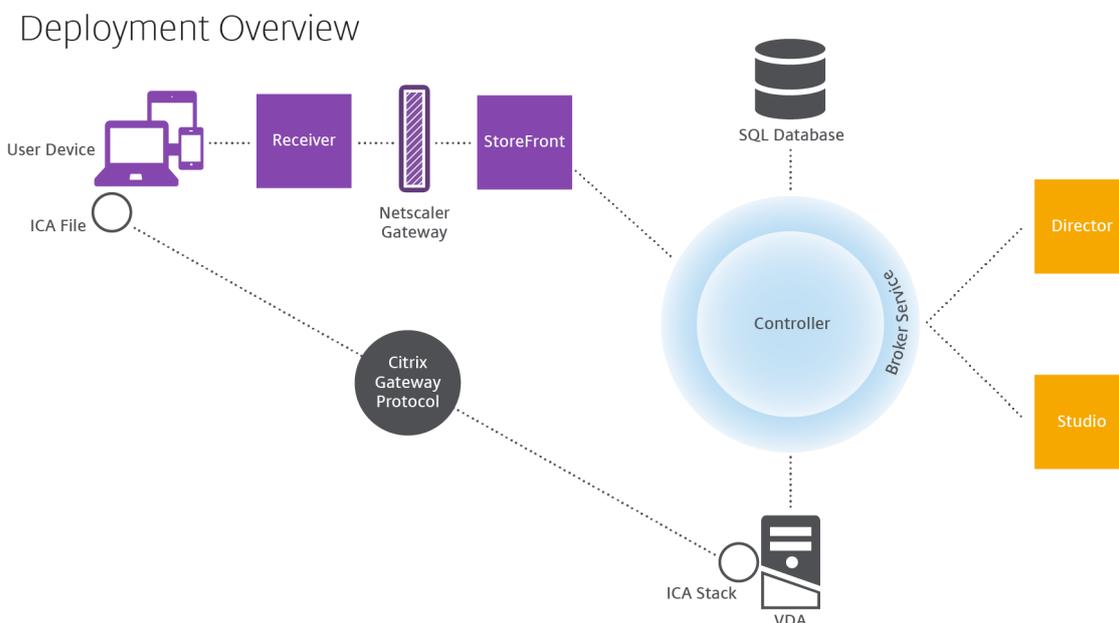
SSL VPN que se implementa en la zona desmilitarizada (DMZ). Proporciona un punto de acceso único y seguro a través del firewall corporativo.

## Citrix SD-WAN

En las implementaciones donde se entregan escritorios virtuales a usuarios de ubicaciones remotas, como sucursales de oficina, se puede emplear la tecnología de Citrix SD-WAN para optimizar el rendimiento. Los repetidores aceleran el rendimiento en redes amplias. Con repetidores presentes en la red, los usuarios de la sucursal experimentan un rendimiento similar al de una LAN a través de la WAN. Citrix SD-WAN puede dar prioridad a diferentes partes de la experiencia de usuario de modo que esta experiencia no empeore en la sucursal cuando, por ejemplo, se envíe un archivo de gran tamaño o un trabajo de impresión por la red. La optimización HDX de WAN ofrece compresión por token y deduplicación de datos, lo que disminuye en gran medida los requisitos de ancho de banda y mejora el rendimiento.

## ¿Cómo funciona una implementación típica?

Un sitio se compone de máquinas con roles dedicados que proporcionan escalabilidad, alta disponibilidad y conmutación por error, en una solución integral que está diseñada ya con funciones de seguridad. Un sitio se compone de máquinas de servidor y escritorio con VDA instalado, y Delivery Controller, que se encarga de administrar el acceso.



El VDA permite a los usuarios conectarse a escritorios y aplicaciones. Para la mayoría de los métodos de entrega, el VDA se instala en máquinas de servidor o de escritorio, aunque también se puede

instalar en PC físicos para el acceso con Remote PC.

El Controller se compone de servicios Windows independientes que administran los recursos, las aplicaciones y los escritorios, y optimizan y equilibran la carga de conexiones de usuarios. Cada sitio tiene uno o varios Delivery Controllers. Como las sesiones dependen de la latencia, el ancho de banda y la fiabilidad de la red, lo ideal es que todos los Controllers se encuentren en la misma LAN.

Los usuarios nunca acceden directamente al Controller. El VDA funciona como intermediario entre los usuarios y el Controller. Cuando los usuarios inician sesión mediante StoreFront, sus credenciales pasan al servicio Broker Service presente en el Controller. A continuación, el Broker Service obtiene los perfiles y los recursos disponibles en función de las directivas establecidas para ellos.

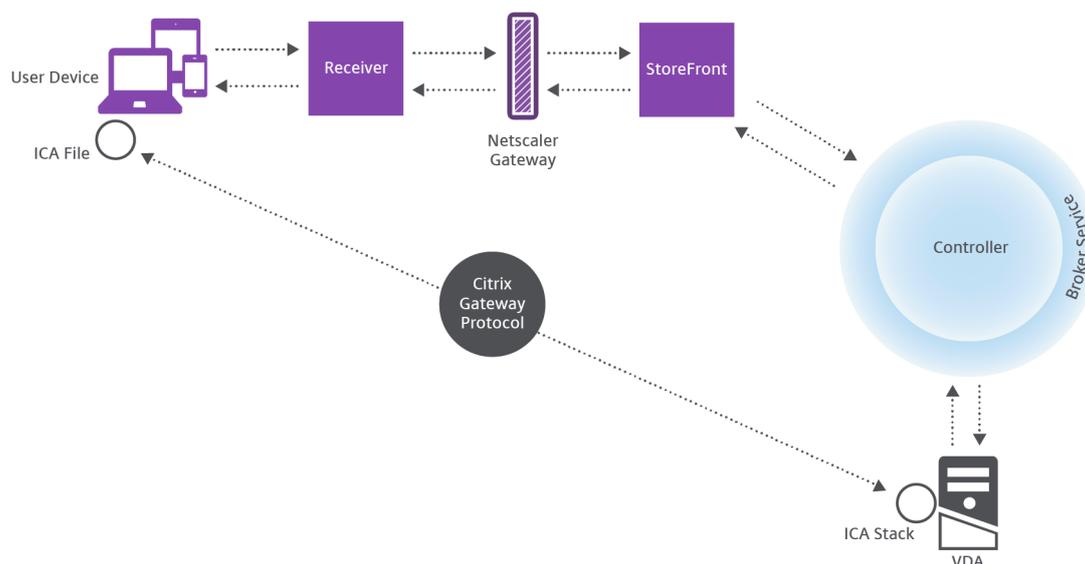
### ¿Cómo se gestionan las conexiones de usuario?

Para iniciar una sesión, el usuario se conecta a través de la aplicación Citrix Workspace, instalada en su dispositivo, o bien a través de un sitio web de StoreFront.

El usuario selecciona el escritorio virtual o físico, o bien la aplicación virtual que necesite.

Las credenciales de usuario se transfieren por esta ruta para acceder al Controller, que determina los recursos necesarios comunicándose con un Broker Service. Citrix recomienda que los administradores coloquen un certificado SSL en StoreFront para cifrar las credenciales que provienen de la aplicación Citrix Workspace.

#### User connections



El Broker Service determina a qué escritorios y aplicaciones puede acceder el usuario.

Una vez que se verifican las credenciales, la información sobre las aplicaciones o los escritorios disponibles se envía de vuelta al usuario a través de la ruta StoreFront-aplicación Citrix Workspace.

Cuando el usuario selecciona las aplicaciones o los escritorios en esta lista, esa información vuelve por la misma ruta al Controller. Éste determina el VDA adecuado para alojar la aplicación o el escritorio especificados.

El Controller envía un mensaje al VDA con las credenciales del usuario y envía todos los datos sobre el usuario y la conexión al VDA. El VDA acepta la conexión y envía la información a través de las mismas rutas de vuelta a la aplicación Citrix Workspace. Un conjunto de los parámetros requeridos se recopila en StoreFront. A continuación, estos parámetros se envían a la aplicación Citrix Workspace, ya sea como parte de la conversación del protocolo de aplicación-Citrix-Workspace-StoreFront, o convertidos en un archivo de arquitectura ICA (Independent Computing Architecture) y descargados. Si el sitio está configurado correctamente, las credenciales están cifradas durante este proceso.

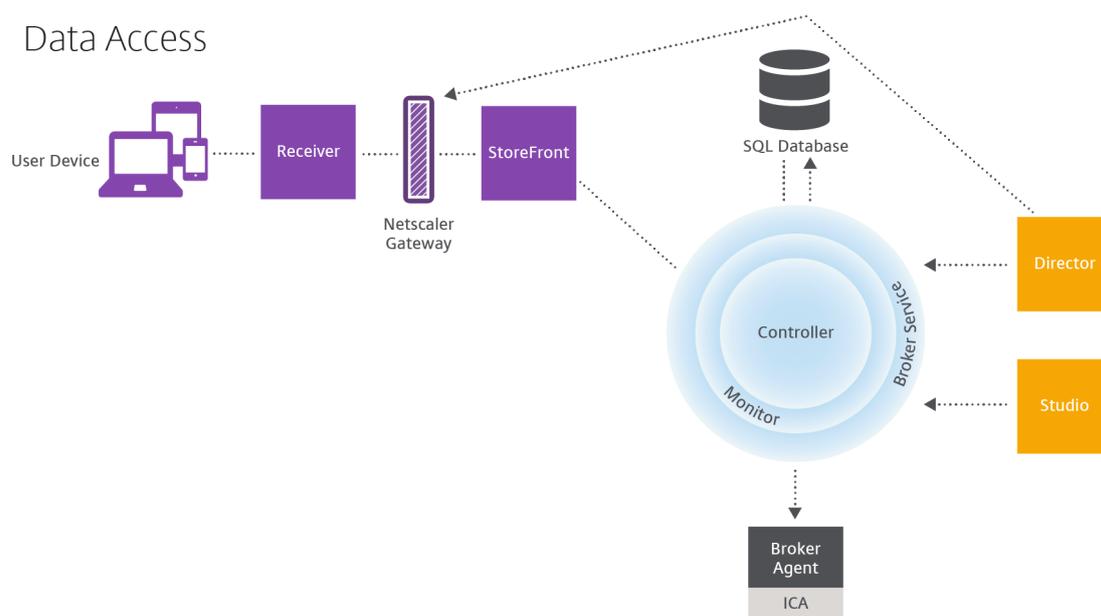
El archivo ICA se copia al dispositivo del usuario y establece una conexión directa entre el dispositivo y la pila ICA que se ejecuta en el VDA. Esta conexión omite la infraestructura de administración (aplicación Citrix Workspace, StoreFront y Controller).

La conexión entre la aplicación Citrix Workspace y el VDA usa el protocolo CGP (Citrix Gateway Protocol). Si la conexión se pierde, la funcionalidad de fiabilidad de la sesión habilita al usuario para reconectar con el VDA en lugar de tener que reiniciarse a través de toda la infraestructura de administración. La fiabilidad de la sesión se puede habilitar o inhabilitar en las directivas de Citrix.

Una vez que el cliente se conecta al VDA, el VDA notifica al Controller que el usuario ha iniciado sesión. El Controller envía esta información a la base de datos del sitio y comienza a registrar datos en la base de datos de supervisión.

## **¿Cómo funciona el acceso a los datos?**

Cada sesión de Citrix Virtual Apps and Desktops produce datos a los que el departamento de TI puede acceder a través de Studio o Director. Studio permite que los administradores accedan a los datos en tiempo real procedentes de Broker Agent para administrar los sitios. Director accede a los mismos datos, además de datos históricos almacenados en la base de datos de supervisión. También accede a los datos HDX de NetScaler Gateway para solucionar problemas y obtener asistencia técnica.



Dentro de Controller, Broker Service notifica datos en tiempo real de cada sesión que haya en la máquina. Monitor Service también realiza un rastreo de los datos en tiempo real y lo almacena como datos históricos en la base de datos de supervisión.

Studio solo se comunica con el Broker Service; por lo tanto, solo tiene acceso a datos en tiempo real. Director se comunica con el Broker Service (a través de un plugin de Broker Agent) para tener acceso a la base de datos del sitio.

Director también puede acceder a Citrix Gateway para obtener información sobre los datos HDX.

## Entregar escritorios y aplicaciones

Configure las máquinas que van a entregar aplicaciones y escritorios con los catálogos de máquinas. Luego, cree grupos de entrega que especifiquen las aplicaciones y los escritorios que estarán disponibles (a través de las máquinas de los catálogos) y qué usuarios pueden acceder a ellos. Si quiere, puede crear grupos de aplicaciones para administrar colecciones de aplicaciones.

## Catálogos de máquinas

Los catálogos de máquinas son colecciones de máquinas virtuales o equipos físicos que se administran como una única entidad. Estas máquinas, y las aplicaciones o los escritorios virtuales que contienen, son los recursos que proporciona a los usuarios. Todas las máquinas de un catálogo tienen el mismo sistema operativo y el mismo VDA instalados. También tienen las mismas aplicaciones o escritorios virtuales.

Por lo general, hay que crear una imagen maestra y usarla para crear máquinas virtuales idénticas en el catálogo. Puede especificar el método de aprovisionamiento de las máquinas de ese catálogo: herramientas de Citrix (Citrix Provisioning o Machine Creation Services) u otras herramientas. De forma alternativa, puede utilizar sus propias imágenes existentes. En este caso, deberá administrar los dispositivos de destino de forma individual o colectiva con herramientas de terceros para la distribución electrónica de software o ESD (Electronic Software Distribution).

Los tipos de máquina válidos son:

- **SO multisesión:** Máquinas virtuales o físicas con un sistema operativo multisesión. Se utilizan para entregar las aplicaciones publicadas de Citrix Virtual Apps (también conocidas como aplicaciones alojadas en servidores) y los escritorios publicados de Citrix Virtual Desktops (también conocidos como escritorios alojados en servidores). Estas máquinas permiten que varios usuarios se conecten a ellas simultáneamente.
- **SO de sesión única:** Máquinas virtuales o físicas con sistema operativo de sesión única. Se utilizan para entregar escritorios VDI (escritorios con SO de sesión única que pueden personalizarse), aplicaciones alojadas en VM (aplicaciones con SO de sesión única) y escritorios físicos alojados. Solo un usuario a la vez puede conectarse a cada uno de estos escritorios.
- **Acceso con Remote PC:** Permite a los usuarios remotos acceder a sus PC de oficina físicos desde cualquier dispositivo que ejecute la aplicación Citrix Workspace. Los PC de oficina se administran a través de la implementación de Citrix Virtual Desktops y requieren que los dispositivos del usuario se especifiquen en una lista de permitidos.

Para obtener más información, consulte [Administración de imágenes de Citrix Virtual Apps and Desktops](#) y [Crear catálogos de máquinas](#).

## Grupos de entrega

Los grupos de entrega especifican los usuarios que pueden acceder a las aplicaciones y/o los escritorios y las máquinas que se pueden utilizar para ello. Los grupos de entrega contienen máquinas del catálogo y usuarios de Active Directory que tienen acceso al sitio. Puede asignar usuarios a los grupos de entrega según el grupo de Active Directory que tengan, porque tanto los grupos de Active Directory como los grupos de entrega son modos de agrupar usuarios que tienen requisitos similares.

Cada grupo de entrega puede contener máquinas de varios catálogos, y cada catálogo puede suministrar sus máquinas a más de un grupo de entrega. Sin embargo, cada máquina individual solo puede pertenecer a un grupo de entrega a la vez.

Usted define a qué recursos pueden acceder los usuarios del grupo de entrega. Por ejemplo, si quiere entregar diferentes aplicaciones a diferentes usuarios, puede instalar todas las aplicaciones en la imagen maestra de un catálogo de máquinas, y crear máquinas suficientes en ese catálogo para distribuir las entre varios grupos de entrega. A continuación, puede configurar cada grupo de entrega para entregar distintos subconjuntos de las aplicaciones instaladas en las máquinas.

Para obtener más información, consulte [Crear grupos de entrega](#).

## Grupos de aplicaciones

Los grupos de aplicaciones ofrecen ventajas para la administración de aplicaciones y para el control de los recursos frente a la opción de grupos de entrega. Con la restricción por etiquetas, puede usar las máquinas existentes para más de una tarea de publicación, con lo que se ahorran los costes asociados a la implementación y la administración de máquinas adicionales. La restricción por etiquetas puede entenderse como una subdivisión (o partición) de las máquinas de un grupo de entrega. Usar grupos de aplicaciones puede ser útil para aislar un subconjunto de las máquinas de un grupo de entrega y solucionar los problemas que presentan.

Para obtener más información, consulte [Crear grupos de aplicaciones](#).

## Más información

[Diagramas de Citrix Virtual Apps and Desktops](#)

## Active Directory

November 4, 2022

Para la autenticación y la autorización es necesario usar Active Directory. La infraestructura de Kerberos en Active Directory se usa para garantizar la autenticidad y confidencialidad de las comunicaciones con los Delivery Controllers. Para obtener más información sobre Kerberos, consulte la documentación de Microsoft.

En el artículo [Requisitos del sistema](#), se ofrece una lista de los niveles funcionales admitidos para el dominio y el bosque.

Este producto admite lo siguiente:

- **Implementaciones donde las cuentas de usuario y las cuentas de equipo existen en dominios de un único bosque Active Directory.** Las cuentas de usuario y de equipo pueden existir en dominios arbitrarios dentro de un único bosque. En este tipo de implementación se admiten todos los niveles funcionales de dominio y bosque.
- **Las implementaciones en las que las cuentas de usuario existen en un bosque Active Directory que es diferente al bosque Active Directory que contiene las cuentas de equipo de los Controllers y los escritorios virtuales.** En este tipo de implementación, los dominios que contienen las cuentas de equipo de los escritorios virtuales y del Controller deben confiar en

los dominios que contienen las cuentas de usuario. Se pueden utilizar relaciones de confianza de bosque o externas. En este tipo de implementación se admiten todos los niveles funcionales de dominio y bosque.

- **Las implementaciones en las que las cuentas de equipo para los Controllers existen en un bosque Active Directory que es diferente de al menos un bosque Active Directory adicional que contenga las cuentas de equipo de los escritorios virtuales.** En este tipo de implementación, se requiere una relación de confianza bidireccional entre los dominios que contienen las cuentas de equipo de los Controllers y todos los dominios que contienen las cuentas de equipo de los escritorios virtuales. En este tipo de implementación, todos los dominios que contienen cuentas de equipo para los escritorios virtuales o para Controller deben tener un nivel funcional “Windows 2000 nativo” o superior. Se admiten todos los niveles funcionales de bosque.
- **Controladores de dominio que permiten la escritura.** No se admiten controladores de dominio que sean de solo lectura.

Opcionalmente, los Virtual Delivery Agent (VDA) pueden usar la información publicada en Active Directory para determinar en qué Controllers se pueden registrar (detección). Este método se ofrece principalmente con fines de compatibilidad con versiones anteriores, y solo está disponible si los VDA y los Controllers se encuentran en el mismo bosque de Active Directory. Para obtener información acerca de este método de detección, consulte [Detección de Controllers basada en unidades organizativas de Active Directory](#) y [CTX118976](#).

**Nota:**

No cambie el nombre de equipo ni la pertenencia al dominio de un Delivery Controller una vez configurado el sitio.

## Implementación en un entorno de Active Directory de varios bosques

Esta información se aplica a XenDesktop 7.1 y XenApp 7.5 (versiones mínimas). No se aplica a versiones anteriores de XenDesktop o XenApp.

En un entorno de Active Directory con varios bosques, si hay confianza unidireccional o bidireccional, se pueden usar reenviadores DNS o condicionales para la búsqueda de nombres y registros. Para permitir que los usuarios correspondientes de Active Directory puedan crear cuentas de equipo, use el Asistente para delegación de control. Consulte la documentación de Microsoft para obtener información sobre este asistente.

No se necesitan zonas DNS inversas en la infraestructura DNS si se incluyen los reenviadores DNS adecuados entre los bosques.

La clave `SupportMultipleForest` es necesaria si el VDA y el Controller se encuentran en bosques separados, independientemente de si los nombres de Active Directory y NetBIOS son diferentes. Use

la información siguiente para agregar la clave de Registro:

**Precaución:**

Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

En el VDA, configure:

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\SupportMultipleForest`

- Nombre: `SupportMultipleForest`
- Tipo: `REG_DWORD`
- Datos: `0x00000001` (1)

En todos los Delivery Controllers, configure: `HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer\SupportMultipleForest`.

- Nombre: `SupportMultipleForest`
- Tipo: `REG_DWORD`
- Datos: `0x00000001` (1)

Es posible que sea necesaria la configuración de DNS inversa si el espacio de nombres DNS es diferente del de Active Directory.

Si existen confianzas externas durante la instalación, se necesita la clave del Registro `ListOfSIDs`. La clave del Registro `ListOfSIDs` también es necesaria si el FQDN de Active Directory difiere del FQDN de DNS o si el dominio que contiene el controlador de dominio tiene un nombre de NetBIOS que difiere del FQDN de Active Directory. Para agregar la clave del Registro, utilice la siguiente información:

Para el VDA, busque la clave de Registro `HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs`

- Nombre: `ListOfSIDs`
- Tipo: `REG\_SZ`
- Datos: identificador de seguridad (SID) de los Controllers (los SID se incluyen en los resultados del cmdlet `Get-BrokerController`).

En caso de que haya relaciones de confianza con elementos externos, realice el siguiente cambio en el VDA:

1. Localice el archivo `Program Files\Citrix\Virtual Desktop Agent\brokeragent.exe.config`.

2. Haga una copia de seguridad del archivo.
3. Abra el archivo en un programa para edición de texto, como por ejemplo el Bloc de notas.
4. Busque `text allowNtlm="false"` y cambie el texto a `allowNtlm="true"`.
5. Guarde el archivo.

Después de agregar la clave del Registro `ListOfSIDs` y de modificar el archivo `brokeragent.exe.config`, reinicie Citrix Desktop Service para aplicar los cambios.

La siguiente tabla muestra los tipos de confianza admitidos:

Tipo de confianza	Transitividad	Dirección	Se admite en esta versión
Elemento primario y secundario	Transitiva	Bidireccional	Sí
Raíz del árbol	Transitiva	Bidireccional	Sí
Externa	No transitiva	Unidireccional o bidireccional	Sí
Bosque	Transitiva	Unidireccional o bidireccional	Sí
Acceso directo	Transitiva	Unidireccional o bidireccional	Sí
Dominio	Transitiva o no transitiva	Unidireccional o bidireccional	No

Para obtener más información sobre entornos de Active Directory complejos, consulte [CTX134971](#).

## Bases de datos

November 15, 2022

Un sitio de Citrix Virtual Apps o Citrix Virtual Desktops usa tres bases de datos de SQL Server:

- **Sitio:** También conocida como Configuración del sitio, esta base de datos almacena la configuración activa del sitio, el estado actual de la sesión y la información de conexión.
- **Registro de configuración:** También conocida como Registro, esta base de datos almacena información acerca de actividades de tipo administrativo y los cambios de configuración en el sitio. Esta base de datos se usa cuando la función Registro de configuración está habilitada (opción predeterminada).
- **Supervisión:** Esta base de datos almacena los datos que utiliza Director, como la información de conexión y de sesión.

Cada Delivery Controller se comunica con la base de datos del sitio. Se requiere la autenticación de Windows entre el Controller y las bases de datos. Un Controller se puede desconectar o apagar sin que esta acción afecte a los otros Controllers del sitio. No obstante, esto significa que la base de datos del sitio representa un punto único de fallo. Si el servidor de base de datos da error, las conexiones existentes seguirán funcionando hasta que el usuario cierre sesión o se desconecte. Para obtener información sobre el comportamiento de las conexiones cuando la base de datos del sitio no está disponible, consulte [Caché de host local](#).

Citrix recomienda realizar una copia de seguridad de las bases de datos periódicamente para poder restaurarla a partir de esa copia si el servidor de base de datos falla. La estrategia de copia de seguridad para cada base de datos puede ser distinta. Para obtener instrucciones, consulte [CTX135207](#).

Si el sitio contiene más de una zona, la zona principal siempre debe contener la base de datos del sitio. Los Controllers de cada zona se comunicarán con esa base de datos.

## Alta disponibilidad

Existen varias soluciones de alta disponibilidad que es conveniente tener en cuenta para garantizar la conmutación por error automática:

- **Grupos de disponibilidad AlwaysOn (incluidos los grupos de disponibilidad básica):** Esta solución de alta disponibilidad y recuperación ante desastres para empresas introducida en SQL Server 2012 permite maximizar la disponibilidad de una o varias bases de datos. Los grupos de disponibilidad AlwaysOn requieren que las instancias de SQL Server residan en los nodos de clústeres de conmutación por error de Windows Server (WSFC). Para obtener más información, consulte <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/always-on-availability-groups-sql-server?redirectedfrom=MSDN&view=sql-server-ver15>.
- **Crear imágenes reflejo de la base de datos de SQL Server:** Reflejar la base de datos garantiza que, si se pierde la conexión con el servidor de base de datos activo, el proceso automático de conmutación por error se produzca rápidamente (en cuestión de segundos) para que los usuarios en general no resulten afectados. No obstante, este método es más costoso que las soluciones alternativas, ya que se requieren licencias de SQL Server completas en cada servidor de base de datos; tenga en cuenta que no se puede usar SQL Server Express en un entorno reflejado.
- **Agrupación en clústeres de SQL:** La tecnología de agrupación en clústeres de SQL de Microsoft se puede usar para permitir automáticamente que un servidor tome el control de las tareas y las responsabilidades de otro servidor que ha fallado. No obstante, la instalación de esta solución es más complicada y el proceso automático de conmutación por error generalmente es más lento que con las soluciones alternativas como la creación de reflejo de SQL.
- **Con las funciones de alta disponibilidad del hipervisor:** Con este método, la base de datos se puede implementar como una máquina virtual y se pueden utilizar las funciones de alta disponi-

bilidad del hipervisor. Esta solución es menos costosa que la creación de reflejo, ya que utiliza el software existente del hipervisor y también permite usar SQL Server Express Edition. No obstante, el proceso automático de conmutación por error es más lento ya que es posible que una máquina nueva tarde mucho en iniciar la base de datos, lo que puede interrumpir el servicio a los usuarios.

La función Caché de host local complementa las prácticas recomendadas de alta disponibilidad de SQL Server porque permite a los usuarios conectarse varias veces a los últimos escritorios y aplicaciones que han utilizado, incluso cuando la base de datos del sitio no está disponible. Para obtener más información, consulte [Caché de host local](#).

Si se producen fallos en todos los Delivery Controllers de un sitio, es posible configurar los agentes VDA de modo que funcionen en el modo de alta disponibilidad y, así, los usuarios puedan seguir accediendo y mediante sus escritorios y aplicaciones. En el modo de alta disponibilidad, el VDA acepta conexiones ICA directas de los usuarios en lugar de conexiones con el Controller como intermediario. Utilice esta función solo en el caso poco corriente de que falle la comunicación con todos los Controllers; no es una alternativa a otras soluciones de alta disponibilidad. Para obtener más información, consulte [CTX 127564](#).

No se admite la instalación de Controller en un nodo de clúster de SQL o de instalación duplicada (mirroring) de SQL.

## Instalar software de base de datos

De forma predeterminada y si no se detecta ninguna otra instancia de SQL Server en ese servidor, se instala SQL Server Express Edition al instalar el primer Delivery Controller. Por lo general, esa acción predeterminada es suficiente para implementaciones piloto o de pruebas de concepto. Sin embargo, SQL Server Express no admite funciones de alta disponibilidad de Microsoft.

La instalación predeterminada usa las cuentas y los permisos predeterminados del servicio de Windows. Consulte la documentación de Microsoft para ver información detallada de estos valores predeterminados, incluida la incorporación de cuentas de servicio Windows en el rol de sysadmin. Controller usa la cuenta de Servicio de red en esta configuración. Controller no necesita permisos ni roles adicionales de SQL Server.

Si es necesario, puede seleccionar **Ocultar instancia** para la instancia de la base de datos. Al configurar la dirección de la base de datos en Studio, introduzca el número de puerto estático de la instancia, en lugar de su nombre. Consulte la documentación de Microsoft para obtener información más detallada sobre cómo ocultar una instancia del motor de base de datos de SQL Server.

Por lo tanto, la mayoría de las implementaciones de producción y cualquier implementación que use funciones de alta disponibilidad de Microsoft deben instalar otras ediciones de SQL Server admitidas (que no sean Express) en máquinas que no sean el servidor donde está instalado el primer Controller.

En el artículo Requisitos del sistema, se ofrece una lista de las versiones admitidas de SQL Server. Las bases de datos pueden residir en una o varias máquinas.

Antes de crear un sitio, compruebe que el software de SQL Server está instalado. No es necesario crear la base de datos pero, si la crea, debe estar vacía. También se recomienda configurar las tecnologías de alta disponibilidad de Microsoft.

Use Windows Update para mantener SQL Server actualizado.

## Configurar bases de datos desde el asistente para la creación de sitios

Especifique los nombres de las bases de datos y sus direcciones (ubicación) en la página **Bases de datos** del asistente para la creación de sitios. (Consulte Formatos de direcciones de bases de datos.) Para evitar posibles errores cuando Director consulte Monitor Service, no use espacios en blanco en el nombre de la base de datos de supervisión.

La página **Bases de datos** ofrece dos opciones para configurar bases de datos: automáticamente o mediante scripts. Por lo general, puede usar la opción automática si usted (como usuario de Studio y administrador Citrix) tiene los privilegios de base de datos pertinentes. (Consulte Permisos necesarios para configurar bases de datos.)

Puede cambiar la ubicación de la base de datos de registros de configuración y supervisión más adelante, después de crear el sitio. Consulte Cambiar ubicaciones de base de datos.

Para que un sitio utilice una base de datos reflejada, complete lo siguiente y continúe con el procedimiento de configuración automática o por script.

1. Instale el software de SQL Server en dos servidores, A y B.
2. En el servidor A, cree la base de datos que se utilizará como principal. Haga una copia de seguridad de la base de datos ubicada en el servidor A y, a continuación, cópiela al servidor B.
3. En el servidor B, restaure el archivo de copia de seguridad.
4. Inicie la creación de reflejo en el servidor A.

Para verificar la creación de la base de datos reflejada después de crear el sitio, ejecute el cmdlet `get-configdbconnection` de PowerShell para asegurarse de que el socio de conmutación por error se ha definido en la cadena de conexión para la base de datos reflejada.

Si más adelante quiere agregar, mover o quitar un Delivery Controller de un entorno de base de datos reflejada, consulte [Delivery Controllers](#).

## Configuración automática

Si tiene los privilegios de base de datos necesarios, seleccione la opción “Crear y configurar bases de datos desde Studio” en la página **Bases de datos** del asistente para la creación de sitios. A continuación, especifique los nombres y las direcciones de las bases de datos principales.

Si ya existe una base de datos en una dirección que especifique, esta debe estar vacía. Si no existen bases de datos en la dirección especificada, se le informa que no se ha podido encontrar ninguna base de datos y se le solicita crear una. Tras confirmar esa acción, Studio crea automáticamente las bases de datos y aplica los scripts de inicialización a las bases de datos principales y de réplica.

### Configuración por script

Si no tiene los privilegios necesarios de bases de datos, deberá pedir ayuda a alguien con esos privilegios, como a un administrador de base de datos. Aquí se presenta el orden de pasos a seguir:

1. En el asistente para la creación de sitios, seleccione la opción **Generar scripts**. Esta acción genera seis scripts: dos para cada una de las tres bases de datos (una para cada base de datos principal y otra para cada réplica). Puede indicar dónde almacenar los scripts.
2. Facilite esos scripts al administrador de base de datos. El asistente para la creación de sitios se detiene automáticamente en este punto y se le pedirá continuar con la creación de sitios cuando vuelva de nuevo al asistente.

El administrador de base de datos crea la base de datos. Cada base de datos debe tener las siguientes funciones:

- Usar una intercalación que termine con “\_CI\_AS\_KS”. Citrix recomienda usar una intercalación que termine con “\_100\_CI\_AS\_KS”.
- Para un rendimiento óptimo, habilite la instantánea de lectura confirmada de SQL Server. Para obtener más información, consulte [CTX 137161](#).
- Funciones de alta disponibilidad configuradas, si se quiere.
- Para configurar la creación de reflejo, primero debe configurar la base de datos para que use el modelo de recuperación completa (a diferencia del modelo simple, que es el valor predeterminado). Haga una copia de seguridad de la base de datos principal en un archivo y cópielo al servidor reflejado. En la base de datos reflejada, restaure el archivo de copia de seguridad para el servidor reflejado. A continuación, inicie la creación de reflejo en el servidor principal.

El administrador de base de datos usa la herramienta de línea de comandos SQLCMD o SQL Server Management Studio en modo SQLCMD para ejecutar cada script de xxx\_Replica.sql en las instancias de alta disponibilidad de base de datos de SQL Server (si se ha configurado la alta disponibilidad) y para ejecutar luego cada script de xxx\_Principal.sql en las instancias de base de datos principal de SQL Server. Consulte la documentación de Microsoft para obtener información más detallada acerca de SQLCMD.

Cuando todos los scripts finalizan correctamente, el administrador de base de datos facilita al administrador Citrix las tres direcciones de bases de datos principales.

En Studio, se le solicitará continuar con la creación de sitios y se volverá a la página **Bases de datos**. Escriba las direcciones. Si no se puede establecer contacto con alguno de los servidores que alojan

una base de datos, aparecerá un mensaje de error.

### Permisos necesarios para configurar bases de datos

Debe ser un administrador local y un usuario de dominio para crear e inicializar bases de datos (o cambiar la ubicación de estas). También debe tener ciertos permisos de SQL Server. Los siguientes permisos se pueden configurar explícitamente o se pueden adquirir por la pertenencia a grupos de Active Directory. Si las credenciales de usuario de Studio no incluyen estos permisos, se le solicitarán las credenciales de usuario de SQL Server.

Operación	Propósito	Rol del servidor	Rol de la base de datos
Crear una base de datos	Crear una base de datos vacía adecuada	dbcreator	
Crea un esquema	Crear los esquemas de cada servicio y agregar el primer Controller al sitio	securityadmin*	db_owner
Agregar un Controller	Agregar un Controller (aparte del primero) al sitio	securityadmin*	db_owner
Agregar un Controller (servidor reflejado)	Agregar un inicio de sesión de Controller al servidor de la base de datos que se encuentra actualmente en el rol de reflejo de la base de datos reflejada	securityadmin*	
Quitar Controller	Quitar Controller del sitio	**	db_owner
Actualizar un esquema	Aplicar parches rápidos o actualizaciones a los esquemas		db_owner

\* Aunque sea técnicamente más restrictivo, en la práctica, el rol de servidor securityadmin debe tratarse como equivalente al rol de servidor sysadmin.

\*\* Cuando se quita un Controller de un sitio, ya sea directamente a través de Desktop Studio o mediante los scripts generados por Desktop Studio o SDK, no se quita el inicio de sesión del Controller en

el servidor de base de datos. De esta forma, se evita el peligro potencial de quitar un inicio de sesión que utilicen otros servicios que no son de XenDesktop en la misma máquina. En caso de que ya no sea necesario, el inicio de sesión se debe quitar manualmente. Para hacerlo, se necesita el permiso del rol de servidor `securityadmin`.

Cuando se utiliza Studio para realizar estas operaciones, la cuenta de usuario debe formar parte del rol de servidor `sysadmin`.

### Scripts de derechos preferidos sobre bases de datos

En entornos empresariales, la configuración de la base de datos incluye scripts que deben gestionarse por diferentes equipos de personas con diferentes roles (derechos): `securityadmin` o `db_owner`.

Con PowerShell, ahora puede especificar los derechos preferidos sobre bases de datos (esta función no está disponible en Studio, el cual admite un único script que contenga todas las tareas).

Si se especifica un valor no predeterminado, se crean scripts independientes. Un script contiene tareas que requieren el rol `securityadmin`. El otro script requiere solamente los derechos de `db_owner`, y lo puede ejecutar un administrador de Citrix sin tener que contactar con un administrador de bases de datos.

En los cmdlets `get-*DBSchema`, la opción `-DatabaseRights` tiene los siguientes valores válidos:

- **SA**: Genera un script que crea las bases de datos y las credenciales de Delivery Controller. Estas tareas requieren derechos del tipo `securityadmin`.
- **DBO**: Genera un script que crea los roles de usuario en la base de datos, agrega las credenciales y, a continuación, crea los esquemas de la base de datos. Estas tareas requieren derechos del tipo `db_owner`.
- **Mixed** (predeterminado): Todas las tareas en un script, independientemente de los derechos necesarios.

Para obtener más información, consulte la ayuda de los cmdlets.

### Formatos de direcciones de bases de datos

Puede especificar una dirección de base de datos de una de las siguientes formas:

- `ServerName`
- `ServerName\InstanceName`
- `ServerName,PortNumber`

Para un grupo de disponibilidad AlwaysOn, especifique el servidor de escucha del grupo en el campo de ubicación.

## Cambiar ubicaciones de base de datos

Después de crear un sitio, puede cambiar la ubicación de las bases de datos de registros de configuración y supervisión. (No se puede cambiar la ubicación de la base de datos del sitio.) Al cambiar la ubicación de una base de datos:

- Los datos de la base de datos anterior no se importarán en la nueva base de datos.
- Los registros no pueden combinarse desde ambas bases de datos al consultarlos.
- La primera entrada del registro en la nueva base de datos indica que se ha producido un cambio en la base de datos, pero no identifica la base de datos anterior.

No es posible cambiar la ubicación de la base de datos de registros de configuración cuando está habilitado el registro obligatorio.

Para cambiar la ubicación de una base de datos:

1. Compruebe que haya instalada una versión admitida de Microsoft SQL Server en el servidor donde residirá la base de datos. Configure las funciones de alta disponibilidad, si fuera necesario.
2. Seleccione **Configuración** en el panel de navegación de Studio.
3. Seleccione la base de datos para la que quiere especificar una nueva ubicación y, a continuación, seleccione **Cambiar base de datos** en el panel **Acciones**.
4. Especifique la nueva ubicación y el nombre de la base de datos.
5. Si quiere que Studio cree la base de datos y si tiene los permisos adecuados, haga clic en **Aceptar**. Cuando se le solicite, haga clic en **Aceptar** y Studio creará automáticamente la base de datos. Studio intenta acceder a la base de datos mediante las credenciales. Si no puede, el sistema pedirá las credenciales del usuario de la base de datos. Studio carga el esquema de base de datos en la base de datos. Las credenciales se conservan solo durante el período de creación de la base de datos.
6. Si no quiere que Studio cree la base de datos o no dispone de los permisos necesarios, haga clic en **Generar script**. Los scripts generados incluyen instrucciones para crear manualmente la base de datos y una base de datos reflejada, si es necesario. Antes de cargar el esquema, compruebe que la base de datos está vacía y de que al menos un usuario tiene permiso para acceder a ella y cambiarla.

## Más información

- [Herramienta para calcular el tamaño de la base de datos.](#)

- [Tamaño de la base de datos del sitio](#) y [Configurar las cadenas de conexión](#) cuando se utilizan soluciones de alta disponibilidad de SQL Server.

## Métodos de entrega

November 4, 2021

Citrix Virtual Apps and Desktops ofrece varios métodos de entrega. Es probable que un único método de entrega no cubra todas sus necesidades.

### Introducción

Elegir el método adecuado para entregar aplicaciones ayuda a mejorar la escalabilidad, la administración y la experiencia del usuario.

- **Aplicación instalada:** La aplicación es parte de la imagen base del escritorio. El proceso de instalación implica realizar modificaciones en el Registro y copiar archivos DLL y EXE, entre otros, a la unidad de la imagen. Para obtener más información, consulte [Crear catálogos de máquinas](#).
- **Aplicación distribuida por streaming (Microsoft App-V):** La aplicación se incluye en un perfil y se entrega a demanda a los escritorios de toda la red. Los archivos de aplicación y los parámetros de Registro se colocan en un contenedor del escritorio virtual y se aíslan del sistema operativo base y entre ellos. Este aislamiento ayuda a solucionar los problemas de compatibilidad. Para obtener más información, consulte [App-V](#).
- **Aplicación por capas (Citrix App Layering):** Cada capa contiene una sola aplicación, agente o sistema operativo. Al integrar una capa de sistema operativo, una capa de plataforma (VDA, un agente de Citrix Provisioning) y muchas capas de aplicaciones, un administrador puede crear fácilmente nuevas imágenes a implementar. La distribución en capas facilita el mantenimiento cotidiano, ya que el sistema operativo, el agente y la aplicación se encuentran en una capa cada uno. Cuando actualiza una capa, todas las imágenes implementadas que contienen esa capa se actualizan. Para obtener más información, consulte [Citrix App Layering](#).
- **Aplicación alojada en Windows:** Una aplicación se instala en un host multiusuario de Citrix Virtual Apps y se implementa como una aplicación, no como un escritorio. Un usuario accede a la aplicación Windows alojada en servidores directamente desde el dispositivo de punto final o un escritorio VDI, con lo que se oculta el hecho de que la aplicación se ejecuta de forma remota. Para obtener más información, consulte [Crear grupos de entrega](#).
- **Aplicación local:** Una aplicación se implementa en el dispositivo de punto final. La interfaz de la aplicación aparece en la sesión de usuario alojada en el VDI, aunque se ejecute en el punto final. Para obtener más información, consulte [Acceso a aplicaciones locales y redirección de URL](#).

- **Acceso con Remote PC:** El acceso con Remote PC permite a los empleados acceder de forma remota a sus PC de oficina físicos. Cuando los usuarios acceden a sus PC de oficina, pueden acceder a todas las aplicaciones, datos y recursos que necesitan para hacer su trabajo. Acceso con Remote PC elimina la necesidad de introducir y proporcionar otras herramientas para adaptarse al teletrabajo. Para obtener más información, consulte [Acceso con Remote PC](#).

Para los escritorios, puede utilizar escritorios VDI o escritorios publicados.

## Aplicaciones y escritorios publicados de Citrix Virtual Apps

Use máquinas de SO multisesión para entregar aplicaciones y escritorios publicados de Citrix Virtual Apps and Desktops.

### Caso de uso:

- Quiere una entrega de recursos basada en servidores, que no sea muy costosa, para minimizar el coste de entregar aplicaciones a muchos usuarios, al tiempo que les ofrece una experiencia de usuario segura y de alta definición.
- Sus usuarios realizan tareas bien definidas y no requieren personalización ni acceso sin conexión a las aplicaciones. Los usuarios pueden ser trabajadores de tareas, como operadores de centros de llamadas o trabajadores del sector comercial, o usuarios que comparten estaciones de trabajo.
- Tipos de aplicaciones: cualquier aplicación.

### Ventajas y consideraciones:

- Una solución fácilmente administrable y ampliable dentro del centro de datos.
- La solución de entrega de aplicaciones más rentable.
- Las aplicaciones alojadas se administran de forma centralizada y los usuarios no pueden modificarlas. Eso proporciona una experiencia de usuario uniforme, segura y fiable.
- Los usuarios deben estar conectados a la red para acceder a sus aplicaciones.

### Experiencia de usuario:

- El usuario solicita una o varias aplicaciones desde StoreFront, el menú **Inicio** o una URL que le haya sido suministrada.
- Las aplicaciones se entregan virtualmente y se muestran en alta definición en los dispositivos de usuario.
- Los cambios que haga el usuario se guardan cuando se cierra la sesión de aplicación, siempre que así lo indiquen los parámetros del perfil. Si no es así, los cambios se eliminan.

### Procesamiento, alojamiento y entrega de aplicaciones:

- El procesamiento de las aplicaciones tiene lugar en las máquinas que las alojan (hosts), en lugar de procesarse en los dispositivos de usuario. Estas máquinas host pueden ser físicas o virtuales.
- Las aplicaciones y los escritorios residen en una máquina con SO multisesión.
- Las máquinas están disponibles a través de los catálogos de máquinas.
- Las máquinas incluidas en catálogos se organizan en grupos de entrega que se encargan de entregar un mismo conjunto de aplicaciones a grupos de usuarios.
- Las máquinas con SO multisesión admiten grupos de entrega que alojan o aplicaciones o escritorios, o ambos.

### **Administración de sesiones y asignación:**

- Las máquinas de SO multisesión ejecutan varias sesiones desde una sola máquina para entregar varias aplicaciones y escritorios a varios usuarios conectados simultáneamente. Cada usuario requiere una sola sesión desde la que puede ejecutar todas sus aplicaciones alojadas.

Por ejemplo, un usuario inicia una sesión y solicita una aplicación. Una sesión en esa máquina deja de estar disponible para otros usuarios. Un segundo usuario inicia una sesión y solicita una aplicación alojada en esa máquina. Ahora, hay una segunda sesión que ya no está disponible para otros usuarios. Si ambos usuarios solicitan aplicaciones adicionales, no se necesitarán sesiones adicionales porque un usuario puede ejecutar varias aplicaciones en la misma sesión. Si otros dos usuarios más inician sesiones y solicitan escritorios, y hay dos sesiones disponibles en esa misma máquina, esa máquina estará mediante cuatro sesiones para alojar a cuatro usuarios diferentes.

- Dentro del grupo de entrega al que esté asignado el usuario, se selecciona una máquina del servidor que tenga la menor carga. Se asigna, de forma aleatoria, una máquina con disponibilidad de la sesión para entregar aplicaciones a un usuario cuando este inicia sesión.

### **Aplicaciones alojadas en VM**

Usar máquinas con SO de sesión única para entregar aplicaciones alojadas en VM

#### **Caso de uso:**

- Quiere una solución de entrega de aplicaciones basada en clientes que sea segura, que permita una administración centralizada y que admita muchos usuarios por servidor host. Quiere ofrecer a los usuarios unas aplicaciones que se muestran perfectamente en alta definición.
- Sus usuarios son contratistas externos o internos, colaboradores de terceros y otros miembros de equipo de carácter provisional. Los usuarios no necesitan acceso sin conexión a las aplicaciones alojadas.
- Tipos de aplicaciones: Aplicaciones que podrían no funcionar correctamente con otras aplicaciones o que podrían interactuar con el sistema operativo, como Microsoft .NET Framework. Estos tipos de aplicaciones son ideales para alojarlos en máquinas virtuales.

### **Ventajas y consideraciones:**

- Las aplicaciones y los escritorios incluidos en la imagen maestra se administran, alojan y ejecutan de forma segura dentro del centro de datos, con lo que se ofrece una solución de entrega de aplicaciones más rentable.
- Cuando el usuario inicia sesión, se le puede asignar aleatoriamente una máquina dentro del grupo de entrega que está configurado para alojar una misma aplicación. También se puede asignar estáticamente una única máquina para entregar la aplicación a un único usuario cada vez que éste inicia una sesión. Las máquinas asignadas de forma estática permiten a los usuarios instalar y administrar sus propias aplicaciones en la máquina virtual.
- La ejecución de sesiones múltiples no se admite en máquinas de SO de sesión única. Por lo tanto, cada usuario que inicia una sesión consume una máquina dentro del grupo de entrega, y los usuarios deben estar conectados a la red para acceder a sus aplicaciones.
- Este método puede aumentar la cantidad de recursos de servidor necesarios para el procesamiento de las aplicaciones y aumentar la cantidad de almacenamiento necesaria para los datos de los usuarios.

### **Experiencia de usuario:**

- La misma experiencia de aplicación integrada que tiene lugar con las aplicaciones alojadas compartidas en máquinas con SO multisesión.

### **Procesamiento, alojamiento y entrega de aplicaciones:**

- Lo mismo que las máquinas con SO multisesión, excepto que son máquinas virtuales con SO de sesión única.

### **Administración de sesiones y asignación:**

- Las máquinas con SO de sesión única ejecutan una única sesión de escritorio desde una única máquina. Al acceder solo a las aplicaciones, un solo usuario puede utilizar varias aplicaciones (no está limitado a una sola aplicación) porque el sistema operativo percibe cada aplicación como una nueva sesión.
- En un grupo de entrega, cuando los usuarios inician sesión, pueden acceder a una máquina asignada estáticamente (el usuario siempre inicia sesión en la misma máquina), o bien acceden a una máquina asignada aleatoriamente que se selecciona en función de la disponibilidad de la sesión.

## **Escritorios VDI**

Utilice máquinas con SO de sesión única para entregar escritorios VDI de Citrix Virtual Apps and Desktops.

Los escritorios VDI se alojan en máquinas virtuales y entregan a cada usuario un sistema operativo de escritorio.

Los escritorios VDI necesitan más recursos que los escritorios publicados, pero no es necesario que las aplicaciones instaladas en ellos sean compatibles con sistemas operativos de servidor. Además, según el tipo de escritorio VDI que elija, estos escritorios se pueden asignar a usuarios individuales. Esto permite a los usuarios un alto grado de personalización.

Al crear un catálogo de máquinas para escritorios VDI, hay que crear uno de estos tipos de escritorios:

- **Escritorio aleatorio no persistente, también conocido como escritorio de VDI agrupado:** Cada vez que un usuario inicia sesión en uno de estos escritorios, se conecta a un escritorio seleccionado de un grupo de escritorios. Este grupo se basa en una sola imagen maestra. Todos los cambios realizados en el escritorio se pierden tras reiniciarse la máquina.
- **Escritorio estático no persistente:** Durante el primer inicio de sesión, a un usuario se le asigna un escritorio proveniente de un grupo de escritorios (todas las máquinas del grupo se basan en una sola imagen maestra). Después del primer uso, cada vez que el usuario inicie sesión para usar un escritorio, se conectará al mismo escritorio que le fue asignado la primera vez. Todos los cambios realizados en el escritorio se pierden tras reiniciarse la máquina.
- **Escritorio estático persistente:** A diferencia de otros tipos de escritorios VDI, los usuarios pueden personalizar completamente estos escritorios. Durante el primer inicio de sesión, a un usuario se le asigna un escritorio proveniente de un grupo de escritorios. Las siguientes conexiones del usuario se establecen con el mismo escritorio que se asignó la primera vez. Los cambios realizados en el escritorio se conservan tras reiniciarse la máquina.

## Puertos de red

September 22, 2021

En las tablas siguientes se indican los puertos de red predeterminados que utilizan los Delivery Controllers, los VDA de Windows, Director y Citrix License Server. Cuando se instalan los componentes de Citrix, el firewall host del sistema operativo también se actualiza, de manera predeterminada, para coincidir con estos puertos de red predeterminados.

Para ver una descripción general de los puertos de comunicación utilizados en otras tecnologías y componentes de Citrix, consulte [CTX101810](#).

Puede llegar a necesitar esta información de puertos:

- Con fines de cumplimiento de normativas.

- Si hay un firewall de red entre estos componentes y otros productos o componentes de Citrix, para poder configurar el firewall adecuadamente.
- Si utiliza un firewall host de terceros, como el que se suministra con un paquete antimalware, en lugar de utilizar el firewall host del sistema operativo.
- Si modifica la configuración del firewall host en estos componentes (normalmente Windows Firewall Service).
- Si reconfigura cualquiera de las funciones de estos componentes para que utilicen un puerto o un intervalo de puertos diferente, y luego quiere inhabilitar o bloquear puertos no utilizados en su configuración. Consulte la documentación del componente para encontrar más información.
- Para obtener información acerca de puertos de otros componentes, como StoreFront y Citrix Provisioning (antes Provisioning Services), consulte el artículo actual “Requisitos del sistema” del componente en cuestión.

En las tablas solo se indican los puertos de entrada. Los puertos de salida vienen determinados normalmente por el sistema operativo y usan números no relacionados. La información sobre puertos de salida normalmente no es necesaria con los fines descritos más arriba.

Algunos de estos puertos están registrados en la autoridad de números asignados de Internet o IANA (Internet Assigned Numbers Authority). Dispone de información detallada sobre estas asignaciones en <http://www.iana.org/assignments/port-numbers>. Sin embargo, la información descriptiva que indica IANA no siempre refleja el uso actual.

Además, el sistema operativo en el VDA y el Delivery Controller requiere puertos de entrada para su propio uso. Para obtener información más detallada, consulte la documentación de Microsoft Windows.

## **VDA, Delivery Controller y Director**

Componente	Uso	Protocolo	Puerto de entrada predeterminado	Notas
VDA	ICA/HDX	TCP, UDP	1494	El protocolo de transporte de datos más ligero (EDT) requiere que 1494 esté abierto para UDP. Consulte <a href="#">Configuraciones de directiva de ICA</a> .
VDA	ICA/HDX con fiabilidad de la sesión	TCP, UDP	2598	El protocolo de transporte de datos más ligero (EDT) requiere que 2598 esté abierto para UDP. Si se habilitan varios flujos y varios puertos, el administrador define los números de puerto para los tres flujos adicionales. Consulte <a href="#">Configuraciones de directiva de ICA</a> .
VDA	ICA/HDX sobre TLS/DTLS	TCP, UDP	443	Todas las aplicaciones Citrix Workspace

Componente	Uso	Protocolo	Puerto de entrada predeterminado	Notas
VDA	ICA/HDX sobre WebSocket	TCP	8008	La aplicación Citrix Workspace para HTML5 y la aplicación Citrix Workspace para Chrome 1.6 y versiones anteriores solamente
VDA	Transporte de audio en tiempo real ICA/HDX por UDP	UDP	16500...16509	
VDA	ICA/Universal Print Server	TCP	7229	Utilizado por el agente de escucha del protocolo CGP para el flujo de datos de impresión proveniente de Universal Print Server.
VDA	ICA/Universal Print Server	TCP	8080	Utilizado por el agente de escucha de Universal Print Server para solicitudes HTTP/SOAP entrantes.
VDA	Wake On LAN	UDP	9	Administración de energía de Acceso con Remote PC

Componente	Uso	Protocolo	Puerto de entrada predeterminado	Notas
VDA	Proxy de reactivación	TCP	135	Administración de energía de Acceso con Remote PC
VDA	Delivery Controller	TCP	80	
Delivery Controller	VDA, StoreFront, Director, Studio	TCP	80	
Delivery Controller	StoreFront, Director, Studio sobre TLS	TCP	443	
Delivery Controller	Delivery Controller, VDA	TCP	89	Memoria caché del host local (Este uso del puerto 89 podría cambiar en versiones futuras.)
Delivery Controller	Orchestration	TCP	9095	Orchestration
Director	Delivery Controller	TCP	80, 443	

## Citrix Licensing

Los siguientes puertos se utilizan para Citrix Licensing.

Componente	Uso	Protocolo	Puerto de entrada predeterminado
Servidor de licencias	Servidor de licencias	TCP	27000
Servidor de licencias	License Server para Citrix (demonio de proveedor)	TCP	7279
Servidor de licencias	License Administration Console	TCP	8082

Componente	Uso	Protocolo	Puerto de entrada predeterminado
Servidor de licencias	Web Services for Licensing	TCP	8083

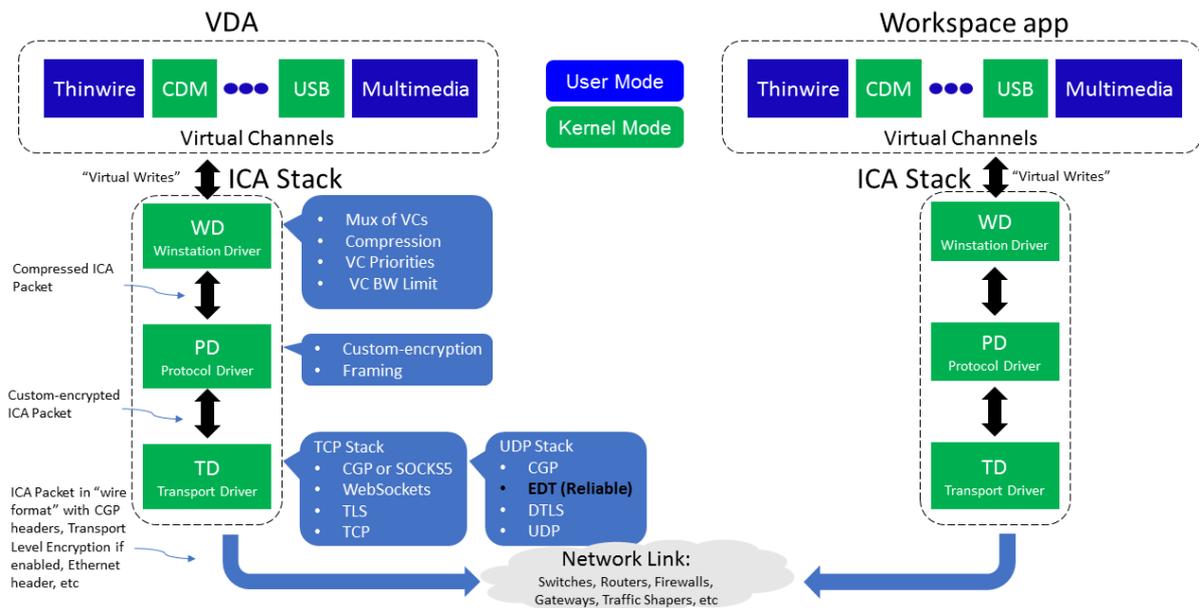
## HDX

April 19, 2024

### Advertencia:

Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Citrix HDX incluye una amplia gama de tecnologías que ofrecen una experiencia de alta definición a los usuarios de aplicaciones y escritorios centralizados, en cualquier dispositivo y en cualquier red.

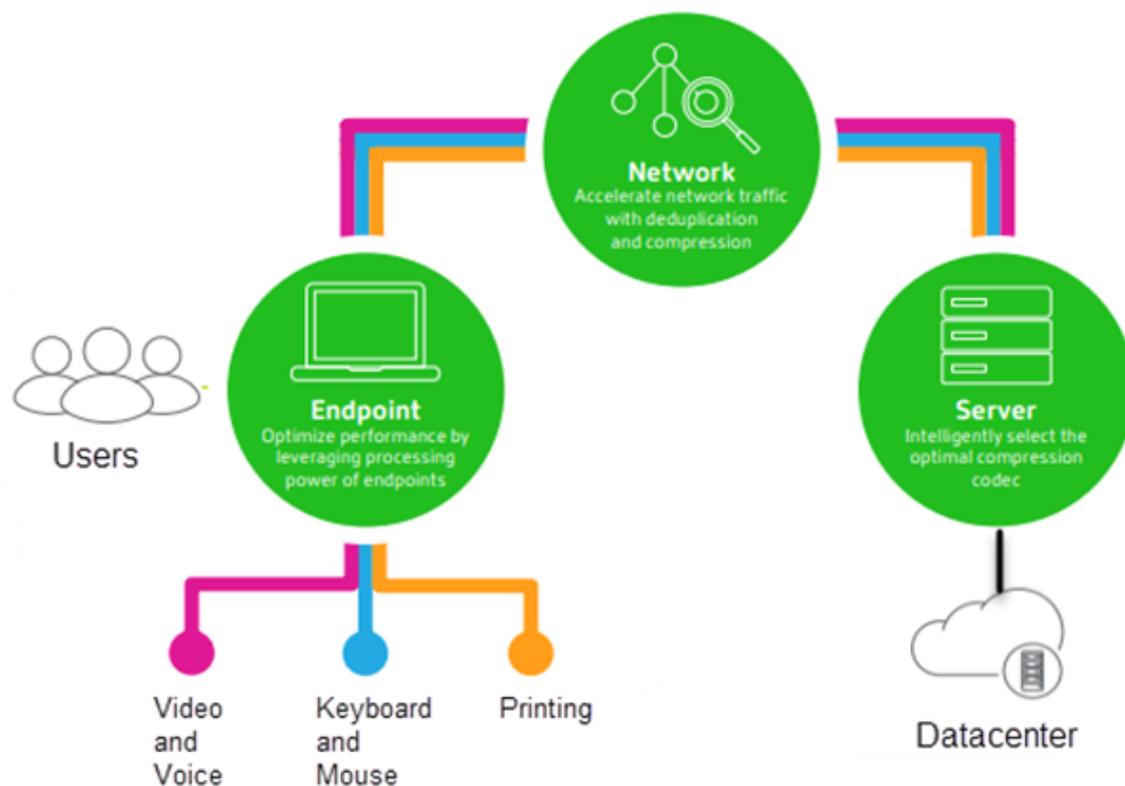


El diseño de HDX responde a tres principios técnicos:

- Redirección inteligente
- Compresión adaptable
- Evitar solapamiento de datos

Aplicados en diferentes combinaciones, optimizan la TI y la experiencia del usuario, disminuyen el consumo de ancho de banda y aumentan la densidad de usuarios por servidor host.

- **Redirección inteligente:** La redirección inteligente examina la actividad de la pantalla, los comandos de la aplicación, el dispositivo de punto final y las capacidades de la red y el servidor para determinar de manera instantánea cómo y dónde generar una actividad de escritorio o aplicación. La representación puede ocurrir en el dispositivo de punto final o en el servidor de alojamiento.
- **Compresión adaptable:** La compresión adaptable permite que se entreguen pantallas con muchos contenidos multimedia en conexiones de red débiles. HDX primero evalúa algunas variables, como el tipo de entrada, el dispositivo y la pantalla (texto, vídeo, voz y multimedia). Elige el códec de compresión óptimo y la mejor proporción de uso de CPU y GPU. A continuación, se adapta de forma inteligente según cada usuario y frecuencia únicos. Esta adaptación inteligente es por usuario o incluso por sesión.



- **Evitar solapamiento de datos:** Al evitar el solapamiento del tráfico de red se reducen los datos agregados enviados entre el cliente y el servidor. Esto se consigue aprovechando los patrones repetidos en los datos a los que se accede de forma común, como gráficos de mapas de bits,

documentos, trabajos de impresión y contenido en streaming. El almacenamiento en caché de estos patrones permite que solo los cambios se transmitan a través de la red, eliminando el tráfico duplicado. HDX también admite la multidifusión de transmisiones multimedia, donde varios suscriptores ven una única transmisión desde la fuente en una ubicación, en lugar de tener que establecer una conexión individual para cada usuario.

Para obtener más información, consulte [Potenciar la productividad con un espacio de trabajo de usuario de alta definición](#).

## **En el dispositivo**

HDX usa la capacidad de computación de los dispositivos de usuario para mejorar y optimizar la experiencia del usuario. La tecnología HDX garantiza que los usuarios tengan una experiencia de contenido multimedia integrada y fruida en sus aplicaciones y escritorios virtuales. El control del área de trabajo permite a los usuarios poner en pausa sus aplicaciones y escritorios virtuales y reanudar su trabajo desde otro dispositivo, retomando la sesión en el mismo punto donde la dejaron.

## **En la red**

HDX incorpora capacidades avanzadas de optimización y aceleración para conseguir el mejor rendimiento sobre cualquier tipo de red, incluidas las conexiones WAN con poco ancho de banda y alta latencia.

Las funciones de HDX se adaptan a los cambios en el entorno. Las funciones están diseñadas para buscar el equilibrio entre el rendimiento y el consumo del ancho de banda. Las funciones de HDX aplican la mejor tecnología aplicable para cada caso de uso, independientemente de si se accede al escritorio o la aplicación localmente dentro de la red de la empresa o si se accede de manera remota desde fuera del firewall de la empresa.

## **En el centro de datos**

HDX usa la capacidad de procesamiento y la escalabilidad de los servidores para ofrecer un rendimiento avanzado de gráficos, independientemente de la capacidad del dispositivo cliente.

La supervisión del canal HDX, proporcionada por Citrix Director, muestra el estado de los canales HDX conectados en los dispositivos de usuario.

## **HDX Insight**

HDX Insight es la integración de NetScaler Network Inspector y Performance Manager en Director. Captura datos sobre el tráfico ICA y ofrece una vista panel de datos en tiempo real e históricos. Esta infor-

mación incluye la latencia de sesión ICA del lado del cliente y del lado del servidor, el uso del ancho de banda por parte de los canales ICA y el valor de tiempo de ida y vuelta de ICA en cada sesión.

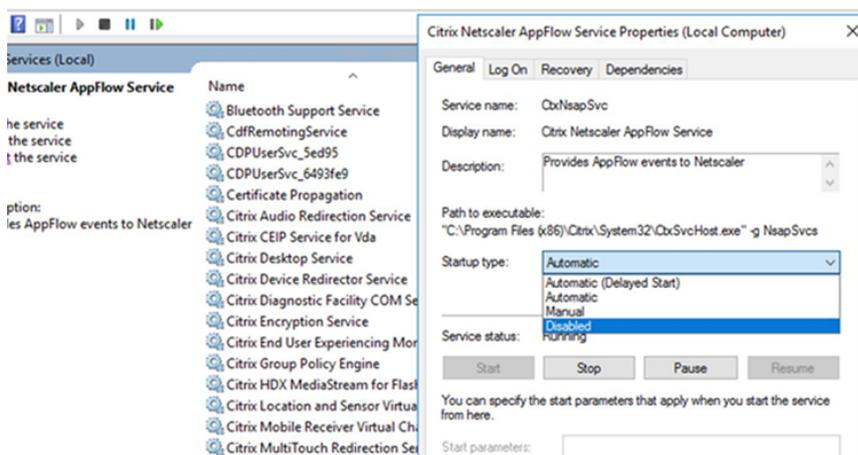
Puede habilitar NetScaler para usar el canal virtual HDX Insight y mover todos los puntos de datos requeridos en un formato sin comprimir. Si inhabilita esta función, el dispositivo NetScaler descifrará y descomprimirá el tráfico ICA que haya en varios canales virtuales. Usar el canal virtual único disminuye la complejidad, mejora la escalabilidad y es más rentable.

### Requisitos mínimos:

- Citrix Virtual Apps and Desktops 7 1808
- XenApp y XenDesktop 7.17
- NetScaler 12.0 compilación 57.x
- Aplicación Citrix Workspace para Windows 1808
- Citrix Receiver para Windows 4.10
- Aplicación Citrix Workspace para Mac 1808
- Citrix Receiver para Mac 12.8

### Habilitar o inhabilitar el canal virtual HDX Insight

Para inhabilitar esta función, inhabilite las propiedades del servicio Citrix NetScaler Application Flow. Para habilitarla, establezca el servicio en Automático. En ambos casos, le recomendamos que reinicie la máquina del servidor después de cambiar estas propiedades. Este servicio está habilitado (Automático) de forma predeterminada.



### Experimentar con las capacidades HDX en su escritorio virtual

- Para ver cómo la redirección de contenido de exploradores (una de las cuatro tecnologías HDX de redirección multimedia) acelera la entrega de contenido multimedia HTML5 y WebRTC:

1. Descargar la [Extensión del explorador Chrome](#) e instalarla en el escritorio virtual.
  2. Para ver cómo la redirección de contenido de exploradores acelera la entrega de contenido multimedia a los escritorios virtuales, vea un vídeo en su escritorio desde un sitio web que contenga vídeos HTML5, como YouTube. Los usuarios no saben cuándo se está ejecutando la redirección de contenido de exploradores. Para ver si se está utilizando la redirección de contenido de exploradores, arrastre la ventana del explorador rápidamente. Verá una demora o falta de marco entre la ventana gráfica y la interfaz de usuario. También puede hacer clic con el botón derecho en la página web y buscar **Acerca de la Redirección de explorador HDX** en el menú.
- Para ver cómo HDX entrega sonido de alta definición:
    1. Configure el cliente Citrix con la máxima calidad de audio; consulte la documentación de la aplicación Citrix Workspace para obtener más información.
    2. Reproduzca archivos de música mediante un reproductor de audio digital (como iTunes) en el escritorio.

HDX ofrece una experiencia de alta calidad de gráficos y vídeo para la mayoría de los usuarios de manera predeterminada, sin necesidad de realizar configuración alguna. Las configuraciones de directivas Citrix que ofrecen la mejor experiencia integrada para la mayoría de los casos de uso están habilitadas de manera predeterminada.

- HDX selecciona automáticamente el mejor método de entrega basándose en el cliente, la plataforma, la aplicación y el ancho de banda de la red, y luego hace los ajustes necesarios automáticamente según cambien las condiciones de la conexión.
- HDX optimiza el rendimiento de gráficos 2D y 3D y vídeo.
- HDX permite que los dispositivos de usuario reciban archivos multimedia por streaming directamente desde el proveedor de origen en Internet o en la intranet, en lugar de hacerlo a través del servidor host. Si no se cumplen los requisitos para la obtención de contenido del lado del cliente, la entrega de elementos multimedia recurre a la obtención de contenido del lado del servidor y la redirección multimedia. Por lo general, no es necesario ajustar las directivas para la redirección de elementos multimedia.
- HDX entrega, a los escritorios virtuales, contenido sofisticado de vídeo generado en el servidor cuando la redirección multimedia no está disponible: consulte un vídeo de un sitio web que contiene vídeos de alta definición, como <http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/>.

#### Información útil:

- Para obtener información acerca de la asistencia y los requisitos de las funciones HDX, consulte el artículo [Requisitos del sistema](#). A menos que se indique lo contrario, las funciones de HDX están disponibles para máquinas con los sistemas operativos compatibles multisesión Windows y de sesión única Windows, además de los escritorios de acceso con Remote PC.

- Esta sección describe cómo optimizar más la experiencia de usuario, mejorar la escalabilidad de los servidores o reducir los requisitos de ancho de banda. Para obtener más información sobre cómo usar las directivas Citrix y sus configuraciones, consulte la documentación de las [directivas Citrix](#) para esta versión.
- Para las instrucciones que impliquen modificar el Registro, tenga cuidado: si se modifica de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

## Fiabilidad de la sesión y reconexión automática de clientes

A la hora de acceder a aplicaciones o escritorios alojados, pueden producirse interrupciones de red. Para una reconexión más fluida, se ofrecen las funcionalidades Fiabilidad de la sesión y Reconexión automática de clientes. En una configuración predeterminada, se empieza con la Fiabilidad de la sesión, seguida de la Reconexión automática de clientes.

### Reconexión automática de clientes:

La reconexión automática de clientes reinicia el motor del cliente para volver a conectarse a una sesión desconectada. La reconexión automática de clientes cierra (o desconecta) la sesión del usuario después del tiempo especificado en la configuración. Durante la reconexión automática de clientes, el sistema envía la siguiente notificación de interrupción de red al usuario de las aplicaciones y los escritorios:

- **Escritorios.** La ventana de sesión se oscurece y aparece un temporizador de cuenta atrás que muestra el tiempo que falta hasta que se produzcan las reconexiones.
- **Aplicaciones.** La ventana de sesión se cierra y aparece un diálogo con un temporizador de cuenta atrás que muestra el tiempo que falta hasta que se intenten reconexiones.

Durante la reconexión automática de clientes, las sesiones se reinician a condición de una buena conectividad de red. El usuario no puede interactuar con las sesiones mientras la reconexión automática de clientes está en curso.

En la reconexión, las sesiones desconectadas vuelven a conectarse mediante la información guardada de la conexión. El usuario puede interactuar con las aplicaciones y los escritorios de la forma habitual.

Configuración predeterminada de la reconexión automática de clientes:

- Tiempo de espera de la reconexión automática de clientes: 120 segundos
- Reconexión automática de clientes: Habilitada
- Autenticación para la reconexión automática de clientes: Inhabilitada

- Captura de registro de la reconexión automática de clientes: Inhabilitada

Para obtener más información, consulte [Configuraciones de directiva de Reconexión automática de clientes](#).

### **Fiabilidad de la sesión:**

La fiabilidad de la sesión vuelve a conectar sesiones ICA sin problemas cuando se producen interrupciones de red. La fiabilidad de la sesión cierra (o desconecta) la sesión de usuario después de que haya transcurrido el tiempo especificado en la opción de configuración. Una vez agotado el tiempo de espera de la fiabilidad de la sesión, se aplicará la configuración de directiva de Reconexión automática de clientes y se intentará reconectar al usuario con la sesión desconectada. Durante la fiabilidad de la sesión, se envían las siguientes notificaciones de interrupción de red al usuario de las aplicaciones y los escritorios:

- **Escritorios.** La ventana de sesión se vuelve transparente y aparece un temporizador de cuenta atrás que muestra el tiempo hasta que se produzcan las reconexiones.
- **Aplicaciones.** La ventana se vuelve transparente y aparecen elementos emergentes que indican una conexión interrumpida en el área de notificaciones.

Mientras la fiabilidad de la sesión está activa, el usuario no puede interactuar con las sesiones ICA. No obstante, las acciones del usuario (como pulsaciones de teclado) se almacenan en búfer durante los segundos inmediatos tras la interrupción de red y se retransmiten una vez que la red está disponible.

En la reconexión, el cliente y el servidor reanudan la actividad desde el mismo punto donde estaban en su intercambio de protocolo. Las ventanas de sesión pierden transparencia y aparecen las notificaciones correspondientes en forma de elementos emergentes en el área de notificaciones para las aplicaciones.

Configuración predeterminada de fiabilidad de la sesión

- Tiempo de espera de fiabilidad de la sesión: 180 segundos
- Nivel de opacidad de la interfaz de usuario durante la reconexión: 80 %
- Conexión de fiabilidad de la sesión: Habilitada
- Número de puerto para fiabilidad de la sesión: 2598

Para obtener más información, consulte [Configuraciones de directiva de Fiabilidad de la sesión](#).

### **NetScaler con fiabilidad de la sesión y reconexión automática de clientes:**

La reconexión automática de clientes no funciona si las directivas de Multisequencia y de Puertos múltiples están habilitadas en el servidor y si se da una de las siguientes condiciones o todas ellas:

- La fiabilidad de la sesión está inhabilitada en NetScaler Gateway.
- Se produce una conmutación por error en el dispositivo NetScaler.
- NetScaler SD-WAN se utiliza con NetScaler Gateway.

## Rendimiento HDX adaptable

El rendimiento HDX adaptable ajusta de manera inteligente el rendimiento máximo de la sesión ICA porque adapta los búferes de salida. Al principio, la cantidad de búferes de salida se establece en un valor alto. Este valor alto permite que los datos se transmitan al cliente de manera más rápida y eficiente, especialmente en redes de latencia alta. Así, se obtiene una mejor interactividad, transferencias de archivos más rápidas, reproducciones de vídeo más fluidas, mayor velocidad de fotogramas y mayor resolución en una experiencia de usuario mejorada.

La interactividad de la sesión se mide constantemente para determinar si algún flujo de datos de la sesión ICA está afectando negativamente a la interactividad. Si eso ocurre, el rendimiento se reduce para disminuir el impacto del flujo de datos de gran tamaño en la sesión y permitir que se recupere la interactividad.

### Importante:

El rendimiento HDX adaptable cambia la forma en que se configuran los búferes de salida, porque transfiere este mecanismo del cliente al VDA y no se necesita ninguna configuración manual.

Esta función presenta los siguientes requisitos:

- VDA 1811 o una versión posterior
- Aplicación Workspace para Windows 1811 o una versión posterior

## Mejorar la calidad de imagen enviada a los dispositivos de usuario

Las siguientes configuraciones de directiva de presentación visual controlan la calidad de las imágenes que se envían desde los escritorios virtuales a los dispositivos de los usuarios.

- Calidad visual. Controla la calidad visual de las imágenes que se muestran en el dispositivo de usuario: media, alta, siempre sin pérdida, gradual sin pérdida (la opción predeterminada es media). La calidad real del vídeo con la configuración predeterminada media depende del ancho de banda disponible.
- Velocidad de fotogramas de destino. Especifica la cantidad máxima de fotogramas por segundo que se envían desde el escritorio virtual al dispositivo de usuario (la opción predeterminada es 30). Para dispositivos que tienen unidades CPU lentas, especifique un valor bajo para mejorar la experiencia de usuario. La velocidad máxima permitida es de 60 fotogramas por segundo.
- Límite de memoria de presentación. Especifica el tamaño máximo de búfer para vídeos de la sesión en kilobytes (la opción predeterminada es 65536 KB). Para las conexiones que requieran mayor profundidad de color y mayor resolución, aumente el límite. Puede calcular la memoria máxima necesaria.

## Mejorar el rendimiento de las conferencias de vídeo

Se han optimizado varias aplicaciones conocidas de conferencias de vídeo para la entrega con Citrix Virtual Apps and Desktops a través de la redirección multimedia (consulte, por ejemplo, [HDX Real-Time Optimization Pack](#)). Para las aplicaciones que no se han optimizado, la compresión de vídeo de cámara web HDX mejora la eficiencia del ancho de banda y la tolerancia a la latencia para las cámaras web durante las sesiones de conferencias de vídeo. Esta compresión de vídeo dirige el tráfico de la cámara web a través de un canal virtual multimedia dedicado. Esta tecnología utiliza menos ancho de banda en comparación con la funcionalidad de redirección USB de HDX Plug-n-Play isócrono, y funciona bien en conexiones WAN.

Los usuarios de la aplicación Citrix Workspace pueden supeditar este comportamiento predeterminado. Para ello, deben seleccionar el parámetro **No usar mi micrófono ni mi cámara web** en Micrófono y cámara web de Desktop Viewer. Para evitar que los usuarios cambien la compresión de vídeo de cámaras web de HDX, inhabilite la redirección de dispositivos USB desde las configuraciones de la directiva ICA > configuraciones de la directiva Dispositivos USB.

La compresión de vídeo de cámaras web de HDX requiere que las siguientes configuraciones de directiva estén habilitadas (están todas habilitadas de forma predeterminada).

- Redirección de audio del cliente
- Redirección de micrófonos del cliente
- Conferencia multimedia
- Redirección de Windows Media

Si una cámara web es compatible con la codificación por hardware, la compresión de vídeo de HDX utiliza la codificación por hardware de manera predeterminada. La codificación por hardware puede consumir más ancho de banda que la codificación por software. Para forzar la compresión de software, agregue el siguiente valor de clave DWORD a la clave del Registro HKCU\Software\Citrix\HdxRealTime: DeepCompress\_ForceSWEncode=1.

## Prioridades del tráfico de red

Se asignan prioridades al tráfico de red en varias conexiones para una sesión con enrutadores que use QoS (calidad de servicio). Existen cuatro secuencias TCP y dos secuencias UDP que están disponibles para transportar el tráfico ICA entre el dispositivo de usuario y el servidor:

- Secuencias TCP: en tiempo real, interactivo, de fondo y en masa
- Secuencias UDP: voz y pantallas remotas de Framehawk

Cada canal virtual se asocia a una prioridad específica y se transporta en la conexión correspondiente. Según el número de puerto TCP usado para la conexión, se pueden definir canales de forma independiente.

Se admiten varias conexiones de multisequencia de canales para los agentes VDA instalados en máquinas Windows 10, Windows 8 y Windows 7. Póngase en contacto con el administrador de la red para comprobar que los puertos del protocolo CGP definidos en la configuración de Directiva de puertos múltiples están correctamente asignados en los enrutadores de la red.

La función de calidad de servicio (QoS) solo se admite si se configuran múltiples puertos de fiabilidad de sesión o los puertos CGP.

**Advertencia:**

Use algún tipo de seguridad en el transporte cuando aplique esta función. Citrix recomienda el uso del protocolo de seguridad de Internet (IPsec) o Transport Layer Security (TLS). Las conexiones TLS (Secure Sockets Layer) solo se admiten cuando atraviesan un dispositivo NetScaler Gateway compatible con ICA de multisequencia. Dentro de una red interna de la empresa, no se admiten las conexiones multisequencia con TLS.

Para establecer la calidad de servicio en conexiones de multisequencia, agregue las siguientes configuraciones de directiva Citrix (consulte [Configuraciones de directiva de Conexiones de multisequencia](#) para obtener más información):

- Directiva de puertos múltiples: Esta configuración especifica los puertos para el tráfico ICA en varias conexiones y establece prioridades de red.
  - En la lista de prioridades de puertos CGP predeterminados, seleccione una prioridad. De forma predeterminada, el puerto primario (2598) tiene prioridad Alta.
  - Escriba los puertos CGP adicionales en CGP port1, CGP port2 y CGP port3 según sea necesario, e identifique las prioridades para cada puerto. Cada puerto debe tener una prioridad exclusiva.

Configure explícitamente los firewalls en los VDA para que permitan el tráfico TCP adicional.

- Configuración de equipo para multisequencia: Esta configuración está inhabilitada de forma predeterminada. Si usa Citrix NetScaler SD-WAN con la funcionalidad de multisequencia en el entorno, no es necesario definir esta configuración. Defina esta configuración de directiva cuando esté utilizando enrutadores externos o versiones antiguas de Branch Repeater para conseguir el nivel de Calidad de servicio (QoS) que necesite.
- Configuración de usuario para multisequencia: Esta configuración está inhabilitada de forma predeterminada.

Para que las directivas que contienen estas configuraciones tengan efecto, los usuarios deben cerrar la sesión y después volver a iniciar una sesión en la red.

## Mostrar u ocultar la barra de idioma remota

La barra de idioma muestra el idioma de entrada preferido en una sesión de aplicación. Si esta función está habilitada (la configuración predeterminada), puede mostrar u ocultar la barra de idioma en la interfaz de usuario desde **Preferencias avanzadas > Barra de idioma** en la aplicación Citrix Workspace para Windows. Mediante una configuración de Registro en el lado del VDA, puede inhabilitar el control sobre la función de la barra de idioma por parte del cliente. Si esta función está inhabilitada, la configuración de la interfaz de usuario del cliente no surte efecto, y la configuración actual por usuario determina el estado de la barra de idioma. Para obtener más información, consulte [Mejorar la experiencia del usuario](#).

Para inhabilitar el control sobre la función de la barra de idioma por parte del cliente desde el VDA:

1. En el editor de Registro, vaya a HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\T
2. Cree una clave de valor DWORD, SeamlessFlags, y configúrela en 0x40000.

## Asignar teclado Unicode

Los Citrix Receiver que no sean Windows usa la distribución del teclado local (Unicode). Si un usuario cambia la distribución del teclado local y la distribución del teclado de servidor (código de escaneo), puede que ambos teclados se desincronicen y el resultado de la salida de caracteres sea incorrecto. Por ejemplo, Usuario 1 cambia la distribución del teclado local de inglés a alemán. A continuación, Usuario 1 cambia el teclado del servidor a alemán. Aunque las distribuciones de ambos teclados sean en alemán, puede que no estén sincronizados, lo que provoca una salida incorrecta de caracteres.

### Habilitar o inhabilitar la asignación de distribución de teclado Unicode:

De forma predeterminada, la función está inhabilitada en el lado del agente VDA. Para habilitar la función, debe activarla desde el editor del Registro regedit en el VDA.

En HKEY\_LOCAL\_MACHINE/SOFTWARE/Citrix, cree la clave CtxKIMap.

Establezca el valor DWORD de EnableKIMap en 1.

Para inhabilitar esta función, establezca el valor DWORD de EnableKIMap en 0 o elimine la clave CtxKIMap.

### Habilitar el modo compatible de la asignación de distribución de teclado Unicode:

De forma predeterminada, la asignación de distribución de teclado Unicode vincula automáticamente algunas API de Windows para volver a cargar el nuevo mapa de distribución de teclado Unicode cuando la distribución del teclado se cambia en el servidor. Algunas aplicaciones no se pueden vincular. Para mantener la compatibilidad, puede cambiar la función al modo compatible para admitir esas aplicaciones no vinculadas.

1. En la clave HKEY\_LOCAL\_MACHINE/SOFTWARE/Citrix/CtxKIMap, establezca el valor DWORD DisableWindowHook en 1.

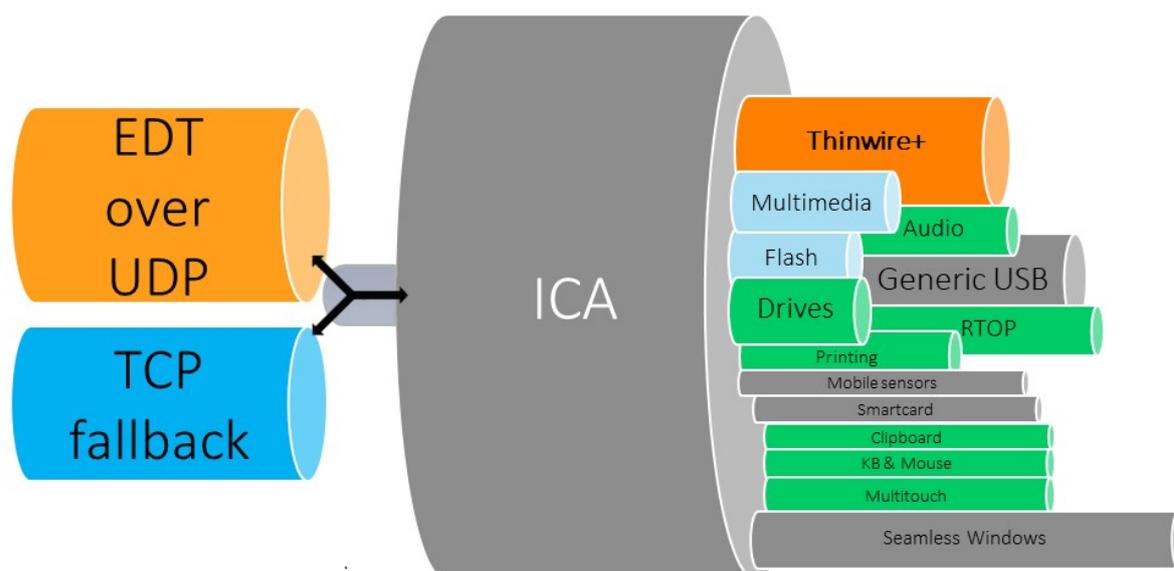
2. Para usar la asignación de distribución de teclado Unicode normal, establezca el valor DWORD de DisableWindowHook en 0.

## Transporte adaptable

January 23, 2024

El transporte adaptable es un mecanismo de Citrix Virtual Apps and Desktops que permite utilizar Enlightened Data Transport (EDT) como protocolo de transporte para conexiones ICA. El transporte adaptable cambia a TCP cuando EDT no está disponible.

EDT es un protocolo de transporte propiedad de Citrix basado en el protocolo de datagramas de usuario (UDP). Ofrece una experiencia de usuario superior en complicadas conexiones de larga distancia al tiempo que mantiene la escalabilidad de los servidores. EDT mejora el procesamiento de datos de todos los canales virtuales ICA en redes no fiables para ofrecer una experiencia de usuario mejor y más coherente.

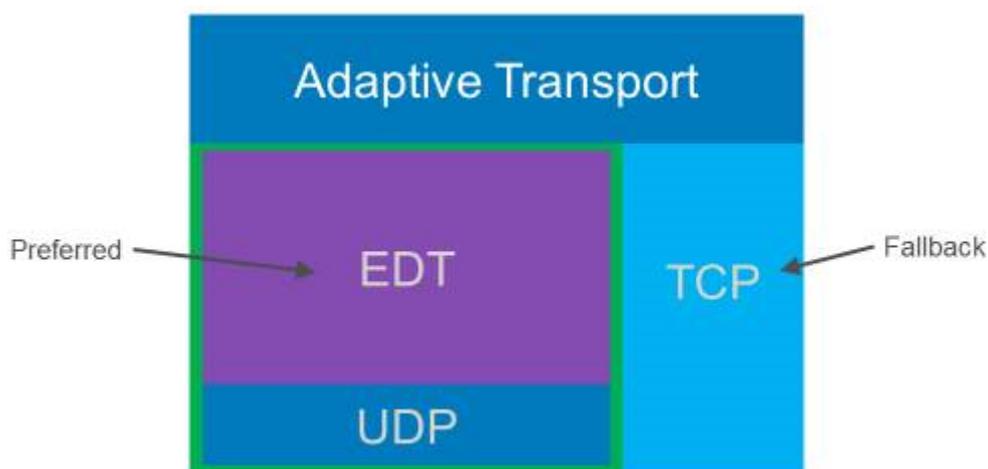


Cuando el transporte adaptable se establece en **Preferido**, EDT se utiliza como el protocolo de transporte principal y TCP se utiliza como reserva. De forma predeterminada, el transporte adaptable se establece en **Preferido**. Puede establecer el transporte adaptable en **Modo de diagnóstico** para pruebas, lo que solo permite EDT e inhabilita TCP como opción de reserva.

Con la aplicación Citrix Workspace para Windows, Mac y iOS, se intentan conexiones EDT y TCP en paralelo durante la conexión inicial, la reconexión de fiabilidad de la sesión y la reconexión automática de clientes. Al hacerlo, se reduce el tiempo de conexión si el transporte UDP subyacente no está

disponible y debe utilizarse TCP en su lugar. Si el transporte adaptable se establece en **Preferido** y la conexión se establece mediante TCP, el transporte adaptable sigue intentando cambiar a EDT cada cinco minutos.

Con la aplicación Citrix Workspace para Linux y Android, se intentan primero las conexiones EDT. Si la conexión no se realiza correctamente, la aplicación Citrix Workspace intenta conectarse mediante TCP una vez agotado el tiempo de espera de la solicitud de EDT.



## Requisitos del sistema

A continuación se detallan los requisitos para utilizar el transporte adaptable y EDT:

- Plano de control
  - Citrix Virtual Apps and Desktops Service
  - Citrix Virtual Apps and Desktops 1912 o versiones posteriores.
- Virtual Delivery Agent
  - Versión 1912 o una posterior (se recomienda 2103 o una posterior)
  - La versión 2012 es la mínima necesaria para utilizar EDT con Citrix Gateway Service
- StoreFront
  - Versión 3.12.x
  - Versión 1912.0.x
- Aplicación Citrix Workspace
  - Windows: Versión 1912 o una posterior (se recomienda 2105 o una posterior)
  - Linux: Versión 1912 o una posterior (se recomienda 2104 o una posterior)
  - Mac: Versión 1912 o una posterior (se recomienda 2108 o una posterior)
  - iOS: La versión más reciente disponible en el App Store de Apple

- Android: La versión más reciente disponible en Google Play
- Citrix Gateway (ADC)
  - 13.0.52.24 o una versión posterior
  - 12.1.56.22 o una versión posterior
- Firewall (desde la perspectiva del VDA)
  - UDP 1494 entrante: Si la fiabilidad de la sesión está inhabilitada
  - UDP 2598 entrante: Si la fiabilidad de la sesión está habilitada
  - UDP 443 entrante: Si SSL del VDA está habilitado para el cifrado ICA (DTLS)
  - UDP 443 saliente: Si utiliza Citrix Gateway Service. Para obtener más información, consulte la documentación de [Citrix Gateway Service](#).

## Consideraciones

- Habilite la fiabilidad de la sesión para utilizar la detección de MTU en EDT y usar EDT con Citrix Gateway y Citrix Gateway Service.
- La unidad de transmisión máxima o MTU en EDT debe estar configurada adecuadamente para evitar la fragmentación. De lo contrario, el rendimiento puede verse afectado o es posible que no se inicien sesiones en algunas situaciones. Para obtener más información, consulte [Detección de MTU en EDT](#).
- Para obtener información detallada sobre los requisitos y las consideraciones al utilizar EDT con Citrix Gateway Service, consulte [Transporte adaptable HDX con posibilidad de usar EDT para Citrix Gateway Service](#).
- Para obtener información detallada sobre la configuración de Citrix Gateway para compatibilidad con EDT, consulte [Configurar Citrix Gateway para que admita Enlightened Data Transport y HDX Insight](#).
- IPv6 no se admite por ahora.

## Configuración

El transporte adaptable está habilitado de forma predeterminada. Puede configurar estas opciones mediante el parámetro **Transporte adaptable HDX** de la directiva de Citrix.

- **Preferido.** Esta es la opción predeterminada. El transporte adaptable está habilitado y utiliza EDT como protocolo de transporte preferido, con TCP como opción de reserva.
- **Modo de diagnóstico.** El transporte adaptable está habilitado y obliga a usar EDT. La opción de reserva de TCP está inhabilitada. Esta configuración se recomienda únicamente para pruebas y solución de problemas.

- **Desactivado.** El transporte adaptable está inhabilitado y solamente TCP se utiliza para el transporte.

Para confirmar que EDT se usa como protocolo de transporte de la sesión, puede utilizar Director o la utilidad de la línea de comandos CtxSession.exe en el VDA.

En Director, busque la sesión y seleccione **Detalles**. Si el **Tipo de conexión** es **HDX** y el **Protocolo** es **UDP**, EDT se utiliza como protocolo de transporte de la sesión. Si el **Tipo de conexión** es **RDP**, ICA no se usa y el **Protocolo** muestra N/A. Para obtener más información, consulte [Supervisar sesiones](#).

Session Details		
Session Control ▾	Shadow	Send Message
<b>ID</b>	2	
<b>Session State</b>	Active	
<b>Application State</b>	Desktop	
<b>Anonymous</b>	No	
<b>Time in state</b>	0 minutes	
<b>Endpoint name</b>		
<b>Endpoint IP</b>		
<b>Connection type</b>	HDX	
<b>Protocol</b>	UDP	
<b>Citrix Workspace App Version</b>	21.5.0.48	
<b>ICA RTT</b>	67 ms	
<b>ICA Latency</b>	65 ms	
<b>Launched via</b>	n/a	
<b>Connected via</b>		

Para usar la utilidad CtxSession.exe, inicie un símbolo del sistema o PowerShell dentro de la sesión y ejecute `ctxsession.exe`. Para ver estadísticas detalladas, ejecute `ctxsession.exe -v`. Si EDT se está usando, el protocolo de transporte muestra uno de estos elementos:

- **UDP > ICA** (fiabilidad de la sesión inhabilitada)
- **UDP > CGP > ICA** (fiabilidad de la sesión habilitada)

- **UDP > DTLS > CGP > ICA** (ICA está cifrada con DTLS de extremo a extremo)

```
Administrator: Windows PowerShell
PS C:\windows\system32> ctxsession -v

Session Id 2:
Transport Protocols: UDP -> DTLS -> CGP -> ICA
  Local Address:
  Remote Address:
  Client Address:
Security Protocol: UNKNOWN VALUE - 131072
Security Cipher: 128 bit AES
Cipher Strength: 128 bits
ICA Encryption: Basic

EDT Reliable Statistics:
Bandwidth 121.777 Mbps, Send Rate 0 bps, Recv Rate 0 bps, RTT 65.531 ms
Sent 0, Sent Lost 0 (0.00%), Rcvd 0, Rcvd Lost 0 (0.00%)
Sent ACKs 0, Sent NAKs 0, Rcvd ACKs 0, Rcvd NAKs 0
Flow Window 16383, Congest Window 4050, Delivery Rate 7591
EDT MTU: 1400

ICA Statistics:
SentBandwidth (bps) = 6376 RecvBandwidth (bps) = 568
SentPreCompression = 1800688 RecvPreExpansion = 32864
SentPostCompression = 1429125 RecvPostExpansion = 137041
Compression Ratio % = 79 Expansion Ratio % = 23
LastLatency = 67 AverageLatency = 53
IcaBufferLength = 980
```

## DetECCIÓN DE MTU EN EDT

La detección de MTU permite a EDT determinar automáticamente la unidad de transmisión máxima (MTU) al establecer una sesión. Al hacerlo, se evita la fragmentación de paquetes de EDT que podría provocar una degradación del rendimiento o un error al establecer una sesión.

## Requisitos

- Versión 1912 mínima de VDA (se recomienda 2103 o una posterior)
- Aplicación Citrix Workspace
  - Windows: Versión 1912 o una posterior (se recomienda 2105 o una posterior)
  - Mac: Versión 2108 o una posterior
  - Android: Versión 21.5 o una posterior
- Citrix ADC:
  - 13.0.52.24
  - 12.1.56.22
- Fiabilidad de la sesión debe estar habilitada

Si utiliza plataformas de cliente o versiones que no admiten esta función, consulte [CTX231821](#) para obtener información detallada sobre la configuración de una unidad de transmisión máxima de EDT personalizada adecuada para su entorno.

**Importante:**

La detección de MTU no es compatible con ICA de multisequencia.

**Para habilitar o inhabilitar la detección de MTU en EDT en el VDA**

Establezca la siguiente clave de Registro:

- Clave: HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd
- Nombre del valor: MtuDiscovery
- Tipo de valor: DWORD
- Información del valor: 00000001

Reinicie el VDA y espere a que se registre.

Para inhabilitar la detección de MTU en EDT, elimine este valor del Registro y reinicie el VDA.

Esta configuración es aplicable a nivel de toda la máquina y afecta a todas las sesiones que se conectan desde un cliente compatible.

**Advertencia:**

Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

**Requisitos**

- Citrix Virtual Delivery Agent (VDA) 2003
- Aplicación Citrix Workspace 2002 para Windows
- Fiabilidad de la sesión habilitada. Para obtener más información sobre la fiabilidad de las sesiones, consulte [Configuración de la directiva de fiabilidad de la sesión](#)

**Problemas conocidos**

El transporte adaptable y EDT contienen estos problemas:

- La fragmentación de paquetes puede degradar el rendimiento o incluso impedir el inicio de sesiones. Puede ajustar la MTU en EDT para evitarlo. Utilice la detección de MTU o la solución temporal descrita en [CTX231821](#).
- Es posible que aparezca una pantalla gris o negra al iniciar una sesión desde un cliente Windows si la detección de MTU está habilitada. Para solucionar este problema, actualice la aplicación Workspace para Windows a la versión 2105 o a una posterior o a la versión 1912 CU4 o a una posterior.
- Es posible que no se pueda recurrir a TCP en clientes Linux y Android al conectarse a través de Citrix Gateway o Citrix Gateway Service. Esto ocurre cuando la negociación de EDT entre el cliente y la puerta de enlace es correcta, y la negociación de EDT entre la puerta de enlace y el VDA falla. Para solucionar este problema, actualice la aplicación Workspace para Linux a la versión 2104 o a una posterior y la aplicación Workspace para Android a la versión 21.5 o a una posterior.
- Las rutas de red asimétricas pueden provocar que la detección de MTU falle en las conexiones que no pasan por Citrix Gateway o Citrix Gateway Service. Para solucionar este problema, actualice la versión del VDA a la 2103 o a una posterior. [CVADHELP-16654]
- Al utilizar Citrix Gateway o Citrix Gateway Service, las rutas de red asimétricas pueden provocar un error en la detección de MTU. Esto se debe a un problema en Gateway que provoca que la parte Don't Fragment (DF) del encabezado de los paquetes EDT no se propague. Todavía no hay una solución para este problema. [CGOP-18438]
- La detección de MTU puede fallar para los usuarios que se conectan a través de una red DS-Lite. Algunos módems no respetan la parte DF cuando el procesamiento de paquetes está habilitado, lo que impide que la detección de MTU detecte la fragmentación. En esta situación, estas son las opciones disponibles:
  - Inhabilitar el procesamiento de paquetes en el módem del usuario.
  - Inhabilitar la detección de MTU y utilizar una MTU codificada como se describe en [CTX231821](#).
  - Inhabilitar el transporte adaptable para obligar a las sesiones a utilizar TCP. Si solo se ve afectado un subconjunto de usuarios, considere inhabilitarlo en el lado del cliente para que otros usuarios puedan seguir utilizando EDT.

## Solucionar problemas

Para solucionar problemas relacionados con el transporte adaptable y EDT, sugerimos lo siguiente:

1. Revise exhaustivamente y valide los [requisitos](#), las [consideraciones](#) y los [problemas conocidos](#).
2. Compruebe si hay directivas de Citrix en Studio o GPO que sobrescriben la configuración de **HDX Adaptive Transport** deseada.

3. Compruebe si hay parámetros en el cliente que sobrescriben la configuración de HDX Adaptive Transport deseada. Puede ser una preferencia de GPO, un parámetro configurado mediante la plantilla administrativa opcional de la aplicación Workspace o una configuración manual del parámetro **HDXoverUDP** del Registro o del archivo de configuración del cliente.
4. En máquinas VDA con multisesión, compruebe que las escuchas UDP estén activas. Abra un símbolo del sistema en la máquina VDA y ejecute `netstat -a -p udp`. Para obtener más información, consulte [Cómo confirmar el protocolo HDX Enlightened Data Transport](#).
5. Inicie una sesión directa internamente, omita Citrix Gateway y compruebe el protocolo que se está usando. Si la sesión utiliza EDT, el VDA está listo para usar EDT para conexiones externas a través de Citrix Gateway.
6. Si EDT funciona para conexiones internas directas y no para sesiones que pasan por Citrix Gateway:
  - Compruebe que la fiabilidad de la sesión esté habilitada
  - Compruebe que la puerta de enlace tenga habilitado DTLS
7. Compruebe si se han configurado las reglas de firewall adecuadas tanto en los firewalls de la red como en los firewalls activos en las máquinas VDA.
8. Compruebe si las conexiones de sus usuarios requieren una MTU no estándar. Las conexiones con una MTU efectiva inferior a 1500 bytes provocan la fragmentación de paquetes EDT, lo que a su vez puede afectar al rendimiento o incluso impedir el inicio de sesiones. Este problema es común cuando se utilizan VPN, algunos puntos de acceso Wi-Fi y redes móviles, como 4G y 5G. Para obtener información sobre cómo solucionar este problema, consulte la sección [Detección de MTU](#).

## Interoperabilidad con Citrix SD-WAN

La optimización de WAN de Citrix SD-WAN (WANOP) ofrece la compresión por tokens entre sesiones (desduplicación de datos), incluido el almacenamiento en caché de vídeo basado en URL, lo que reduce significativamente el ancho de banda. Dicha reducción se lleva a cabo si dos o más personas ubicadas en la oficina miran el mismo vídeo obtenido en el cliente, o si transfieren o imprimen partes grandes del mismo archivo o documento. Además, al ejecutar los procesos de reducción de datos ICA y compresión de trabajos de impresión en el dispositivo de la sucursal, WANOP ofrece la descarga de la CPU del servidor VDA y permite una mayor escalabilidad del servidor de Citrix Virtual Apps and Desktops.

Por ahora, SD-WAN WANOP no admite EDT. Sin embargo, no es necesario inhabilitar el transporte adaptable si SD-WAN WANOP se utiliza. Cuando un usuario inicia una sesión que pasa por un dispositivo SD-WAN con WANOP habilitado, configura automáticamente la sesión para que use TCP como protocolo de transporte. Las sesiones sin WANOP siguen utilizando EDT siempre que sea posible.

## Canales virtuales ICA de Citrix

March 10, 2022

### Advertencia

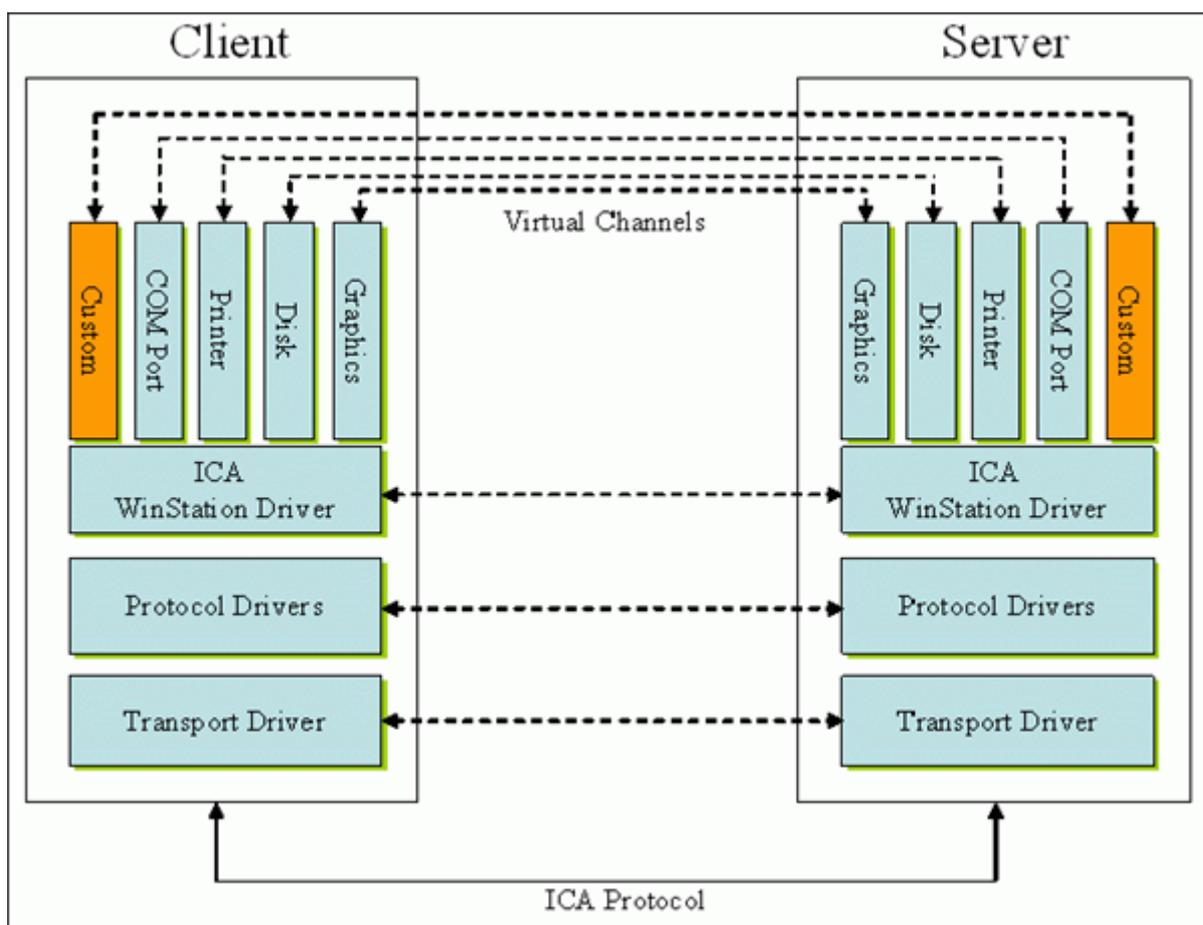
Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

### ¿Qué son los canales virtuales ICA?

Una gran parte de la funcionalidad y la comunicación entre la aplicación Citrix Workspace y los servidores de Citrix Virtual Apps and Desktops se produce a través de canales virtuales. Los canales virtuales son una parte necesaria de la experiencia informática remota de los servidores de Citrix Virtual Apps and Desktops. Los canales virtuales se utilizan en los siguientes aspectos:

- Audio
- Puertos COM
- Discos
- Gráficos
- Puertos LPT
- Impresoras
- Tarjetas inteligentes
- Canales virtuales personalizados de terceros
- Vídeo

A veces se publican nuevos canales virtuales con nuevas versiones de los servidores de Citrix Virtual Apps and Desktops y de los productos de la aplicación Citrix Workspace para ofrecer más funcionalidades.



Un canal virtual es un controlador virtual del lado del cliente que se comunica con una aplicación del lado del servidor. Citrix Virtual Apps and Desktops ya contiene varios canales virtuales. Estos están diseñados para que los clientes y los proveedores externos puedan crear sus propios canales virtuales mediante uno de los kits de desarrollo de software (SDK) que se proporcionan.

Los canales virtuales ofrecen una forma segura de realizar varias tareas. Por ejemplo, una aplicación que se ejecuta en un servidor de Citrix Virtual Apps y se comunica con un dispositivo del lado del cliente o una aplicación que se comunica con el entorno del lado del cliente.

En el lado del cliente, los canales virtuales corresponden a los controladores virtuales. Cada controlador virtual ofrece una función específica. Algunos son necesarios para un funcionamiento normal y otros son opcionales. Los controladores virtuales operan al nivel del protocolo de la capa de presentación. Puede haber varios protocolos activos en un momento dado mediante la multiplexación de canales que proporciona la capa de protocolos de Windows Station (WinStation).

Las siguientes funciones se encuentran en el valor de Registro VirtualDriver de esta ruta de acceso del Registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0`

O bien:

HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\  
Configuration\Advanced\Modules\ICA 3.0 (para 64 bits)

- Thinwire 3.0 (obligatoria)
- ClientDrive
- ClientPrinterQueue
- ClientPrinterPort
- Portapapeles
- ClientComm
- ClientAudio
- LicenseHandler (obligatoria)
- TWI (obligatoria)
- SmartCard
- ICACTL (obligatoria)
- SSPI
- TwainRdr
- UserEXperience
- Vd3d

**Nota:**

Puede inhabilitar funcionalidades específicas del cliente si quita uno o varios de estos valores de la clave de Registro. Por ejemplo, si quiere quitar el Portapapeles del cliente, quite la palabra **Clipboard**.

Esta lista contiene los archivos de controlador virtual del cliente y sus funciones respectivas. Citrix Virtual Apps y la aplicación Citrix Workspace para Windows los utilizan. Tienen forma de bibliotecas de vínculos dinámicos (modo usuario) y no de controladores de Windows (modo kernel), excepto la función USB genérico tal y como se describe en Canal virtual USB genérico.

- vd3dn.dll: Canal virtual Direct3D utilizado para la redirección de composiciones de escritorio.
- vdcamN.dll: Audio bidireccional.
- vdcdm30n.dll: Asignación de unidades del cliente.
- vdcom30N.dll: Asignación de puertos COM del cliente.
- vdcpm30N.dll: Asignación de impresoras del cliente.
- vdctlN.dll: Canal de controles ICA.
- vddvc0n.dll: Canal virtual dinámico.
- vdeuemn.dll: Supervisión de la experiencia de usuario final.
- vdgusbn.dll: Canal virtual USB genérico.
- vdkbhook.dll: Paso de clave transparente.
- vdlfpn.dll: Canal de visualización Framehawk por transporte similar al protocolo UDP.

- vdmn.dll: Compatibilidad multimedia.
- vdmvc.dll: Canal virtual de Mobile Receiver.
- vdmchn.dll: Funcionalidad multitoque.
- vdscardn.dll: Compatibilidad con tarjetas inteligentes.
- vdsens.dll: Canal virtual de sensores.
- vdspl30n.dll: Protocolo UDP del cliente.
- vdsspin.dll: Kerberos.
- vdtuin.dll: Interfaz de usuario transparente.
- vdtw30n.dll: Cliente Thinwire.
- vdtwin.dll: Conexión directa.
- vdtwn.dll: TWAIN.

Algunos canales virtuales se compilan en otros archivos. Por ejemplo, la asignación de Clipboard está disponible en wfica32.exe.

### **Compatibilidad con 64 bits**

La aplicación Citrix Workspace para Windows es compatible con 64 bits. Al igual que con la mayoría de los binarios compilados para 32 bits, estos archivos de cliente tienen equivalentes compilados de 64 bits:

- brapi64.dll
- confmgr.dll
- ctxlogging.dll
- ctxmui.dll
- icaconf.exe
- icaconfs.dll
- icafile.dll
- pnipcn64.dll
- pnsson.dll
- ssoncom.exe
- ssonstub.dll
- vdkbhook64.dll

### **Canal virtual USB genérico**

La implementación del canal virtual USB genérico utiliza dos controladores en modo kernel junto con el controlador de canal virtual vdgusbn.dll:

- ctxusbm.sys
- ctxusbr.sys

## Cómo funcionan los canales virtuales ICA

Los canales virtuales se cargan de varias maneras. El Shell (WfShell para el servidor y PicaShell para la estación de trabajo) carga algunos canales virtuales. Algunos canales virtuales se alojan como servicios de Windows.

Módulos de canal virtual cargados por el Shell. Por ejemplo:

- EUEM
- TWAIN
- Portapapeles
- Contenido multimedia
- Uso compartido de sesiones integradas
- Zona horaria

Algunos se cargan en modo kernel. Por ejemplo:

- CtxDvcs.sys: Canal virtual dinámico.
- Icausbbs.sys: Redirección de USB genérico.
- Picadm.sys: Asignación de unidades del cliente.
- Picaser.sys: Redirección de puertos COM.
- Picapar.sys: Redirección de puertos LPT.

## Canal virtual de gráficos en el lado del servidor

A partir de XenApp 7.0 y XenDesktop 7.0, `ctxgfx.exe` aloja el canal virtual de gráficos para las sesiones basadas en estaciones de trabajo y servidores Terminal Server. `Ctxgfx` aloja módulos de plataformas específicas que interactúan con el controlador correspondiente (`Icardd.dll` para RDSH, y `vdod.dll` y `vidd.dll` para las estaciones de trabajo).

Para las implementaciones de XenDesktop 3D Pro, se instala un controlador de gráficos OEM para la GPU correspondiente del VDA. `Ctxgfx` carga módulos adaptadores especializados para interactuar con el controlador de gráficos OEM.

## Alojar canales especializados en servicios de Windows

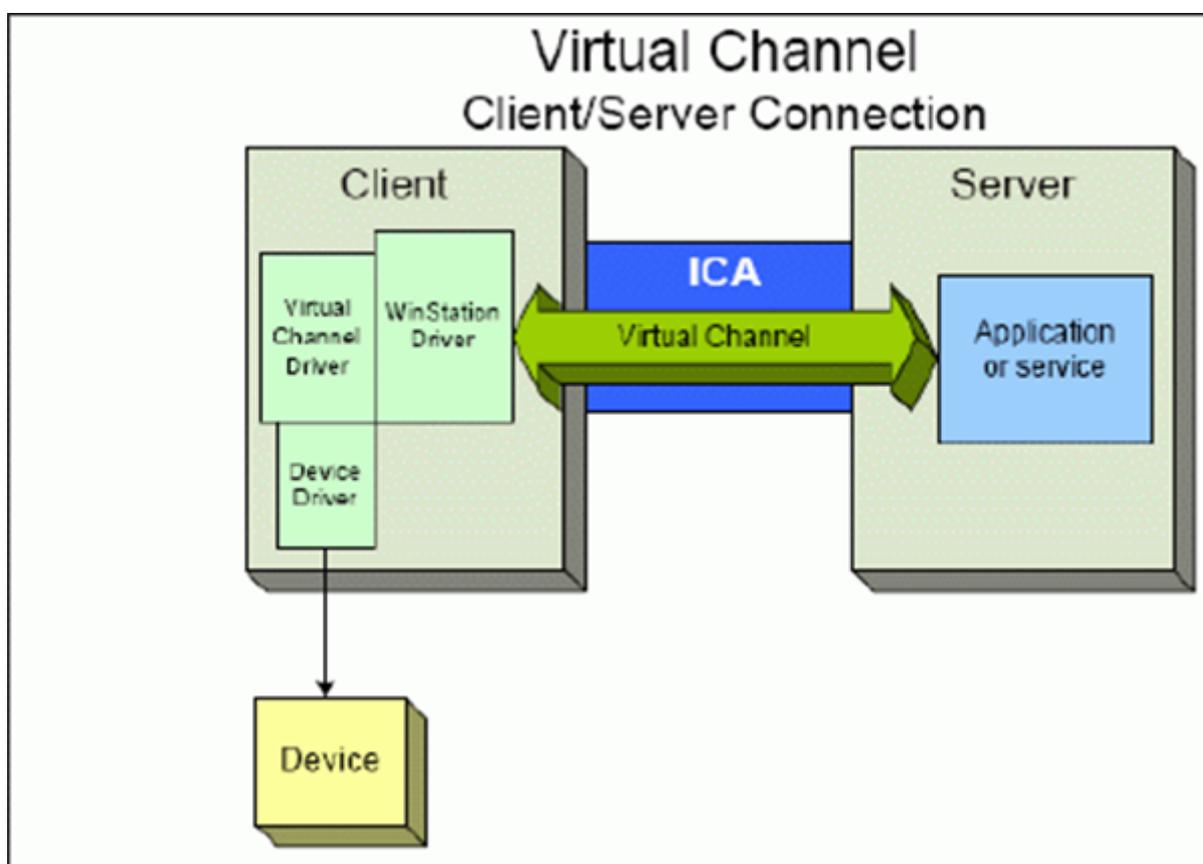
En los servidores de Citrix Virtual Apps and Desktops, varios canales se alojan como servicios de Windows. Este alojamiento ofrece una semántica del tipo “uno a varios” para múltiples aplicaciones en una sesión y múltiples sesiones en el servidor. He aquí algunos ejemplos de tales servicios:

- Citrix Device Redirector Service
- Citrix Dynamic Virtual Channel Service

- Citrix End User Experience Monitoring Service
- Citrix Location and Sensor Virtual Channel Service
- Citrix MultiTouch Redirection Service
- Citrix Print Manager Service
- Citrix Smartcard Service
- Citrix Audio Redirection Service (solo para Citrix Virtual Desktops)

El canal virtual de audio de Citrix Virtual Apps se aloja mediante el Servicio de Audio de Windows.

En el lado del servidor, todos los canales virtuales del cliente se enrutan a través del controlador de WinStation: Wdica.sys. En el lado del cliente, el controlador de WinStation correspondiente, integrado en wfica32.exe, sondea los canales virtuales del cliente. Esta imagen ilustra la conexión servidor-cliente del canal virtual.



He aquí un resumen con un intercambio de datos cliente-servidor mediante un canal virtual.

1. El cliente se conecta al servidor de Citrix Virtual Apps and Desktops. El cliente pasa información al servidor sobre los canales virtuales que admite.
2. La aplicación del lado del servidor se inicia, obtiene un identificador para el canal virtual y, de forma opcional, envía consultas para obtener más información sobre el canal.
3. El controlador virtual del cliente y la aplicación del lado del servidor pasan datos mediante estos

dos métodos:

- Si la aplicación del servidor tiene datos para enviar al cliente, los datos se envían al cliente inmediatamente. Cuando el cliente recibe los datos, el controlador de WinStation desmultiplexa los datos del canal virtual de la secuencia ICA e inmediatamente los pasa al controlador virtual del cliente.
  - Si el controlador virtual del cliente tiene datos para enviar al servidor, los datos se envían la próxima vez que el controlador de WinStation lo sondee. Cuando el servidor recibe los datos, se ponen en cola hasta que la aplicación del canal virtual los lea. No hay forma de alertar a la aplicación del canal virtual del servidor de que los datos se han recibido.
4. Cuando se completa la aplicación del canal virtual del servidor, el canal virtual se cierra y se liberan los recursos asignados.

### Crear un canal virtual propio mediante Virtual Channel SDK

La creación de un canal virtual mediante Virtual Channel SDK requiere conocimientos intermedios de programación. Utilice este método para proporcionar una ruta principal de comunicación entre el cliente y el servidor. Por ejemplo, si implementa el uso de un dispositivo en el lado del cliente, como un escáner, que se utilizará con algún proceso de la sesión.

Notas:

- El Virtual Channel SDK requiere el SDK de WFAPI para escribir la parte del lado del servidor del canal virtual.
- Debido a la seguridad mejorada de Citrix Virtual Apps and Desktops y la aplicación Citrix Workspace para Windows, debe dar un paso más al instalar un canal virtual personalizado.

### Crear un canal virtual propio mediante ICA Client Object SDK

Crear un canal virtual con el objeto de cliente ICA (ICO) es más fácil que usar Virtual Channel SDK. Utilice el ICO mediante la creación de un objeto con nombre asignado en el programa con el método **CreateChannels**.

Importante:

Debido a la seguridad mejorada que llega con la versión 10.00 de Citrix Receiver para Windows y versiones posteriores (y las aplicaciones de Citrix Workspace para Windows), debe dar un paso más al crear un canal virtual ICO.

Para obtener más información, consulte [Client Object API Specification Programmer's Guide](#).

## **Funcionalidad de paso de canales virtuales**

La mayoría de los canales virtuales que Citrix proporciona funcionan sin modificar cuando se utiliza la aplicación Citrix Workspace para Windows en sesiones ICA (también conocidas como sesiones de paso). Hay ciertos aspectos a tener en cuenta al usar el cliente en saltos adicionales.

Las siguientes funciones operan de la misma manera tanto en saltos simples como en múltiples:

- Asignación de puertos COM del cliente
- Asignación de unidades del cliente
- Asignación de impresoras del cliente
- UDP del cliente
- Supervisión de la experiencia de usuario final
- USB genérico
- Kerberos
- Compatibilidad multimedia
- Compatibilidad con tarjetas inteligentes
- Paso de clave transparente
- TWAIN

Como la naturaleza inherente de la latencia y de factores como la compresión, la descompresión y el renderizado de cada salto, el rendimiento puede verse afectado con cada salto adicional que haga el cliente. Las zonas afectadas son:

- Audio bidireccional
- Transferencias de archivos
- Redirección de USB genérico
- Conexión directa
- Thinwire

### **Importante:**

De forma predeterminada, las unidades del cliente asignadas por una instancia del cliente que se ejecuta en una sesión de paso están restringidas a las unidades del cliente que se conecta.

## **Funcionalidad de paso de canales virtuales entre una sesión de Citrix Virtual Desktops y una sesión de Citrix Virtual Apps**

La mayoría de los canales virtuales proporcionados por Citrix funcionan sin modificar cuando se utiliza la aplicación Citrix Workspace para Windows en sesiones ICA (también conocidas como sesiones de paso) en un servidor de Citrix Virtual Desktops.

En concreto, en el servidor de Citrix Virtual Desktops, hay un enlace de VDA que ejecuta **pica-PassthruHook**. Este enlace hace que el cliente crea que se ejecuta en un servidor CPS y coloca al cliente en su modo tradicional de paso.

Se admiten los siguientes canales virtuales tradicionales y su funcionalidad:

- Cliente
- Asignación de puertos COM del cliente
- Asignación de unidades del cliente
- Asignación de impresoras del cliente
- USB genérico (limitado por rendimiento)
- Compatibilidad multimedia
- Compatibilidad con tarjetas inteligentes
- SSON
- Paso de clave transparente

## Seguridad y canales virtuales ICA

La seguridad es una parte importante de la planificación, el desarrollo y la implementación de canales virtuales. Hay varias referencias a áreas específicas de seguridad en este documento.

### Prácticas recomendadas

Abra los canales virtuales cuando **se conecte** y **se vuelva a conectar**. Cierre los canales virtuales cuando cierre la sesión y **se desconecte**.

Tenga en cuenta las siguientes pautas al crear scripts que utilizan funciones de los canales virtuales.

#### Asignar nombres a los canales virtuales:

Puede crear hasta 32 canales virtuales. 17 de los 32 canales están reservados para fines especiales.

- Los nombres de los canales virtuales no deben tener más de 7 caracteres.
- Los 3 primeros caracteres están reservados para el nombre del proveedor, y los 4 siguientes, para el tipo de canal. Por ejemplo, **CTXAUD** representa el canal virtual de audio de Citrix.

Los canales virtuales tienen un nombre ASCII de 7 caracteres (o menos). En algunas versiones anteriores del protocolo ICA, los canales virtuales estaban numerados. Ahora, los números se asignan de forma dinámica en función del nombre ASCII, lo que facilita la implementación. Los usuarios que estén desarrollando código de un canal virtual para uso interno solo pueden usar nombres de 7 caracteres que coincidan con otros canales virtuales existentes. Utilice solamente números y caracteres ASCII en mayúsculas y minúsculas. Siga la convención de nomenclatura existente al agregar canales

virtuales propios. Hay varios canales predefinidos. Los canales predefinidos comienzan con el identificador OEM “CTX” y son de uso exclusivo de Citrix.

**Compatibilidad con doble salto:**

---

Canal virtual	¿Compatible con doble salto?
Audio	No
Redirección de contenido de explorador web	No
CDM	Sí
CEIP	No
Portapapeles	Sí
Continuum (MRVC)	No
Control VC	Sí
Redirección de vídeo HTML5 (v1)	Sí
Teclado, puntero	Sí
Multitoque	No
NSAPVC	No
Impresión	Sí
SensVC	No
Tarjeta inteligente	Sí
TWAIN	Sí
USB VC	Sí
Dispositivos WAYCOM-K2M con USB VC	Sí
Compresión de vídeo de cámara web	Sí
Redirección de Windows Media	Sí

---

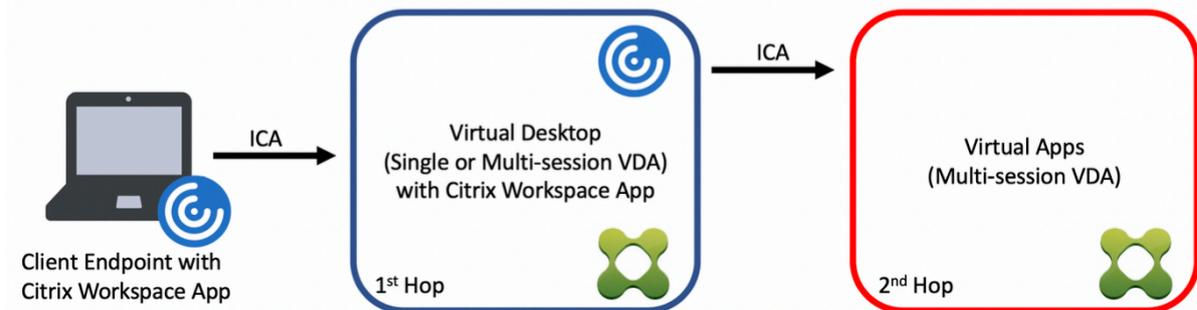
**También puede consultar**

- [ICA Virtual Channel SDK](#)
- [Citrix Developer Network](#) es el centro de todos los recursos y debates técnicos relacionados con el uso los SDK de Citrix. En esta red, puede encontrar acceso a los SDK, código y scripts de ejemplo, extensiones, plug-ins y documentación de los SDK. También se encuentran los foros de Citrix Developer Network, donde se llevan a cabo debates técnicos sobre cada SDK de Citrix.

## Doble salto en Citrix Virtual Apps and Desktops

May 24, 2024

En el contexto de una sesión de cliente de Citrix, el término “doble salto” se refiere a una sesión de Citrix Virtual Apps activa dentro de una sesión de Citrix Virtual Desktops. El siguiente diagrama ilustra un doble salto.



En el caso de un salto doble, cuando el usuario se conecta a una sesión de Citrix Virtual Desktops, en un VDA de SO de sesión única (conocido como VDI) o en un VDA de SO multisesión (conocido como escritorio publicado), se considera el primer salto. Una vez que el usuario se haya conectado al escritorio virtual, puede iniciar una sesión de Citrix Virtual Apps. Eso se considera el segundo salto.

Puede utilizar un modelo de implementación de doble salto para disponer de varios casos de uso. Un ejemplo común es el caso en el que diferentes entidades administran los entornos de Citrix Virtual Desktops y Citrix Virtual Apps. Este método también puede ser eficaz para resolver problemas de compatibilidad de aplicaciones.

### Requisitos del sistema

Todas las ediciones de Citrix Virtual Apps y Citrix Virtual Desktops, incluido Citrix Cloud Services, admiten el doble salto.

El primer salto debe utilizar una versión compatible del VDA de SO de sesión única o multisesión y de la aplicación Citrix Workspace. El segundo salto debe utilizar una versión compatible del VDA de SO multisesión. Consulte la página [Tabla de productos](#) para ver las versiones compatibles.

Para obtener un rendimiento y una compatibilidad óptimos, Citrix recomienda utilizar un cliente Citrix de la misma versión o de una más reciente que las versiones de VDA que se utilicen.

En entornos en los que el primer salto implica una solución de escritorios virtuales de terceros (que no sea de Citrix) junto con una sesión de Citrix Virtual Apps, la compatibilidad se limita al entorno de Citrix Virtual Apps. En caso de que surja algún problema relacionado con el escritorio virtual de terceros, como, entre otros, la compatibilidad de la aplicación Citrix Workspace, la redirección de

dispositivos de hardware o el rendimiento de la sesión, Citrix puede proporcionar asistencia técnica limitada. Es posible que se necesite Citrix Virtual Desktops en el primer salto como parte de la solución de problemas.

## **Aspectos a tener en cuenta en las implementaciones para HDX en doble salto**

En general, cada sesión en un doble salto es única, y las funciones cliente-servidor están limitadas a un salto específico. Esta sección incluye áreas que requieren una atención especial por parte de los administradores de Citrix. Citrix recomienda que los clientes realicen pruebas exhaustivas de las prestaciones de HDX necesarias para garantizar que la experiencia de usuario y el rendimiento sean adecuados para una configuración de entorno determinada.

### **Gráficos**

Utilice los parámetros gráficos predeterminados (codificación selectiva) en el primer y el segundo salto. En el caso de [HDX 3D Pro](#), Citrix recomienda encarecidamente que todas las aplicaciones que requieran aceleración gráfica se ejecuten localmente en el primer salto con los recursos de GPU adecuados que haya disponibles para el VDA.

### **Latencia**

La latencia de extremo a extremo puede afectar a la experiencia general del usuario. Tenga en cuenta la latencia adicional entre el primer y el segundo salto. Esto es especialmente importante con la redirección de dispositivos de hardware.

### **Contenido multimedia**

La representación de contenido de audio y vídeo en el lado del servidor (en sesión) funciona mejor en el primer salto. La reproducción de vídeo en el segundo salto requiere decodificación y recodificación en el primer salto, lo que aumenta el ancho de banda y el consumo de recursos de hardware. El contenido de audio y vídeo debe limitarse al primer salto siempre que sea posible.

### **Redirección de dispositivos USB**

HDX incluye modos de redirección genéricos y optimizados para admitir una amplia gama de tipos de dispositivos USB. Preste especial atención al modo que se utilice en cada salto y sírvase de la tabla siguiente como referencia para obtener resultados óptimos. Para obtener más información sobre los modos de redirección genéricos y optimizados, consulte [Dispositivos USB genéricos](#).

Primer salto (VDI o escritorio publicado)	Segundo salto (Virtual Apps)	Notas sobre la compatibilidad
Optimizado	Optimizado	Recomendado (según la compatibilidad del dispositivo). Por ejemplo: almacenamiento masivo USB, escáneres TWAIN, cámara web, audio.
Genérico	Genérico	Para dispositivos donde la opción optimizada no está disponible.
Genérico	Optimizado	Aunque técnicamente es posible, se recomienda utilizar el modo optimizado en ambos saltos cuando la compatibilidad del dispositivo lo permita.
Optimizado	Genérico	No se admite

**Nota:**

Debido a la elevada actividad inherente de los protocolos USB, el rendimiento puede disminuir entre saltos. La funcionalidad y los resultados varían según los requisitos específicos de los dispositivos y las aplicaciones. Las pruebas de validación son muy recomendables en todos los casos de redirección de dispositivos y son especialmente importantes en casos de doble salto.

**Excepciones de compatibilidad**

Las sesiones de doble salto admiten la mayoría de las funciones y prestaciones HDX, excepto las siguientes:

- [Redirección de contenido de explorador web](#)
- [Acceso a aplicaciones locales](#)
- [RealTime Optimization Pack para Skype Empresarial](#)
- [Optimización para Microsoft Teams](#)

## Instalación y configuración

May 5, 2023

Revise los artículos a los que se hace referencia para iniciar cada paso de implementación. De este modo, sabrá lo que verá y deberá especificar durante la implementación.

Use la siguiente secuencia para implementar Citrix Virtual Apps and Desktops.

### Preparar

Consulte el artículo [Antes de instalar](#), y realice todas las tareas necesarias.

- Se explica dónde encontrar información sobre conceptos, funciones, diferencias de versiones anteriores, requisitos del sistema y bases de datos.
- Consideraciones al decidir dónde instalar los componentes principales.
- Permisos y requisitos de Active Directory.
- Información sobre los instaladores, las herramientas y las interfaces disponibles.

### Instalar componentes principales

Instale Delivery Controller, Citrix Studio, Citrix Director, el servidor de licencias y Citrix StoreFront. Para obtener más información, consulte [Instalación de componentes principales](#) o [Instalación desde la línea de comandos](#).

### Crear un sitio

Después de instalar los componentes principales e iniciar Studio, se le dirigirá automáticamente a [crear un sitio](#).

### Instalar uno o varios agentes VDA (Virtual Delivery Agent)

Instale un VDA en una máquina que ejecute un sistema operativo Windows, ya sea en una imagen maestra o directamente en cada máquina. Consulte [Instalar agentes VDA](#) o [Instalación desde la línea de comandos](#). Se ofrecen [scripts](#) de ejemplo si quiere instalar agentes VDA a través de Active Directory.

Para máquinas con un sistema operativo Linux, siga las instrucciones que aparecen en [Linux Virtual Delivery Agent](#).

Para implementaciones de acceso con Remote PC, instale un VDA para SO de escritorio en cada PC de la oficina. Si necesita solamente los servicios principales del agente VDA, utilice el programa de instalación independiente VDAWorkstationCoreSetup.exe y sus métodos existentes de distribución electrónica de software (ESD). ([Antes de la instalación](#) contiene información completa sobre los programas de instalación de VDA disponibles.)

## Instalar componentes opcionales

Si va a usar el servidor de Citrix Universal Print Server, instale su componente de servidor correspondiente en los servidores de impresión. Consulte [Instalar componentes principales](#) o [Instalación desde la línea de comandos](#).

Para permitir que StoreFront use opciones de autenticación tales como aserciones SAML, instale el [Servicio de autenticación federada de Citrix](#).

Para que los usuarios finales tengan un mayor control sobre sus cuentas de usuario, instale el [Autoservicio de restablecimiento de contraseñas](#).

Si lo prefiere, puede integrar otros componentes de Citrix en la implementación de Citrix Virtual Apps and Desktops.

- [Citrix Provisioning](#) es un componente optativo que aprovisiona máquinas transmitiendo por streaming una imagen maestra a los dispositivos de destino.
- [Citrix Gateway](#) es una solución de acceso seguro a aplicaciones, que ofrece a los administradores un control más preciso de las acciones y las directivas al nivel de aplicación, para proteger el acceso a las aplicaciones y los datos.
- [Citrix SD-WAN](#) es un conjunto de dispositivos que optimizan el rendimiento en WAN.

## Crear un catálogo de máquinas

Después de crear un sitio en Studio, se le dirigirá a [crear un catálogo de máquinas](#).

Un catálogo puede contener máquinas físicas o virtuales (VM). Las máquinas virtuales se pueden crear a partir de una imagen maestra. Si usa un hipervisor o un servicio de nube para proporcionar máquinas virtuales, primero debe crear una imagen maestra en ese host. A continuación, al crear el catálogo, debe especificar esa imagen, que se usará para crear máquinas virtuales.

## Crear un grupo de entrega

Después de crear el primer catálogo de máquinas en Studio, se le dirigirá a [crear un grupo de entrega](#).

Un grupo de entrega especifica los usuarios que pueden acceder a las máquinas de un catálogo de máquinas concreto y las aplicaciones disponibles para esos usuarios.

### **Crear un grupo de aplicaciones (optativo)**

Después de crear un grupo de entrega, si quiere puede [crear un grupo de aplicaciones](#). Puede crear grupos de aplicaciones para las aplicaciones compartidas entre varios grupos de entrega o que son utilizadas por un subconjunto de usuarios dentro de un grupo de entrega.

## **Antes de la instalación**

May 24, 2024

La implementación de Citrix Virtual Apps and Desktops comienza con la instalación de los siguientes componentes. Este proceso prepara la entrega de aplicaciones y escritorios a los usuarios dentro del firewall.

- Uno o varios Delivery Controllers
- Citrix Studio
- Citrix Director
- Citrix StoreFront
- Citrix License Server
- Uno o varios agentes VDA (Citrix Virtual Delivery Agent)
- Tecnologías y componentes optativos (como el Servidor Universal Print Server, el Servicio de autenticación federada, y el Autoservicio de restablecimiento de contraseñas)

Para los usuarios que estén fuera del firewall, instale y configure un componente adicional como, por ejemplo, Citrix Gateway. Para ver una introducción, consulte [Integrar Citrix Virtual Apps and Desktops con Citrix Gateway](#).

Puede usar el instalador de producto completo, incluido en el archivo ISO, para implementar muchos de los componentes y las tecnologías. También puede usar el instalador independiente de VDA para instalar los VDA. Todos los instaladores ofrecen interfaces gráficas y de línea de comandos. Consulte Instaladores.

Las ISO de producto contienen scripts de ejemplo para instalar, actualizar o quitar los agentes Virtual Delivery Agent de máquinas en Active Directory. También puede usar los scripts para administrar las imágenes maestras que utilicen Machine Creation Services (MCS) y Citrix Provisioning (antes Provisioning Services). Para obtener más información, consulte [Instalar agentes VDA mediante scripts](#).

[Puede obtener información sobre los cambios en los nombres de producto aquí.](#)

## Información que revisar antes de la instalación

- **Información técnica general:** Si no conoce el producto ni sus componentes.
- **Seguridad:** Al planificar el entorno de la implementación.
- **Problemas conocidos:** Los problemas que pueden aparecer en esta versión.
- **Bases de datos:** Si quiere obtener información sobre las bases de datos del sistema y cómo configurarlas. Durante la instalación de Controllers, puede instalar SQL Server Express para usarlo como la base de datos del sitio. Puede configurar la mayor parte de la información de la base de datos al crear un sitio, después de instalar los componentes principales.
- **Acceso con Remote PC:** Si implementa un entorno que permite a los usuarios acceder remotamente a sus equipos físicos en la oficina.
- **Conexiones y recursos:** Si usa un hipervisor o servicio de nube para alojar o aprovisionar máquinas virtuales para aplicaciones y escritorios. Puede configurar la primera conexión cuando cree un sitio, después de instalar los componentes principales. Configure el entorno de virtualización en cualquier momento anterior.
- **Microsoft System Center Configuration Manager:** Si usa Configuration Manager para administrar el acceso a las aplicaciones y los escritorios, o bien si usa la funcionalidad Wake on LAN con el acceso con Remote PC.

## Dónde instalar los componentes

Revise [Requisitos del sistema](#) para conocer las versiones, las plataformas y los sistemas operativos compatibles. Los requisitos previos de los componentes se instalan automáticamente; las excepciones se indican. Consulte la documentación de Citrix StoreFront y de Citrix License Server para saber cuáles son sus requisitos previos y sus plataformas compatibles.

Puede instalar los componentes principales en el mismo servidor o en servidores diferentes.

- Instalar los componentes principales en un servidor puede servir para evaluarlos o probarlos, o bien puede ser útil en implementaciones pequeñas de producción.
- Para permitir expansiones futuras, considere la posibilidad de instalar los componentes en servidores diferentes. Por ejemplo: instalar Studio en otra máquina que el servidor donde instaló el Controller permite administrar el sitio de forma remota.
- Para la mayoría de las implementaciones de producción, se recomienda instalar los componentes principales en servidores independientes.
- Para instalar un componente compatible en un SO Server Core (como un Delivery Controller), debe [usar la línea de comandos](#). Ese tipo de sistema operativo no ofrece una interfaz gráfica, por lo que debe instalar Studio y otras herramientas en otro lugar y apuntarlos al servidor del Controller.

Puede instalar un Delivery Controller y un agente VDA para SO multisesión en el mismo servidor. Inicie

el instalador y seleccione el Delivery Controller (además de cualquier otro componente principal que quiera instalar en esa máquina). A continuación, vuelva a iniciar el instalador y seleccione el agente Virtual Delivery Agent (VDA) para el SO multisesión.

Compruebe que cada sistema operativo tiene las actualizaciones más recientes. Por ejemplo, si no se instala la actualización KB2919355 de Windows, se detiene la instalación de un Controller o un VDA en Windows Server 2012 R2.

Compruebe que todas las máquinas tengan los relojes del sistema sincronizados. La infraestructura Kerberos que protege la comunicación entre las máquinas requiere sincronización.

Dispone de directrices de optimización para máquinas Windows 10 con SO de sesión única en [CTX216252](#).

Donde NO instalar los componentes:

- No instale componentes en controladores de dominio de Active Directory.
- No se admite la instalación de un Controller en un nodo de una instalación en clúster de SQL Server ni en una instalación reflejada de SQL Server ni en un servidor con Hyper-V.
- No instale Studio en servidores que ejecutan XenApp 6.5 Feature Pack 2 para Windows Server 2008 R2 o versiones anteriores de XenApp.

Si intenta instalar (o actualizar) un Windows VDA en un sistema operativo que no admite esta versión del producto, aparece un mensaje que le guiará un artículo Citrix que describe las opciones de que dispone.

## Permisos y requisitos de Active Directory

Debe ser un usuario de dominio y un administrador local en las máquinas donde instale los componentes.

Para usar el instalador independiente de VDA, debe tener privilegios administrativos elevados, o bien, debe usar **Ejecutar como administrador**.

Configure su dominio de Active Directory antes de comenzar la instalación.

- [Requisitos del sistema](#) ofrece una lista de los niveles funcionales disponibles de Active Directory. En [Active Directory](#), se ofrece información adicional.
- Debe tener al menos un controlador de dominio que ejecute los Servicios de dominio de Active Directory.
- No instale ningún componente de Citrix Virtual Apps and Desktops en un controlador de dominio.
- No use barras diagonales (/) cuando indique nombres de unidades organizativas en Studio.

La cuenta de usuario de Windows que se utilizó para instalar el servidor de licencias de Citrix se configura automáticamente como una cuenta de administrador total de Administración delegada en el servidor de licencias.

Para obtener más información:

- [Recomendaciones referentes a la seguridad](#)
- [Administración delegada](#)
- Documentación de Microsoft sobre la configuración de Active Directory

## **Instrucciones de instalación, procedimientos recomendados y aspectos a tener en cuenta**

### **Durante la instalación de un componente**

- Al instalar o actualizar componentes principales (Delivery Controller, Studio, servidor de licencias, Director, StoreFront) de la ISO del producto completo, si el instalador de Citrix detecta que en la máquina hay un reinicio pendiente de una instalación anterior de Windows, el instalador se detiene con el código 9 de salida/retorno. Se le pedirá que reinicie la máquina.

Esto no es un reinicio forzado de Citrix. Se debe a otros componentes que se han instalado anteriormente en la máquina. Si esto ocurre, reinicie la máquina y vuelva a iniciar el instalador de Citrix.

Cuando utilice la interfaz de línea de comandos, puede impedir la comprobación de reinicios pendientes. Para ello, incluya la opción `/no_pending_reboot_check` en el comando.

- En la mayoría de los casos, si un componente tiene requisitos previos, el instalador los instala, si no están presentes. Algunos requisitos previos pueden requerir un reinicio de la máquina.
- Al crear objetos antes, durante y después de la instalación, se recomienda especificar nombres exclusivos para cada objeto. Por ejemplo: proporcione nombres únicos a redes, grupos, catálogos y recursos.
- Si un componente no se instala correctamente, la instalación se detiene y aparece un mensaje de error. Los componentes que se instalaron correctamente se conservarán. No tendrá que volver a instalarlos.
- Los datos de Citrix Analytics se recopilan automáticamente cuando se instalan (o actualizan) componentes. De forma predeterminada, los datos se cargan en Citrix automáticamente cuando se completa la instalación. Además, cuando se instalan los componentes, se inscribe automáticamente en el programa Citrix Customer Experience Improvement Program (CEIP), que carga datos anónimos. Durante la instalación, también puede optar por participar en otras tecnologías de Citrix que recopilan diagnósticos para el mantenimiento y la solución

de problemas. Para obtener información acerca de estos programas, consulte [Citrix Insight Services](#).

- Los datos de Google Analytics se recopilan (y luego se cargan) automáticamente cuando se instala (o se actualiza) Studio. Después de instalar Studio, puede cambiar esta configuración con la clave del Registro `HKLM\Software\Citrix\DesktopStudio\GAEnabled`. El valor 1 habilita la recopilación y la carga, mientras que el valor 0 las inhabilita.
- Si falla la instalación del VDA, un analizador MSI revisa el registro MSI del fallo, y muestra el código de error exacto. El analizador sugiere un artículo de Citrix si se trata de un problema conocido. El analizador también recopila datos anónimos sobre el código del error. Estos datos se incluyen con otros recopilados por el programa CEIP. (Si finaliza la inscripción en CEIP, los datos del analizador MSI recopilados ya no se envían a Citrix.)

### **Durante la instalación de VDA**

La aplicación Citrix Workspace para Windows está disponible, pero no se instala de manera predeterminada cuando instala un VDA. Usted o sus usuarios pueden descargarse e instalar (y actualizar) la aplicación Citrix Workspace para Windows y otras aplicaciones Citrix Workspace desde el sitio web de Citrix. También puede poner esas aplicaciones Citrix Workspace a disposición de los usuarios desde el servidor de StoreFront. Consulte la documentación de StoreFront.

El servicio Print Spooler Service está habilitado de forma predeterminada en servidores Windows admitidos. Si inhabilita este servicio, no podrá instalar un VDA con SO Windows multisesión, así que compruebe que este servicio está habilitado antes de instalar un VDA.

La mayoría de las ediciones Windows admitidas ya tienen Microsoft Media Foundation instalado. Si la máquina donde quiere instalar el VDA no tiene instalado Media Foundation (como las ediciones N), algunas funciones multimedia no se instalarán y no funcionarán. Puede aceptar la limitación o finalizar la instalación del VDA y reiniciar la máquina más tarde, después de instalar Media Foundation. En la interfaz gráfica, se presenta esta opción en un mensaje. En la línea de comandos, puede usar `/no_mediafoundation_ack` para aceptar la limitación.

Si Media Foundation no está presente en la máquina del VDA, estas funciones multimedia no funcionarán:

- Redirección de Windows Media
- Redirección de vídeo HTML5
- Redirección de cámaras web de HDX RealTime

Al instalar el VDA, se crea automáticamente un grupo de usuarios locales llamado Usuarios de acceso directo. En un VDA para SO de sesión única, este grupo solo se aplica a las conexiones RDP. En un VDA para SO multisesión, este grupo se aplica a conexiones ICA y RDP.

El VDA debe tener direcciones válidas de Controller para comunicarse. De lo contrario, las sesiones no se pueden establecer. Puede especificar direcciones de Controller en el momento de instalar el VDA, o más adelante; pero recuerde que tiene que hacerlo.

## Herramientas de compatibilidad para VDA

Todos los instaladores de VDA incluyen un MSI de compatibilidad. Este MSI contiene herramientas de Citrix para verificar el rendimiento del VDA (es decir, su estado general y la calidad de las conexiones). Puede habilitar o inhabilitar la instalación de ese MSI desde la página **Componentes adicionales** de la interfaz gráfica del instalador de VDA. Desde la línea de comandos, puede inhabilitar la instalación con la opción `/exclude "Citrix Supportability Tools"`.

De forma predeterminada, el MSI de compatibilidad se instala en `c:\Program Files (x86)\Citrix\Supportability Tools\`. Puede cambiar esta ubicación desde la página **Componentes** de la interfaz gráfica del instalador de VDA o con la opción `/installdir` desde la línea de comandos. Tenga en cuenta que, si cambia esta ubicación, se cambiará la ubicación de todos los componentes de VDA instalados, no solo de las herramientas de compatibilidad.

Herramientas disponibles actualmente en el MSI de compatibilidad:

- Citrix Health Assistant: Para obtener información, consulte [CTX207624](#).
- Utilidad de limpieza del VDA: Para obtener información, consulte [CTX209255](#).

Si no instala las herramientas de compatibilidad cuando instala el VDA, el artículo de CTX contiene un enlace al paquete de descarga actual.

## Reinicios durante y después de la instalación de VDA

Se necesita reiniciar el sistema una vez al final de la instalación del VDA. Dicho reinicio se produce automáticamente de forma predeterminada.

Para minimizar la cantidad de reinicios necesarios durante la instalación de VDA:

- Compruebe que haya una versión compatible de .NET Framework instalada antes de iniciar la instalación del agente VDA.
- Para máquinas con SO Windows multisesión, instale y habilite los servicios de rol de Servicios de escritorio remoto (RDS) antes de instalar el agente VDA.

Si no instala esos requisitos previos antes de instalar el VDA:

- La máquina se reiniciará automáticamente después de instalar cada requisito previo si usa la interfaz gráfica o la interfaz de línea de comandos sin la opción `/noreboot`.
- Si utiliza la interfaz de línea de comandos con la opción `/noreboot`, deberá iniciar el proceso de reinicio.

Después de cada reinicio, la instalación del VDA continúa. (Si va a realizar la instalación desde la línea de comandos, puede evitar esto con la opción `/noresume`.)

**Nota:**

Se produce un reinicio al actualizar un VDA a la versión 7.17 o una versión posterior compatible. Ese reinicio no se puede evitar.

## Instaladores

### Instalador de producto completo

Con el instalador de producto completo, incluido en la imagen ISO del producto, puede:

- Instalar, actualizar o quitar los componentes principales: Delivery Controller, Studio, Director, StoreFront, License Server.
- Instalar o actualizar agentes VDA para Windows en sistemas operativos de servidor o de escritorio.
- Instalar el componente UpsServer de Universal Print Server en los servidores de impresión.
- Instalar el [Servicio de autenticación federada](#).
- Instalar el Autoservicio de restablecimiento de contraseñas.

Para entregar un escritorio desde un sistema operativo multisesión a un solo usuario (por ejemplo, para tareas de desarrollo web), use la interfaz de línea de comandos del instalador de producto completo. Para obtener más información, consulte [VDI de servidor](#).

### Instaladores independientes de VDA

Los instaladores independientes de VDA están disponibles en las páginas de descarga de Citrix. Los instaladores independientes de VDA son mucho más pequeños que la imagen ISO del producto completo. Se acomodan más fácilmente a las implementaciones que:

- Utilizan paquetes ESD (Electronic Software Distribution) que se almacenan provisionalmente o se copian localmente
- Tienen máquinas físicas
- Tienen oficinas remotas

De forma predeterminada, los archivos de los VDA autoextraíbles independientes se extraen en la carpeta `Temp`. Se necesita más espacio de disco en la máquina al extraer los archivos a la carpeta `Temp` que cuando se usa el instalador de producto completo. Sin embargo, los archivos que se extraen en la carpeta `Temp` se eliminan automáticamente una vez completada la instalación. También puede usar el comando `/extract` con una ruta de acceso absoluta.

Dispone de tres instaladores independientes de VDA para la descarga. (No están disponibles en los medios de instalación del producto completo.)

**VDA Server Setup.exe:**

Instala un VDA para SO multisesión. Admite todas las opciones del VDA para SO multisesión que están disponibles con el instalador de producto completo.

**VDA Workstation Setup.exe:**

Instala un VDA para SO de sesión única. Admite todas las opciones del VDA para SO de sesión única que están disponibles con el instalador de producto completo.

**VDA Workstation Core Setup.exe:**

Instala un VDA para SO de sesión única, optimizado para implementaciones de acceso con Remote PC o instalaciones básicas de VDI. El acceso con Remote PC usa máquinas físicas. Las instalaciones básicas de VDI son máquinas virtuales que no se utilizan como imagen maestra. Solo instala los servicios básicos necesarios para las conexiones de VDA de estas implementaciones. Por lo tanto, solo admite un subconjunto de las opciones que son válidas con el instalador de producto completo o [VDA Workstation Setup](#).

Este instalador no instala ni contiene los componentes utilizados para:

- App-V.
- Profile Management. Excluir Citrix Profile Management de la instalación afecta a las pantallas de Citrix Director. Para obtener más información, consulte [Instalar agentes VDA](#).
- Machine Identity Service.
- Personal vDisk o AppDisk.
- Citrix Supportability Tools.
- Citrix Files para Windows.
- Citrix Files para Outlook.

Este instalador [VDA Workstation Core Setup.exe](#) no instala ni contiene ninguna aplicación Citrix Workspace para Windows.

Utilizar [VDA Workstation Core Setup.exe](#) equivale a usar el instalador [VDA Workstation Setup](#) o del producto completo para instalar un VDA de SO de sesión única y una de las siguientes opciones:

- En la interfaz gráfica: Marcar la opción Acceso con Remote PC en la página **Entorno**.
- En la interfaz de línea de comandos: Especificar la opción `/remotepc`.
- En la interfaz de línea de comandos: Especificar `/components vda` y `/exclude "Citrix Personalization for App-V - VDA" "Personal vDisk" "Machine Identity Service" "Citrix User Profile Manager" "Citrix User Profile Manager WMI Plugin" "Citrix Supportability Tools" "Citrix Files for Windows"`.

Puede instalar los componentes y las funciones omitidas más adelante. Para ello, vuelva a ejecutar el instalador del producto. Esta acción instalará todos los componentes que falten.

El instalador `VDAWorkstationCoreSetup.exe` no instala automáticamente el MSI de redirección de contenido del explorador. (Todos los demás instaladores de VDA instalan ese MSI automáticamente). Para habilitar el uso de la función de redirección de contenido del explorador, instale `BCR_x64.msi` en la máquina después de instalar el VDA. El MSI se encuentra en la carpeta `x64 > Virtual Desktop Components` de los medios de instalación del producto completo.

## Códigos de retorno en la instalación de Citrix

El registro de instalación contiene el resultado de las instalaciones de los componentes en el formato de un código de retorno Citrix, no como un valor de Microsoft.

- 0 = Success (Operación correcta)
- 1 = Failed (Operación fallida)
- 2 = PartialSuccess (Operación parcialmente correcta)
- 3 = PartialSuccessAndRebootNeeded (Operación parcialmente correcta, reinicio necesario)
- 4 = FailureAndRebootNeeded (Fallo, reinicio necesario)
- 5 = UserCanceled (Operación cancelada por el usuario)
- 6 = MissingCommandLineArgument (Argumento de línea de comando que falta)
- 7 = NewerVersionFound (Versión más reciente encontrada)
- 8 = SuccessRebootNeeded (Se requiere reinicio)
- 9 = FileLockReboot (Reinicio de bloqueo de archivo)
- 10 = Aborted (Operación anulada)
- 11 = FailedMedia (Error de medios)
- 12 = FailedLicense (Error de licencia)
- 13 = FailedPrecheck (Error de comprobación previa)
- 14 = AbortedPendingRebootCheck (Comprobación anulada, pendiente de reinicio)
- -1 = Exit (Salir)

Por ejemplo: cuando se usan herramientas como Microsoft System Center Configuration Manager, una instalación por scripts de VDA puede aparecer como fallida cuando el registro de instalación contiene el código de retorno 3. Puede ocurrir cuando el instalador VDA espera un reinicio que usted debe iniciar (por ejemplo, después de una instalación de requisitos previos del rol de Servicios de Escritorio remoto en un servidor). Una instalación de VDA se considera correcta únicamente después de que todos los requisitos previos y los componentes seleccionados se hayan instalado y la máquina se reinicie después de la instalación.

Como alternativa, puede empaquetar la instalación en scripts CMD (que devuelven códigos de Microsoft) o cambiar los códigos de operación correcta en el paquete de Configuration Manager.

## Entornos de virtualización de Microsoft Azure Resource Manager

November 15, 2022

Siga estas instrucciones si usa Azure Resource Manager para aprovisionar máquinas virtuales en su entorno.

Familiarícese con lo siguiente:

- Azure Active Directory: <https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-create-new-tenant>
- Marco de consentimiento: <https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app>
- Entidad principal de servicio: <https://docs.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals>

### Limitaciones

Tenga en cuenta esta limitación al utilizar Azure Resource Manager:

- Este producto no admite VDA en un entorno de Windows Virtual Desktop (WVD). Para WVD, utilice el servicio Citrix Virtual Apps and Desktops o el servicio Citrix Virtual Apps and Desktops Standard para Azure.

### Aprovisionamiento a demanda de Azure

Cuando se usa MCS para crear catálogos de máquinas en Azure Resource Manager, la función de aprovisionamiento a demanda de Azure:

- Reduce los costes de almacenamiento
- Proporciona una creación de catálogos más rápida
- Proporciona unas operaciones de energía más rápidas para las máquinas virtuales (VM)

Para el administrador, el aprovisionamiento a demanda no conlleva diferencias entre los procedimientos de Studio para crear conexiones de host o catálogos de máquinas de Machine Creation Services. Las diferencias consisten en cómo y cuándo se crean y se administran los recursos en Azure, así como en la visibilidad de las VM en Azure Portal.

Cuando MCS creaba un catálogo, las máquinas virtuales se creaban en Azure durante el proceso de aprovisionamiento.

Con el aprovisionamiento a demanda de Azure, las máquinas virtuales se crean solo cuando Citrix Virtual Apps and Desktops inicia una acción de encendido, después de completarse el aprovisionamiento. Una máquina virtual solo aparece en Azure Portal cuando se está ejecutando. (En Studio, las máquinas virtuales aparecen tanto si se están ejecutando como si no.)

Cuando se crea un catálogo con Machine Creation Services, Azure Portal muestra los grupos de recursos, el grupo de seguridad de red, las cuentas de almacenamiento, las interfaces de red, las imágenes base y los discos de identidad. Azure Portal no muestra ninguna máquina virtual hasta que Citrix Virtual Apps and Desktops inicie una acción de encendido en ella. Entonces, el estado de la máquina virtual en Studio cambia a **encendido**.

- Para una máquina agrupada, el disco del sistema operativo y la caché de reescritura solo existen cuando existe la máquina virtual. Las máquinas agrupadas pueden resultar en un ahorro considerable del espacio de almacenamiento si apaga frecuentemente las máquinas (por ejemplo, fuera del horario de trabajo).
- Para una máquina dedicada, el disco del sistema operativo se crea la primera vez que se enciende la máquina virtual. Almacena datos hasta que se elimina la máquina.

Al iniciar una acción de apagado para una máquina virtual, Azure la elimina. Dicha máquina virtual ya no aparece en el portal de Azure. En Studio, el estado de la máquina virtual cambia a **apagado**.

### **Catálogos creados antes del aprovisionamiento a demanda**

Si dispone de catálogos de máquinas creados antes de que Citrix Virtual Apps and Desktops ofreciera soporte para el aprovisionamiento a demanda de Azure (mediados de 2017), las máquinas de esos catálogos aparecerán en el portal de Azure independientemente de si se están ejecutando o no. No se puede convertir esas máquinas virtuales en máquinas a demanda.

Para aprovechar las mejoras de rendimiento y los ahorros en costes de almacenamiento que ofrece el aprovisionamiento a demanda, cree catálogos con MCS.

### **Azure Managed Disks**

Azure Managed Disks es un sistema de almacenamiento de disco elástico que puede usar con los catálogos de máquinas creados por MCS, como alternativa al uso de cuentas de almacenamiento convencionales.

La función Managed Disks esconde la complejidad de crear y administrar cuentas de almacenamiento. Proporciona una solución simple y de alta disponibilidad para crear y administrar discos. Puede usar discos administrados como imágenes maestras, así como máquinas virtuales. El uso de discos administrados puede mejorar la creación de catálogos de máquinas y el tiempo de actualización. Para obtener más información, consulte [Learn about Managed Disks](#).

De manera predeterminada, un catálogo de máquinas usa discos administrados. Cuando cree un catálogo, puede anular este valor predeterminado.

### Usar discos administrados

Cuando se crea un catálogo de máquinas en Studio, la página **Imagen maestra** del asistente de creación de catálogos ofrece una lista de los discos administrados de Managed Disks, así como las VM y los discos VHD. No todas las regiones de Azure admiten la función Managed Disks para discos administrados. Los discos administrados aparecen en la lista de cualquier región que sea visible para la conexión de host del catálogo.

El tiempo de creación del catálogo se optimiza cuando la imagen y el catálogo se encuentran en la misma región.

La función Managed Disks no ofrece actualmente la función de copia de discos entre regiones de Azure. Al seleccionar una imagen en una región que no sea donde MCS aprovisionará el catálogo, la imagen se copia a un VHD en una cuenta de almacenamiento convencional de la región del catálogo. La imagen aparece en la región del catálogo y, a continuación, se convierte de nuevo en un disco administrado.

En la página **Almacenamiento y tipos de licencia** del asistente de creación de catálogos, puede seleccionar una casilla de verificación para usar cuentas de almacenamiento convencionales en lugar de discos administrados. Esta casilla de verificación no se puede seleccionar cuando se está aprovisionando en una región de Azure que no admite discos administrados.

### Crear una conexión a Azure Resource Manager

Consulte el artículo [Conexiones y recursos](#) para obtener información sobre los asistentes que crean conexiones. En los siguientes artículos, se describen datos específicos de las conexiones con Azure Resource Manager.

Consideraciones:

- Las entidades principales de servicio deben contar con el rol Colaborador para la suscripción.
- Al crear la primera conexión, Azure pide conceder a ese rol los permisos necesarios. Para conexiones futuras, aún deberá autenticarse, pero Azure recuerda su consentimiento anterior y no vuelve a mostrar la solicitud.
- Las cuentas utilizadas para la autenticación deben ser de un coadministrador de la suscripción.
- La cuenta utilizada para la autenticación debe ser un miembro del directorio de suscripción. Hay dos tipos de cuentas a tener en cuenta: cuenta profesional o educativa y cuenta personal de Microsoft. Consulte [CTX219211](#) para obtener más información.

- Puede utilizar una cuenta Microsoft tras agregarla como miembro del directorio de la suscripción. Sin embargo, puede haber complicaciones si al usuario se le concedió previamente acceso de invitado a uno de los recursos del directorio. En ese caso, hay una entrada de marcador de posición en el directorio que no le concederá los permisos necesarios, y se producirá un error.  
Para resolver el problema de acceso, quite los recursos del directorio y agréguelos de nuevo explícitamente. Sin embargo, use esta opción con cuidado, ya que tiene efectos no deseados para otros recursos a los que pueda acceder la cuenta.
- Hay un problema conocido que consiste en que algunas cuentas se detectan como invitados del directorio cuando en realidad son miembros. Las cuentas detectadas como invitados suelen darse con cuentas de directorio establecidas más antiguas. Solución temporal: Agregue una cuenta al directorio, con el valor correcto de membresía.
- Los grupos de recursos son simplemente contenedores de recursos, y contienen recursos de regiones distintas a su propia región. Los grupos de recursos pueden resultar confusos si espera que los recursos se muestren en la región de un grupo de recursos.
- Su red y subred deben ser lo suficientemente grandes como para alojar la cantidad de máquinas que necesita. El tamaño de la red requiere previsión, pero Microsoft le ayuda a especificar los valores correctos, con orientación sobre la capacidad del espacio de direcciones.

Existen dos métodos para establecer una conexión de host a Azure Resource Manager:

- Autenticarse en Azure Resource Manager para crear una entidad de servicio.
- Usar la información de una entidad de servicio anterior para conectarse a Azure Resource Manager

### **Autenticarse en Azure Resource Manager para crear una entidad de servicio**

Antes de comenzar, compruebe que:

- Tiene una cuenta de usuario en el arrendatario de su suscripción de Azure Active Directory.
- Con la cuenta de usuario de Azure AD, también se coadministra la suscripción de Azure que quiera usar para aprovisionar recursos.

En la instalación del sitio o en el asistente Agregar conexión y recursos:

1. En la página **Conexión**, seleccione el tipo de conexión **Microsoft Azure**. Luego, seleccione su entorno Azure Cloud.
2. En la página **Detalles de conexión**, escriba su ID de suscripción de Azure y un nombre para la conexión. El nombre de conexión puede contener de 1 a 64 caracteres, y no puede contener solo espacios en blanco ni caracteres no alfanuméricos. Después de introducir el ID de suscripción y el nombre de la conexión, se habilita el botón **Crear nueva**.

3. Escriba el nombre de usuario y la contraseña de la cuenta de Azure Active Directory.
4. Haga clic en **Iniciar sesión**.
5. Haga clic en **Aceptar** para conceder a Citrix Virtual Apps and Desktops los permisos mostrados. Citrix Virtual Apps and Desktops crea una entidad de servicio que le permite administrar los recursos de Azure Resource Manager en nombre del usuario especificado.
6. Después de hacer clic en **Aceptar**, volverá a la página **Conexión** en Studio. Tenga en cuenta que, cuando se autentica correctamente en Azure, los botones **Crear nueva** y **Usar existente** se reemplazan por **Conectado** y una marca de verificación verde indica una conexión establecida a la suscripción de Azure.
7. Indique las herramientas a utilizar para crear las máquinas virtuales y, a continuación, haga clic en **Siguiente**. No puede pasar de esta página del asistente hasta que se autentique correctamente en Azure y acepte conceder los permisos necesarios.
8. Los recursos constituyen la región y la red.
  - En la página **Región**, seleccione una región.
  - En la página **Red**, escriba un nombre de recurso de 1 a 64 caracteres para identificar más fácilmente la combinación de región y red en Studio. Un nombre de recurso no puede contener solo espacios en blanco ni caracteres no alfanuméricos.
  - Seleccione una combinación de red virtual y recurso de grupo. Dado que puede tener más de una red virtual con el mismo nombre, el emparejamiento del nombre de red con el grupo de recursos proporciona combinaciones únicas. Si selecciona una región de la página anterior que no tenga redes virtuales, volverá a esa página. Seleccione una región que tenga redes virtuales.
9. Complete el asistente.

### **Usar la información de una entidad de servicio anterior para conectarse a Azure Resource Manager**

Para crear manualmente una entidad de servicio, conéctese a su suscripción de Azure Resource Manager y use los cmdlets de PowerShell que se proporcionan en la siguiente sección.

Requisitos previos:

- **\$SubscriptionId:** `SubscriptionID` de Azure Resource Manager perteneciente a la suscripción donde quiere aprovisionar los agentes VDA.
- **\$AADUser:** Cuenta de usuario de Azure AD perteneciente al arrendatario de su suscripción de AD. Convierta al usuario `$AADUser` en el coadministrador de su suscripción.
- **\$ApplicationName:** Nombre de la aplicación que se va a crear en Azure AD.

- **\$ApplicationPassword:** Contraseña para la aplicación. Usará esta contraseña como secreto de la aplicación cuando cree la conexión de host.

Para crear una entidad de servicio:

1. Conéctese a su suscripción de Azure Resource Manager.

```
Login-AzureRmAccount
```

2. Seleccione la suscripción de Azure Resource Manager donde crear la entidad principal de servicio.

```
Select-AzureRmSubscription -SubscriptionID $SubscriptionId
```

3. Cree la aplicación en su arrendatario de AD.

```
$AzureADApplication = New-AzureRmADApplication -DisplayName  
$ApplicationName -HomePage "https://localhost/$ApplicationName"-  
IdentifierUri https://$ApplicationName -Password $ApplicationPassword
```

4. Cree una entidad principal de servicio.

```
New-AzureRmADServicePrincipal -ApplicationId $AzureADApplication.  
ApplicationId
```

5. Asigne un rol a la entidad principal de servicio.

```
New-AzureRmRoleAssignment -RoleDefinitionName Contributor -  
ServicePrincipalName $AzureADApplication.ApplicationId -scope  
/subscriptions/$SubscriptionId
```

6. En la ventana de resultados de la consola de PowerShell, anote el ID de aplicación (ApplicationId). Debe proporcionar ese ID cuando cree la conexión de host.

En la instalación del sitio o en el asistente Agregar conexión y recursos:

1. En la página **Conexión**, seleccione el tipo de conexión **Microsoft Azure** y su entorno de Azure.
2. En la página **Detalles de conexión**, escriba su ID de suscripción de Azure y un nombre para la conexión. El nombre de conexión puede contener de 1 a 64 caracteres, y no puede contener solo espacios en blanco ni caracteres no alfanuméricos.
3. Haga clic en **Usar existente**. Introduzca el ID de suscripción, el nombre de suscripción, la URL de autenticación, la URL de administración, el sufijo de almacenamiento, el ID de Active Directory o el ID del arrendatario, el ID de aplicación y el secreto de aplicación para la entidad de servicio existente. Después de introducir la información, se habilitará el botón **Aceptar**. Haga clic en **Aceptar**.

4. Indique las herramientas a utilizar para crear las máquinas virtuales y, a continuación, haga clic en **Siguiente**. Se utilizará la información que haya proporcionado sobre la entidad de servicio para conectarse a su suscripción de Azure (no puede pasar de esta página del asistente hasta que proporcione información válida para la opción Usar existente).
5. Los recursos constituyen la región y la red.
  - En la página **Región**, seleccione una región.
  - En la página **Red**, escriba un nombre de recursos de 1 a 64 caracteres para identificar más fácilmente la combinación de región y red en Studio. Un nombre de recurso no puede contener solo espacios en blanco ni caracteres no alfanuméricos.
  - Seleccione una combinación de red virtual y recurso de grupo. Dado que puede tener más de una red virtual con el mismo nombre, emparejar un nombre de red con un grupo de recursos ofrece combinaciones únicas. Si ha seleccionado una región que no tiene redes virtuales en la página anterior, debe volver a esa página y seleccionar una región que las tenga.
6. Complete el asistente.

## Crear un catálogo de máquinas con una imagen maestra de Azure Resource Manager

Esta información complementa a las instrucciones del artículo [Crear catálogos de máquinas](#).

Una imagen maestra es la plantilla que se usa para crear las máquinas virtuales en un catálogo de máquinas. Antes de crear el catálogo de máquinas, cree una imagen maestra en Azure Resource Manager. Para obtener información acerca de las imágenes maestras en general, consulte el artículo “Crear catálogos de máquinas”.

Al crear un catálogo de máquinas en Studio:

- Las páginas **Sistema operativo** y **Administración de máquinas** no contienen información específica de Azure. Siga las instrucciones que se indican en [Crear catálogos de máquinas](#).
- En la página **Imagen maestra**, seleccione un grupo de recursos. Vaya a los contenedores del disco duro virtual (VHD) de Azure que quiere usar como imagen maestra. El VHD debe tener instalado un VDA de Citrix. Si el VHD está asignado a una VM, la VM debe estar detenida.
- La página **Tipos de licencia y almacenamiento** solo aparecerá cuando se use una imagen maestra de Azure Resource Manager.

Seleccione un tipo de almacenamiento: Estándar o Premium. El tipo de almacenamiento influye en el tamaño de las máquinas que se ofrecen en la página **Máquinas virtuales** del asistente. Ambos tipos de almacenamiento realizan varias copias sincrónicas de los datos en un único centro de datos. Para obtener más información acerca de los tipos de almacenamiento y la replicación de almacenamiento de Azure, consulte lo siguiente:

- <https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction>
- <https://docs.microsoft.com/en-us/azure/virtual-machines/premium-storage-performance>
- <https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy>

Seleccione si utilizar las licencias locales (“on-premises”) existentes de Windows Server. Al utilizarlas con las imágenes locales (“on-premises”) existentes de Windows Server se usa Azure Hybrid Use Benefits (HUB). Encontrará más información detallada en <https://azure.microsoft.com/pricing/hybrid-use-benefit/>.

Usar un HUB reduce los costes de ejecutar máquinas virtuales en Azure a la ratio de procesamiento básica. Elimina el precio de licencias adicionales de Windows Server de la galería de Azure. Debe traer sus imágenes locales de Windows Server a Azure para usar HUB. No se admiten las imágenes de la galería de Azure. Las licencias locales de clientes Windows no se admiten en este momento.

Compruebe si las máquinas virtuales aprovisionadas están utilizando correctamente HUB. Ejecute el comando de PowerShell `Get-AzureRmVM -ResourceGroup MyResourceGroup -Name MyVM` y compruebe que el tipo de licencia es `Windows_Server`. Encontrará instrucciones adicionales en <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-benefit-licensing/>.

- En la página **Máquinas virtuales**, indique la cantidad de máquinas virtuales que quiere crear; debe especificar al menos una. Seleccione un tamaño de máquina. Después de crear un catálogo de máquinas, no se puede cambiar el tamaño de máquina. Si, más adelante, quiere otro tamaño, elimine el catálogo y cree uno que utilice la misma imagen maestra; especifique entonces el tamaño de máquina pertinente.

Los nombres de máquina virtual no pueden contener caracteres no ASCII o ni caracteres especiales.

- (Cuando se usa Machine Creation Services) En la página **Grupos de recursos**, elija si quiere crear grupos de recursos o usar los grupos existentes.

Si opta por crear grupos de recursos, haga clic en **Siguiente**.

Si decide utilizar los grupos de recursos existentes, seleccione esos grupos en la lista **Grupos de recursos de aprovisionamiento disponibles**. Debe seleccionar grupos suficientes para las máquinas que está creando en el catálogo. Studio muestra un mensaje si selecciona demasiado pocas. Puede seleccionar más del mínimo requerido de máquinas si va a agregar más máquinas al catálogo más tarde. No se puede agregar más grupos de recursos a un catálogo una vez creado el catálogo.

Para obtener más información, consulte Grupos de recursos de Azure ([#azure-resource-groups](#)).

- Las páginas **Tarjetas de red**, **Cuentas de equipo** y **Resumen** no contienen información específica de Azure. Siga las instrucciones que se indican en [Crear catálogos de máquinas](#).

Complete el asistente.

## Eliminar catálogos de máquinas

Cuando se elimina un catálogo de máquinas de Azure Resource Manager, las máquinas y los grupos de recursos asociados se eliminan de Azure, incluso aunque indique que deben conservarse.

## Grupos de recursos de Azure

Los grupos de recursos de aprovisionamiento de Azure ofrecen una manera de aprovisionar las VM que proporcionan escritorios y aplicaciones a los usuarios. Puede agregar grupos de recursos de Azure vacíos existentes cuando cree un catálogo de máquinas con MCS en Studio. También puede decidir que se creen otros grupos de recursos.

Para obtener información acerca de los grupos de recursos de Azure, consulte la documentación de Microsoft.

## Requisitos

- Cada grupo de recursos puede contener 240 máquinas virtuales como máximo. Debe haber suficientes grupos de recursos vacíos disponibles en la región donde está creando el catálogo. Si quiere utilizar los grupos de recursos existentes cuando cree un catálogo de máquinas, debe seleccionar suficientes grupos disponibles para admitir la cantidad de máquinas que se van a crear en el catálogo. Por ejemplo, si especifica 500 máquinas en el asistente de creación de catálogos, seleccione al menos tres grupos de recursos de aprovisionamiento disponibles.

No se puede agregar grupos de recursos a un catálogo de máquinas una vez creado el catálogo. Sin embargo, puede agregar los grupos de recursos suficientes como para admitir las máquinas que pueda agregar al catálogo más tarde.

- Cree grupos de recursos vacíos en la misma región que su conexión de host.
- Si quiere tener grupos de recursos nuevos para cada catálogo de MCS, configure la entidad de servicio Azure asociada a la conexión de host. Esta entidad debe tener permiso para crear y eliminar grupos de recursos. Si quiere que se utilicen los grupos de recursos vacíos existentes, la entidad de servicio Azure asociada a la conexión de host debe tener el permiso Colaborador en esos grupos de recursos vacíos.

- Cuando crea una conexión de host en Studio mediante la opción **Crear nuevo**, la entidad principal de servicio creada tiene los permisos de colaborador con el ámbito de suscripción. Como alternativa, puede usar la opción **Usar existente** para crear la conexión y proporcionar los datos de una entidad principal de servicio existente con el ámbito de suscripción. Utilice la opción **Crear nuevo** para crear la entidad principal de servicio en Studio. La entidad principal tiene los permisos necesarios para crear y eliminar grupos de recursos o aprovisionar a grupos de recursos vacíos existentes.
- Las entidades de servicio con ámbito restringido deben crearse mediante PowerShell. Además, cuando se usa a una entidad de servicio con ámbito restringido, debe usar PowerShell o el portal de Azure para crear grupos de recursos vacíos destinados a cada catálogo donde MCS aprovisionará las máquinas virtuales.

Si utiliza una entidad de servicio con un ámbito restringido para la conexión de host, pero el grupo de recursos de la imagen maestra no aparece en la página **Imagen maestra** del asistente de creación de catálogos, probablemente es porque esa entidad no tiene el permiso [Microsoft.Resources/subscriptions/resourceGroups/read](#) para poder mostrar el grupo de recursos de la imagen maestra. Cierre el asistente, actualice la entidad de servicio para concederle el permiso (consulte la entrada del blog para obtener instrucciones) y, a continuación, reinicie el asistente. En Azure, la actualización puede tardar hasta 10 minutos en aparecer en Studio.

### **Acerca de las entidades principales de servicio de Azure**

Para aprovisionar máquinas en Azure Resource Manager, se debe conceder acceso a un plug-in a su suscripción de Azure. Esos permisos se conceden a través de una entidad de servicio a la que se han asignado permisos a los recursos pertinentes de Azure. Una entidad principal de servicio cumple el mismo propósito básico que una cuenta de usuario. Proporciona al complemento una identidad de Azure Active Directory que proporciona credenciales para la autenticación y permisos para recursos de Azure. Al igual que las cuentas de usuario, las entidades principales de servicio se configuran mediante control de acceso por roles (RBAC).

Dependiendo de cómo se definan los permisos, las entidades principales de servicio se clasifican como:

- entidades principales de servicio con ámbito de suscripción, o bien
- entidades principales de servicio con ámbito restringido

**Entidades principales de servicio con ámbito de suscripción** Las entidades principales de servicio con ámbito de suscripción tienen *permisos de colaborador* en todos los recursos de la suscripción, lo que facilita su creación y administración. Citrix Studio automatiza el proceso de creación

de entidades principales de servicio con ámbito de suscripción, o se pueden crear manualmente en PowerShell. Estas entidades principales permiten a Azure Resource Manager Plugin crear grupos de recursos de Azure y automatizar completamente la administración de recursos. La desventaja es que el complemento tiene permisos para recursos de la suscripción que no están relacionados con los recursos que dicho complemento tiene la tarea de administrar.

El uso del *rol colaborador* permite al complemento crear, eliminar, leer y escribir todos los recursos de la suscripción. Los permisos no se extienden a los objetos de Azure Active Directory ni se permite a las entidades principales de servicio con ámbito de suscripción conceder acceso a los recursos a otros usuarios o entidades principales de servicio.

**Entidades principales de servicio con ámbito restringido** Las entidades principales de servicio con ámbito restringido permiten a Azure Resource Manager Plugin acceder a un conjunto limitado de recursos definidos por usted. Azure requiere permisos de ámbito de suscripción para crear grupos de recursos. El complemento no puede crear grupos de recursos cuando se utilizan entidades principales de servicio con ámbito restringido. Además de las entidades principales de servicio, debe proporcionar una agrupación de grupos de recursos para cada catálogo en el que se van a aprovisionar las máquinas.

Citrix Studio no admite la creación de catálogos o entidades principales de servicio con ámbito restringido. Ambas tareas deben realizarse con PowerShell. Sin embargo, una vez creado un catálogo, se puede administrar como cualquier otro catálogo de Studio, incluidas la agregación y eliminación de máquinas. Si en algún momento desea utilizar una entidad principal de servicio con ámbito restringido existente con una nueva agrupación de grupos de recursos, debe agregar explícitamente permisos a la entidad principal de servicio con PowerShell.

**Definición de los requisitos de acceso a la suscripción de Azure** En las técnicas y ejemplos de las siguientes secciones se muestran requisitos comunes, lo que implica cambios para sus circunstancias particulares.

Considere la posibilidad de utilizar una entidad de servicio con ámbito de suscripción si:

- Busca la experiencia de administración más sencilla.
- Desea evitar el uso de PowerShell y administrar todo en Citrix Studio.
- Su suscripción a Azure es para una única instancia de Citrix Virtual Apps and Desktops Service.
- Está realizando una prueba de concepto de instalación de Citrix Virtual Apps and Desktops.
- Sus administradores de Citrix Virtual Apps and Desktops tienen acceso de colaborador en el ámbito de suscripción de Azure.

Considere la posibilidad de utilizar una entidad de servicio con ámbito restringido si:

- Su suscripción a Azure aloja varios servicios no relacionados.
- Sus administradores de Azure tienen permisos de suscripción diferentes en función de su rol.
- Su empresa tiene estándares de seguridad que requieren un control de acceso preciso.
- Cuenta con un proceso para crear entidades principales de servicio con ámbito restringido.

**Sugerencia:**

Puede crear suscripciones *secundarias* que se facturan como parte de su suscripción principal y hacen referencia a la instancia de Azure Active Directory predeterminada en su suscripción principal. Esta configuración proporciona otro mecanismo para controlar el acceso a recursos no relacionados.

**Planificación de un catálogo de entidades principales de servicio con ámbito restringido** Antes de crear un catálogo de entidades principales de servicio con ámbito restringido, decida cuántos grupos de recursos se necesitan para alojar el número inicial y futuro de máquinas virtuales. Debido a una limitación de Machine Creation Services, no es posible agregar grupos de recursos una vez creado un catálogo.

**Aprovisionar un catálogo por agrupación de grupos de recursos** Azure Resource Manager Plugin crea la infraestructura necesaria en cada grupo de recursos. El grupo de recursos consta de cuentas de almacenamiento, grupos de seguridad, interfaces de red, máquinas virtuales, etc. Las cuentas de almacenamiento se crean, si es necesario, al agregar máquinas al catálogo. Esto significa que el tamaño de un catálogo puede crecer hasta un límite superior establecido por el tamaño de la agrupación de grupos de recursos y las cuotas de suscripción a Azure. Una vez creada una cuenta de almacenamiento, no se elimina hasta que se elimina el catálogo. Puesto que cualquier máquina virtual se puede eliminar, es posible que haya cuentas de almacenamiento vacías. Este caso es infrecuente, ya que las máquinas virtuales tienden a distribuirse aleatoriamente entre las cuentas de almacenamiento disponibles. Las máquinas deben seleccionarse tediosamente inspeccionando el contenido de las cuentas de almacenamiento para vaciar deliberadamente una cuenta de almacenamiento.

Azure limita el número de máquinas virtuales de un grupo de recursos a 800, pero Azure Resource Manager Plugin utiliza una medida diferente. Un disco de Azure estándar tiene un límite de 500 operaciones de E/S por segundo (IOPS), y una cuenta de almacenamiento estándar tiene un límite de 20 000. Por esta razón, el plug-in no aprovisiona una cuenta de almacenamiento con más de 40 máquinas. Este límite se aplica tanto al almacenamiento estándar como al almacenamiento premium. Además, el plug-in no crea no más de 19 cuentas de almacenamiento en un grupo de recursos.

Por lo tanto, la fórmula básica para calcular el número de grupos de recursos en función del número máximo de máquinas es:

Número de grupos de recursos = límite máximo (Número máximo de máquinas / (40 \* 19))

Azure Resource Manager Plugin asume que tiene uso exclusivo de la agrupación de grupos de recursos. No hay recursos creados por el usuario en ninguno de los grupos de recursos especificados.

### Conceptos básicos del control de acceso por roles de Azure (RBAC).

El acceso a los recursos de Azure se concede asignando un rol RBAC a una entidad principal de servicio en un ámbito determinado. El ámbito puede ser una suscripción, un grupo de recursos o un recurso específico. Los recursos se organizan en una jerarquía de contención, y los permisos definidos por el rol se aplican a todos los recursos situados bajo el ámbito correspondiente. Un rol aplicado en una suscripción se aplica a todos los recursos de la suscripción. Un rol aplicado a un grupo de recursos se aplica a todos los recursos contenidos en el grupo de recursos.

Una implicación de la jerarquía de recursos de Azure es que solo las entidades principales de servicio con permisos de ámbito de suscripción pueden crear grupos de recursos. Esto no es ideal porque impide que aplicaciones como el plug-in creen grupos de recursos a demanda para un grupo lógico y administren recursos (a no ser que tengan amplios permisos en toda la suscripción).

Azure tiene una gran selección de roles integrados y también admite la definición de roles personalizados. Consulte los [Roles personalizados para recursos de Azure](#) para obtener más información sobre los roles personalizados en control de acceso por roles de Azure.

**Creación de una entidad principal de servicio con ámbito de suscripción** En este ejemplo, se muestra cómo crear una entidad principal de servicio con ámbito de suscripción. Los detalles se pueden usar para crear una conexión de Azure en Citrix Studio. Puede optar por el uso de una entidad principal de servicio existente, o bien crear una conexión de Azure manualmente en PowerShell.

```
1 param(
2 [string]$applicationName = "SubscriptionScopeSP",
3 [Parameter(Mandatory=$true)][string]$applicationPassword,
4 [Parameter(Mandatory=$true)][string]$subscriptionId
5 )
6
7 $application = New-AzureRmADApplication -DisplayName $applicationName -
    HomePage "https://localhost/$applicationName" `
8 -IdentifierUri "https://$applicationName" -Password
    $applicationPassword
9
10 New-AzureRmADServicePrincipal -ApplicationId $application.ApplicationId
11
12 # Wait for the service principal to become available
13 Start-Sleep -s 60
14
15 New-AzureRmRoleAssignment -RoleDefinitionName Contributor -
    ServicePrincipalName $application.ApplicationId `
16 -scope "/subscriptions/$subscriptionId"
17
```

```
18 Write-Host ("Application ID: " + $application.ApplicationId)
19 <!--NeedCopy-->
```

**Creación de una entidad principal de servicio básica con ámbito restringido** En esta sección se describe el proceso para crear la entidad principal de servicio con ámbito restringido más simple posible, donde los permisos se asignan en el ámbito del grupo de recursos.

Azure Resource Manager Plugin necesita permiso para los siguientes recursos:

1. El VHD de la imagen maestra
2. La red virtual de las máquinas
3. Los grupos de recursos en los que se van a aprovisionar las máquinas

Para simplificar el script, asumimos que el acceso de colaborador se puede conceder en el ámbito del grupo de recursos. Azure Resource Manager Plugin tiene permisos de colaborador en el grupo de recursos donde se almacena el VHD de la imagen, el grupo de recursos que contiene la red virtual y la agrupación de grupos de recursos donde se aprovisionan las máquinas.

```
1 param(
2 [string]$applicationName = "BasicNarrowScopeSP",
3 [Parameter(Mandatory=$true)][string]$applicationPassword,
4 [Parameter(Mandatory=$true)][string]$subscriptionId,
5 [Parameter(Mandatory=$true)][string[]]$resourceGroups
6 )
7
8 $application = New-AzureRmADApplication -DisplayName $applicationName -
   HomePage "https://localhost/$applicationName" `
9 -IdentifierUri "https://$applicationName" -Password
   $applicationPassword
10
11 New-AzureRmADServicePrincipal -ApplicationId $application.ApplicationId
12
13 # Wait for the service principal to become available
14 Start-Sleep -s 60
15
16 New-AzureRmRoleAssignment -RoleDefinitionName Citrix-Network-Usage-
   Reader -ServicePrincipalName $application.ApplicationId `
17 -scope "/subscriptions/$subscriptionId/"
18
19 foreach ($rg in $resourceGroups)
20 {
21
22     New-AzureRmRoleAssignment -RoleDefinitionName Contributor -
   ServicePrincipalName $application.ApplicationId `
23     -scope "/subscriptions/$subscriptionId/resourcegroups/$rg"
24 }
25
26
27 Write-Host ("Application ID: " + $application.ApplicationId)
```

### **Crear una entidad principal de servicio con ámbito restringido mediante roles personalizados**

Azure incluye un amplio conjunto de roles RBAC integrados. Citrix utiliza el rol colaborador de la sección anterior. Como se señaló, eso concedía a Azure Resource Manager Plugin permisos ligeramente más amplios que los estrictamente necesarios. En esta sección, se define un rol personalizado y se limita aún más el acceso. Si lo prefiere, el acceso se puede bloquear mediante más roles personalizados y con la aplicación de roles directamente a la imagen y a los recursos de red.

#### **Nota:**

Los permisos necesarios están sujetos a cambios.

Utilice los siguientes permisos para definir un rol personalizado para conceder acceso a la red virtual y a la imagen maestra en el ámbito del grupo de recursos.

#### **El VHD de la imagen maestra.**

Para la creación de catálogos:

- Microsoft.Storage/storageAccounts/read
- Microsoft.Storage/storageAccounts/listKeys/action

Para compatibilidad futura con Citrix Studio:

- Microsoft.Resources/subscriptions/resourceGroups/read

La red virtual de las máquinas:

- Microsoft.Network/virtualNetworks/read
- Microsoft.Network/virtualNetworks/subnets/join/action

#### **Los grupos de recursos para máquinas aprovisionadas.**

Podemos crear otro rol personalizado con los siguientes permisos, pero, para mantener el ejemplo simple, continuaremos utilizando el rol Colaborador para los grupos de recursos de máquina. Estos grupos de recursos no contienen recursos que no se hayan creado con Azure Resource Manager Plugin. El rol colaborador hace menos probable que los cambios en el plug-in requieran cambios en la entidad principal de servicio:

- Microsoft.Compute/virtualMachines/\*
- Microsoft.Network/networkInterfaces/\*
- Microsoft.Network/networkSecurityGroups/\*
- Microsoft.Resources/deployments/\*

- Microsoft.Resources/subscriptions/resourceGroups/read
- Microsoft.Storage/storageAccounts/\*
- Microsoft.Storage/storageAccounts/listKeys/action

### Roles de acceso personalizado de Citrix Virtual Apps and Desktops.

Crear un rol personalizado definiéndolo primero en JSON:

```

1 {
2
3   "Name": "Citrix-Custom-Reader",
4   "Description": "Grants access to Citrix XenDesktop images and virtual
5     networks.",
6   "Actions": [
7     "Microsoft.Storage/storageAccounts/read",
8     "Microsoft.Storage/storageAccounts/listKeys/action",
9     "Microsoft.Network/virtualNetworks/read",
10    "Microsoft.Network/virtualNetworks/subnets/join/action"
11  ],
12  "NotActions": [
13  ],
14  "AssignableScopes": [
15    "/subscriptions/<YOUR-SUBSCRIPTION-ID>"
16  ]
17 }
18 <!--NeedCopy-->

```

Crear el rol haciendo referencia a la definición **JSON**:

```

1 New-AzureRmRoleDefinition -InputFile citrix-custom-reader.json
2 <!--NeedCopy-->

```

Usar el nuevo rol personalizado al crear una entidad principal de servicio:

```

1 param(
2 [string]$applicationName = "NarrowScopeSP",
3 [Parameter(Mandatory=$true)] [string]$applicationPassword,
4 [Parameter(Mandatory=$true)] [string]$subscriptionId,
5 [Parameter(Mandatory=$true)] [string[]]$machineResourceGroups,
6 [Parameter(Mandatory=$true)] [string]$imageResourceGroup,
7 [Parameter(Mandatory=$true)] [string]$networkResourceGroup
8 )
9
10 $application = New-AzureRmADApplication -DisplayName $applicationName -
11   HomePage "https://localhost/$applicationName" `
12   -IdentifierUri "https://$applicationName" -Password
13   $applicationPassword
14
15 # Wait for the service principal to become available

```

```

16 Start-Sleep -s 60
17
18 New-AzureRmRoleAssignment -RoleDefinitionName Citrix-Network-Usage-
    Reader -ServicePrincipalName $application.ApplicationId `
19 -scope "/subscriptions/$subscriptionId/"
20
21 foreach ($rg in $machineResourceGroups)
22 {
23
24     New-AzureRmRoleAssignment -RoleDefinitionName Contributor -
        ServicePrincipalName $application.ApplicationId `
25     -scope "/subscriptions/$subscriptionId/resourcegroups/$rg"
26 }
27
28
29 New-AzureRmRoleAssignment -RoleDefinitionName Citrix-Custom-Reader -
    ServicePrincipalName $application.ApplicationId `
30 -scope "/subscriptions/$subscriptionId/resourcegroups/
    $imageResourceGroup"
31
32 New-AzureRmRoleAssignment -RoleDefinitionName Citrix-Custom-Reader -
    ServicePrincipalName $application.ApplicationId `
33 -scope "/subscriptions/$subscriptionId/resourcegroups/
    $networkResourceGroup"
34
35 Write-Host ("Application ID: " + $application.ApplicationId)
36 <!--NeedCopy-->

```

### Creación de conexiones de Azure para Citrix Virtual Apps and Desktops.

Es razonable crear una conexión de Azure para Citrix Virtual Apps and Desktops en Citrix Studio con una entidad principal de servicio existente. Es igualmente razonable crear la conexión en PowerShell.

A continuación, se muestra un ejemplo de cómo crear una conexión en PowerShell:

```

1 param(
2 [string]$connectionName = "AzureConnection",
3 [Parameter(Mandatory=$true)][string]$applicationId,
4 [Parameter(Mandatory=$true)][string]$applicationPassword,
5 [Parameter(Mandatory=$true)][string]$subscriptionId,
6 [Parameter(Mandatory=$true)][string]$subscriptionName,
7 [Parameter(Mandatory=$true)][string]$tenantId
8 )
9
10 Add-PsSnapin Citrix*
11
12 $customProperties = @"
13 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
14 <Property xsi:type="StringProperty" Name="AuthenticationAuthority"
    Value="https://login.microsoftonline.com/" />

```

```

15 <Property xsi:type="StringProperty" Name="ManagementEndpoint" Value="
    https://management.azure.com/" />
16 <Property xsi:type="StringProperty" Name="StorageSuffix" Value="core.
    windows.net" />
17 <Property xsi:type="StringProperty" Name="TenantId" Value="$tenantId"
    />
18 <Property xsi:type="StringProperty" Name="SubscriptionId" Value="
    $subscriptionId" />
19 <Property xsi:type="StringProperty" Name="SubscriptionName" Value="
    $subscriptionName" />
20 </CustomProperties>
21 "@
22
23 $connection = New-Item -ConnectionType "Custom" -CustomProperties
    $customProperties -HypervisorAddress @"(https://management.azure.com
    /)" `
24 -Path @"(XDHyp:\Connections$connectionName)" -Persist -PluginId "
    AzureRmFactory" -Scope @() `
25 -SecurePassword (ConvertTo-SecureString -AsPlainText -Force
    $applicationPassword) -UserName $applicationId
26
27 New-BrokerHypervisorConnection -HypHypervisorConnectionUid $connection.
    HypervisorConnectionUid
28
29 <!--NeedCopy-->

```

En este punto, agregue recursos a la conexión, a través de Studio o en PowerShell.

### Crear catálogos para Citrix Virtual Apps and Desktops.

En el ejemplo siguiente, se utilizan los complementos de Citrix PowerShell para crear un catálogo de Citrix Virtual Apps and Desktops.

Dado que las entidades principales de servicio con ámbito restringido no permiten que Azure Resource Manager Plugin cree grupos de recursos, deberá:

1. Crear una agrupación de grupos de recursos.
2. Asignar los permisos de entidad principal de servicio en todos los grupos de recursos de la agrupación.
3. Enumerar cada grupo de recursos de la agrupación en una propiedad personalizada al crear el esquema de aprovisionamiento.

La propiedad personalizada se denomina **ResourceGroups** y el valor es una lista separada por comas de nombres de grupos de recursos. En el siguiente ejemplo, se muestra un ejemplo de cómo definir esta propiedad personalizada.

#### Nota:

En la propiedad personalizada, solo se muestran los grupos de recursos destinados a las

máquinas. No se incluyen uno o más grupos de recursos donde se encuentran la imagen o la red virtual. Si se especifican, Azure Resource Manager Plugin intenta aprovisionar máquinas en esos grupos de recursos, lo que puede provocar algún comportamiento no deseado.

En este ejemplo, las máquinas se aprovisionan en dos grupos de recursos denominados xd-sales-1 y xd-sales-2:

```

1 Add-PsSnapin Citrix*
2
3 # The hosting unit name is the name of the Azure connection resources
  that should be used for this catalog
4 $hostingUnitName = "AzureHostingUnit"
5 $domain = "citrix.local"
6 $controllerAddress = ("ddc." + $domain)
7 $adminAddress = ($controllerAddress + ":80")
8 $catalogName = "catalog-name"
9 $network = "network-resource-group.resourcegroup\network-name"
10 $subnet = "subnet-name"
11 $serviceOffering = "Standard_A4"
12 $template = "image-resource-group.resourcegroup\imagestorage.
  storageaccount\images.container\image-name.vhd"
13
14 $customProperties = @" <CustomProperties xmlns="http://schemas.citrix.
  com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
  XMLSchema-instance">
15   <Property xsi:type="StringProperty" Name="StorageAccountType" Value
    ="Standard_LRS" />
16   <Property xsi:type="StringProperty" Name="ResourceGroups" Value="xd
    -sales-1, xd-sales-2" />
17 </CustomProperties>
18 "@
19
20 $identityPool = New-AcctIdentityPool -AdminAddress $adminAddress -
  AllowUnicode -Domain $domain `
21   -IdentityPoolName $catalogName -NamingScheme "vm-#" -
  NamingSchemeType "Numeric" -Scope @()
22
23 $brokerCatalog = New-BrokerCatalog -AdminAddress $adminAddress -
  AllocationType "Random" -IsRemotePC $False `
24   -MinimumFunctionalLevel "L7_9" -Name $catalogName -
  PersistUserChanges "Discard" -ProvisioningType "MCS" -Scope @()
25   -SessionSupport "MultiSession"
26
27 Write-Host $brokerCatalog
28
29 $provScheme = New-ProvScheme -AdminAddress $adminAddress -CleanOnBoot -
  CustomProperties $customProperties `
30   -HostingUnitName $hostingUnitName -IdentityPoolName $catalogName `
31   -MasterImageVM "XDHyp:\HostingUnits$hostingUnitName\image.
  folder$template.vhd" `
32   -NetworkMapping @{

```

```

33 "0"="XDHyp:\HostingUnits$hostingUnitName\virtualprivatecloud.
    folder$network.virtualprivatecloud$subnet.network" }
34 `
35 -ProvisioningSchemeName $catalogName -Scope @() -SecurityGroup @()
36 -ServiceOffering "XDHyp:\HostingUnits$hostingUnitName\
    serviceoffering.folder$serviceOffering.serviceoffering"
37
38 Write-Host $provScheme
39
40 Set-BrokerCatalog -AdminAddress $adminAddress -Name $catalogName -
    ProvisioningSchemeId $provScheme.ProvisioningSchemeUid
41
42 Add-ProvSchemeControllerAddress -AdminAddress $adminAddress.com -
    ControllerAddress $controllerAddress -ProvisioningSchemeName
    $catalogName
43 <!--NeedCopy-->

```

En este punto, puede actualizar la página del catálogo en Citrix Studio, agregar máquinas y administrar máquinas, como con cualquier otro catálogo.

### Configurar grupos de recursos para un catálogo de máquinas en Studio

En la página **Grupos de recursos** del asistente de creación de catálogos, puede elegir si crear grupos de recursos o usar los existentes. Consulte Crear un catálogo de máquinas con una imagen maestra de Azure Resource Manager.

Qué ocurre con los grupos de recursos cuando se elimina un catálogo de máquinas:

- Si permite que Citrix Virtual Apps and Desktops cree grupos de recursos cuando usted crea el catálogo de máquinas y, posteriormente, elimina ese catálogo, esos grupos de recursos y todos los recursos en esos grupos también se eliminan.
- Si usa grupos de recursos existentes cuando cree el catálogo de máquinas y, posteriormente, elimina ese catálogo, todos los recursos en esos grupos de recursos se eliminan, pero los grupos en sí se conservan.

### Consideraciones, limitaciones y solución de problemas

Cuando se usan grupos de recursos existentes, la lista de los grupos de recursos disponibles en la página “Grupos de recursos” del asistente de creación de catálogos no se actualiza automáticamente. Por lo tanto, si tiene abierta esa página del asistente mientras crea o agrega permisos a los grupos de recursos en Azure, esos cambios no se reflejan en la lista del asistente. Para ver los cambios más recientes, dispone de dos opciones: volver a la página **Administración de máquinas** del asistente y volver a seleccionar los recursos asociados a la conexión de host, o cerrar y reiniciar el asistente. Pueden pasar hasta 10 minutos hasta que los cambios realizados en Azure aparezcan en Studio.

Un grupo de recursos debería utilizarse en un solo catálogo de máquinas. No obstante, esto no se aplica. Por ejemplo, se seleccionan 10 grupos de recursos al crear un catálogo, pero solo se crea una máquina en el catálogo. Nueve de los grupos de recursos seleccionados permanecen vacíos una vez creado el catálogo. Puede que tenga la intención de usarlos para expandir su capacidad en el futuro, por lo que permanecen asociados a ese catálogo. No se puede agregar grupos de recursos a un catálogo una vez creado el catálogo, así que es sensato planificar para el futuro durante la creación del catálogo. Sin embargo, si se crea otro catálogo, esos nueve grupos de recursos aparecerán en la lista de grupos disponibles. Actualmente Citrix Virtual Apps and Desktops no realiza ningún seguimiento de qué grupos de recursos se asignan a qué catálogos. Supervisar esa asignación recae sobre usted.

Si la conexión utiliza una entidad de servicio que puede acceder a los grupos de recursos vacíos que se encuentran en varias regiones, todos aparecerán en la lista de grupos disponibles. Debe seleccionar los grupos de recursos de la misma región donde crea el catálogo de máquinas.

Solución de problemas:

- Los grupos de recursos no aparecen en la lista de la página “Grupos de recursos” en el asistente de creación de catálogos.

La entidad principal de servicio debe tener los permisos adecuados aplicados a los grupos de recursos que quiera que aparezcan en la lista. Consulte la sección anterior de requisitos.

- Al agregar máquinas a un catálogo de máquinas creado previamente, no se aprovisionan todas las máquinas.

Después de crear un catálogo, cuando más adelante agregué máquinas a ese catálogo, no exceda la capacidad de máquinas por grupo de recursos originalmente seleccionada para el catálogo (240 por grupo). No se puede agregar grupos de recursos una vez creado el catálogo. Si intenta agregar más máquinas de las que pueden admitir los grupos de recursos existentes, el aprovisionamiento falla.

Por ejemplo, crea un catálogo de máquinas con 300 VM y 2 grupos de recursos. Los grupos de recursos pueden admitir hasta 480 máquinas virtuales (240 multiplicado por 2). Si más adelante intenta agregar 200 VM al catálogo, lo que supera la capacidad de los grupos de recursos (300 VM actuales + 200 VM nuevas = 500, pero los grupos de recursos pueden contener solo 480 VM).

## Más información

- [Conexiones y recursos](#)
- [Crear catálogos de máquinas](#)
- [CTX219211: Set up a Microsoft Azure Active Directory account](#)
- [CTX219243: Grant XenApp and XenDesktop access to your Azure subscription](#)
- [CTX219271: Deploy hybrid cloud using site-to-site VPN](#)

## Entornos de virtualización de Microsoft System Center Virtual Machine Manager

September 22, 2021

Si quiere utilizar Hyper-V con Microsoft System Center Virtual Machine Manager (VMM) para proporcionar máquinas virtuales, siga estas instrucciones.

Esta versión admite las versiones de VMM que figuran en el artículo [Requisitos del sistema](#).

Puede utilizar Machine Creation Services y Citrix Provisioning (antes llamado Provisioning Services) para aprovisionar:

- Máquinas virtuales de SO de servidor o escritorio de 1.<sup>a</sup> generación
- Máquinas virtuales con Windows Server 2012 R2, Windows Server 2019, Windows Server 2016 y Windows 10 (con o sin Secure Boot) de 2.<sup>a</sup> generación

### Instalar y configurar un hipervisor

#### Importante:

Todos los Delivery Controllers deben estar en el mismo bosque que los servidores de VMM.

1. Instale Microsoft Hyper-V Server y VMM en los servidores.
2. Instale la consola de System Center Virtual Machine Manager en todos los Controllers. La versión de la consola debe coincidir con la versión del servidor de administración. Aunque es posible conectar una consola anterior al servidor de administración, se produce un error al aprovisionar los agentes VDA si las versiones son distintas.
3. Compruebe la siguiente información de cuenta:

La cuenta que utilice para indicar los hosts en Studio debe ser un administrador o administrador delegado de VMM para las máquinas Hyper-V en cuestión. Si esta cuenta solo tiene el rol de administrador delegado en VMM, los datos de almacenamiento no aparecen en Studio durante el proceso de creación del host.

La cuenta de usuario utilizada para la integración de Studio también debe ser miembro del grupo local de seguridad de administradores en cada uno de los servidores Hyper-V para poder ofrecer la administración del ciclo de vida de las VM (creación, actualización y eliminación de VM).

No se admite la instalación de Controller en un servidor que ejecuta Hyper-V.

## Crear una VM maestra

1. Instale un agente Virtual Desktop Agent en la VM maestra y seleccione la opción de optimizar el escritorio. Esto mejora el rendimiento.
2. Tome una instantánea de la VM maestra para usarla como copia de seguridad.

## Crear escritorios virtuales

Si utiliza MCS para crear máquinas virtuales, al crear un sitio o una conexión:

1. Seleccione el tipo de host de virtualización Microsoft.
2. Escriba la dirección como el nombre de dominio completo del servidor host.
3. Introduzca las credenciales para la cuenta de administrador que configuró anteriormente y que incluye permisos para crear nuevas VM.
4. En **Detalles del host**, seleccione el clúster o el host independiente que quiere utilizar para crear las VM.

Busque y seleccione un clúster o un host independiente aunque utilice una implementación de host de Hyper-V único.

## MCS en recursos compartidos de archivos SMB 3

En caso de catálogos de máquinas creados a través de MCS en recursos compartidos SMB 3 para el almacenamiento de VM, compruebe que las credenciales cumplen los siguientes requisitos, de modo que las llamadas desde la biblioteca de comunicaciones de hipervisor (HCL) del Controller puedan conectarse al almacenamiento SMB:

- Las credenciales de usuario de VMM deben incluir acceso de escritura y lectura completo al almacenamiento de SMB.
- Las operaciones de disco virtual de almacenamiento durante el ciclo de vida de las máquinas virtuales se realizan a través del servidor Hyper-V mediante las credenciales de usuario de VMM.

Si usa SMB como almacenamiento, habilite el proveedor de compatibilidad para seguridad de autenticación de credenciales (CredSSP) desde el Controller a cada máquina de Hyper-V cuando se utilice VMM 2012 SP1 con Hyper-V en Windows Server 2012. Para obtener más información, consulte CTX137465.

Si usa una sesión remota de PowerShell 3 estándar, HCL usa CredSSP para abrir una conexión con la máquina Hyper-V. Esta función pasa las credenciales de usuario cifradas por Kerberos a la máquina Hyper-V. A continuación, los comandos de PowerShell de la sesión en la máquina Hyper-V remota se

ejecutan con las credenciales proporcionadas (en este caso, las credenciales del usuario de VMM), de forma que los comandos que se comuniquen al almacenamiento funcionen correctamente.

Las siguientes tareas usan scripts de PowerShell que se originan en la HCL y se envían a la máquina Hyper-V para actuar en el almacenamiento de SMB 3.0.

- **Consolidar una imagen maestra:** Una imagen maestra crea un nuevo esquema de aprovisionamiento (catálogo de máquinas) de MCS. Clona y deja la VM maestra lista para crear nuevas VM a partir del nuevo disco creado (y quita la dependencia de la VM maestra original).

ConvertVirtualHardDisk en el espacio de nombres root\virtualization\v2

Ejemplo:

```
1 $ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
2 $result = $ims.ConvertVirtualHardDisk($diskName, $vhdastr)
3 $result
4 <!--NeedCopy-->
```

- **Crear disco de diferenciación:** Crea un disco de diferenciación a partir de la imagen generada al consolidar la imagen maestra. A continuación, el disco de diferenciación se adjunta a una nueva VM.

CreateVirtualHardDisk en el espacio de nombres root\virtualization\v2

Ejemplo:

```
1 $ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
2 $result = $ims.CreateVirtualHardDisk($vhdastr);
3 $result
4 <!--NeedCopy-->
```

- **Cargar discos de identidad:** La biblioteca HCL no puede cargar directamente el disco de identidad en el almacenamiento de SMB. Por lo tanto, la máquina Hyper-V debe cargar y copiar el disco de identidad en el almacenamiento. Debido a que la máquina Hyper-V no puede leer el disco del Controller, la HCL debe copiar primero el disco de identidad mediante la máquina Hyper-V tal y como se indica.

La HCL carga la identidad en la máquina Hyper-V mediante el recurso compartido de administrador.

La máquina Hyper-V copia el disco en el almacenamiento de SMB a través de un script de PowerShell que se ejecuta en la sesión remota de PowerShell. Se crea una carpeta en la máquina Hyper-V y los permisos de la carpeta están bloqueados únicamente para el usuario de VMM (a través de la conexión remota de PowerShell).

La biblioteca HCL elimina el archivo del recurso compartido de administrador.

Cuando la biblioteca HCL completa la carga del disco de identidad en la máquina Hyper-V, la sesión remota de PowerShell copia los discos de identidad al almacenamiento de SMB y, después, los elimina de la máquina Hyper-V.

La carpeta del disco de identidad se vuelve a crear si se elimina para que esté disponible para volver a usarse.

- **Descargar discos de identidad:** Al igual que con las cargas, los discos de identidad pasan a través de la máquina Hyper-V hasta la HCL. El siguiente proceso crea una carpeta que solo tiene permisos de usuario de VMM en el servidor Hyper-V si no existe.

La máquina Hyper-V copia el disco desde el almacenamiento de SMB al almacenamiento de Hyper-V local mediante un script de PowerShell que se ejecuta en la sesión remota de PowerShell V3.

La HCL lee el disco desde el recurso compartido de administrador de la máquina Hyper-V y lo copia en memoria.

La HCL elimina el archivo del recurso compartido de administrador.

- **Crear discos Personal vDisk:** Si el administrador crea la VM en un catálogo de máquinas de Personal vDisk, usted debe crear un disco vacío (PvD).

La llamada para crear un disco vacío no requiere acceso directo al almacenamiento. Si tiene discos PvD que residen en un almacenamiento que no sea el disco principal o el del sistema operativo, use PowerShell de forma remota para crear el disco PvD en una carpeta de directorio que tenga el mismo nombre que la VM desde la que se creó. Para CSV o LocalStorage, no use PowerShell de forma remota. Crear el directorio antes de crear un disco vacío evita errores de comando de VMM.

En la máquina Hyper-V, realice un mkdir en el almacenamiento.

## Entornos de virtualización de Citrix Hypervisor

April 19, 2024

### Crear una conexión con Citrix Hypervisor

Cuando crea una conexión con Citrix Hypervisor (antes XenServer), debe proporcionar las credenciales de un administrador avanzado de VM o de un usuario de nivel superior.

Citrix recomienda utilizar HTTPS para proteger las comunicaciones con Citrix Hypervisor. Para utilizar HTTPS, debe reemplazar el certificado SSL predeterminado que se instaló en Citrix Hypervisor; consulte [CTX128656](#).

Es posible configurar la alta disponibilidad si esta función está habilitada en el servidor de Citrix Hypervisor. Citrix recomienda seleccionar todos los servidores de la agrupación (en Edit High Availability) para permitir la comunicación con el servidor de Citrix Hypervisor en caso de que falle el servidor principal de la agrupación.

Puede seleccionar un tipo y un grupo de GPU o PassThrough si la instancia de Citrix Hypervisor admite el uso de vGPU. La interfaz indica si la selección tiene recursos de GPU dedicados.

Cuando se usa el almacenamiento local en uno o varios hosts de Citrix Hypervisor para el almacenamiento de datos temporales, compruebe que cada ubicación de almacenamiento que forma parte de la agrupación tenga un nombre único. (Para modificar un nombre en XenCenter, haga clic con el botón secundario en el espacio de almacenamiento y modifique la propiedad de nombre.)

### Usar IntelliCache para conexiones de Citrix Hypervisor

Con IntelliCache, las implementaciones de VDI alojadas son más rentables porque le permiten usar una combinación de almacenamiento compartido y almacenamiento local. Esto mejora el rendimiento y reduce el tráfico de red. El almacenamiento local almacena en caché la imagen maestra proveniente del almacenamiento compartido, lo que reduce la cantidad de lecturas en el almacenamiento compartido. Para los escritorios compartidos, las escrituras en los discos de diferenciación se realizan en el almacenamiento local del host y no en el almacenamiento compartido.

- Cuando utiliza IntelliCache, el almacenamiento compartido debe ser NFS.
- Citrix recomienda utilizar un dispositivo de almacenamiento local de alto rendimiento para garantizar la transferencia de datos más rápida que sea posible.

Para utilizar IntelliCache, es necesario habilitarlo en este producto y en Citrix Hypervisor.

- Al instalar Citrix Hypervisor, seleccione **Enable thin provisioning (Optimized storage for Virtual Desktops)**. Citrix no admite agrupaciones mixtas de servidores, donde hay servidores con IntelliCache habilitado y servidores sin ese componente habilitado. Para obtener más información, consulte la documentación de Citrix Hypervisor.
- De forma predeterminada, en Citrix Virtual Apps and Desktops el componente IntelliCache está inhabilitado. Puede cambiar el parámetro únicamente al crear una conexión de Citrix Hypervisor; no podrá inhabilitar IntelliCache más tarde. Al agregar una conexión de Citrix Hypervisor:
  - Seleccione el tipo de almacenamiento **compartido**.
  - Marque la casilla **Usar IntelliCache**.

### Permisos de Citrix Hypervisor necesarios

Los permisos de Citrix Hypervisor se basan en roles (RBAC).

Para obtener más información, consulte [Control de acceso basado en roles](#).

La jerarquía de roles, en orden de aumento de los permisos, es: Solo lectura → Operador de VM → Administrador de VM → Administrador avanzado de VM → Operador de agrupaciones → Administrador de agrupaciones.

En la siguiente sección se resume el rol mínimo requerido para cada tarea de aprovisionamiento.

### Crear una conexión de host

---

Tarea	Rol mínimo requerido
Agregue una conexión de host con la información obtenida de XenServer	Solo lectura
Ver los usuarios y sus roles asignados	Solo lectura

---

### Administración de energía de las máquinas virtuales

---

Tarea	Rol mínimo requerido
Encender o apagar las máquinas virtuales	Operador de VM

---

### Creación, actualización o eliminación de máquinas virtuales

---

Tarea	Rol mínimo requerido
Agregar máquinas virtuales a las programaciones de instantáneas existentes o quitarlas de las mismas	Administrador avanzado de VM
Agregar, modificar y eliminar programaciones de instantáneas	Operador de agrupaciones
Publicar imagen maestra	Operador de agrupaciones (requiere bloqueo de puertos de conmutador)
Creación de un catálogo de máquinas	Operador de agrupaciones: requiere bloqueo de puertos de conmutador
Agregar o quitar máquinas virtuales (no incluye máquinas virtuales habilitadas para GPU)	Administrador de máquinas virtuales

---

Tarea	Rol mínimo requerido
Agregar o quitar máquinas virtuales (máquinas virtuales habilitadas para GPU)	Operador de agrupaciones
Agregar, quitar o configurar dispositivos de CD o discos virtuales	Administrador de máquinas virtuales
Administrar etiquetas	Operador de VM

---

Para obtener más información sobre los roles y los permisos de RBAC, consulte [Roles y permisos de RBAC](#).

Para obtener información sobre el bloqueo de puertos de conmutador, consulte [Usar bloqueo de puertos de conmutador](#).

### Crear un catálogo de máquinas a través una conexión de Citrix Hypervisor

Las máquinas que pueden usar GPU requieren una imagen maestra dedicada. Esas máquinas virtuales requieren controladores de tarjeta de vídeo compatibles con GPU. Configure máquinas que pueden usar GPU para que la máquina virtual funcione con el software que usa la GPU para las operaciones.

1. En XenCenter, cree una VM con VGA estándar, redes y vCPU.
2. Actualice la configuración de la máquina virtual para habilitar el uso de GPU (PassThrough o vGPU).
3. Instale un sistema operativo compatible y habilite el protocolo RDP.
4. Instale Citrix VM Tools y los controladores de NVIDIA.
5. Desactive la consola de administración de Virtual Network Computing (VNC) para optimizar el rendimiento y, a continuación, reinicie la VM.
6. Se le solicitará que use RDP. Mediante RDP, instale el VDA y, a continuación, reinicie la VM.
7. Si quiere, puede crear una instantánea de la VM para establecer un punto de referencia para otras imágenes maestras de GPU.
8. Mediante RDP, instale las aplicaciones específicas del usuario que están configuradas en XenCenter y funcionan con GPU.

### Más información

- [Conexiones y recursos](#)
- [Crear catálogos de máquinas](#)

## Entornos de Microsoft System Center Configuration Manager

March 31, 2021

Los sitios que utilizan Microsoft System Center Configuration Manager (Configuration Manager) para administrar el acceso a aplicaciones y escritorios pueden extender ese uso a Citrix Virtual Apps and Desktops mediante estas opciones:

- [Instalar agentes VDA mediante SCCM](#).
- **Proxy Wake On LAN de Configuration Manager:** La función Wake on LAN del Acceso con Remote PC requiere Configuration Manager. Para obtener más información, consulte [Acceso con Remote PC: Wake on LAN](#).
- **Propiedades de Citrix Virtual Apps and Desktops:** Le permiten identificar Citrix Virtual Desktops para su administración a través de Configuration Manager. (En algunas versiones, Configuration Manager utiliza el nombre anterior de Citrix Virtual Apps and Desktops: XenApp y XenDesktop.)

### Propiedades

Si quiere administrar escritorios virtuales, existen propiedades disponibles para Microsoft System Center Configuration Manager.

Las propiedades de valor booleano que se muestran en Configuration Manager pueden aparecer como 1 ó 0, en lugar de true o false.

Las propiedades están disponibles para la clase `Citrix_virtualDesktopInfo` en el espacio de nombres `Root\Citrix\DesktopInformation`. Los nombres de propiedad proceden del proveedor Instrumental de administración de Windows (WMI).

Propiedad	Descripción
<code>AssignmentType</code>	Establece el valor de <code>IsAssigned</code> . Los valores válidos son <code>ClientIP</code> , <code>ClientName</code> , <code>None</code> y <code>User</code> (se establece <code>IsAssigned</code> en <code>True</code> ).
<code>BrokerSiteName</code>	Sitio. Devuelve el mismo valor que <code>HostIdentifier</code> .
<code>DesktopCatalogName</code>	Catálogo de máquinas asociado al escritorio.
<code>DesktopGroupName</code>	Grupo de entrega asociado al escritorio.
<code>HostIdentifier</code>	Sitio. Devuelve el mismo valor que <code>BrokerSiteName</code> .

Propiedad	Descripción
IsAssigned	<b>True</b> para asignar el escritorio a un usuario y <b>False</b> para un escritorio aleatorio
IsMasterImage	Permite tomar decisiones sobre el entorno. Por ejemplo, es posible que instale aplicaciones en la imagen maestra y no en las máquinas aprovisionadas, sobre todo si esas máquinas están limpias como máquinas de arranque. Los valores válidos son <b>True</b> para una máquina virtual que se usa como una imagen (este valor se establece durante la instalación basada en una selección) o en blanco para una máquina virtual aprovisionada a partir de esa imagen.
IsVirtualMachine	<b>True</b> para una máquina virtual y <b>false</b> para una máquina física.
OSChangesPersist	<b>False</b> si la imagen del sistema operativo del escritorio vuelve a un estado limpio cada vez que se reinicia; de lo contrario, el valor es <b>true</b> .
PersistentDataLocation	La ubicación donde Configuration Manager almacena datos persistentes. Los usuarios no pueden acceder a esta ubicación.
PersonalvDiskDriveLetter	Para un escritorio con un disco Personal vDisk, es la letra de unidad que se asigna al mismo.
BrokerSiteName, DesktopCatalogName, DesktopGroupName, HostIdentifier	Se determina cuando el escritorio se registra en el Controller. No son válidos para un escritorio que no haya terminado el registro.

Para recopilar las propiedades, ejecute un inventario de hardware en Configuration Manager. Para ver las propiedades, use el Explorador de recursos de Configuration Manager. En estos casos, es posible que los nombres incluyan espacios o varíen ligeramente con respecto a los nombres de propiedades. Por ejemplo, es posible que **BrokerSiteName** aparezca como **Broker Site Name**.

- Configurar Configuration Manager para recopilar las propiedades de Citrix WMI desde el VDA de Citrix
- Crear colecciones (recopilaciones) de dispositivos basadas en consultas mediante propiedades de Citrix WMI
- Crear condiciones globales en función de las propiedades de Citrix WMI
- Usar condiciones globales para definir requisitos de tipo de implementación de aplicaciones

También puede utilizar las propiedades de Microsoft en la clase `CCM_DesktopMachine` de Microsoft en el espacio de nombres `Root\ccm_vdi`. Para obtener más información, consulte la documentación de Microsoft.

## Entornos de virtualización de VMware

June 27, 2024

Si quiere utilizar VMware para proporcionar máquinas virtuales, siga estas instrucciones.

Instale vCenter Server y las herramientas de administración adecuadas. (No se admite la operación “Linked Mode” de vSphere vCenter.)

Si va a utilizar Machine Creation Services (MCS), no inhabilite la función de explorador del almacén de datos (Datastore Browser) en el servidor vCenter (descrito en <https://kb.vmware.com/s/article/2101567>). Si inhabilita esta función, MCS no funciona correctamente.

### Privilegios necesarios

Cree una cuenta de usuario de VMware y uno o varios roles de VMware con un conjunto de los permisos que se describen en este artículo. Base la creación de roles en un nivel específico de granularidad necesaria sobre los permisos del usuario para solicitar las distintas operaciones de Citrix DaaS en cualquier momento. Para conceder los permisos específicos al usuario en cualquier momento, asícielos al rol correspondiente, en el nivel de centro de datos como mínimo, con la opción **Propagar a elementos secundarios** seleccionada.

En las siguientes tablas, se muestran las asignaciones entre las operaciones de Citrix Virtual Apps and Desktops y los privilegios mínimos requeridos de VMware.

#### Nota:

El nombre simplificado de la lista de permisos, concretamente *User Interface*, es diferente para algunas versiones de vSphere. Por ejemplo: en vSphere 6.7 el permiso *User Interface* es **Change Memory** y **Change Settings**, en lugar de **Settings** y **Memory**, como se describe en los privilegios requeridos que se indican en esta página.

### Agregar conexiones y recursos

SDK	Interfaz de usuario
System.Anonymous, System.Read y System.View	Se agrega automáticamente. Puede usar el rol integrado de solo lectura.

### Administración de energía

SDK	Interfaz de usuario
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Interact.Reset	Virtual machine > Interaction > Reset
VirtualMachine.Interact.Suspend	Virtual machine > Interaction > Suspend
Datastore.Browse	Datastore > Browse datastore

### Aprovisionar máquinas (Machine Creation Services)

Para aprovisionar máquinas mediante MCS, son obligatorios los siguientes permisos:

SDK	Interfaz de usuario
Datastore.AllocateSpace	Datastore > Allocate space
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
Network.Assign	Network > Assign network
Resource.AssignVMToPool	Resource > Assign virtual machine to resource pool
VirtualMachine.Config.AddExistingDisk	Virtual machine > Configuration > Add existing disk
VirtualMachine.Config.AddNewDisk	Virtual machine > Configuration > Add new disk
Virtual machine.Config.Add or remove device	Virtual machine > Configuration > Add or remove device
VirtualMachine.Config.AdvancedConfig	Virtual machine > Configuration > Advanced
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk

SDK	Interfaz de usuario
VirtualMachine.Config.CPUCount	Virtual machine > Configuration > Change CPU count
VirtualMachine.Config.Memory	Virtual machine > Configuration > Change memory
VirtualMachine.Config.Settings	Virtual machine > Configuration > Change settings
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Interact.Reset	Virtual machine > Interaction > Reset
VirtualMachine.Interact.Suspend	Virtual machine > Interaction > Suspend
VirtualMachine.Inventory.CreateFromExisting	Virtual machine > Inventory > Create from existing
VirtualMachine.Inventory.Create	Virtual machine > Inventory > Create new
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove
VirtualMachine.Provisioning.Clone	Virtual machine > Provisioning > Clone virtual machine
VirtualMachine.State.CreateSnapshot	vSphere 5.0, Update 2, vSphere 5.1, Update 1, and vSphere 6.x, Update 1: Virtual machine > State > Create snapshot; vSphere 5.5: Virtual machine > Snapshot management > Create snapshot

### Actualizar y revertir imagen

SDK	Interfaz de usuario
Datastore.AllocateSpace	Datastore > Allocate space
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
Network.Assign	Network > Assign network
Resource.AssignVMToPool	Resource > Assign virtual machine to resource pool
VirtualMachine.Config.AddExistingDisk	Virtual machine > Configuration > Add existing disk

SDK	Interfaz de usuario
VirtualMachine.Config.AddNewDisk	Virtual machine > Configuration > Add new disk
VirtualMachine.Config.AdvancedConfig	Virtual machine > Configuration > Advanced
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Interact.Reset	Virtual machine > Interaction > Reset
VirtualMachine.Inventory.CreateFromExisting	Virtual machine > Inventory > Create from existing
VirtualMachine.Inventory.Create	Virtual machine > Inventory > Create new
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove
VirtualMachine.Provisioning.Clone	Virtual machine > Provisioning > Clone virtual machine

### Eliminar máquinas aprovisionadas

SDK	Interfaz de usuario
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove

### Perfil de almacenamiento (vSAN)

Para ver, crear o eliminar directivas de almacenamiento durante la creación de catálogos en un almacén de datos de vSAN, son obligatorios los siguientes permisos:

SDK	Interfaz de usuario
StorageProfile.Update	PROFILE-DRIVEN STORAGE > Profile-driven storage update. Para vSphere 8: VM storage policies > Update VM storage policies
StorageProfile.View	PROFILE-DRIVEN STORAGE > Profile-driven storage view. Para vSphere 8: VM storage policies > View VM storage policies

### Etiquetas y atributos personalizados

Las etiquetas y los atributos personalizados permiten adjuntar metadatos a las máquinas virtuales creadas en el inventario de vSphere y facilitan la búsqueda y el filtrado de estos objetos. Para crear, modificar, asignar y eliminar etiquetas o categorías, son obligatorios los siguientes permisos:

SDK	Interfaz de usuario
InventoryService.Tagging.CreateTag	vSphere Tagging > Create vSphere Tag
InventoryService.Tagging.CreateCategory	vSphere Tagging > Create vSphere Tag Category
InventoryService.Tagging.EditTag	vSphere Tagging > Edit vSphere Tag
InventoryService.Tagging.EditCategory	vSphere Tagging > Edit vSphere Tag Category
InventoryService.Tagging.DeleteTag	vSphere Tagging > Delete vSphere Tag
InventoryService.Tagging.DeleteCategory	vSphere Tagging > Delete vSphere Tag Category
InventoryService.Tagging.AttachTag	vSphere Tagging > Assign or Unassign vSphere Tag
InventoryService.Tagging.ObjectAttachable	vSphere Tagging > Assign or Unassign vSphere Tag on Object
Global.ManageCustomFields	Global > Manage custom attributes
Global.SetCustomField	Global > Set custom attribute

#### Nota:

Cuando MCS crea un catálogo de máquinas, etiqueta las máquinas virtuales de destino con etiquetas con nombres especiales. Estas etiquetas diferencian la imagen maestra de las máquinas virtuales creadas por MCS e impiden el uso de máquinas virtuales creadas por MCS para la preparación de imágenes. Puede identificar la diferencia por el valor del atributo `XdProvisioned` en vCenter. El atributo se establece en **True** si MCS crea las máquinas

virtuales.

## Operaciones de cifrado

Los privilegios relativos a las operaciones de cifrado determinan quién puede realizar los distintos tipos de operaciones de cifrado en los diferentes tipos de objetos. El proveedor de claves nativas de vSphere usa los privilegios de **Cryptographer** . \*. Para las operaciones de cifrado, se requieren los siguientes permisos mínimos:

SDK	Interfaz de usuario
Cryptographer.Access	Privileges > All Privileges > Cryptographic operations > Direct Access
Cryptographer.AddDisk	Privileges > All Privileges > Cryptographic operations > Add disk
Cryptographer.Clone	Privileges > All Privileges > Cryptographic operations > Clone
Cryptographer.Encrypt	Privileges > All Privileges > Cryptographic operations > Encrypt
Cryptographer.EncryptNew	Privileges > All Privileges > Cryptographic operations > Encrypt new
Cryptographer.Decrypt	Privileges > All Privileges > Cryptographic operations > Decrypt
Cryptographer.Migrate	Privileges > All Privileges > Cryptographic operations > Migrate
Cryptographer.ReadKeyServersInfo	Privileges > All Privileges > Cryptographic operations > Read KMS information

## Aprovisionar máquinas (Citrix Provisioning)

Estos permisos para clonar e implementar una plantilla son necesarios para aprovisionar máquinas virtuales mediante el asistente Citrix Virtual Apps and Desktops Setup Wizard y el asistente Export Devices Wizard a través de la consola de Citrix Provisioning. Establezca los permisos al crear una conexión de alojamiento. Necesita todos los permisos de Aprovisionar máquinas (Machine Creation Services) y lo siguiente:

SDK	Interfaz de usuario
VirtualMachine.Config.AddRemoveDevice	Virtual machine > Configuration > Add or remove device
VirtualMachine.Config.CPUCount	Virtual machine > Configuration > Change CPU Count
VirtualMachine.Config.Memory	Virtual machine > Configuration > Memory
VirtualMachine.Config.Settings	Virtual machine > Configuration > Settings
VirtualMachine.Provisioning.CloneTemplate	Virtual machine > Provisioning > Clone template
VirtualMachine.Provisioning.DeployTemplate	Virtual machine > Provisioning > Deploy template
VApp.Export	vApp > Export

**Nota:**

[VApp.Export](#) es necesario para crear catálogos de máquinas de MCS mediante perfiles de máquina.

**Crear AppDisks**

Válido para VMware vSphere 5.5, como mínimo, y XenApp y XenDesktop 7.8, como mínimo.

SDK	Interfaz de usuario
Datastore.AllocateSpace	Datastore > Allocate space
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
VirtualMachine.Config.AddExistingDisk	Virtual machine > Configuration > Add existing disk
VirtualMachine.Config.AddNewDisk	Virtual machine > Configuration > Add new disk
VirtualMachine.Config.AdvancedConfig	Virtual machine > Configuration > Advanced
VirtualMachine.Config.EditDevice	Virtual machine > Configuration > Modify Device Settings
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On

## Eliminar AppDisks

Válido para VMware vSphere 5.5, como mínimo, y XenApp y XenDesktop 7.8, como mínimo.

---

SDK	Interfaz de usuario
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off

---

## Obtener e importar un certificado

Para proteger las comunicaciones de vSphere, Citrix recomienda utilizar HTTPS en lugar de HTTP. HTTPS requiere certificados digitales. Citrix recomienda utilizar un certificado digital emitido por una entidad de certificación conforme a la directiva de seguridad de la organización.

Si no puede utilizar un certificado digital emitido por una entidad de certificación y las directivas de seguridad de la organización lo permiten, puede utilizar el certificado autofirmado instalado por VMware. Agregue el certificado de VMware vCenter a cada Delivery Controller.

1. Agregue el nombre de dominio completo (FQDN) del equipo que ejecuta vCenter Server al archivo hosts de ese servidor, ubicado en %SystemRoot%/WINDOWS/system32/Drivers/etc/. Este paso solo es necesario si el nombre FQDN del equipo que ejecuta vCenter Server aún no está presente en el sistema de nombres de dominio.
2. Obtenga el certificado de vCenter con alguno de los tres métodos siguientes:

### Desde el servidor vCenter.

- a) Copie el archivo rui.crt desde el servidor vCenter a una ubicación accesible en los Delivery Controllers.
- b) En Controller, vaya a la ubicación donde está el certificado exportado y abra el archivo rui.crt.

**Descargue el certificado mediante un explorador web.** Si está utilizando Internet Explorer, dependiendo de la cuenta de usuario, puede que tenga que hacer clic con el botón secundario en Internet Explorer y elegir **Ejecutar como administrador** para descargar o instalar el certificado.

- a) Abra el explorador web y establezca una conexión web segura con el servidor vCenter (por ejemplo <https://server1.domain1.com>).

- b) Acepte las advertencias de seguridad.
- c) Haga clic en la barra de dirección donde aparece el error de certificado.
- d) Revise el certificado y haga clic en la ficha Detalles.
- e) Seleccione **Copiar a archivo y exportar en formato CER** y escriba un nombre cuando lo pida el procedimiento.
- f) Guarde el certificado exportado.
- g) Vaya a la ubicación del certificado exportado y abra el archivo CER.

### **Impórtelo directamente desde Internet Explorer ejecutado como administrador.**

- Abra el explorador web y establezca una conexión web segura con el servidor vCenter (por ejemplo <https://server1.domain1.com>).
  - Acepte las advertencias de seguridad.
  - Haga clic en la barra de dirección donde aparece el error de certificado.
  - Vea el certificado.
3. Importe el certificado en el almacén de certificados de cada uno de los Controllers.
    - a) Haga clic en **Instalar certificado**, seleccione **Máquina local** y, a continuación, haga clic en **Siguiente**.
    - b) Seleccione **Colocar todos los certificados en el siguiente almacén** y, a continuación, haga clic en **Examinar**. Seleccione **Personas de confianza** y haga clic en **Aceptar**. Haga clic en **Siguiente** y, a continuación, en **Finalizar**.

Si cambia el nombre del servidor vSphere después de la instalación, debe generar un certificado autofirmado nuevo en ese servidor antes de importar el certificado nuevo.

## **Consideraciones sobre la configuración**

### **Crear una VM maestra:**

Use una VM maestra para proporcionar las aplicaciones y los escritorios de los usuarios en un catálogo de máquinas. En el hipervisor:

1. Instale el VDA en la VM maestra y seleccione la opción de optimizar el escritorio, lo que mejora el rendimiento.
2. Tome una instantánea de la VM maestra para usarla como copia de seguridad.

### **Crear una conexión:**

En el asistente para la creación de conexiones:

- Seleccione el tipo de conexión VMware.
- Especifique la dirección del punto de acceso para el SDK de vCenter.

- Especifique las credenciales de la cuenta de usuario VMware que ha configurado y que incluye permisos para crear nuevas VM. Especifique el nombre de usuario en el formato dominio/nombre\_de\_usuario.

## Huella digital SSL de VMware

La funcionalidad huella digital SSL de VMware resuelve un error frecuente que se daba al crear una conexión de host a un hipervisor VMware vSphere. Anteriormente, los administradores tenían que crear manualmente una relación de confianza entre los Delivery Controllers del sitio y el certificado del hipervisor antes de crear una conexión. La función huella digital SSL de VMware elimina ese requisito manual: la huella digital del certificado que no es de confianza se almacena en la base de datos del sitio, de modo que el hipervisor puede identificarse continuamente como hipervisor de confianza por Citrix Virtual Apps and Desktops o, incluso si no es por ellos, por los Controllers.

Al crear una conexión de host de vSphere en Studio, un cuadro de diálogo le permite ver el certificado de la máquina a la que se está conectando. Por lo que puede elegir si quiere confiar en ella.

## Entornos de virtualización de Nutanix

October 6, 2022

Siga estas instrucciones si usa Nutanix Acropolis para ofrecer máquinas virtuales en su entorno de Citrix Virtual Apps and Desktops. El proceso de configuración incluye las siguientes tareas:

- Instalar y registrar el plug-in de Nutanix en el entorno de Citrix Virtual Apps and Desktops.
- Crear una conexión con el hipervisor Nutanix Acropolis.
- Crear un catálogo de máquinas que usa una instantánea de la imagen maestra que se ha creado en el hipervisor Nutanix.

Para obtener más información, consulte la guía de instalación de plug-ins MCS de Nutanix Acropolis, disponible en el [portal de asistencia de Nutanix](#).

## Prepare la instalación del plug-in MCS de Nutanix para Citrix Cloud Connector

Los requisitos previos para la integración de Nutanix Acropolis en el Delivery Controller de Citrix Virtual Apps and Desktops incluyen lo siguiente:

- Los usuarios con el plug-in MCS de AHV para el instalador de Citrix Cloud Connector deben tener privilegios de administrador en la VM de Citrix Cloud Connector.

- Registre la VM de Citrix Cloud Connector con una ubicación de recursos en el arrendatario de Citrix Cloud.
- Instale el plug-in MCS de AHV para Citrix Cloud Connector en todos los Cloud Connectors registrados con el arrendatario de Citrix Cloud. Realice esta instalación aunque los Connectors comuniquen una ubicación de recursos sin AHV.

## Instalar y registrar el plug-in de Nutanix

Después de instalar los componentes de Citrix Virtual Apps and Desktops, complete el siguiente procedimiento para instalar y registrar el plug-in de Nutanix en los Delivery Controllers. Entonces, podrá usar Studio para crear una conexión con el hipervisor Nutanix y, a continuación, crear un catálogo de máquinas que use una instantánea de la imagen maestra que creó en el entorno de Nutanix.

1. Obtenga el plug-in de Nutanix, e instálelo en los Delivery Controllers.
2. Compruebe que se ha creado una carpeta de Nutanix Acropolis en C:\Archivos de programa\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0.
3. Ejecute `C:\Program Files\Common Files\Citrix\HCLPlugins\RegisterPlugins.exe -PluginsRoot "C:\Program Files\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0"`.
4. Reinicie los servicios Citrix Host Service, Citrix Broker Service y Citrix Machine Creation Services.
5. Ejecute los siguientes cmdlets de PowerShell para comprobar que el plug-in de Nutanix Acropolis se ha registrado:

```
1 Add-PSSnapin Citrix*
2 Get-HypervisorPlugin
3 <!--NeedCopy-->
```

## Crear una conexión con Nutanix

Consulte [Crear un sitio](#) y [Conexiones y recursos](#) para obtener información completa sobre todas las páginas de los asistentes que crean conexiones.

En el asistente “Configuración de sitio” o “Agregar conexión y recursos”, seleccione el tipo de conexión **Nutanix** en la página **Conexión** y luego especifique la dirección y las credenciales del hipervisor, así como un nombre para la conexión. En la página **Red**, seleccione una red para la unidad de alojamiento.

## Crear un catálogo de máquinas mediante una instantánea de Nutanix

Esta información complementa las instrucciones del artículo [Crear catálogos de máquinas](#). Solo describe los campos que son específicos de Nutanix.

La instantánea que seleccione es la plantilla que se usará para crear las máquinas virtuales del catálogo. Antes de crear el catálogo de máquinas, cree las imágenes y las instantáneas en Nutanix.

- Para obtener información acerca de las imágenes maestras en general, consulte el artículo “Crear catálogos de máquinas”.
- Para obtener información sobre los procedimientos de Nutanix para la creación de imágenes y las instantáneas, consulte la documentación de Nutanix a la que se hace referencia.

Las páginas **Sistema operativo** y **Administración de máquinas** no contienen información específica de Nutanix. Siga las instrucciones indicadas en el artículo [Crear catálogos de máquinas](#).

En la página **Contenedor**, que es específica de Nutanix, seleccione el contenedor donde se colocarán los discos de las VM.

En la página **Imagen maestra**, seleccione la instantánea de la imagen. Los nombres de instantánea de Acropolis deben llevar el prefijo “XD\_” para usarse en Citrix Virtual Apps and Desktops. Utilice la consola de Acropolis para cambiar el nombre de las instantáneas, si es necesario. Si cambia el nombre de las instantáneas, reinicie el asistente [Crear catálogos](#) para ver una lista con los nombres actualizados.

En la página **Máquinas virtuales**, indique la cantidad de unidades CPU virtuales y la cantidad de núcleos por cada CPU virtual.

Las páginas **Tarjetas de red**, **Cuentas de equipo** y **Resumen** no contienen información específica de Nutanix. Siga las instrucciones indicadas en el artículo [Crear catálogos de máquinas](#).

## Entornos de virtualización de Microsoft Azure

August 10, 2023

### NOTA:

Este artículo contiene información sobre Azure (Classic). Para obtener información sobre Azure Resource Manager, consulte [Entornos de virtualización para Azure Resource Manager](#).

## Configurar conexión

Cuando se utiliza Studio para crear una conexión de Microsoft Azure, se necesita información del archivo de configuración de publicación de Microsoft Azure. La información de ese archivo XML ref-

erente a cada suscripción es similar al ejemplo siguiente (el certificado de administración real será mucho más largo):

```
1 <Subscription
2 ServiceManagementUrl="\*address\*"
3 Id="o1455234-0r10-nb93-at53-21zx6b87aabb7p"
4 Name="Test1"
5 ManagementCertificate=";alkjdflaksdjfl;akjsdfl;akjsdfl;
   sdjfklsdfilaskjdfklquweiopruaiopdfaklsdjfjsdílfasdkl;fjerioup" />
6 <!--NeedCopy-->
```

En el siguiente procedimiento, se presupone que está creando una conexión desde Studio y ha iniciado el asistente para la creación de sitios o el asistente para la creación de conexiones.

1. En un explorador web, vaya a <https://manage.windowsazure.com/publishsettings/index>.
2. Haga clic en el icono Cloud Shell, situado junto al cuadro de búsqueda y siga las [instrucciones](#) para descargar el archivo de parámetros de publicación.
3. En Studio, en la página **Conexión** del asistente, después de seleccionar el tipo de conexión de Microsoft Azure, haga clic en **Importar**.
4. Si tiene más de una suscripción, se le pedirá que seleccione la suscripción pertinente.

El identificador y el certificado se importan automática y silenciosamente en Studio.

Las acciones de energía que se llevan a cabo mediante una conexión están sujetas a umbrales. Por lo general, los valores predeterminados son adecuados y no se deben cambiar. Sin embargo, puede modificar una conexión y cambiarlos (no puede, en cambio, cambiar estos valores cuando cree la conexión). Para obtener más información, consulte [Modificar parámetros de conexión](#).

## Máquinas virtuales

En Studio, al crear un catálogo de máquinas, la selección del tamaño de cada máquina virtual depende de las opciones que presente Studio, el coste y el rendimiento del tipo seleccionado de instancia de VM, además de la escalabilidad.

Studio presenta todas las opciones de instancia de máquina virtual que Microsoft Azure ofrece en una región seleccionada; Citrix no puede modificar esta presentación. Por lo tanto, debe conocer sus aplicaciones y sus CPU, su memoria y sus requisitos de E/S. Dispone de varias opciones de rendimiento a precios diferentes; consulte los siguientes artículos de Microsoft para entenderlas mejor.

- Tamaños de máquinas virtuales y el servicio de nube para Azure: <https://docs.microsoft.com/en-us/azure/cloud-services/cloud-services-sizes-specs>
- Precios de máquinas virtuales: <http://azure.microsoft.com/en-us/pricing/details/virtual-machines>

**Nivel Básico:** Las máquinas virtuales que tengan como prefijo “Básico” representan el disco básico. Están limitadas principalmente por el nivel 300 de IOPS que admite Microsoft. Estos parámetros no se

recomiendan para cargas de trabajo de SO de escritorio (VDI) o SO de servidor RDSH (host de sesión de Escritorio remoto).

**Nivel estándar:** Las VM de nivel estándar aparecen en cuatro series: A, D, DS y G.

Serie	Aparecen en Studio como
A	Muy pequeña, pequeña, mediana, grande, muy grande, A5, A6, A7, A8, A9, A10, A11. Las medianas y grandes se recomiendan para pruebas con cargas de trabajo de SO de escritorio (VDI) o SO de servidor (RDSH), respectivamente.
D	Standard_D1, D2, D3, D4, D11, D12, D13, D14. Estas máquinas virtuales ofrecen SSD para almacenamiento temporal.
DS	Standard_DS1, DS2, DS3, DS4, DS11, DS12, DS13, DS14. Estas máquinas virtuales ofrecen almacenamiento de SSD local para todos los discos.
G	Standard_G1–G5. Estas máquinas virtuales están diseñadas para informática de alto rendimiento.

Al aprovisionar máquinas en el almacenamiento premium de Azure, debe seleccionar un tamaño de máquinas que se admita en la cuenta de almacenamiento premium.

### Coste y rendimiento de tipos de instancias de máquinas virtuales

Para obtener la lista de precios de EE. UU., el coste de cada tipo de instancia de máquina virtual por hora está disponible en <http://azure.microsoft.com/en-us/pricing/details/virtual-machines/>.

Cuando se trabaja con entornos de nube, es importante entender los requisitos informáticos reales. En pruebas de concepto u otras actividades de prueba, puede ser tentador aprovechar los tipos de instancias de máquinas virtuales de alto rendimiento. También puede resultar tentador utilizar las máquinas virtuales de menor rendimiento para ahorrar costes. Sin embargo, el objetivo es usar una máquina virtual apropiada para la tarea en cuestión. Empezar por las de mayor rendimiento puede no darle los resultados que necesita y será muy caro con el tiempo (en algunos casos, en solo siete días). En caso de tipos de instancias de máquinas virtuales de bajo rendimiento con un coste menor, el rendimiento y la usabilidad pueden no ser adecuados para la tarea.

Para cargas de trabajo de SO de escritorio (VDI) o SO de servidor (RDSH), los resultados de las pruebas con LoginVSI y su carga media de trabajo muestran que los tipos de instancia Mediana (A2) y Grande (A3) ofrecen la mejor relación entre precio y rendimiento.

Los tipos de instancia Mediana (A2) y Grande (A3 o A5) representan la mejor relación entre coste y rendimiento para evaluar cargas de trabajo. No se recomienda nada menor. Una serie de máquinas virtuales con mayores capacidades pueden ofrecer a aplicaciones o usuarios el rendimiento y la usabilidad que estos necesiten. Sin embargo, es mejor usar los tres tipos de instancia mencionados como referencia para determinar si el coste más elevado que implica un tipo de instancia de VM con mayores capacidades se traduce en un valor real.

## **Escalabilidad**

Existen varias restricciones que afectan la escalabilidad de catálogos en una unidad de alojamiento. Algunas restricciones, como la cantidad de núcleos de CPU en una suscripción de Azure, se pueden solventar poniéndose en contacto con el servicio de asistencia de Microsoft Azure para aumentar su valor predeterminado (20). Otros, como la cantidad de máquinas virtuales en una red virtual por suscripción (2048), no se pueden cambiar.

Actualmente, Citrix admite 1000 máquinas virtuales en un catálogo.

Para ampliar la cantidad de máquinas virtuales en un catálogo o un host, póngase en contacto con el servicio de asistencia de Microsoft Azure. Los límites predeterminados de Microsoft Azure impiden la ampliación a más de una cantidad determinada de máquinas virtuales; no obstante, este límite cambia con frecuencia. Consulte la información más reciente en: <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/azure-subscription-service-limits>.

Una red virtual de Microsoft Azure admite un máximo de 2048 máquinas virtuales.

Microsoft recomienda un límite de 40 imágenes de VM de disco estándar por servicio de nube. A la hora de realizar ampliaciones de escala, tenga en cuenta la cantidad de servicios de nube necesarios para la cantidad de máquinas virtuales de toda la conexión. Asimismo, tenga en mente la cantidad de máquinas virtuales necesarias para proporcionar las aplicaciones alojadas.

Póngase en contacto con el servicio de asistencia de Microsoft Azure para determinar si se deben aumentar las limitaciones predeterminadas de núcleos de CPU para ajustarse a sus cargas de trabajo.

## **Instalar componentes principales**

September 22, 2021

Los componentes principales presentes en los medios de instalación son Citrix Delivery Controller, Citrix Studio, Citrix Director y Citrix License Server

(en versiones anteriores a 1912 LTSR CU1, los componentes principales incluían Citrix StoreFront; todavía puede instalar StoreFront si hace clic en el icono de **Citrix StoreFront** desde la sección **Ampliar implementación** o ejecuta el comando disponible en los medios de instalación).

Antes de comenzar una instalación, consulte este artículo y [Antes de instalar](#).

En este artículo, se describe la secuencia de pasos que se siguen en el asistente de instalación de los componentes principales. Se ofrecen asimismo los equivalentes de línea de comandos. Para obtener más información, consulte [Instalación desde la línea de comandos](#).

### **Paso 1. Descargue el software del producto e inicie el asistente**

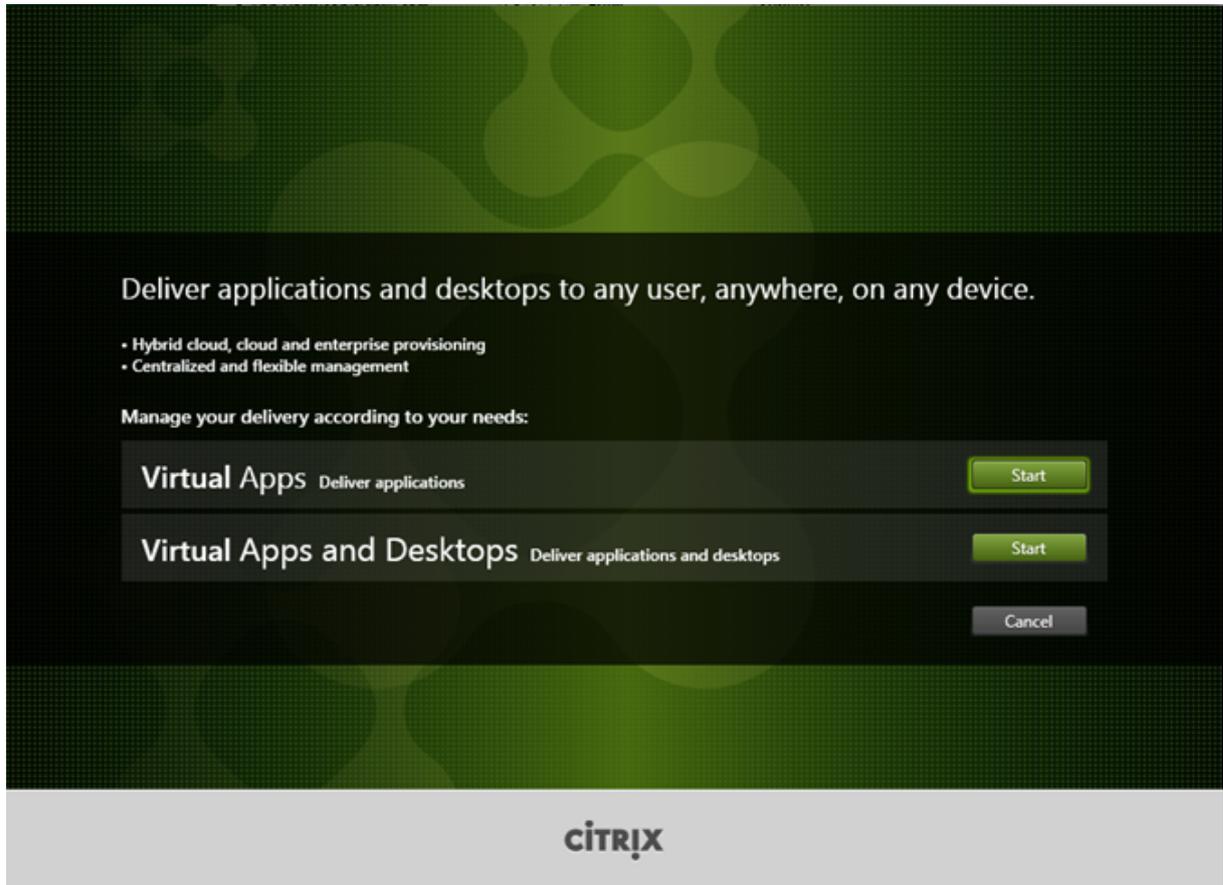
Utilice las credenciales de su cuenta de Citrix para acceder a la página de descargas de Citrix Virtual Apps and Desktops. Descargue el archivo ISO del producto.

Descomprima el archivo. Si lo prefiere, puede grabar un DVD del archivo ISO.

Inicie sesión en la máquina donde quiere instalar los componentes. Para ello, utilice una cuenta de administrador local.

Introduzca el DVD en la unidad o monte el archivo ISO. Si el instalador no se inicia automáticamente, haga doble clic en la aplicación **AutoSelect** o la unidad montada.

## Paso 2. Elija el producto a instalar

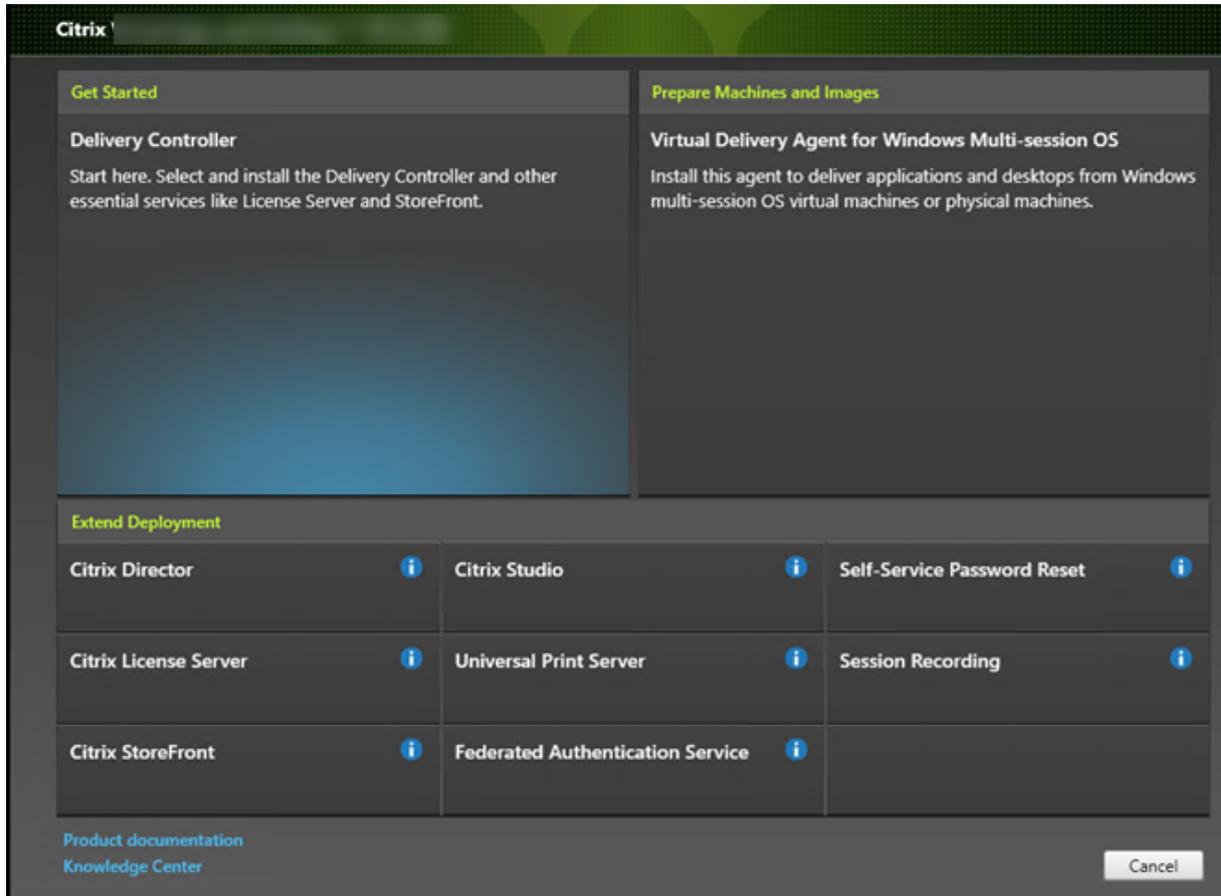


Haga clic en **Iniciar** situado junto al producto a instalar: Virtual Apps o Virtual Apps and Desktops.

(Si la máquina ya tiene instalados componentes de Citrix Virtual Apps and Desktops, esta página no aparecerá.)

Opción de la línea de comandos: `/xenapp` para instalar Citrix Virtual Apps; se instalan Citrix Virtual Apps and Desktops si se omite la opción

### Paso 3. Elija qué instalar

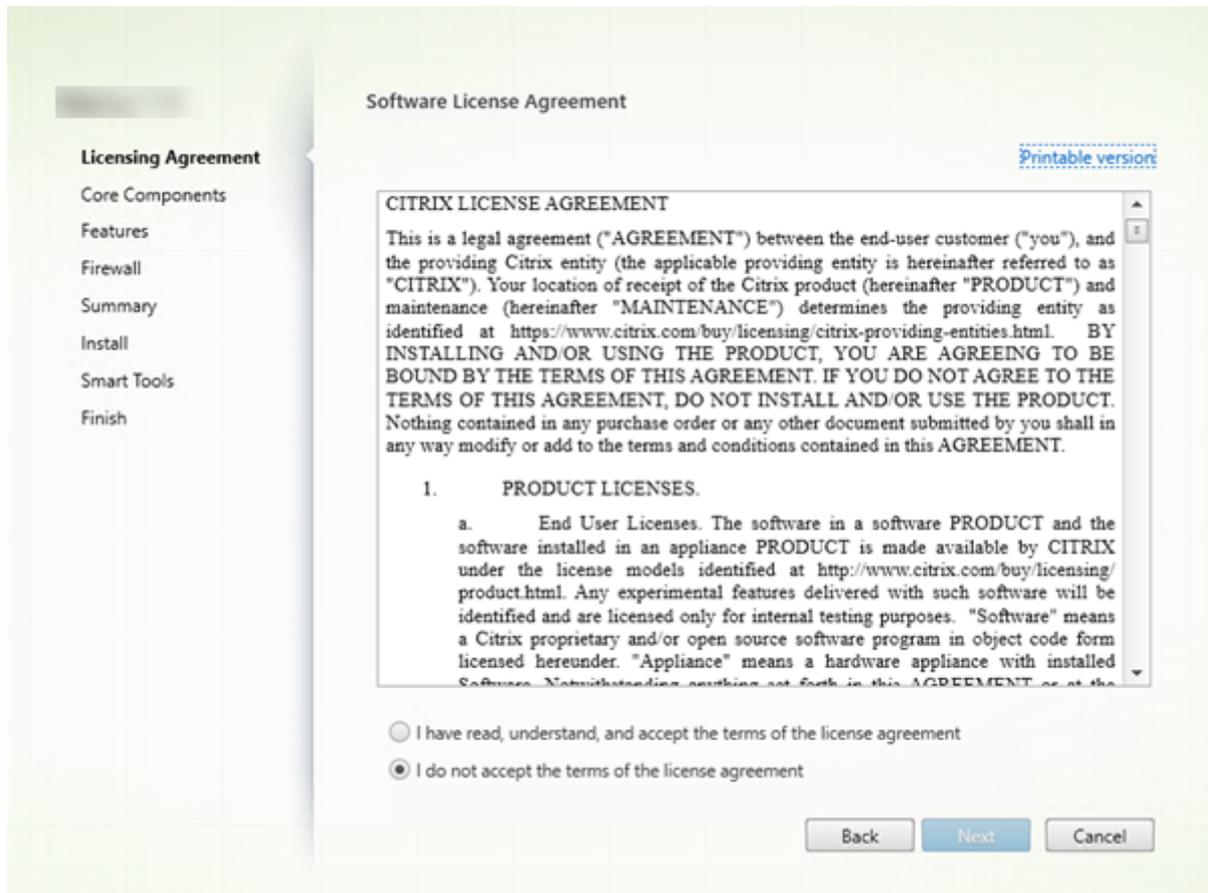


Si acaba de empezar, seleccione **Delivery Controller**. (En una página posterior, seleccionará los componentes concretos que se instalarán en esta máquina.)

Si ya ha instalado un Controller (en esta máquina o en otra) y quiere instalar otro componente, selecciónelo en la sección **Ampliar implementación**.

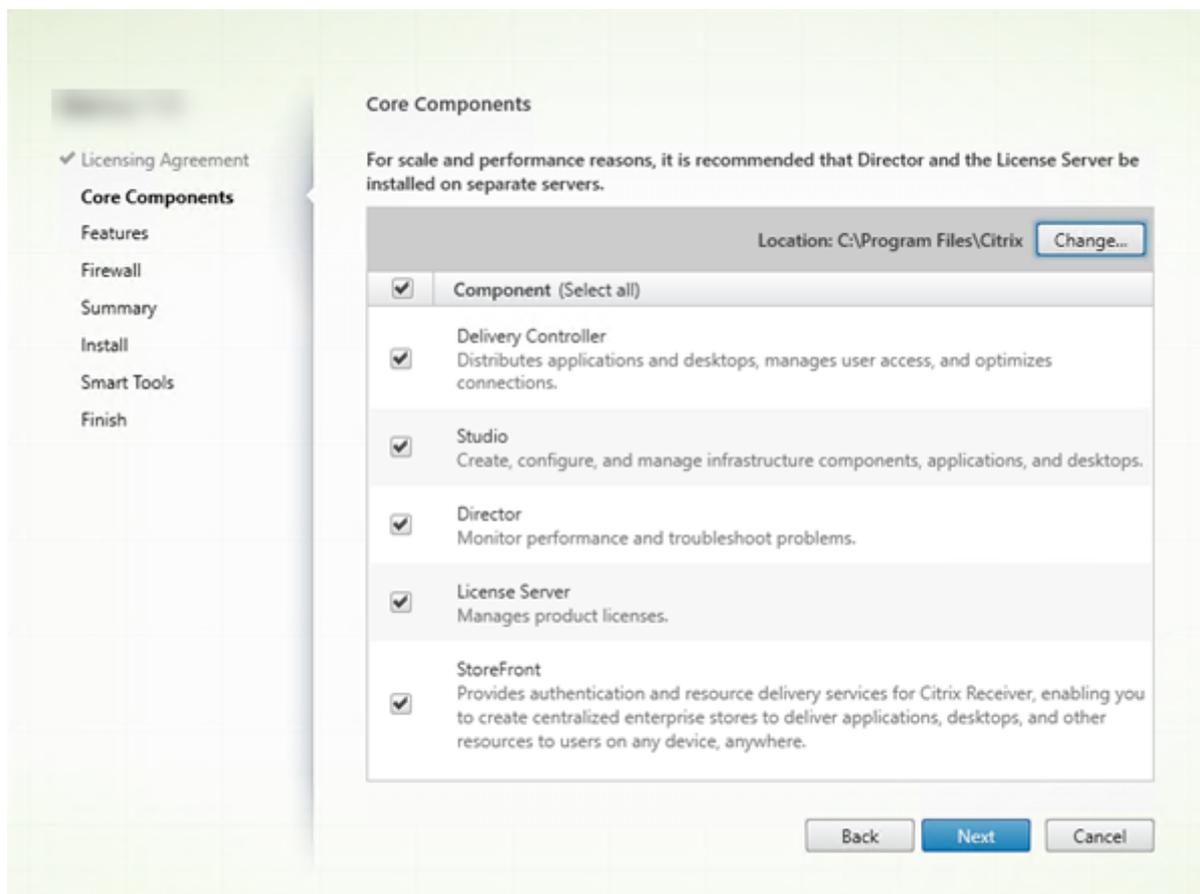
Opción de línea de comandos: `/components`

## Paso 4. Lea y acepte el contrato de licencia



En la página **Contrato de licencia**, después de leer el contrato de licencia, indique que lo ha leído y lo acepta. A continuación, haga clic en **Siguiente**.

## Paso 5. Seleccione los componentes a instalar y la ubicación de la instalación



En la página **Componentes principales**:

- **Ubicación:** De forma predeterminada, los componentes se instalan en C:\Archivos de programa\Citrix. La opción predeterminada no presenta problemas para la mayoría de las implementaciones. Si indica otra ubicación, esta debe tener permisos de ejecución para el servicio de red.
- **Componentes:** De forma predeterminada, están marcadas las casillas de todos los componentes principales. Instalar todos los componentes principales en un servidor puede servir para pruebas o pruebas de concepto, o bien puede ser útil en implementaciones pequeñas de producción. No obstante, para entornos de producción grandes, Citrix recomienda instalar Director, StoreFront y el Servidor de licencias en servidores independientes.

Indique solo los componentes que quiera instalar en esta máquina. Después de instalar los componentes en esta máquina, podrá ejecutar de nuevo el instalador en otras máquinas para instalar otros componentes.

Aparecerá un icono para avisarle si decide no instalar un componente principal necesario en esta máquina. Ese aviso le recordará que debe instalar ese componente, aunque no sea nece-

sariamente en esta máquina.

Haga clic en **Siguiente**.

Opción de la línea de comandos: `/installdir, /components, /exclude`

### **Comprobación de hardware**

Al instalar o actualizar un Delivery Controller, se comprueba el hardware. El instalador le avisa si la máquina tiene menos RAM de la recomendada (5 GB), lo que puede afectar a la estabilidad del sitio (Para obtener más información, consulte [Requisitos de hardware](#)).

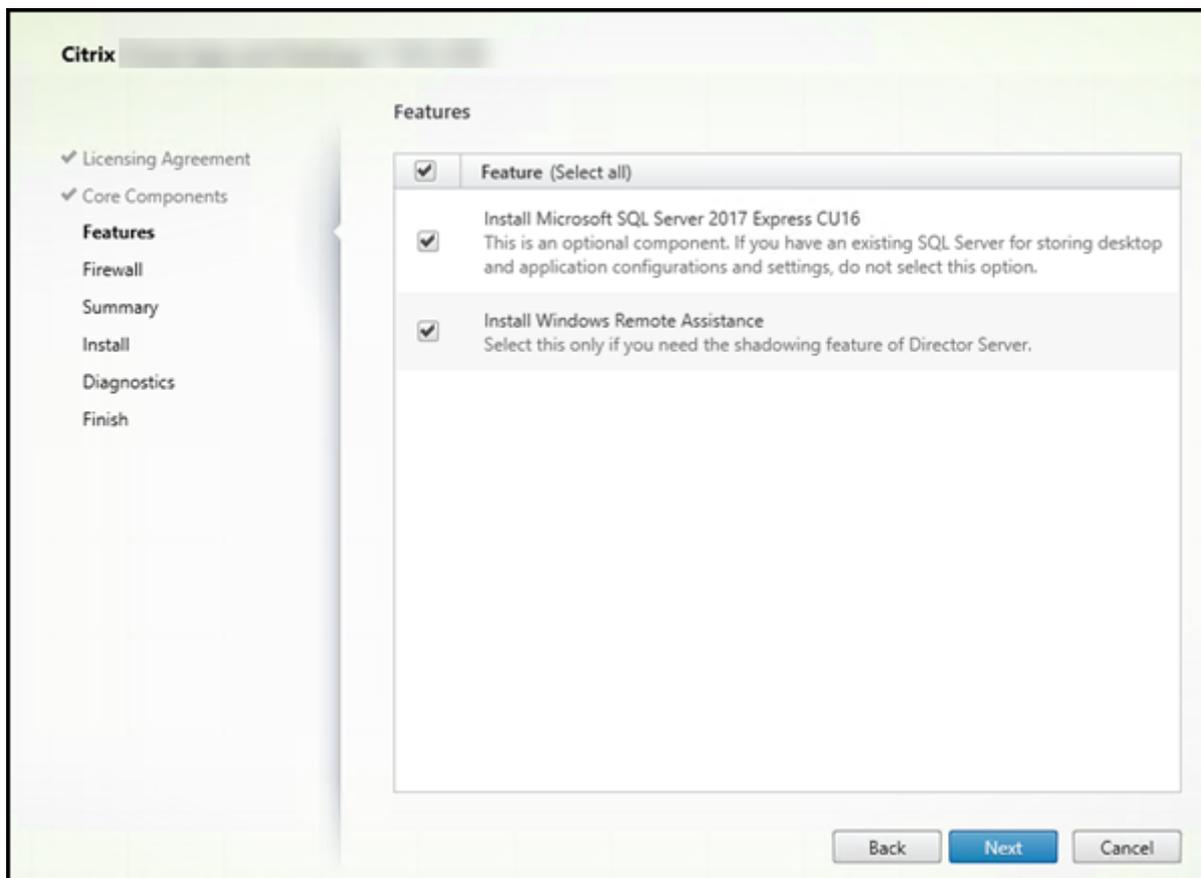
**Interfaz gráfica:** Aparece un cuadro de diálogo.

- Recomendación: Haga clic en **Cancelar** para detener la instalación. Agregue más RAM a la máquina y vuelva a iniciar la instalación.
- También puede hacer clic en **Siguiente** para continuar con la instalación. Es posible que el sitio tenga problemas de estabilidad.

**Interfaz de la línea de comandos:** La instalación/actualización finaliza. Los registros de instalación contienen un mensaje que describe lo que se ha encontrado y las opciones disponibles.

- Recomendación: Agregue más RAM a la máquina y vuelva a ejecutar el comando.
- Si no, como alternativa, ejecute el comando de nuevo con la opción `/ignore_hw_check_failure` para anular la advertencia. Es posible que su sitio tenga problemas de estabilidad.

## Paso 6. Habilite o inhabilite las funciones



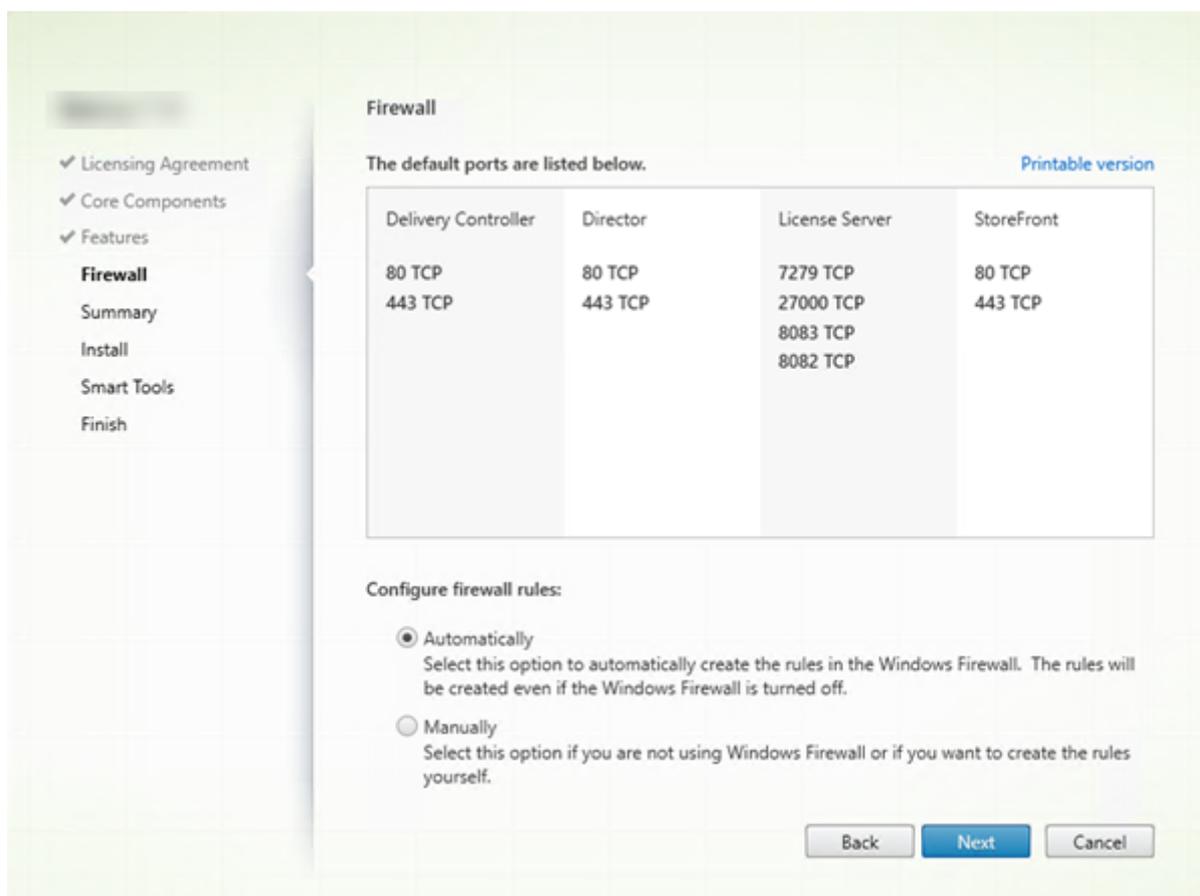
En la página **Funciones**:

- Seleccione si instalar Microsoft SQL Server Express para usarlo como la base de datos del sitio. De forma predeterminada, esta opción está habilitada. Si no conoce las bases de datos de Citrix Virtual Apps and Desktops, consulte [Bases de datos](#).
- Al instalar Director, la Asistencia remota de Windows se instala automáticamente. Puede elegir si quiere habilitar el remedo en la Asistencia remota de Windows para utilizarlo con el remedo de usuarios de Director. Habilitar el remedo abre el puerto TCP 3389. De manera predeterminada, esta función está habilitada. La opción predeterminada no presenta problemas para la mayoría de las implementaciones. Esta funcionalidad aparece solamente cuando se instala Director.

Haga clic en **Siguiente**.

Opciones de la línea de comandos: `/nosql` (para impedir la instalación), `/no_remote_assistance` (para impedir que se habilite)

## Paso 7. Abra los puertos del Firewall de Windows



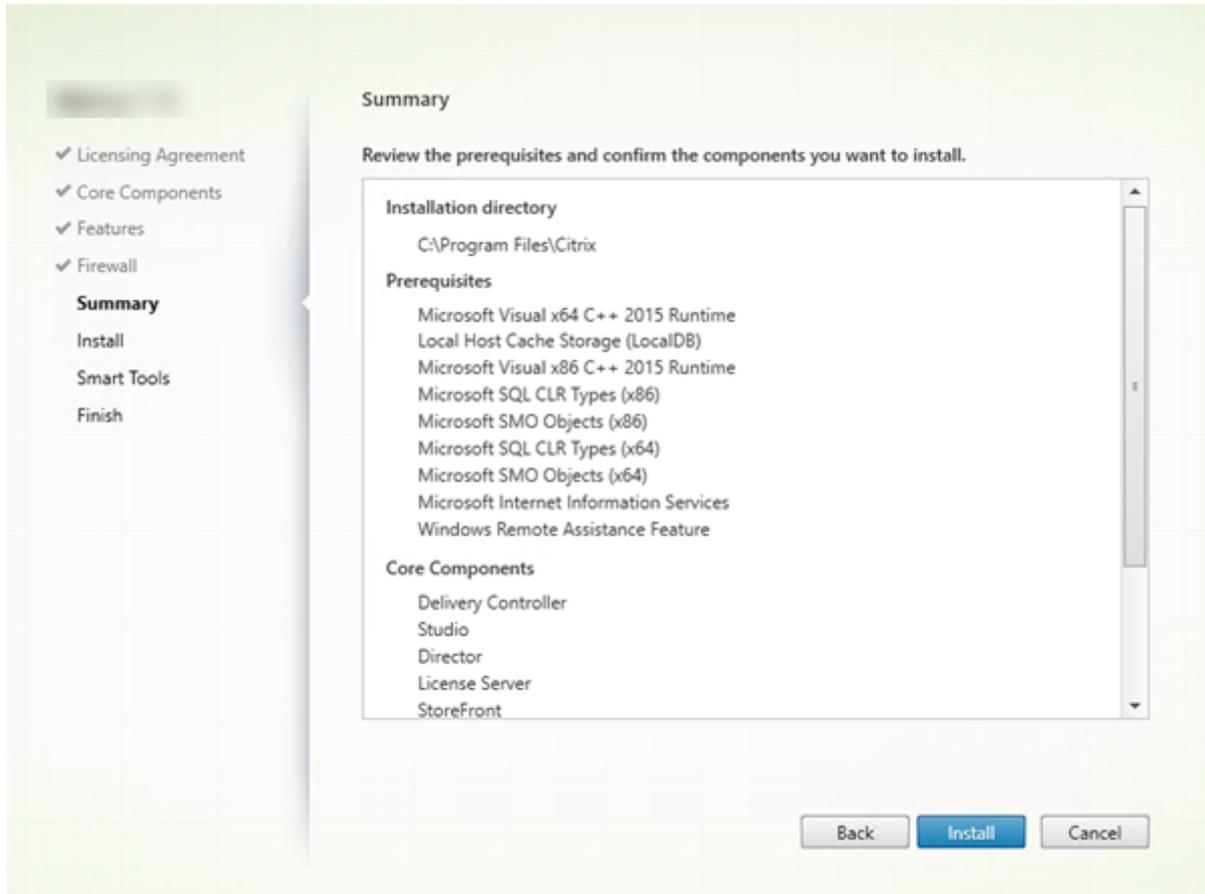
De forma predeterminada, los puertos que aparecen en la página **Firewall** se abren automáticamente si el servicio Firewall de Windows se está ejecutando, incluso aunque el firewall no esté habilitado. La opción predeterminada no presenta problemas para la mayoría de las implementaciones. Para obtener información acerca de los puertos, consulte [Puertos de red](#).

Haga clic en **Siguiente**.

(En el gráfico, se muestran las listas de los puertos que aparecen si se elige instalar todos los componentes principales en esta máquina. Por regla general, este tipo de instalación solo se realiza para las implementaciones de prueba.)

Opción de línea de comandos: `/configure_firewall`

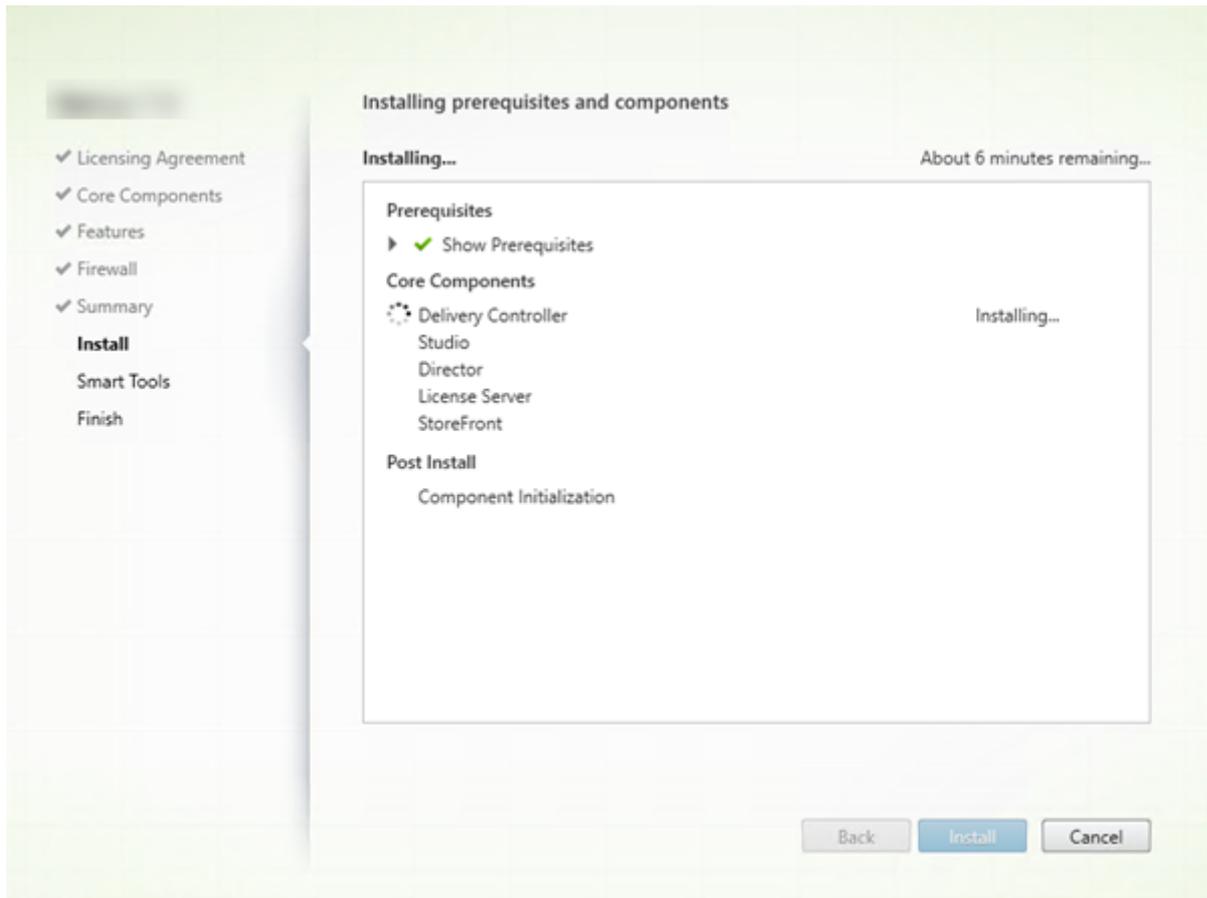
## Paso 8. Revise los requisitos previos y confirme la instalación



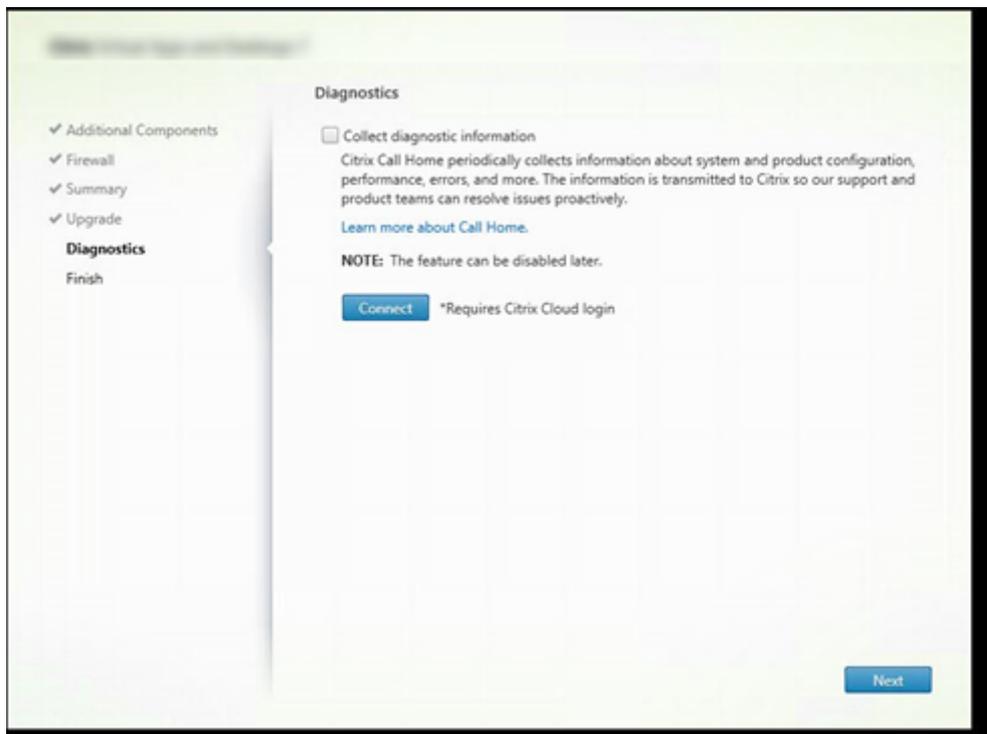
La página **Resumen** muestra lo que se instalará. Si fuera necesario, puede usar el botón Atrás para volver a las páginas anteriores del asistente y cambiar las opciones.

Cuando haya terminado, haga clic en **Instalar**.

La pantalla muestra el progreso de la instalación.



## Paso 9: Diagnóstico



En la página **Diagnósticos**, elija si quiere participar en Citrix Call Home.

Esta página aparece al instalar un Delivery Controller mediante la interfaz gráfica. Cuando instala StoreFront (pero no un Controller), el asistente muestra esta página. Cuando instala otros componentes principales (pero no un Controller o StoreFront), el asistente no muestra esta página.

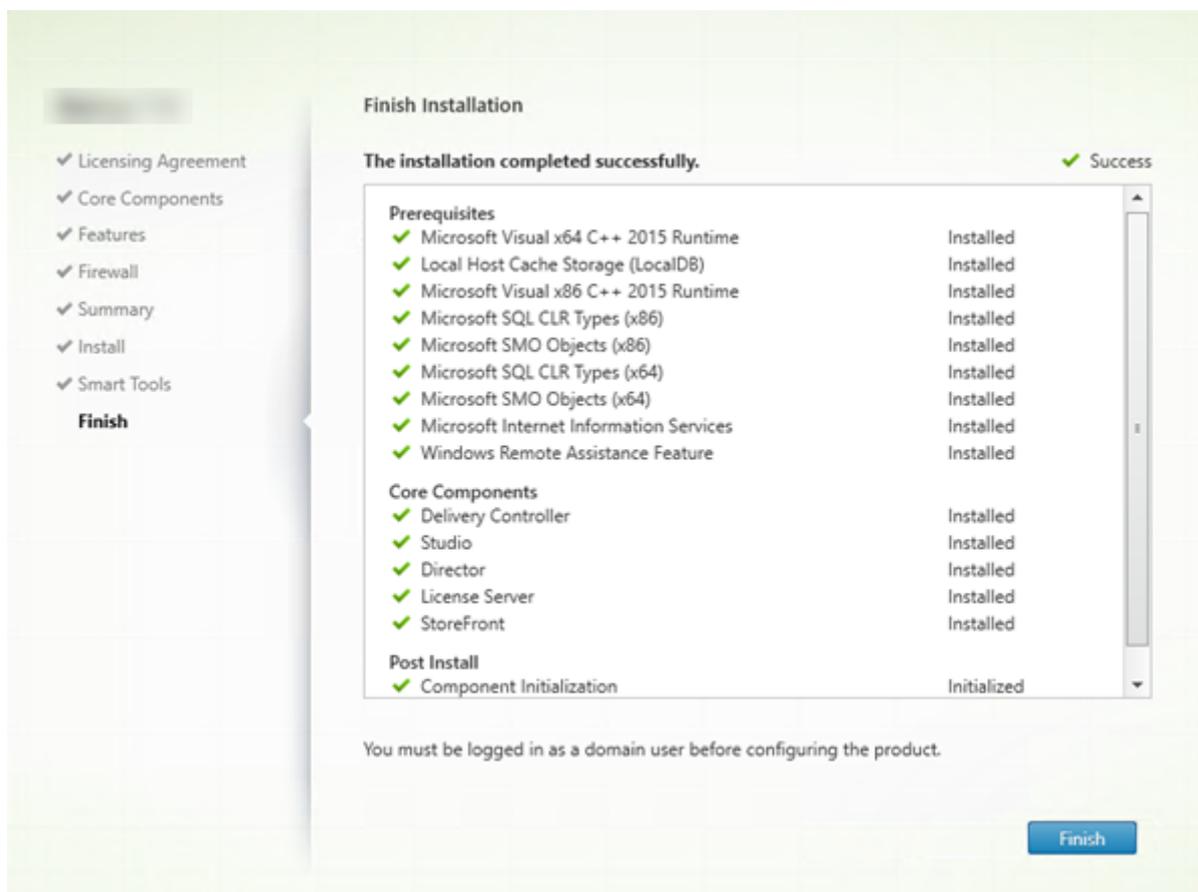
Durante una actualización, esta página no aparece si Call Home ya está habilitado o si se produce un error relacionado con Citrix Telemetry Service en el instalador.

Si elige participar (opción predeterminada), haga clic en **Conectar**. Cuando se le solicite, introduzca las credenciales de su cuenta de Citrix (puede cambiar su opción de inscripción más tarde, después de la instalación).

Una vez validadas las credenciales (o si elige no participar), haga clic en **Siguiente**.

Para obtener más información, consulte [Call Home](#).

## Paso 10: Finalice la instalación



La página **Finalizar** presenta marcas de verificación verdes para todos los requisitos previos y los componentes que se hayan instalado e inicializado correctamente.

Haga clic en **Finalizar**.

## Paso 11: Instale los componentes principales restantes en otras máquinas

Si ha instalado todos los componentes principales en una máquina, continúe con Sigüientes pasos. De lo contrario, ejecute el instalador en las demás máquinas para instalar otros componentes principales. También puede instalar más Controllers en otros servidores.

### Sigüientes pasos

Después de instalar todos los componentes principales, use Studio para [crear un sitio](#).

Después de crear el sitio, [instale agentes VDA](#).

Puede usar el instalador de producto completo en cualquier momento para ampliar la implementación con los sigüientes componentes:

- **Componente de servidor Universal Print Server:** Inicie el instalador en el servidor de impresión. Seleccione **Universal Print Server** en la sección **Ampliar implementación**. Acepte el contrato de licencia. De forma predeterminada, en la página **Firewall**, los puertos TCP 7229 y 8080 se abren en el firewall si el servicio Firewall de Windows se está ejecutando, incluso si el firewall no está habilitado. Puede inhabilitar esa acción predeterminada si quiere abrir los puertos manualmente.

Para instalar este componente desde la línea de comandos, consulte [Instalación desde la línea de comandos](#).

- [Servicio de autenticación federada](#).
- [Autoservicio de restablecimiento de contraseñas](#).
- [Grabación de sesiones](#).

## Instalar VDA

November 15, 2022

### Importante:

Si va a actualizar un VDA que tiene instalado Personal vDisk (PvD), consulte [Actualizar los VDA a la versión 1912 o una posterior](#).

Existen dos tipos de VDA para máquinas Windows: VDA para SO multisesión y VDA para SO de sesión única. (Para obtener más información acerca de los agentes VDA para máquinas Linux, consulte la documentación de [Linux Virtual Delivery Agent](#).)

Antes de comenzar una instalación, consulte [Antes de la instalación](#) y complete todas las tareas de preparación.

Antes de instalar agentes VDA, debe tener instalados los componentes principales. También puede crear el sitio antes de instalar los agentes VDA.

En este artículo, se describe la secuencia de pasos que se siguen en el asistente de instalación de un VDA. Se ofrecen asimismo los equivalentes de línea de comandos. Para obtener más información, consulte [Instalación desde la línea de comandos](#).

### Paso 1. Descargue el software del producto e inicie el asistente

Si usa el instalador de producto completo:

1. Si aún no ha descargado la imagen ISO del producto:

- Utilice las credenciales de su cuenta de Citrix para acceder a la página de descargas de Citrix Virtual Apps and Desktops. Descargue el archivo ISO del producto.
  - Descomprima el archivo. Si lo prefiere, puede grabar un DVD del archivo ISO.
2. Use una cuenta de administrador local en la imagen o la máquina donde esté instalando el VDA. Introduzca el DVD en la unidad o monte el archivo ISO. Si el instalador no se inicia automáticamente, haga doble clic en la aplicación **AutoSelect** o la unidad montada.

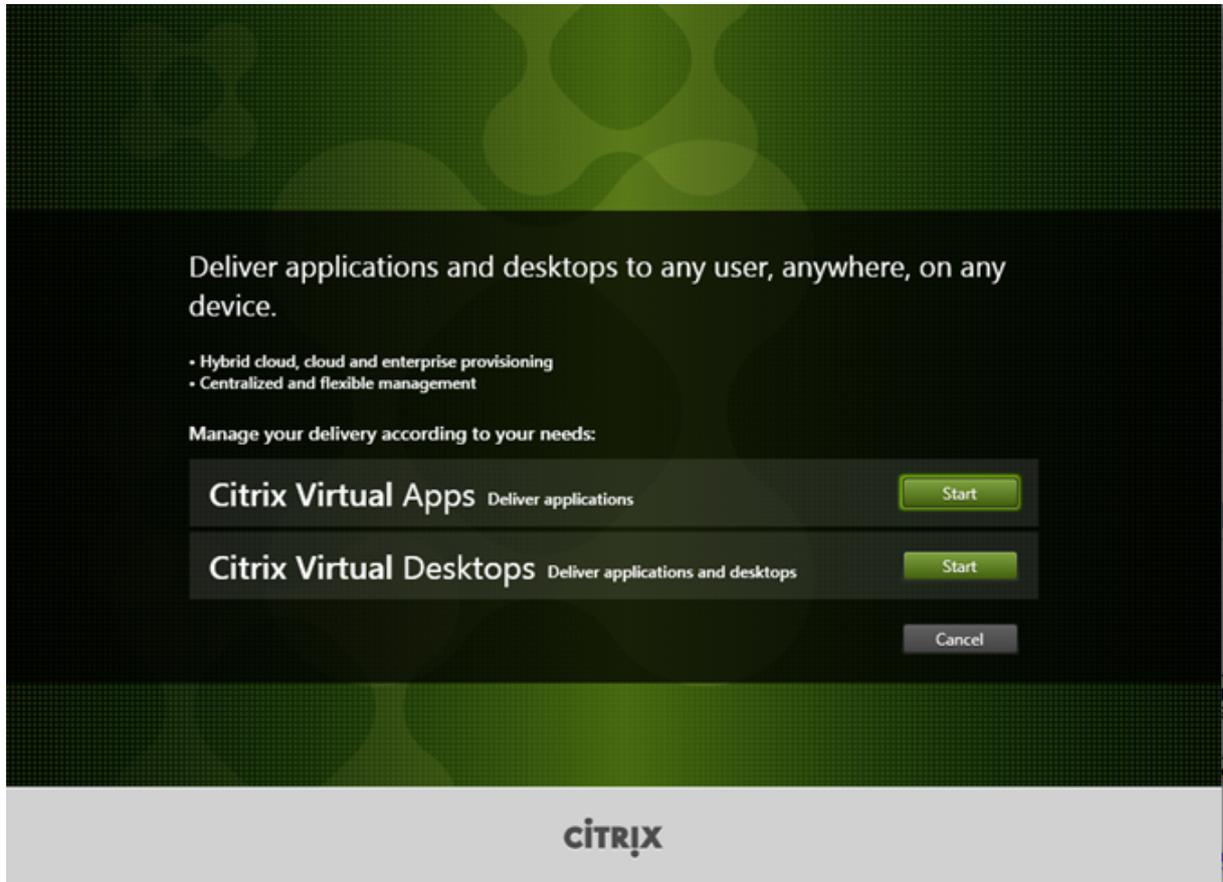
Se iniciará el asistente de instalación.

Si usa un paquete independiente:

1. Utilice las credenciales de su cuenta de Citrix para acceder a la página de descargas de Citrix Virtual Apps and Desktops. Descargue el paquete correspondiente:
  - VDAServerSetup.exe: VDA de SO multisesión *versión*
  - VDAWorkstationSetup.exe: VDA de SO de sesión única *versión*
  - VDAWorkstationCoreSetup.exe: VDA de servicios básicos de SO de sesión única *versión*
2. Haga clic con el botón secundario en el paquete que ha descargado y seleccione **Ejecutar como administrador**.

Se iniciará el asistente de instalación.

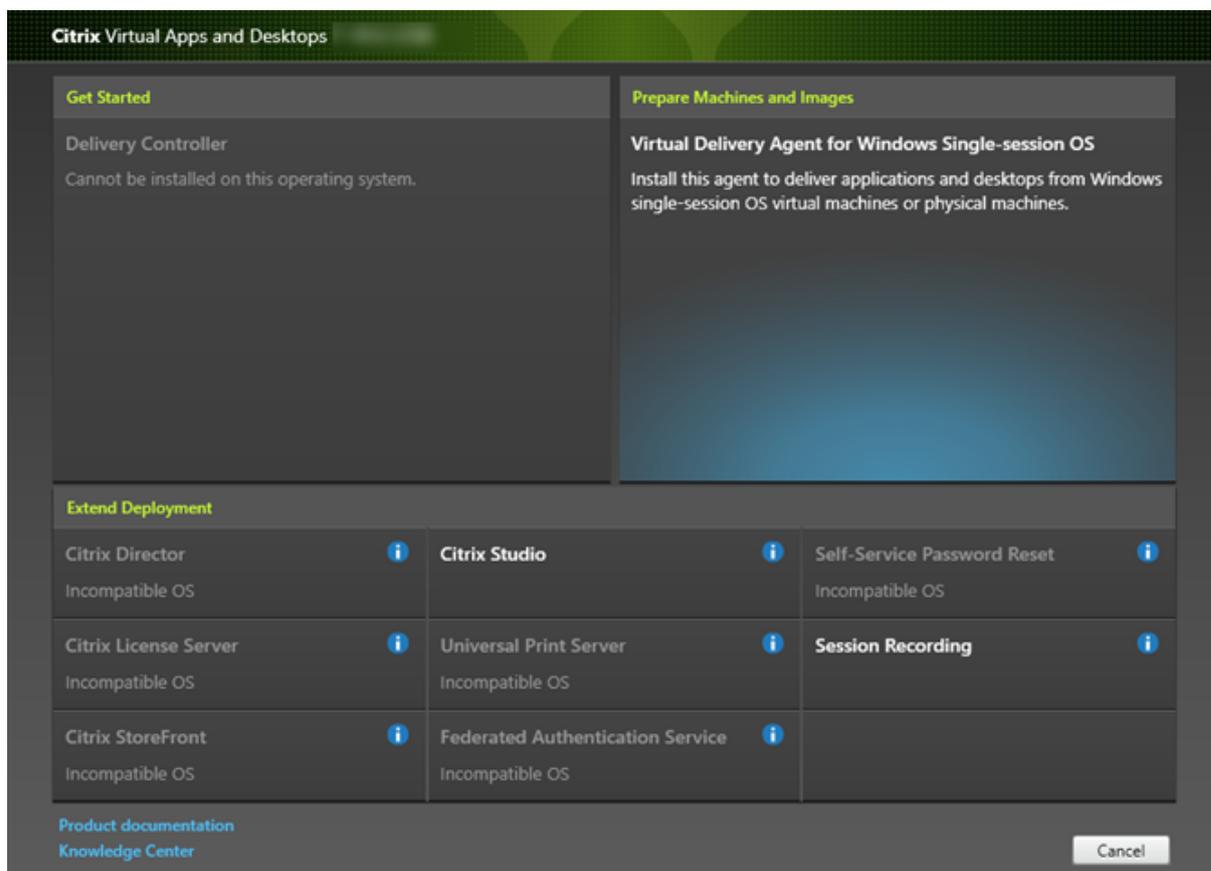
## Paso 2. Elija el producto a instalar



Haga clic en **Iniciar**, situado junto al producto a instalar: Citrix Virtual Apps o Citrix Virtual Desktops. (Si la máquina ya tiene instalados componentes de Citrix Virtual Apps o Citrix Virtual Desktops, esta página no aparecerá.)

Opción de línea de comandos: `/xenapp` para instalar Citrix Virtual Apps. Citrix Virtual Desktops se instala si se omite la opción

### Paso 3. Seleccione el VDA

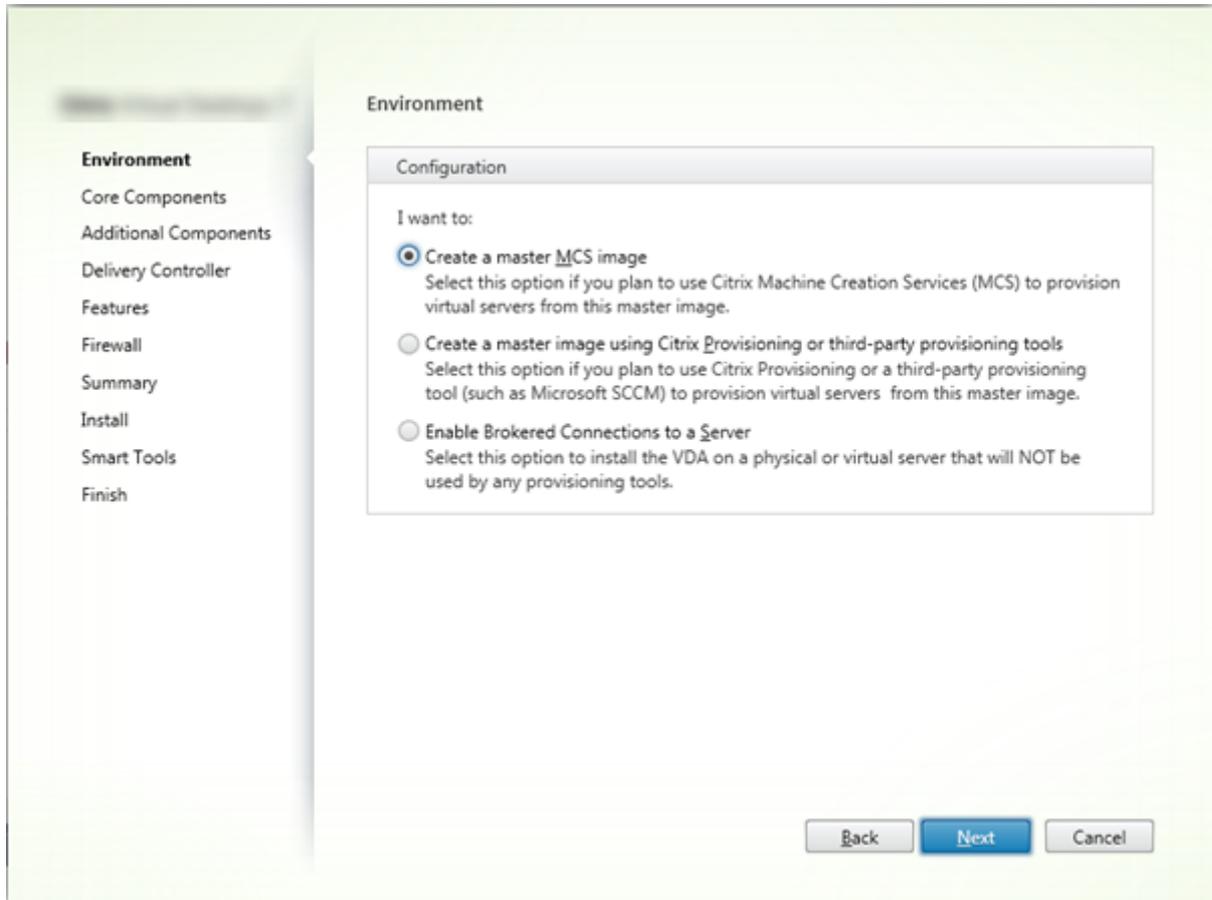


Seleccione la entrada **Virtual Delivery Agent**. El instalador sabe si se está ejecutando en un sistema operativo de sesión única o multisesión, por lo que solo ofrece el tipo de VDA apropiado.

Por ejemplo, si ejecuta el instalador en una máquina Windows Server 2016, se ofrece la opción de VDA para sistema operativo multisesión. No se ofrece la opción VDA para SO de sesión única.

Si intenta instalar (o actualizar) un Windows VDA en un sistema operativo que no admite esta versión de Citrix Virtual Apps and Desktops, aparece un mensaje que le guiará a la información donde se describen las opciones de que dispone.

## Paso 4. Especifique cómo se usará el VDA



En la página **Entorno**, especifique cómo va a usar el VDA e indique si usará esta máquina como imagen maestra para aprovisionar máquinas adicionales.

La opción que elija afecta a las herramientas de aprovisionamiento de Citrix que se instalan automáticamente (si las hay) y a los valores predeterminados de la página Componentes adicionales del instalador de VDA.

Varios MSI (de aprovisionamiento y otros) se instalan automáticamente cuando instala un VDA. La única forma de impedir su instalación es con la opción `/exclude` en una instalación de línea de comandos. Para obtener más información, consulte [Instalación desde la línea de comandos](#).

Elija una de las siguientes opciones:

- **Crear una imagen maestra de MCS:** Seleccione esta opción para instalar un VDA en una imagen maestra de VM, si va a usar Machine Creation Services para aprovisionar las máquinas virtuales. Esta opción instala Machine Identity Service, que incluye el archivo TargetOSOptimizer.exe. Esta es la opción predeterminada. Opción de la línea de comandos: `/mastermcsimage` o `/masterimage`
- **Crear una imagen maestra con Citrix Provisioning o herramientas de aprovisionamiento de terceros:** Seleccione esta opción para instalar un VDA en una imagen maestra de VM, si va a

usar Citrix Provisioning o herramientas de aprovisionamiento de terceros (como Microsoft System Center Configuration Manager) para aprovisionar las máquinas virtuales. Opción de línea de comandos: `/masterpvsimage`

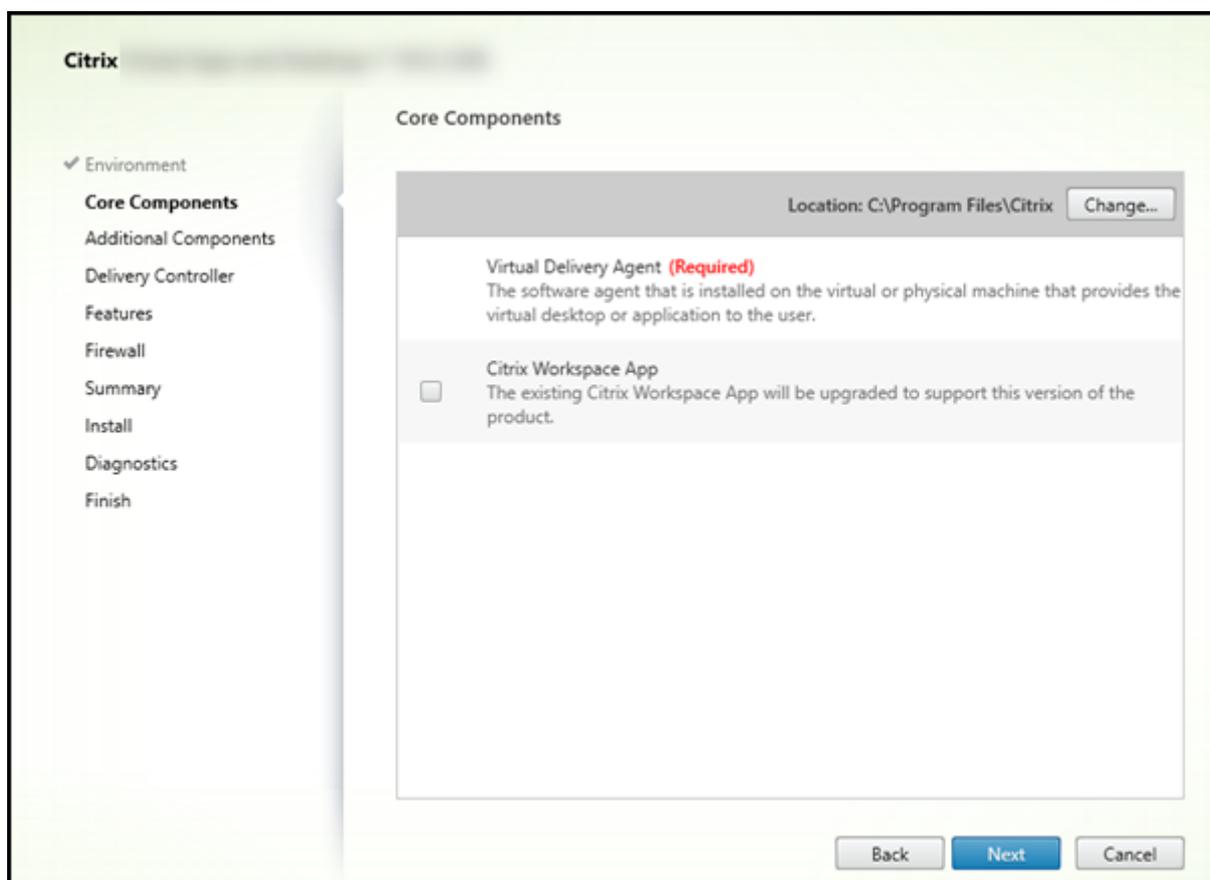
- (Aparece solo en las máquinas con SO multisesión) **Habilitar conexiones de broker con servidores:** Seleccione esta opción para instalar un VDA en una máquina física o virtual que no se utilizará como imagen maestra para aprovisionar otras máquinas. Opción de línea de comandos: `/remotepc`
- (Aparece solo en las máquinas con SO de sesión única) **Habilitar el acceso con Remote PC:** Seleccione esta opción para instalar un VDA en una máquina física que se usará para acceso con Remote PC. Opción de línea de comandos: `/remotepc`

Haga clic en **Siguiente**.

Esta página no aparecerá:

- Si actualiza la versión de un VDA
- Si utiliza el instalador `VDAWorkstationCoreSetup.exe`

## Paso 5. Seleccione los componentes a instalar y la ubicación de la instalación



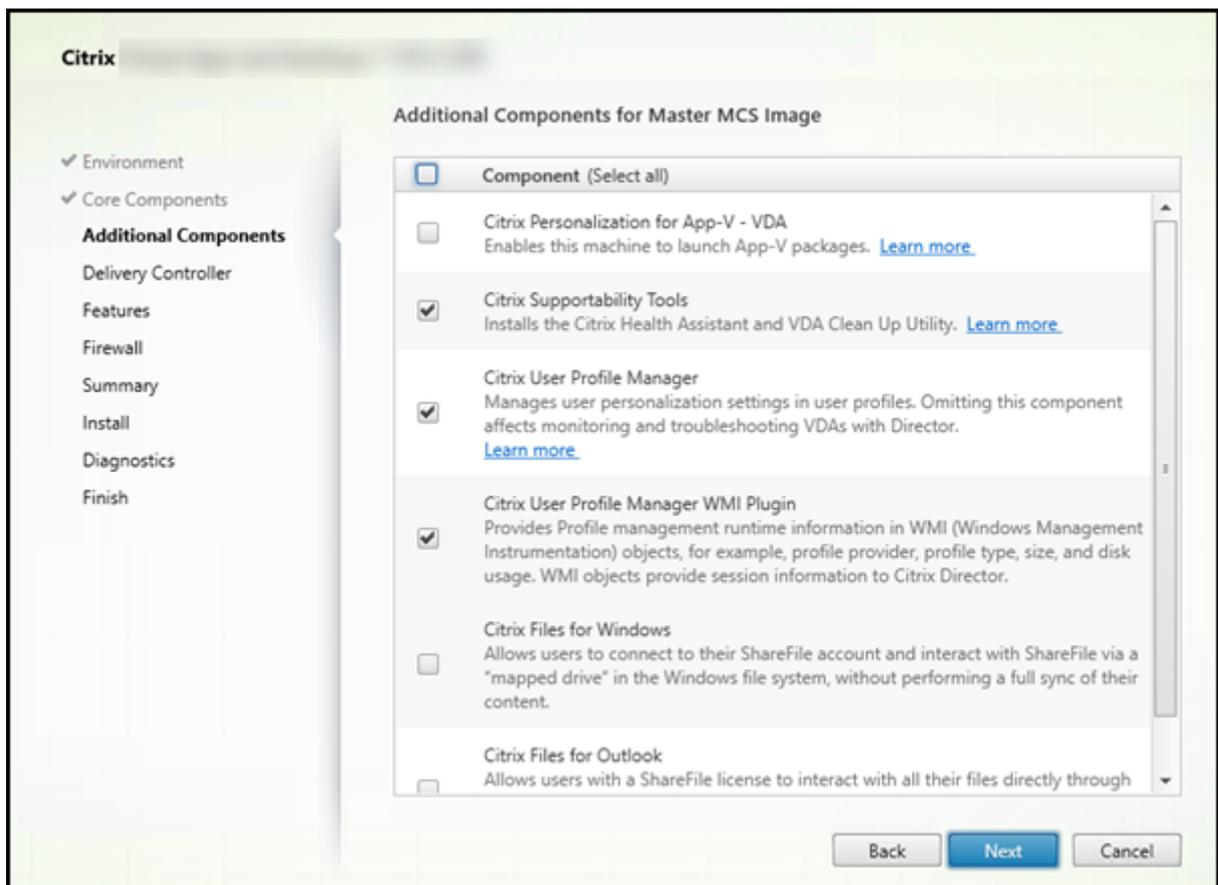
En la página **Componentes principales**:

- **Ubicación:** De forma predeterminada, los componentes se instalan en C:\Archivos de programa\Citrix. Esta opción predeterminada no presenta problemas para la mayoría de las implementaciones. Si indica otra ubicación, esta debe tener permisos de ejecución para el servicio de red.
- **Componentes:** De forma predeterminada, no se instala la aplicación Citrix Workspace para Windows con el VDA. Si utiliza el instalador VDAWorkstationCoreSetup.exe, la aplicación Citrix Workspace para Windows no se instala nunca, así que esta casilla no aparece.

Haga clic en **Siguiente**.

Opciones de línea de comandos: `/installdir,/components vda plugin` para instalar el VDA y la aplicación Citrix Workspace para Windows

## Paso 6. Instale componentes adicionales



La página **Componentes adicionales** contiene casillas de verificación para habilitar o inhabilitar la instalación de otras funcionalidades y tecnologías con el VDA. En una instalación de línea de comandos,

puede usar la opción `/exclude` o `/includeadditional` para omitir o incluir expresamente uno o varios de los componentes disponibles.

En la siguiente tabla se indica el parámetro predeterminado de los elementos en esta página. El parámetro predeterminado depende de la opción que seleccione en la página Entorno.

Página Componentes adicionales	Página Entorno: “Imagen maestra con MCS” o “Imagen maestra con Citrix Provisioning” seleccionado	Página Entorno: “Habilitar conexiones de broker con servidores”(para SO multisesión) o “Acceso con Remote PC”(para SO de sesión única) seleccionado
Citrix Personalization for App-V	No seleccionado	No seleccionado
Capa de personalización de usuarios	No seleccionado	No se muestra porque no es válido para este caso de uso.
Citrix Supportability Tools	Seleccionado	No seleccionado
Citrix User Profile Manager	Seleccionado	No seleccionado
Citrix User Profile Manager WMI Plugin	Seleccionado	No seleccionado
Citrix Files para Windows	No seleccionado	No seleccionado
Citrix Files para Outlook	No seleccionado	No seleccionado

Esta página no aparecerá si:

- Se usa el instalador `VDAWorkstationCoreSetup.exe`. Además, las opciones de la línea de comandos para los componentes adicionales no son válidas cuando se utilizan junto con ese instalador.
- Actualiza un VDA y todos los componentes adicionales ya están instalados. (Si alguno de los componentes adicionales ya está instalado, la página muestra solo aquellos que no están instalados.)

Marque o desmarque las siguientes casillas de verificación:

- **Personalización de Citrix para App-V:** Instale este componente si va a usar aplicaciones provenientes de paquetes de Microsoft App-V. Para obtener más información, consulte [App-V](#).

Opción de línea de comandos: `/includeadditional "Citrix Personalization for App-V – VDA"` para habilitar la instalación del componente, `/exclude "Citrix Personalization for App-V – VDA"` para impedir la instalación del componente

- **Capa de personalización de usuarios:** Instala el MSI para la capa de personalización de usuarios. Para obtener más información, consulte [Capa de personalización de usuarios](#).

Este componente aparece solo cuando se instala un VDA en una máquina Windows 10 de sesión única.

La tecnología de capa de personalización del usuario no puede coexistir con los componentes Personal vDisk (PvD) y AppDisk.

- Para una instalación limpia, el componente Personal vDisk o AppDisk no está disponible.
- Para una actualización:
  - \* Si PvD, AppDisk o la capa de personalización del usuario ya están instalados y los medios de instalación contienen una versión más reciente del componente instalado, el componente instalado se actualizará.
  - \* Si PvD o AppDisk ya está instalado y los medios de instalación no contienen una versión más reciente de ellos, se puede seleccionar la capa de personalización del usuario para la instalación.
  - \* Si ni PVD, ni AppDisk ni la capa de personalización del usuario están instalados, se instala el componente de la capa de personalización del usuario.

Opción de línea de comandos: `/includeadditional "User Personalization Layer"` para habilitar la instalación del componente, `/exclude "User Personalization Layer"` para impedir la instalación del componente

- **Citrix Supportability Tools:** Instala el MSI que contiene las herramientas de compatibilidad de Citrix, como Citrix Health Assistant.

Opción de línea de comandos: `/includeadditional "Citrix Supportability Tools"` para habilitar la instalación del componente, `/exclude "Citrix Supportability Tools"` para impedir la instalación del componente

- **Citrix User Profile Manager:** Este componente administra los parámetros de personalización de usuario en los perfiles de usuario. Para obtener más detalles, consulte [Profile Management](#).

Excluir Citrix Profile Management de la instalación afecta a la supervisión y la solución de problemas de los agentes VDA a través de Citrix Director. En las páginas Detalles del usuario y Punto final, fallan los paneles Personalización y Duración de inicio de sesión. En las páginas Panel de mandos y Tendencias, el panel **Duración media de inicios de sesión** solo mostrará datos para máquinas que tengan Profile Management instalado.

Aunque use una solución de terceros para la administración de perfiles de usuario, Citrix recomienda instalar y ejecutar el servicio Citrix Profile Management. No es necesario habilitar el servicio Citrix Profile Management.

Opción de línea de comandos: `/includeadditional "Citrix User Profile Manager"` para habilitar la instalación del componente, `/exclude "Citrix User Profile Manager"` para impedir la instalación del componente

- **Citrix user Profile Manager WMI Plugin:** Este plug-in ofrece información del tiempo de ejecución de Profile Management en objetos WMI (Windows Management Instrumentation); por ejemplo, el proveedor del perfil, el tipo de perfil, el tamaño y el uso del disco. Los objetos WMI proporcionan información acerca de las sesiones a Citrix Director.

Opción de línea de comandos: `/includeadditional "Citrix User Profile Manager WMI Plugin"` para habilitar la instalación del componente, `/exclude "Citrix User Profile Manager WMI Plugin"` para impedir la instalación del componente

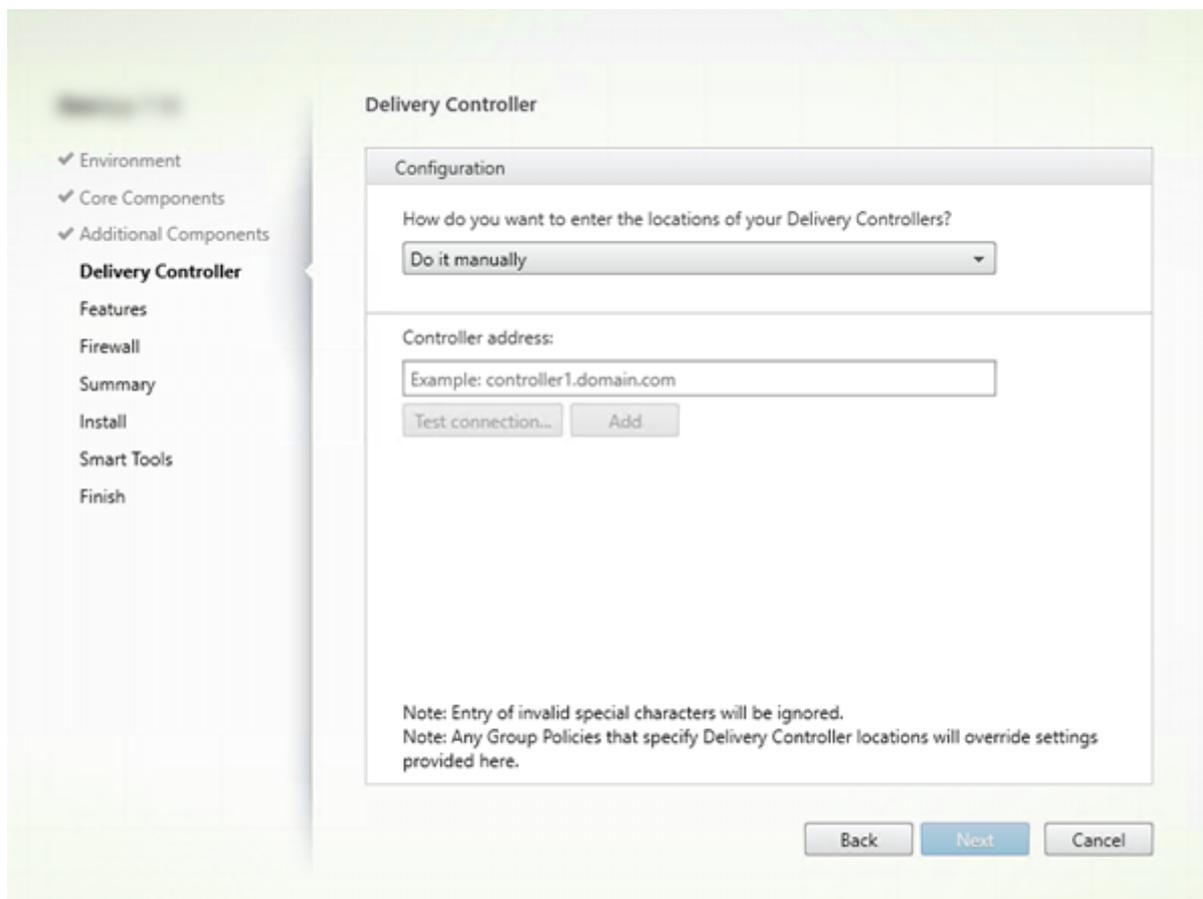
- **Citrix Files para Windows:** Este componente permite a los usuarios conectarse a su cuenta de Citrix Files. Una vez conectados, pueden interactuar con Citrix Files a través de una unidad asignada en el sistema de archivos de Windows (sin requerir una sincronización completa de su contenido).

Opciones de línea de comandos: `/includeadditional "Citrix Files for Windows"` para habilitar la instalación del componente, `/exclude "Citrix Files for Windows"` para impedir la instalación del componente

- **Citrix Files para Outlook:** Citrix Files para Outlook le permite hacer envíos a través de Citrix Files para omitir las restricciones de tamaño de archivo y agregar seguridad a sus archivos adjuntos o correos electrónicos. Puede proporcionar una solicitud de carga segura de archivos para compañeros de trabajo, clientes y socios directamente en su correo electrónico. Para obtener más información, consulte [Citrix Files para Outlook](#).

Opciones de línea de comandos: `/includeadditional "Citrix Files for Outlook"` para habilitar la instalación del componente, `/exclude "Citrix Files for Outlook"` para impedir la instalación del componente

## Paso 7. Direcciones de Delivery Controller



En la página **Delivery Controller**, elija cómo especificar las direcciones de los Controllers instalados. Citrix recomienda especificar las direcciones de los Controllers ahora (“Hacerlo manualmente”), mientras instala el VDA. El VDA no puede registrarse en el Controller sin esta información. Si un VDA no puede registrarse, los usuarios no podrán acceder a las aplicaciones ni a los escritorios que contenga ese VDA.

- **Hacerlo manualmente:** Opción predeterminada. Introduzca el nombre de dominio completo (FQDN) de un Controller instalado y, a continuación, haga clic en **Agregar**. Si ha instalado Controllers adicionales, agregue sus direcciones respectivas.
- **Hacerlo más tarde (Avanzado):** Si elige esta opción, el asistente le solicitará confirmación antes de continuar. Para especificar más adelante esas direcciones, puede volver a ejecutar el instalador más adelante o usar una directiva de grupo de Citrix. El asistente también se lo recordará en la página **Resumen**.
- **Elegir ubicaciones desde Active Directory:** Esta opción es válida solamente cuando la máquina está unida a un dominio y el usuario es un usuario de dominio.
- **Dejar que Machine Creation Services lo haga automáticamente:** Esta opción es válida solamente si utiliza Machine Creation Services (MCS) para aprovisionar máquinas.

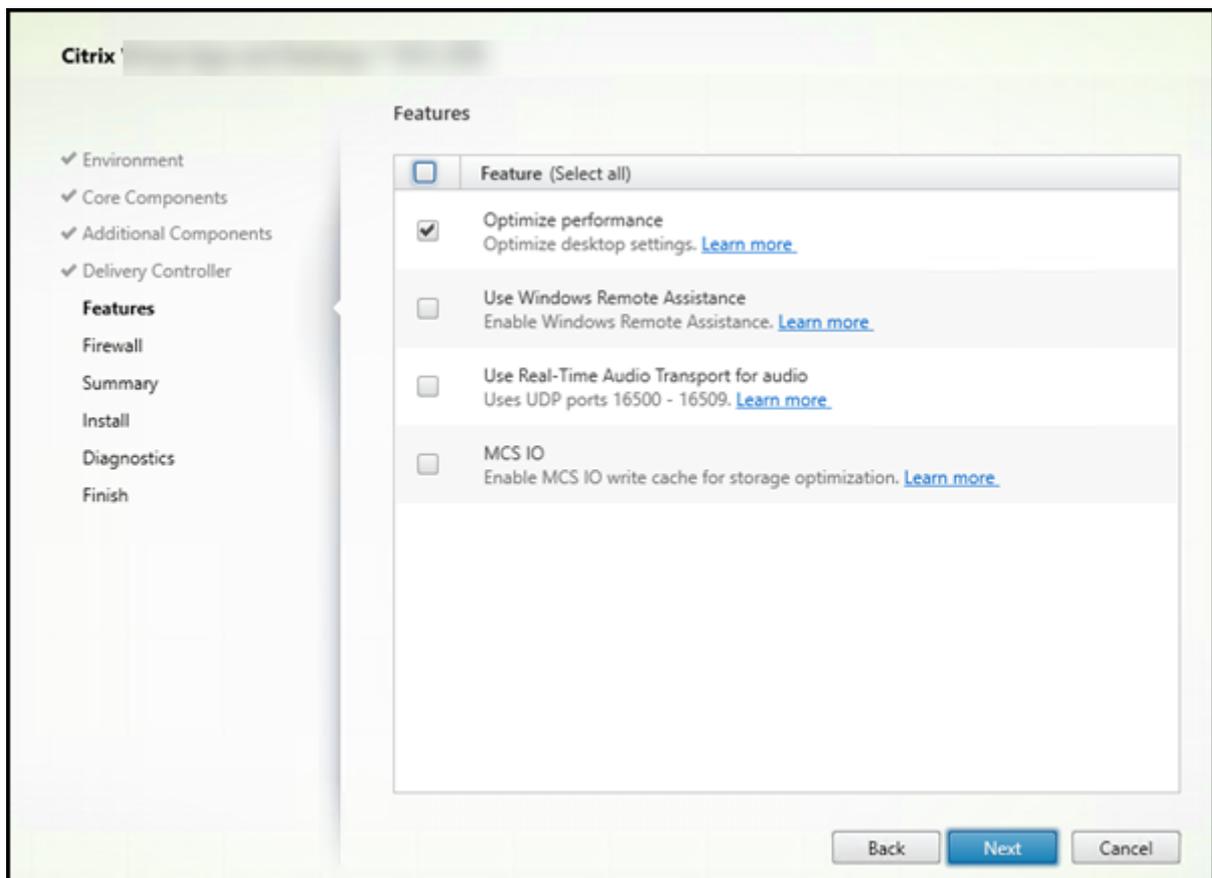
Haga clic en **Siguiente**. Si ha seleccionado la opción “Hacerlo más tarde (avanzado)”, se le pedirá que confirme que especificará las direcciones de Controller más adelante.

Otras consideraciones

- La dirección solo puede contener caracteres alfanuméricos.
- Si especifica direcciones durante la instalación del VDA y en la directiva de grupo, las configuraciones de directiva sobrescribirán las configuraciones que defina durante la instalación.
- Un registro correcto de VDA también requiere que los puertos del firewall que se utilizan para la comunicación con el Controller estén abiertos. Se habilitan de forma predeterminada en la página **Firewall** del asistente.
- Después de especificar las ubicaciones de los Controllers (al instalar el VDA o más adelante), puede usar la funcionalidad de actualización automática para actualizar los VDA cuando se instalen o se quiten Controllers. Para obtener más información sobre cómo los agentes VDA detectan Controllers y se registran en ellos, consulte [Registro de VDA](#).

Opción de línea de comandos: `/controllers`

## Paso 8: Habilite o inhabilite las funciones



En la página **Funciones**, marque o desmarque las casillas de verificación para habilitar o inhabilitar respectivamente las funcionalidades que quiera utilizar.

- **Optimizar el rendimiento:** Cuando utiliza MCS y habilita esta funcionalidad (predeterminada), la optimización de VM inhabilita los archivos sin conexión y la desfragmentación en segundo plano, y reduce el tamaño del registro de eventos. Para obtener más información, consulte [CTX224676](#).

Además de habilitar esta función, la optimización requiere que se instale Machine Identity Service. Ese servicio contiene el archivo `TargetOSOptimizer.exe`. Machine Identity Service se instala automáticamente cuando:

- En la interfaz gráfica, seleccione **Crear una imagen maestra de MCS** en la página **Entorno**.
- En la interfaz de línea de comandos, especifique `/mastermcsimage` o `/masterimage` (y no especifique `/exclude "Machine Identity Service"`).

Opción de línea de comandos: `/optimize`

Si utiliza el instalador `VDAWorkstationCoreSetup.exe`, esta función no aparecerá en el asistente y la opción de línea de comandos no será válida. Si usa otro instalador en un entorno de acceso con Remote PC, inhabilite esta función.

- **Usar Asistencia remota de Windows:** Si esta opción está habilitada, la Asistencia remota de Windows se usa con la función de remedo de usuarios en Director. La Asistencia remota de Windows abre los puertos dinámicos en el firewall. Opción inhabilitada de forma predeterminada.

Opción de línea de comandos: `/enable_remote_assistance`

- **Usar transporte de audio Real-Time:** Habilite esta función si en su red se utiliza ampliamente voz sobre IP. Esta función reduce la latencia y mejora la resistencia del audio en redes con pérdida. Lo que permite que los datos de audio se transmitan mediante RTP sobre UDP. Opción inhabilitada de forma predeterminada.

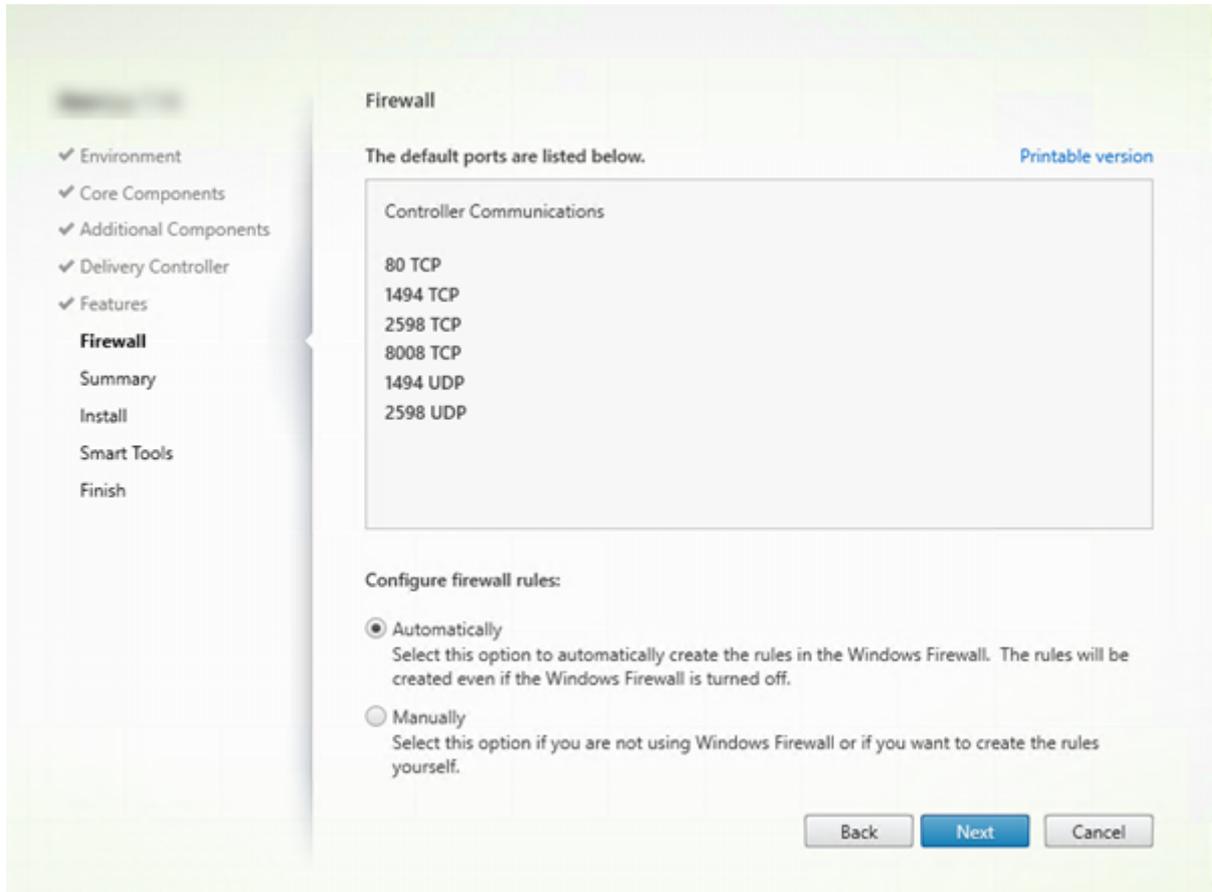
Opción de línea de comandos: `/enable_real_time_transport`

- **E/S de MCS:** Válido solo cuando se usa MCS para aprovisionar las máquinas virtuales. Cuando se selecciona, se instala el controlador de la caché de escritura MCSIO. Para obtener más información, consulte [Almacenamiento compartido por los hipervisores](#) y [Configurar caché para datos temporales](#).

Opción de línea de comandos: `/install_mcsio_driver`

Haga clic en **Siguiente**.

## Paso 9: Puertos de firewall

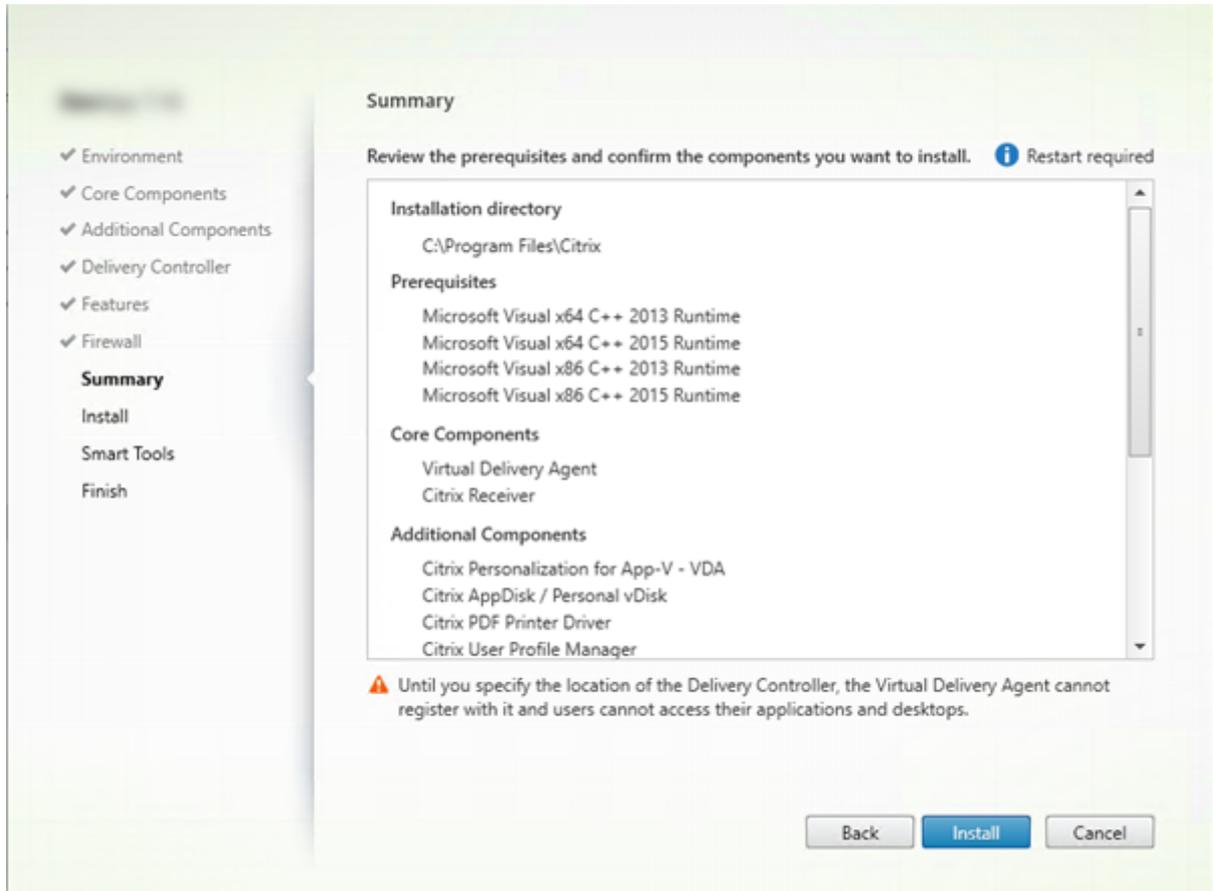


De forma predeterminada, los siguientes puertos se abren automáticamente en la página **Firewall** si el servicio Firewall de Windows se está ejecutando, incluso aunque no esté habilitado. Esta opción predeterminada no presenta problemas para la mayoría de las implementaciones. Para obtener información acerca de los puertos, consulte [Puertos de red](#).

Haga clic en **Siguiente**.

Opción de línea de comandos: `/enable_hdx_ports`

## Paso 10: Revise los requisitos previos y confirme la instalación

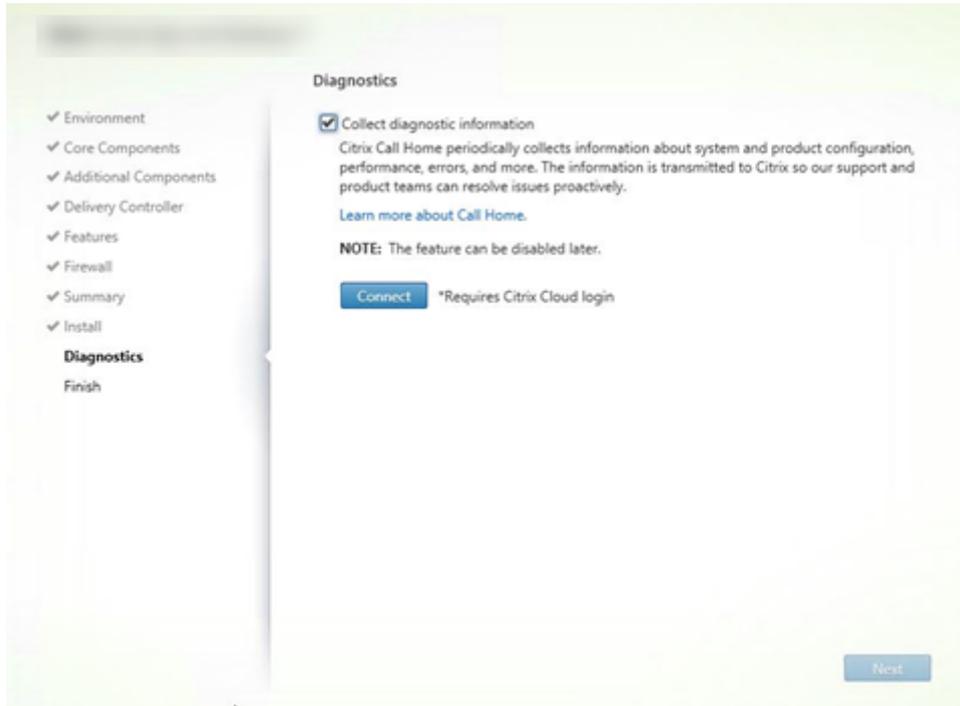


La página **Resumen** muestra lo que se instalará. Use el botón Atrás para volver a las páginas anteriores del asistente y cambiar las opciones.

Cuando haya terminado, haga clic en **Instalar**.

Es posible que la máquina se reinicie una o dos veces si los requisitos previos todavía no están instalados o habilitados. Consulte [Antes de instalar](#).

## Paso 11: Diagnóstico

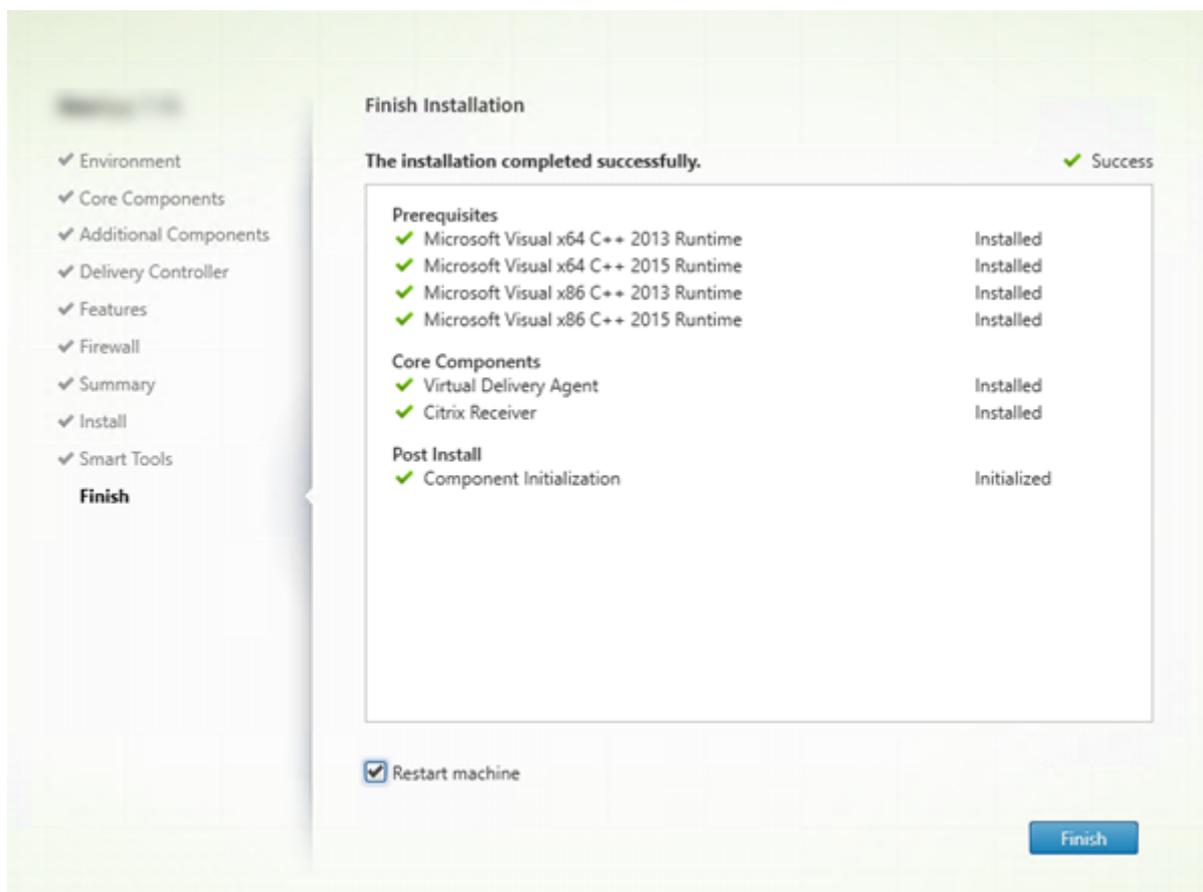


En la página **Diagnósticos**, elija si quiere participar en Citrix Call Home. Si elige participar (opción predeterminada), haga clic en **Conectar**. Cuando se le solicite, introduzca las credenciales de su cuenta de Citrix

Una vez validadas las credenciales (o si elige no participar), haga clic en **Siguiente**.

Para obtener más información, consulte [Call Home](#).

## Paso 12: Finalice la instalación



La página **Finalizar** presenta marcas de verificación verdes para todos los requisitos previos y los componentes que se hayan instalado e inicializado correctamente.

Haga clic en **Finalizar**. De forma predeterminada, la máquina se reinicia automáticamente. (Aunque puede inhabilitar este reinicio automático, el VDA no se podrá utilizar hasta que se reinicie la máquina.)

### Siguientes pasos

Repita el procedimiento anterior para instalar agentes VDA en otras máquinas o imágenes si fuera necesario.

Después de instalar todos los VDA, inicie Studio. Si aún no ha creado ningún sitio, Studio le guiará automáticamente cuando lo haga. Una vez que haya terminado, Studio le guiará para crear un catálogo de máquinas y un grupo de entrega. Consulte:

- [Crear un sitio](#)
- [Crear catálogos de máquinas](#)
- [Crear grupos de entrega](#)

## Personalizar un VDA

Si quiere personalizar un VDA ya instalado:

1. Desde la función de Windows para quitar o cambiar programas, seleccione **Citrix Virtual Delivery Agent** o **Citrix Remote PC Access/VDI Core Services VDA**. A continuación, haga clic con el botón secundario y seleccione **Cambiar**.
2. Seleccione **Personalizar configuración de Virtual Delivery Agent**. Cuando se inicie el instalador, puede cambiar:
  - Direcciones de Controller
  - El puerto TCP/IP utilizado para registrarse en el Controller (predeterminado = 80)
  - Si abrir automáticamente los puertos del Firewall de Windows

## Solución de problemas

Para obtener información sobre cómo informa Citrix del resultado de la instalación de un componente, consulte [Códigos de retorno en la instalación de Citrix](#).

En Studio, la versión instalada de VDA en el panel **Detalles** referente al grupo de entrega puede no ser la versión real instalada en las máquinas. La pantalla Programas y características de la máquina Windows muestra la versión real del VDA.

## Instalación desde la línea de comandos

January 3, 2023

Lo descrito en este artículo se aplica en caso de instalar componentes en máquinas con sistemas operativos Windows. Para obtener información acerca de los agentes VDA para sistemas operativos Linux, consulte [Agentes Virtual Delivery Agent de Linux](#).

En este artículo, se describe cómo emitir comandos de instalación de producto. Antes de comenzar cualquier instalación, consulte el artículo [Antes de instalar](#). Este artículo contiene las descripciones de los instaladores disponibles.

Para ver el progreso de ejecución del comando y los valores de retorno, debe ser el administrador original o debe utilizar la opción **Ejecutar como administrador**. Para obtener más información, consulte la documentación de comandos de Microsoft.

Para complementar el uso de los comandos de instalación directamente, se proporcionan scripts de ejemplo en la imagen ISO del producto. Puede usarlos para instalar, actualizar o quitar máquinas VDA de Active Directory. Para obtener más información, consulte [Instalar agentes VDA mediante scripts](#).

Si intenta instalar (o actualizar) un Windows VDA en un sistema operativo que no admite esta versión del producto, aparece un mensaje que le guiará a la información donde se describen las opciones de que dispone. Esta información también está disponible en [Sistemas operativos anteriores](#).

Para obtener información sobre cómo informa Citrix del resultado de la instalación de un componente, consulte [Códigos de retorno en la instalación de Citrix](#).

## Usar el instalador de producto completo

Para acceder a la interfaz de línea de comandos del instalador de producto completo:

1. Descargue el paquete de productos de Citrix. Se necesitan credenciales de cuenta de Citrix para tener acceso al sitio de descargas.
2. Descomprima el archivo. Si lo prefiere, puede grabar un DVD del archivo ISO.
3. Inicie una sesión con una cuenta de administrador local en el servidor donde quiera instalar los componentes.
4. Introduzca el DVD en la unidad o monte el archivo ISO.
5. Desde el directorio `\x64\XenDesktop Setup` de los medios de instalación, ejecute el comando correspondiente.

**Para instalar los componentes principales:** Ejecute `XenDesktopServerSetup.exe` con las opciones que aparecen en Opciones de línea de comandos para instalar componentes principales.

**Para instalar StoreFront:** Siga las instrucciones que se indican en [Para instalar StoreFront desde un símbolo del sistema](#).

**Para instalar un VDA:** Ejecute `XenDesktopVDASetup.exe` con las opciones que aparecen en Opciones de línea de comandos para instalar un VDA.

**Para instalar el Universal Print Server:** Siga las instrucciones que se indican en Opciones de línea de comandos para instalar Universal Print Server.

**Para instalar el Servicio de autenticación federada:** Citrix recomienda usar la interfaz gráfica.

**Para instalar el Autoservicio de restablecimiento de contraseñas:** Consulte las instrucciones indicadas en [Autoservicio de restablecimiento de contraseñas](#).

**Para instalar la Grabación de sesiones:** Siga las instrucciones indicadas en [Grabación de sesiones](#).

## Opciones de línea de comandos para instalar componentes principales

Las siguientes opciones son válidas para instalar los componentes principales con el comando `XenDesktopServerSetup.exe`. Para obtener más información acerca de las opciones, consulte [Instalar componentes principales](#).

- **/components** *component* [, \*component\*]...

Lista de los componentes, separados por comas, para instalar o quitar. Los valores válidos son:

- **CONTROLLER**: Controller
- **DESKTOPSTUDIO**: Studio
- **DESKTOPDIRECTOR**: Director
- **LICENSESERVER**: Citrix License Server

Si se omite esta opción, se instalarán todos los componentes o se quitarán si también se especifica la opción `/remove`.

(En versiones anteriores a 1912 LTSR CU1, los valores válidos incluían **STOREFRONT**; A partir de la versión 1912 LTSR CU1, utilice las instrucciones de instalación dedicadas de StoreFront que se indican en [Usar el instalador de producto completo](#).)

- **/configure\_firewall**

Si el servicio Firewall de Windows se está ejecutando, abre todos los puertos del Firewall de Windows que necesitan los componentes que se están instalando, incluso aunque el firewall no esté habilitado. Si se utiliza un firewall de terceros o no se utiliza ninguno, es necesario abrir esos puertos manualmente.

- **/disableexperiencemetrics**

Impide que los análisis recopilados durante la instalación, la actualización o la eliminación se carguen automáticamente en Citrix.

- **/exclude** “función”[,,”función”]

Impide la instalación de una o varias funciones, servicios o tecnologías, separadas por comas y escritas entre comillas rectas (no tipográficas). Los valores válidos son:

- **"Local Host Cache Storage (LocalDB)"**: Impide la instalación de la base de datos utilizada para la Caché de host local. Esta opción no afecta a la instalación de SQL Server Express para usarlo como la base de datos del sitio.

- **/help** o **/h**

Muestra la ayuda del comando.

- **/ignore\_hw\_check\_failure**

Permite que la instalación o actualización del Delivery Controller continúe, aunque las comprobaciones de hardware fallen (por ejemplo, por falta de memoria RAM). Para obtener más información, consulte [Comprobación de hardware](#).

- **/ignore\_site\_test\_failure**

Válido solo durante la actualización del Controller. Se ignoran todos los fallos en las pruebas del sitio y la actualización continúa. Si se omite (o se establece en false), una prueba de sitio que haya fallado detiene el instalador, sin realizar la actualización. De forma predeterminada, False.

- ***/installdir directorio***

Directorio vacío existente donde se instalarán los componentes. Valor predeterminado = C:\Archivos de programa\Citrix.

- ***/logpath ruta***

Ubicación del archivo de registro. La carpeta especificada debe existir. El instalador no puede crearla. Predeterminado = “%TEMP%\Citrix\XenDesktop Installer”

- ***/no\_pending\_reboot\_check***

Al instalar o actualizar componentes principales, impide comprobar si hay un reinicio pendiente de una instalación anterior de Windows en la máquina.

- ***/no\_remote\_assistance***

Válido solamente cuando se instala Director. Inhabilita la funcionalidad de remedio de usuarios que utiliza la Asistencia remota de Windows.

- ***/noreboot***

Impide que se reinicie el sistema después de la instalación. (para la mayoría de los componentes principales, el reinicio no está habilitado de forma predeterminada).

- ***/nosql***

Impide la instalación de Microsoft SQL Server Express en el servidor donde se instala Controller. Si se omite esta opción, se instalará SQL Server Express para usar como la base de datos del sitio. (esta opción no afecta a la instalación de la LocalDB de SQL Server Express, que se puede utilizar para la Memoria caché del host local).

- ***/quiet* o */passive***

No aparece ninguna interfaz de usuario durante la instalación. La única evidencia de que está teniendo lugar el proceso de instalación aparece en el Administrador de tareas de Windows. Si se omite esta opción, se abre la interfaz gráfica.

- ***/remove***

Quita los componentes principales especificados con la opción */components*.

- ***/removeall***

Quita todos los componentes principales instalados.

- **/sendexperiencemetrics**

Envía automáticamente a Citrix los análisis recopilados durante la instalación, la actualización o la eliminación. Si se omite esta opción (o se indica la opción `/disableexperiencemetrics`), los análisis se recopilan localmente, pero no se envían automáticamente.

- **/tempdir** *directorio*

Directorio que contiene los archivos temporales durante la instalación. Valor predeterminado = `c:\Windows\Temp`.

- **/xenapp**

Instala Citrix Virtual Apps. Si se omite esta opción, se instala Citrix Virtual Apps and Desktops.

## Ejemplos de instalación de componentes principales

El siguiente comando instala el Controller de Citrix Virtual Apps and Desktops, Studio, Citrix Licensing y SQL Server Express en un servidor. Los puertos de firewall necesarios para la comunicación entre componentes se abrirán automáticamente.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller,desktopstudio,licenseserver /configure_firewall
```

El siguiente comando instala un Controller de Citrix Virtual Apps, Studio y SQL Server Express en el servidor. Los puertos de firewall necesarios para la comunicación entre componentes se abrirán automáticamente.

```
\x64\XenDesktop Setup\\XenDesktopServerSetup.exe /xenapp /components controller,desktopstudio /configure_firewall
```

## Usar el instalador independiente de VDA

Se necesitan credenciales de cuenta de Citrix para tener acceso al sitio de descargas. Debe tener privilegios administrativos elevados antes de iniciar la instalación o debe usar la opción **Ejecutar como administrador**.

1. Descargue el paquete correspondiente de Citrix:
  - Virtual Delivery Agent de SO multisesión: `VDAServerSetup.exe`
  - Virtual Delivery Agent de SO de sesión única: `VDASessionSetup.exe`
  - Servicios principales de Virtual Delivery Agent para sistema operativo de sesión única: `VDASessionCoreSetup.exe`
2. Extraiga primero los archivos del paquete a un directorio existente y ejecute el comando de instalación, o bien ejecute el paquete directamente.

Para extraer los archivos antes de la instalación, use la opción `/extract` con la ruta de acceso absoluta, por ejemplo: `.\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia` (el directorio debe existir; de lo contrario, la extracción falla). A continuación, en un comando aparte, ejecute el comando correspondiente que aparece más abajo con las opciones válidas que se indican en este artículo.

- Para `VDA ServerSetup_XXXX.exe`, ejecute `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`
- Para `VDA WorkstationCoreSetup_XXXX.exe`, ejecute `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopRemotePCSetup.exe`
- Para `VDA WorkstationSetup_XXXX.exe`, ejecute `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`

Para ejecutar el paquete descargado, ejecute su nombre: `VDA ServerSetup.exe`, `VDA WorkstationSetup.exe` o `VDA WorkstationCoreSetup.exe`. Use las opciones válidas que aparecen a continuación.

Si conoce el instalador de producto completo:

- Ejecute el paquete independiente `VDA ServerSetup.exe` o `VDA WorkstationSetup.exe` como si fuera el comando `XenDesktopVdaSetup.exe` en todo excepto el nombre.
- El instalador `VDA WorkstationCoreSetup.exe` es diferente, porque solo admite un subconjunto de las opciones disponibles para los demás.

## Opciones de línea de comandos para instalar un VDA

Las siguientes opciones son válidas con uno o más de los comandos (instaladores): `XenDesktopVDASetup.exe`, `VDA ServerSetup.exe`, `VDA WorkstationSetup.exe` o `VDA WorkstationCoreSetup.exe`.

Para obtener más información acerca de las opciones, consulte [Instalar agentes VDA](#).

- **/baseimage**

Válido solo cuando se instala un VDA para SO de sesión única en una VM. Habilita el uso de discos Personal vDisk con una imagen maestra. Personal vDisk [se ha retirado](#).

Esta opción no es válida cuando se utiliza el instalador `VDA WorkstationCoreSetup.exe`.

- **/components** *componente[,componente]*

Lista de los componentes, separados por comas, para instalar o quitar. Los valores válidos son:

- **VDA**: Virtual Delivery Agent

- **PLUGINS:** Aplicación Citrix Workspace para Windows

Para instalar el VDA y la aplicación Citrix Workspace para Windows, especifique `/components vda plugins`.

Si se omite esta opción, solo se instala el VDA (no la aplicación Citrix Workspace).

Esta opción no es válida cuando se utiliza el instalador `VDAWorkstationCoreSetup.exe`. Ese instalador no puede instalar la aplicación Citrix Workspace.

- **/controllers** “`controller [controller]`”

Lista de nombres de dominio completos (FQDN) de Controllers, separados por espacios y entre comillas rectas, con los que se puede comunicar el VDA. No especifique ambas opciones, `/site_guidy/controllers`.

- **/disableexperiencemetrics**

Impide que los análisis recopilados durante la instalación, la actualización o la eliminación se carguen automáticamente en Citrix.

- **/enable\_hdx\_ports**

Abre los puertos del Firewall de Windows requeridos por el VDA y por las funciones especificadas (excepto la Asistencia remota de Windows) si se detecta el servicio del Firewall de Windows, incluso aunque el firewall no esté habilitado. Si se utiliza un firewall distinto o no se utiliza ninguno, es necesario configurar el firewall manualmente. Para obtener información acerca de los puertos, consulte [Puertos de red](#).

Para abrir los puertos UDP que usa el transporte adaptable HDX, especifique la opción `/enable_hdx_udp_ports`, además de la opción `/enable_hdx_ports`.

- **/enable\_hdx\_udp\_ports**

Abre los puertos UDP en el firewall de Windows que utiliza el transporte adaptable HDX, si se detecta el servicio Firewall de Windows (incluso aunque el firewall no esté habilitado). Si se utiliza un firewall distinto o no se utiliza ninguno, es necesario configurar el firewall manualmente. Para obtener información acerca de los puertos, consulte [Puertos de red](#).

Para abrir puertos adicionales que utiliza el VDA, especifique la opción `/enable_hdx_ports`, además de la opción `/enable_hdx_udp_ports`.

- **/enable\_real\_time\_transport**

Habilita o inhabilita el uso de UDP para los paquetes de audio (Transferencia de audio RealTime para audio). Habilitar esta función puede mejorar el rendimiento del audio. Incluya la opción `/enable_hdx_ports` si quiere que los puertos UDP se abran automáticamente si se detecta el servicio de Firewall de Windows.

- **/enable\_remote\_assistance**

Habilita la función de remedeo en la Asistencia remota de Windows para utilizarla con Director. Si especifica esta opción, la Asistencia remota de Windows abrirá los puertos dinámicos en el firewall.

- **/exclude** “componente”[,”componente”]

Impide la instalación de uno o varios componentes opcionales, separados por comas y escritos entre comillas rectas. Por ejemplo, instalar o actualizar un VDA en una imagen que no se administra mediante Machine Creation Services no requiere el componente Machine Identity Service.

Los valores válidos son:

- AppDisks VDA Plug-in
- Personal vDisk
- Machine Identity Service (incluye TargetOSOptimizer.exe)
- Citrix User Profile Manager
- Citrix User Profile Manager WMI Plug-in
- Citrix Universal Print Client
- Citrix Telemetry Service
- Citrix Personalization **for** App-V - VDA
- Citrix Supportability Tools
- Citrix Files **for** Windows
- Citrix Files **for** Outlook
- User Personalization Layer

Excluir Citrix Profile Management de la instalación (`/exclude "Citrix User Profile Manager"`) afecta a la supervisión y la solución de problemas de los agentes VDA a través de Citrix Director. En las páginas **Detalles del usuario** y **Punto final**, el panel “Personalización” y el panel “Duración de inicio de sesión” fallan. En las páginas **Panel de mandos** y **Tendencias**, el panel “Duración media de inicios de sesión” solo muestra datos de máquinas que tengan Profile Management instalado.

Aunque use una solución de terceros para la administración de perfiles de usuario, Citrix recomienda instalar y ejecutar el servicio Citrix Profile Management. No es necesario habilitar el servicio Citrix Profile Management.

Si va a usar MCS para aprovisionar máquinas virtuales, no excluya Machine Identity Service. Excluir ese servicio también excluye la instalación de `TargetOSOptimizer.exe`.

Si especifica `/exclude` e `/includeadditional` con el mismo nombre de componente adicional, ese componente no se instala.

Esta opción no es válida cuando se utiliza el instalador `VDAWorkstationCoreSetup.exe`. El instalador excluye automáticamente muchos de los elementos.

- **/h o /help**

Muestra la ayuda del comando.

- **/includeadditional** “*componente*”[,”*componente*”]

Incluye la instalación de uno o varios componentes opcionales, separados por comas y escritos entre comillas. Los nombres de los componentes distinguen entre mayúsculas y minúsculas. Esta opción puede ser útil cuando está creando una implementación de acceso con Remote PC y quiere instalar componentes adicionales que no están incluidos de manera predeterminada. Los valores válidos son:

- Personal vDisk
- Citrix User Profile Manager
- Citrix User Profile Manager WMI Plug-in
- Citrix Universal Print Client
- Citrix Telemetry Service
- Citrix Personalization **for** App-V - VDA
- Citrix Supportability Tools
- Citrix Files **for** Windows
- Citrix Files **for** Outlook
- User Personalization Layer

Si especifica `/exclude` e `/includeadditional` con el mismo nombre de componente adicional, ese componente no se instala.

Si incluye ambos, `Personal vDisk` y `user personalization layer`, en el mismo comando, solo se instala `user personalization layer`.

- **/installdir** *directorio*

Directorio vacío existente donde se instalarán los componentes. Valor predeterminado = C:\Archivos de programa\Citrix.

- **/install\_mcsio\_driver**

Habilita la memoria caché de escritura de E/S de MCS para optimizar el almacenamiento.

- **/logpath \*path**

Ubicación del archivo de registro. La carpeta especificada debe existir. El instalador no puede crearla. Predeterminado = “%TEMP%\Citrix\XenDesktop Installer”

Esta opción no está disponible en la interfaz gráfica.

- **/masterimage**

Válido solamente cuando se instala un VDA en una VM. Establece el VDA como imagen maestra. Esta opción equivale a `/mastermcsimage`.

Esta opción no es válida cuando se utiliza el instalador `VDAWorkstationCoreSetup.exe`.

- **`/mastermcsimage`**

Especifica que esta máquina se utilizará como imagen maestra con Machine Creation Services. Esta opción también instala TargetOSOptimizer.exe (a menos que también especifique `/exclude "Machine Identity Service"`, que incluye el instalador del optimizador). Esta opción equivale a `/masterimage`.

- **`/masterpvsimage`**

Especifica que esta máquina se utilizará como imagen maestra con Citrix Provisioning o una herramienta de aprovisionamiento de terceros (como Microsoft System Center Configuration Manager) para aprovisionar las máquinas virtuales.

- **`/no_mediafoundation_ack`**

Comprueba que Microsoft Media Foundation no está instalado, y algunas funciones multimedia de HDX no se instalarán y no funcionarán. Si se omite esta opción y Media Foundation no está instalado, falla la instalación de VDA. La mayoría de las ediciones Windows admitidas vienen con Media Foundation ya instalado, a excepción de las ediciones N.

- **`/nodesktopexperience`**

Válido solo cuando se instala un VDA para SO multisesión. Impide la habilitación de la función Enhanced Desktop Experience. Esta función también se controla con la configuración de directiva de Citrix **Enhanced Desktop Experience**.

- **`/noreboot`**

Impide que se reinicie el sistema después de la instalación. El VDA no se puede usar hasta después de reiniciarse.

- **`/noresume`**

De forma predeterminada, cuando se necesita reiniciar la máquina durante una instalación, el instalador se reanuda automáticamente después de que se complete el reinicio. Para anular el valor predeterminado, especifique `/noresume`. Puede ser útil si debe volver a montar el medio o quiere capturar información durante una instalación automatizada.

- **`/optimize`**

Cuando utiliza MCS y habilita esta funcionalidad (predeterminada), la optimización de VM inhabilita los archivos sin conexión y la desfragmentación en segundo plano, y reduce el tamaño del registro de eventos. Para obtener más información, consulte [CTX224676](#).

Además de habilitar esta función, la optimización requiere que se instale Machine Identity Service. Ese servicio contiene el archivo TargetOSOptimizer.exe. Machine Identity Service se instala automáticamente cuando se especifican `/mastermcsimage` o `/masterimage` (y no se especifica `/exclude "Machine Identity Service"`).

No especifique esta opción para implementaciones de acceso con Remote PC.

- **/portnumber** *puerto*

Válido solamente si se especifica la opción `/reconfig`. Número de puerto para habilitar las comunicaciones entre VDA y Controller. El puerto previamente configurado queda inhabilitado a menos que sea el puerto 80.

- **/quiet** o **/passive**

No aparece ninguna interfaz de usuario durante la instalación. La única prueba de que está teniendo lugar el proceso de instalación y configuración aparece en el Administrador de tareas de Windows. Si se omite esta opción, se abre la interfaz gráfica.

- **/reconfigure**

Personaliza los parámetros de VDA configurados anteriormente cuando se usa con las opciones `/portnumber`, `/controllers` o `/enable_hdx_ports`. Si se especifica esta opción sin especificar también la opción `/quiet`, se abrirá la interfaz gráfica para personalizar VDA.

- **/remotepc**

Válido solo para implementaciones de acceso con Remote PC (SO de sesión única) o conexiones intermediadas (SO multisesión). Excluye la instalación de los siguientes componentes en un sistema operativo de sesión única:

- Citrix Personalization for App-V
- Citrix User Profile Manager
- Citrix User Profile Manager WMI Plugin
- Servicio de identidad de máquinas (incluye TargetOSOptimizer.exe)
- Personal vDisk
- Citrix Supportability Tools
- Citrix Files para Windows
- Citrix Files para Outlook
- Capa de personalización de usuarios

Esta opción no es válida cuando se utiliza el instalador `VDAWorkstationCoreSetup.exe`. El instalador excluye la instalación de estos componentes.

- **/remove**

Quita los componentes especificados con la opción `/components`.

- **/removeall**

Quita todos los componentes de VDA instalados.

- **/sendexperiencemetrics**

Envía automáticamente a Citrix los análisis recopilados durante la instalación, la actualización o la eliminación. Si se omite esta opción (o se indica la opción `/disableexperiencemetrics`), los análisis se recopilan localmente, pero no se envían automáticamente.

- **`/servervdi`**

Instala un VDA para SO de sesión única en una máquina Windows compatible con SO multi-sesión. Omita esta opción al instalar un VDA para SO multisesión en una máquina Windows con SO multisesión. Antes de usar esta opción, consulte [VDI de servidor](#).

Esta opción debe usarse solamente con el instalador de VDA completo. Esta opción no está disponible en la interfaz gráfica.

- **`/site_guid`** *guid*

Identificador único global de la unidad organizativa (OU) de Active Directory para el sitio. Esto asocia un escritorio virtual con un sitio cuando se usa Active Directory para la detección (el método de descubrimiento predeterminado y recomendado es la actualización automática). El GUID del sitio es una de las propiedades del sitio que se muestra en Studio. No especifique ambas opciones, `/site_guid` y `/controllers`.

- **`/tempdir`** *directorio*

Directorio que contiene los archivos temporales durante la instalación. Valor predeterminado = `c:\Windows\Temp`.

Esta opción no está disponible en la interfaz gráfica.

- **`/virtualmachine`**

Válido solamente cuando se instala un VDA en una VM. Invalida la detección de un equipo físico por parte del instalador, donde la información de BIOS que se pasa a las VM las hace aparecer como equipos físicos.

Esta opción no está disponible en la interfaz gráfica.

## Ejemplos de instalación de un VDA

### Instalar un VDA con el instalador de producto completo:

El siguiente comando instala un VDA para SO de sesión única y la aplicación Citrix Workspace en la ubicación predeterminada en una VM. Este VDA se utilizará como imagen maestra y usará MCS para aprovisionar las máquinas virtuales. El VDA se registrará inicialmente en el Controller de un servidor llamado `Contr-Main` en el dominio `mydomain`. El VDA utilizará la capa de personalización de usuarios, la optimización y la Asistencia remota de Windows.

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,  
plugins /controllers "Contr-Main.mydomain.local"/enable_hdx_ports /
```

```
includeadditional "User Personalization Layer"/optimize /mastermcsimage
/enable_remote_assistance
```

### Instalar un VDA de SO de sesión única con el instalador independiente VDAWorkstationCore-Setup:

El siguiente comando instala un VDA con los servicios principales en un SO de sesión única para utilizarlo en una implementación de VDI o de acceso con Remote PC. La aplicación Citrix Workspace y otros servicios no principales no se instalan. Se especifica la dirección de un Controller, y los puertos del Firewall de Windows se abrirán automáticamente. El administrador gestionará los reinicios.

```
VDAWorkstationCoreSetup .exe /quiet /controllers "Contr-East.domain.
com"/enable_hdx_ports /noreboot
```

### Personalizar un VDA

Después de instalar un VDA, puede personalizar varios parámetros. Desde el directorio `\x64\XenDesktop Setup` de los medios del producto, ejecute `XenDesktopVdaSetup.exe`, mediante una o varias de las siguientes opciones, descritas en Opciones de línea de comandos para instalar un VDA.

- `/reconfigure` (opción necesaria para personalizar un VDA)
- `/h o /help`
- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber port`
- `/enable_hdx_ports`

### Opciones de línea de comandos para instalar Universal Print Server

La siguiente opción es válida con el comando `XenDesktopPrintServerSetup.exe`.

- `/enable_upsserver_port`

Software	Carpeta	Nombre de archivo
Runtime de Microsoft Visual C++ 2017 (de 32 y 64 bits).	Support > VcRedist_2017	<code>vcredist_x64.exe</code> <code>yvcredist_x86.exe</code>
Citrix Diagnostic Facility	x64> Componentes de escritorio virtual	<code>cdf_x64.msi</code>

---

Software	Carpeta	Nombre de archivo
Componente de servidor de impresión universal (Universal Print Server)	x64 > Universal Print Server	UpsServer_x64.msi

---

Cuando no se especifica esta opción, el instalador muestra la página **Firewall** de la interfaz gráfica. Seleccione **Automáticamente** para que el instalador agregue automáticamente las reglas del firewall de Windows o **Manualmente** para permitir que el administrador configure manualmente el firewall.

Después de instalar el software en los servidores de impresión, configure el Universal Print Server siguiendo las instrucciones de [Aprovisionar impresoras](#).

## Instalar agentes VDA mediante scripts

May 5, 2023

### Nota:

Citrix no se hace responsable de los problemas causados por scripts adaptados a los entornos de producción de los clientes. Para cualquier problema de Citrix relacionado con la instalación, inicie un caso de asistencia técnica con los registros de instalación pertinentes en el [portal de Citrix Support](#).

Este artículo se aplica en caso de instalar agentes VDA en máquinas con sistemas operativos Windows. Para obtener información acerca de los agentes VDA para sistemas operativos Linux, consulte la documentación de [Linux Virtual Delivery Agent](#).

Los medios de instalación contienen scripts de ejemplo para instalar, actualizar o quitar los agentes Virtual Delivery Agent (VDA) de máquinas en Active Directory. También puede usar los scripts para mantener las imágenes maestras que utilicen Machine Creation Services y Citrix Provisioning (antes Provisioning Services).

Acceso requerido:

- El script necesita acceso de lectura para Todos en el recurso compartido de red donde se encuentra el comando de instalación de VDA. El comando de instalación es `XenDesktopVdaSetup.exe` en la imagen ISO del producto completo; `VDAWorkstationSetup.exe` o `VDAServerSetup.exe` en un instalador independiente.
- Los detalles de registros se almacenan localmente en cada máquina. Si quiere registrar los resultados en una ubicación centralizada, para poder consultarlos y analizarlos, los scripts necesitan acceso de Lectura y Escritura para Todos en el recurso compartido de red correspondiente.

Para comprobar los resultados de la ejecución de un script, consulte el recurso compartido de registros centralizados. Los registros capturados incluyen el registro del script, el registro del instalador y los registros de instalación de MSI. Cada intento de instalación o eliminación se registra en una carpeta con su fecha y hora. El nombre de la carpeta indica si la operación se realizó o no correctamente, con el prefijo PASS o FAIL, respectivamente. Puede usar herramientas estándar de búsqueda de directorios para buscar una instalación o eliminación fallidas en el recurso compartido de registros centralizados. Esas herramientas ofrecen una alternativa a la búsqueda local en las máquinas de destino.

Antes de comenzar una instalación, consulte y complete las tareas de [Antes de instalar](#).

## Instalar o actualizar agentes VDA mediante el script

1. Obtenga el script de ejemplo **InstallVDA.bat**, ubicado en el directorio `\Support\AdDeploy\` de los medios de instalación. Citrix recomienda realizar una copia de seguridad de los scripts originales antes de personalizarlos.
2. Modifique el script:
  - Especifique la versión del VDA que quiere instalar: `SET DESIREDVERSION`. Por ejemplo: la versión 7 se puede especificar como 7.0. El valor completo se encuentra en los medios de instalación, en el archivo `ProductVersion.txt`. Sin embargo, no es necesaria una coincidencia completa.
  - Especifique el recurso compartido de red desde donde se invocará al instalador. Indique la raíz de la distribución (el nivel superior del árbol). Cuando se ejecute el script, se invocará automáticamente la versión apropiada del instalador (32 bits o 64 bits). Por ejemplo: `SET DEPLOYSHARE=\\fileserv1\share1`.
  - Si lo desea, puede especificar también una ubicación en el recurso compartido de red para guardar los registros centralizados. Por ejemplo: `SET LOGSHARE=\\fileserv1\log1`.
  - Especifique las opciones de configuración del agente VDA como se describe en [Instalación desde la línea de comandos](#). Las opciones `/quiet` y `/noreboot` se incluyen de manera predeterminada en el script y son necesarias: `SET COMMANDLINEOPTIONS=/QUIET /NOREBOOT`.
3. Mediante la directiva de grupo Scripts de inicio, asigne el script a la unidad organizativa donde se encuentran las máquinas. Esta unidad organizativa debe contener solo las máquinas donde quiere instalar VDA. Cuando se reinicien las máquinas de esa unidad organizativa, el script se ejecutará en todas ellas. Se instala un VDA en cada máquina que tenga un sistema operativo compatible.

## Eliminar agentes VDA mediante el script

1. Obtenga el script de ejemplo UninstallVDA.bat en el directorio \Support\AdDeploy\ de los medios de instalación. Citrix recomienda realizar una copia de seguridad de los scripts originales antes de personalizarlos.
2. Modifique el script.
  - Especifique la versión del VDA que quiere quitar: `SET CHECK\_VDA\_VERSION`. Por ejemplo: la versión 7 se puede especificar como 7.0. El valor completo se puede encontrar en los medios de instalación, en el archivo ProductVersion.txt (por ejemplo, 7.0.0.3018). Sin embargo, no es necesaria una coincidencia completa.
  - Si lo desea, puede especificar también una ubicación en el recurso compartido de red para guardar los registros centralizados.
3. Mediante la directiva de grupo Scripts de inicio, asigne el script a la unidad organizativa donde se encuentran las máquinas. Esta unidad organizativa debe contener solo las máquinas de donde quiere quitar el VDA. Cuando se reinicien las máquinas de esa unidad organizativa, el script se ejecutará en todas ellas. Se elimina el VDA de cada máquina.

## Solución de problemas

El script genera archivos de registros internos que describen el progreso de la ejecución del script. El script copia un registro llamado Kickoff\_VDA\_Startup\_Script en el recurso compartido de registros centralizados a los pocos segundos de iniciarse la implementación. Eso permite comprobar que el proceso global está funcionando. Si este registro no se copia al recurso compartido de registros centralizados como es de esperar, puede inspeccionar la máquina local para buscar a qué se debe. El script coloca dos archivos de registro de depuración en la carpeta %temp% de cada máquina:

- Kickoff\_VDA\_Startup\_Script\_<FechaHora>.log
- VDA\_Install\_ProcessLog\_<FechaHora>.log

Revise el contenido de esos registros para comprobar que el script:

- Se ejecuta según lo previsto.
- Detecta correctamente el sistema operativo de destino.
- Está configurado correctamente para que apunte a la raíz de DEPLOYSHARE (que contiene el archivo AutoSelect.exe).
- Es capaz de autenticarse en los dos puntos compartidos DEPLOYSHARE y LOGSHARE.

## Instalar agentes VDA mediante SCCM

May 5, 2023

### Nota:

Citrix no se hace responsable de los problemas que puedan surgir por la implementación de un Virtual Delivery Agent (VDA) mediante herramientas de distribución de software, como Microsoft System Center Configuration Manager (SCCM), adaptadas a los entornos de producción de los clientes. Para cualquier problema de Citrix relacionado con la instalación, inicie un caso de asistencia técnica con los registros de instalación pertinentes en el [portal de Citrix Support](#).

### Introducción

Para implementar correctamente un Virtual Delivery Agent (VDA) con Microsoft System Center Configuration Manager (SCCM) o herramientas de distribución de software similares, Citrix recomienda usar el instalador de VDA a través de una serie de pasos.

Citrix no recomienda utilizar la utilidad de limpieza de VDA como parte de la instalación o la actualización de un VDA. Utilice la utilidad de limpieza de VDA solamente en el caso limitado en que el instalador de VDA haya fallado antes.

### Reinicios

La cantidad de reinicios necesarios durante la instalación del VDA depende del entorno. Por ejemplo:

- Es posible que necesite reiniciar por actualizaciones pendientes o instalaciones de software anteriores.
- Es posible que haya archivos previamente bloqueados por otros procesos que necesiten actualizaciones, lo que obliga a realizar un reinicio más.
- Es posible que algunos componentes opcionales del instalador de VDA (como Citrix Profile Management o Citrix Files) requieran un reinicio.

El secuenciador de tareas de SCCM administra todos los reinicios necesarios.

### Definir la secuencia de tareas

Después de identificar todos los requisitos previos y reinicios, utilice el secuenciador de tareas de SCCM para completar lo siguiente:

- Los VDA se pueden instalar desde una copia accesible de los medios de instalación o desde uno de los instaladores independientes de VDA:
  - `VDAWorkstationSetup_XXXX.exe`
  - `VDA ServerSetup_XXXX.exe`
  - `VDAWorkstationCoreSetup_XXXX.exe`

Para obtener más información sobre los instaladores de VDA, consulte [Instaladores](#).

- Al actualizar la versión de un VDA, la máquina en la que está instalado debe estar en modo de mantenimiento, sin sesiones.
- Cuando se ejecuta la instalación de un VDA por primera vez en una máquina, el instalador de VDA que se utiliza se copia en esa máquina.
  - Al utilizar un instalador de VDA que no sea `VDAWorkstationCoreSetup_XXXX.exe`, el instalador de VDA se copia en `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopVdaSetup.exe`.
  - Al utilizar `VDAWorkstationCoreSetup_XXXX.exe`, el instalador de VDA se copia en `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopRemotePCSetup.exe`.
- La ubicación del directorio del instalador de VDA también se almacena en el Registro “`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaInstall`” “`MetaInstallerInstallLocation`”.
- Agregue las opciones `/NOREBOOT`, `/NORESUME` y `/QUIET` de la línea de comandos a sus opciones de línea de comandos.
  - `/QUIET`: No muestra la interfaz de usuario durante la instalación, de modo que SCCM controla el proceso de la instalación.
  - `/NOREBOOT`: Impide que el instalador de VDA se reinicie automáticamente. SCCM activa los reinicios cuando es necesario.
  - `/NORESUME`: Normalmente, cuando es necesario reiniciar durante la instalación, el instalador de VDA establece una clave del Registro `runonce` (`\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`). Al reiniciar la máquina, Windows utiliza la clave para iniciar el instalador de VDA. Esto es un problema para SCCM, ya que SCCM no puede supervisar la instalación ni capturar el código de salida.

## Ejemplo de secuencia de instalación mediante SCCM

En este ejemplo se muestra la secuencia de instalación.

1. **SCCM TASK1:** Prepare la máquina mediante un reinicio de la máquina.
2. **SCCM TASK2:** Inicie la instalación de VDA.
  - a) Agregue las opciones `/quiet`, `/noreboot` y `/noresume` a sus opciones de línea de comandos.
  - b) Ejecute el instalador de VDA que prefiera (imagen local o uno de los instaladores mínimos).
  - c) SCCM debe capturar el código de devolución.
    - Si el código de devolución es 0 u 8, la instalación se ha completado y es necesario reiniciar.
    - Si el código de devolución es 3, reinicie la máquina y, a continuación, pase el control a SCCM TASK3.
3. **SCCM TASK3:** Continúa con la instalación de VDA.
  - a) Si SCCM TASK2 no devuelve un 0 o un 8, la instalación debe continuar una vez finalizado el reinicio.
  - b) SCCM TASK3 se repite hasta que el instalador de VDA devuelve un 0 o un 8 (lo que indica que la instalación se realizó correctamente) o un 3 (lo que indica que debe repetirse SCCM TASK3). Trate los demás códigos de devolución como un error y SCCM TASK3 debería notificar un error y detenerse.
  - c) Para reanudar la instalación de VDA, ejecute el instalador de VDA adecuado ([XenDesktopVdaSetup.exe](#) en la mayoría de los casos o [XenDesktopRemotePCSetup.exe](#) si se utilizó [VDAWorkstationCoreSetup\\_XXXX.exe](#)) desde la ubicación en la que se copió (como se describe en Definir la secuencia de tareas), sin parámetros de la línea de comandos (el instalador de VDA utiliza los parámetros que guardó durante la primera ejecución del instalador).
  - d) Preste atención al código de devolución del instalador de VDA.
    - 0 u 8: Operación correctamente realizada, instalación completa, es necesario reiniciar.
    - 3: La instalación no se ha completado. Reinicie la máquina y repita SCCM TASK3 hasta que se devuelva un 0 o un 8. Trate los demás códigos de devolución como un error y SCCM TASK3 debería notificar un error y cerrarse.

Para obtener más información acerca de los códigos de retorno, consulte [Códigos de retorno en la instalación de Citrix](#).

## Ejemplos de comandos de instalación de VDA

Las opciones de instalación disponibles varían dependiendo del instalador que se utilice. Consulte los siguientes artículos para obtener información detallada sobre las opciones de línea de comandos

- [Instalar VDA](#)

- [Instalación desde la línea de comandos](#)

### Comandos de instalación para Acceso con Remote PC

- Este comando utiliza el instalador de VDA básico de sesión única (`VDAWorkstationCoreSetup.exe`):

```
VDAWorkstationCoreSetup.exe /quiet /controllers "control.domain.com" /enable_hdx_ports /noresume /noreboot
```

- Este comando utiliza el instalador de VDA completo de sesión única (`VDAWorkstationSetup.exe`):

```
VDAWorkstationSetup.exe /quiet /remotepc /controllers "control.domain.com" /enable_hdx_ports /noresume /noreboot
```

### Comando de instalación para imagen de disco virtual (VDI) dedicada

- Este comando utiliza el instalador de VDA completo de sesión única (`VDAWorkstationSetup.exe`):

```
VDAWorkstationSetup.exe /quiet /components vda /controllers "control.domain.com" /enable_hdx_ports /enable_remote_assistance /noresume /noreboot
```

## Crear un sitio

November 4, 2021

Un *sitio* es el nombre que se da a una implementación de Citrix Virtual Apps and Desktops. Incluye Delivery Controllers y otros componentes principales, los VDA (Virtual Delivery Agent), las conexiones a hosts (si las hay), además de los catálogos de máquinas y los grupos de entrega. Puede crear el sitio después de instalar los componentes principales, antes de crear el primer catálogo de máquinas y el primer grupo de entrega.

Si el Controller está instalado en Server Core, use los cmdlets de PowerShell en [Citrix Virtual Apps and Desktops SDK](#) para crear un sitio.

Cuando se crea un sitio, usted queda inscrito automáticamente en el programa CEIP de mejora de la experiencia del cliente (Citrix Customer Experience Improvement Program). CEIP recopila estadísticas y datos de uso anónimos y, a continuación, los envía a Citrix. El primer paquete de datos se

envía a Citrix aproximadamente siete días después de crear el sitio. Puede cambiar su inscripción en cualquier momento después de crear el sitio. Seleccione **Configuración** en el panel de navegación de Studio. A continuación, seleccione la ficha **Asistencia para productos** y siga las instrucciones. Para obtener información detallada, consulte <http://more.citrix.com/XD-CEIP>.

El usuario que crea un sitio se convierte en un administrador total; para obtener más información, consulte [Administración delegada](#).

Consulte este artículo antes de crear el sitio, para saber cuál debería ser el procedimiento.

## Paso 1. Abra Studio e inicie el Asistente para creación de sitios

Abra Studio, si aún no está abierto. Se le guiará automáticamente a la acción que inicia el Asistente para la creación de sitios. Seleccione esa acción.

## Paso 2. Nombre y tipo de sitio

En la página **Introducción**, elija un tipo de sitio:

- **Sitio de entrega de aplicaciones y escritorios.** Cuando crea un sitio de entrega de aplicaciones y escritorios, también puede decidir si crear un sitio de implementación completa (recomendado) o un sitio vacío. Un sitio vacío solo está configurado parcialmente y son los usuarios avanzados los que suelen crearlo.
- **Sitio de acceso con Remote PC.** Un sitio de acceso con Remote PC permite a usuarios designados acceder a sus equipos de oficina de forma remota a través de una conexión segura.

Si crea ahora una implementación de entrega de aplicaciones y escritorios, puede agregar más adelante una implementación de acceso con Remote PC. De igual manera, si ahora crea una implementación de acceso con Remote PC, puede agregar más adelante una implementación completa.

Escriba un nombre para el sitio. Una vez creado el sitio, aparece el nombre de este en la parte superior del panel de navegación de Studio: **Citrix Studio** (*nombre del sitio*).

## Paso 3. Bases de datos

La página **Bases de datos** contiene selecciones para configurar la base de datos del sitio, la base de datos de supervisión y la base de datos de registros de configuración. Para obtener más información acerca de las opciones y los requisitos de configuración de las bases de datos, consulte [Bases de datos](#).

Si instala SQL Server Express para usarlo como la base de datos del sitio, se producirá un reinicio después de la instalación de ese software. Ese reinicio no se producirá si no instala el software SQL Server Express para usarlo como la base de datos del sitio.

Si no utiliza el software SQL Server Express predeterminado, compruebe que el software de SQL Server está instalado en las máquinas antes de crear el sitio. En [Requisitos del sistema](#) se ofrece una lista de las versiones compatibles.

Si quiere agregar más Delivery Controllers al sitio y ya ha instalado el software de Controller en otros servidores, puede agregar esos Controllers desde esta página. Si también va a generar scripts para configurar las bases de datos, agregue los Controllers antes de generarlos.

#### **Paso 4. Licencias**

En la página **Licencias**, especifique la dirección del servidor de licencias y, a continuación, indique la licencia a utilizar (instalar).

- Especifique la dirección del servidor de licencias en el formato **name** : [ **port** ] . El *nombre* debe ser un nombre de dominio completo (FQDN), un nombre NetBIOS o una dirección IP. Se recomienda FQDN. Si se omite el número de puerto, el predeterminado es 27000. Haga clic en **Conectar**. No se puede pasar a la siguiente página hasta que se establezca una conexión con el servidor de licencias.
- Cuando se establece una conexión, se selecciona **Usar una licencia existente** de forma predeterminada. La pantalla muestra los productos compatibles con los que se puede configurar este producto, en función de las licencias instaladas actualmente.
  - Si quiere configurar este producto como uno de los productos indicados (por ejemplo, Citrix Virtual Apps Premium o Citrix Virtual Desktops Premium), con una de esas licencias, seleccione esa entrada.
  - Si ya ha asignado y descargado una licencia (con la ayuda de Citrix Manage Licenses Tool) para usarla con este producto, pero aún no ha instalado la licencia:
    - \* Haga clic en **Buscar un archivo de licencias**.
    - \* En el explorador de archivos, busque y seleccione la licencia que descargó. Los productos asociados aparecen ahora en la página **Licencias** del asistente de creación de sitios. Seleccione la entrada que quiere utilizar.
  - Si no se muestra el producto que quiere, o si no tiene licencias asignadas y descargadas, puede asignar, descargar e instalar una licencia. Para ello, el servidor de licencias debe tener acceso a Internet. Debe tener un código de acceso a licencias para el producto que quiere utilizar. Citrix debería haberle enviado un correo electrónico con ese código.
    - \* Haga clic en **Asignar y descargar**.
    - \* En el cuadro de diálogo **Asignar licencias**, introduzca el código de acceso a licencias enviado por Citrix. Haga clic en **Asignar licencias**.

- \* Los productos asociados a la nueva licencia aparecen en la página **Licencias** del asistente de creación de sitios. Seleccione la entrada que quiere utilizar.

Alternativamente, seleccione **Usar el período de prueba de 30 días gratis** e instale las licencias más tarde. Para obtener información más detallada, consulte la [documentación de Licencias](#).

## **Paso 5. Administración de energía (solo para acceso con Remote PC)**

Consulte el paso 8. Acceso con Remote PC

## **Paso 6. Conexión de host, red y almacenamiento**

Si utiliza máquinas virtuales en un hipervisor o servicio de nube para entregar aplicaciones y escritorios, tiene la opción de crear la primera conexión con el host. También puede especificar los recursos de red y almacenamiento para esa conexión. Después de crear el sitio, puede modificar esa conexión y esos recursos; también puede crear más conexiones. Para obtener más información, consulte [Conexiones y recursos](#).

- Para conocer la información que se especifica en la página **Conexión**, consulte [Conexiones y recursos](#).
  - Si no usa máquinas virtuales alojadas en hipervisores ni servicios de nube (o si usa Studio para administrar escritorios alojados en máquinas blade dedicadas), seleccione el tipo de conexión **Ninguno**.
  - Si configura un sitio de acceso con Remote PC y quiere utilizar la función Wake on LAN, seleccione el tipo **Microsoft System Center Configuration Manager**.

Además del tipo de conexión, especifique si usará las herramientas de Citrix (como Machine Creation Services) u otras herramientas para crear las máquinas virtuales.

- Para conocer la información que se especifica en las páginas **Almacenamiento** y **Red**, consulte [Almacenamiento de host](#), [Administrar almacenamiento](#) y [Seleccionar almacenamiento](#).

## **Paso 7. Funciones adicionales**

En la página **Funciones adicionales**, puede seleccionar funciones para personalizar su sitio. Cuando se marca la casilla de verificación de un elemento que requiere información, aparece un cuadro de configuración.

- **Integración de AppDNA** (esta función se [retiró](#)): Si usa AppDisks y tiene instalado AppDNA. La integración con AppDNA permite analizar las aplicaciones que contienen los AppDisks. Con esos análisis, puede ver si hay problemas de compatibilidad y llevar a cabo acciones para resolverlos.
- **Publicación de App-V**: Seleccione esta funcionalidad si quiere usar aplicaciones de paquetes de Microsoft App-V que se encuentran en servidores de App-V. Facilite la URL del servidor de administración de App-V, así como la URL y el número de puerto del servidor de publicación de App-V.

Si quiere usar aplicaciones procedentes de paquetes de App-V solo en recursos compartidos de red, no es necesario seleccionar esta funcionalidad.

También puede habilitar, inhabilitar o configurar esta funcionalidad más adelante en Studio. Para obtener más información, consulte [App-V](#).

## Paso 8. Acceso con Remote PC

Para obtener información acerca de implementaciones de acceso con Remote PC, consulte [Acceso con Remote PC](#).

Si utiliza la función Wake on LAN, complete los pasos de configuración en System Center Configuration Manager de Microsoft antes de crear el sitio. Para obtener más información, consulte [Configuration Manager y Wake on LAN para Acceso con Remote PC](#).

Al crear un sitio de acceso con Remote PC:

- Si usa la función Wake on LAN, en la página **Administración de energía**, especifique la dirección, las credenciales y la conexión de Microsoft System Center Configuration Manager.
- Especifique los usuarios o los grupos de usuarios en la página **Usuarios**. No hay ninguna acción predeterminada que agregue automáticamente a todos los usuarios. Asimismo, especifique datos sobre cuentas de máquina (dominio y OU) en la página **Cuentas de máquina**.

Para agregar información de los usuarios, haga clic en **Agregar usuarios**. Seleccione usuarios y grupos de usuarios, y luego haga clic en **Agregar usuarios**.

Para agregar información sobre cuentas de máquina, haga clic en **Agregar cuentas de máquina**. Seleccione las cuentas de máquina y, a continuación, haga clic en **Agregar cuentas de máquina**. Haga clic en **Agregar unidades organizativas**. Seleccione el dominio y las unidades organizativas, e indique si deben incluirse los elementos de las subcarpetas. Haga clic en **Agregar unidades organizativas**.

Se crea automáticamente un catálogo de máquinas llamado “Cuentas de máquina de usuarios para Remote PC”. Este catálogo contiene todas las cuentas de máquina que se agregaron en el Asistente para la creación de sitios. Se crea automáticamente un grupo de entrega llamado “Escritorios de

usuario para Remote PC". Este grupo contiene a todos los usuarios y los grupos de usuarios que se hayan agregado.

## Paso 9: Resumen

La página **Resumen** contiene la información especificada. Utilice el botón **Atrás** si quiere cambiar algo. Cuando haya terminado, haga clic en **Crear** y comenzará la creación del sitio.

## Probar la configuración del sitio

Para ejecutar pruebas después de crear un sitio, seleccione **Citrix Studio (Sitio nombre-de-sitio)** en la parte superior del panel de navegación. A continuación, haga clic en **Probar sitio** en el panel central. Puede ver un informe HTML de los resultados de la prueba del sitio.

La prueba de funcionamiento del sitio puede fallar si hay un Controller instalado en Windows Server 2016. El error se produce cuando una base de datos local SQL Server Express se utiliza como la base de datos del sitio y no se ha iniciado el servicio SQL Server Browser. Para evitar este fallo, complete las tareas siguientes.

1. Habilite el servicio SQL Server Browser (si fuera necesario) e inícielo.
2. Reinicie el servicio SQL Server (SQLEXPRESS).

Las pruebas del sitio se ejecutan automáticamente cuando actualiza una implementación anterior. Para ver información más detallada, consulte [Pruebas preliminares en el sitio](#).

## Solución de problemas

Después de configurar el sitio, puede instalar Studio y agregarlo a través de la consola MMC como un complemento en una máquina remota. Si intenta quitar ese complemento más adelante, la consola MMC puede dejar de responder. Como solución temporal, reinicie MMC.

## Crear catálogos de máquinas

June 27, 2024

Las colecciones de máquinas físicas o virtuales se administran como una entidad única, llamada catálogo de máquinas. Las máquinas de un catálogo tienen el mismo tipo de sistema operativo: SO multi-sesión o SO de sesión única. Un catálogo de máquinas con SO multisesión puede contener máquinas Windows o Linux, pero no ambas.

Studio le guiará para crear el primer catálogo de máquinas después de crear el sitio. Después de crear el primer catálogo de máquinas, Studio le guiará para crear su primer grupo de entrega. Posteriormente, puede cambiar el catálogo que haya creado y crear más catálogos.

**Sugerencia:**

Si actualiza una implementación existente que habilita la función de optimización del almacenamiento de Machine Creation Services (MCS), denominada E/S de MCS, no se requiere ninguna configuración adicional. El VDA y la actualización de Delivery Controller gestionan la actualización de E/S de MCS.

## Introducción

Cuando crea un catálogo de máquinas virtuales, debe indicar cómo aprovisionarlas. Puede usar herramientas de Citrix, como Machine Creation Services (MCS) o Citrix Provisioning (antes Provisioning Services). O bien, puede utilizar sus propias herramientas para aprovisionar máquinas.

Tenga en cuenta lo siguiente:

- MCS admite un único disco del sistema en la imagen de la máquina virtual. Ignora el resto de los discos de datos conectados a dicha imagen.
- Si utiliza Citrix Provisioning para crear las máquinas, consulte la documentación de [Citrix Provisioning](#) para obtener instrucciones.
- Si elige Machine Creation Services para aprovisionar las máquinas, debe proporcionar una imagen maestra (o una instantánea de ella) para crear máquinas virtuales idénticas en el catálogo. Antes de crear el catálogo, primero debe usar las herramientas en el hipervisor o servicio de nube para crear y configurar la imagen maestra. Este proceso incluye instalar un Virtual Delivery Agent (VDA) en la imagen. Después, crea un catálogo de máquinas en Studio. Debe seleccionar esa imagen (o instantánea), especificar la cantidad de máquinas virtuales que se van a crear en el catálogo y configurar información adicional.
- Si las máquinas ya están disponibles, debe crear igualmente uno o varios catálogos para esas máquinas.
- Si crea un catálogo directamente mediante el SDK de PowerShell, puede especificar una plantilla de hipervisor (VMTemplates), en vez de una imagen o una instantánea de la imagen.

Si utiliza Machine Creation Services o Citrix Provisioning para crear el primer catálogo de máquinas, debe usar la conexión de host que ha configurado al crear el sitio. Más adelante, después de crear el primer catálogo de máquinas y el grupo de entrega, podrá cambiar la información de esta conexión o crear conexiones adicionales.

Después de completar el Asistente para la creación de catálogos de máquinas, se ejecutan pruebas automáticamente para garantizar que los catálogos se han configurado correctamente. Una vez com-

pletadas las pruebas, generan un informe que podrá ver. Ejecute las pruebas en cualquier momento desde Studio.

**Nota:**

MCS no es compatible con Windows 10 IoT Core ni Windows 10 IoT Enterprise. Consulte el [sitio de Microsoft](#) para obtener más información.

Para obtener detalles técnicos sobre las herramientas de Citrix Provisioning, consulte [Administración de imágenes de Citrix Virtual Apps and Desktops](#).

### Verificar licencias RDS

Por ahora, Citrix Studio no realiza la comprobación de licencias RDS válidas de Microsoft al crear catálogos de máquinas que contengan máquinas con SO Windows multisesión. Para ver el estado de la licencia RDS de Microsoft en una **máquina con SO multisesión** Windows, vaya a Citrix Director. Consulte el estado de la licencia de Microsoft RDS en el panel **Detalles de la máquina** de la página **Detalles de la máquina y Detalles del usuario**. Para obtener más información, consulte [Estado de la licencia RDS de Microsoft](#).

### Registro de VDA

El agente VDA debe registrarse en un Delivery Controller (en implementaciones locales) o Cloud Connector (en implementaciones Citrix Cloud) para que se le tenga en cuenta cuando se inicien sesiones con broker. Los VDA no registrados pueden derivar en una infrutilización de los recursos disponibles. Existen diversos motivos por los que un VDA puede no registrarse, y un administrador puede solucionar muchos de ellos. Para solucionar problemas, Studio proporciona información en el Asistente para la creación de catálogos, y después de agregar máquinas de un catálogo a un grupo de entrega.

En el Asistente para la creación de catálogos de máquinas, después de agregar las máquinas existentes, la lista de nombres de cuenta de equipo indicará si cada máquina es adecuada para agregarla al catálogo. Pase el puntero sobre el icono situado junto a cada máquina para ver un mensaje informativo sobre esa máquina.

Si el mensaje indica una máquina problemática, puede quitarla (mediante el botón **Quitar**) o agregarla. Por ejemplo, si un mensaje indica que es posible que no se obtenga información acerca de una máquina (tal vez porque nunca se registró), agréguela de todos modos.

Para obtener más información, consulte:

- [CTX136668](#) para obtener instrucciones de solución de problemas en el registro de los VDA
- Niveles funcionales y versiones de VDA
- [Métodos de registro de los VDA](#)

## Resumen de la creación de catálogos con MCS

A continuación, se ofrece un breve resumen de las acciones de MCS predeterminadas después de proporcionar información en el Asistente para la creación de catálogos de máquinas.

- Si seleccionó una imagen maestra (en lugar de una instantánea), MCS crea una instantánea.
- MCS crea una copia completa de la instantánea y la coloca en cada ubicación de almacenamiento definida en la conexión de host.
- MCS agrega las máquinas a Active Directory, lo que crea identidades únicas.
- MCS crea la cantidad de máquinas virtuales especificadas en el asistente, con dos discos definidos para cada máquina virtual. Además de los dos discos por máquina virtual, también se almacena una imagen maestra en la misma ubicación de almacenamiento. Si ha definido varias ubicaciones de almacenamiento, cada una obtiene los siguientes tipos de disco:
  - La copia completa de la instantánea, que es de solo lectura, y se comparte entre las máquinas virtuales que se acaban de crear.
  - Un disco de identidad único de 16 MB que proporciona a cada máquina virtual una identidad única. Cada máquina virtual obtiene un disco de identidad.
  - Un disco de diferenciación único para almacenar las escrituras realizadas en la máquina virtual. Este disco es de aprovisionamiento ligero (si el almacenamiento del host lo admite) y aumenta al tamaño máximo de la imagen maestra, si fuera necesario. Cada máquina virtual obtiene un disco de diferenciación. El disco de diferenciación contiene los cambios realizados durante las sesiones. Es permanente para los escritorios dedicados. Para escritorios agrupados, se elimina y se crea uno después de cada reinicio a través del Delivery Controller.

Como alternativa, al crear máquinas virtuales para entregar escritorios estáticos, puede especificar (en la página **Máquinas** del Asistente para la creación del catálogo de máquinas) que se creen clones de máquinas virtuales pesados (de copia completa). Los clones completos no necesitan retener la imagen maestra en cada almacén de datos. Cada máquina virtual tiene su propio archivo.

## Consideraciones sobre el almacenamiento de Machine Creation Services

Hay muchos factores al tomar una decisión sobre las soluciones de almacenamiento, las configuraciones y las prestaciones para MCS. La siguiente información proporciona consideraciones adecuadas para la capacidad de almacenamiento:

*Consideraciones de capacidad:*

- Discos

Los discos Delta o de diferenciación (Diff) consumen la mayor cantidad de espacio en la mayoría de las implementaciones de MCS para cada máquina virtual. Cada máquina virtual creada por

MCS se da en un mínimo de 2 discos tras la creación.

- Disco0 = Disco de diferenciación: contiene el sistema operativo cuando se copia de la imagen base maestra.
- Disk1 = Disco de identidad: 16 MB. Contiene datos de Active Directory para cada máquina virtual.

A medida que el producto evoluciona, es posible que tenga que agregar más discos para satisfacer determinados casos de uso y el consumo de funciones. Por ejemplo:

- [Personal vDisk](#) ofrece a los usuarios finales la capacidad de instalar aplicaciones sin intervención del administrador en un disco aparte, conectado a la máquina virtual.
- [AppDisk](#) ofrece a los usuarios finales la capacidad de adjuntar los discos de solo aplicaciones a máquinas virtuales, principalmente para catálogos de SO multisesión.
- [Optimización de almacenamiento de MCS](#) crea un disco de estilo de caché de escritura para cada máquina virtual.
- MCS ha agregado la capacidad de usar [clones de copia completa](#) en lugar del caso de uso del disco Delta descrito anteriormente.

Las funciones del hipervisor también pueden entrar en la ecuación. Por ejemplo:

- [Citrix Hypervisor IntelliCache](#) crea un disco de lectura en el almacenamiento local para que cada Citrix Hypervisor guarde en IOPS en la imagen maestra que podría mantenerse en la ubicación compartida de almacenamiento.

- Sobrecarga del hipervisor

Cada hipervisor utiliza archivos específicos que crean sobrecarga para las máquinas virtuales. Los hipervisores también usan el almacenamiento para operaciones de administración y registro general. Calcular espacio para incluir la sobrecarga de:

- [Archivos de registros](#)
- Archivos específicos del hipervisor. Por ejemplo:
  - \* VMware agrega más archivos a la carpeta de **almacenamiento de VM**. Consulte [Prácticas recomendadas de VMware](#).
  - \* Calcule los requisitos del tamaño total de máquinas virtuales. Tome como ejemplo una máquina virtual con 20 GB para el disco virtual, 16 GB para el archivo de intercambio de máquina virtual (el tamaño de una memoria asignada) y 100 MB para los archivos de registros, o bien 36,1 GB en total.
- [Instantáneas para XenServer](#); [Instantáneas para VMware](#).

- Sobrecarga del proceso

Crear un catálogo, agregar una máquina y actualizar un catálogo tienen implicaciones únicas en el almacenamiento. Por ejemplo:

- La **creación inicial de catálogos** requiere que se copie una copia del disco base en cada ubicación de almacenamiento.
  - \* También requiere que cree una **máquina virtual de preparación** temporalmente.
- **Agregar una máquina** a un catálogo no requiere copiar el disco base en cada ubicación de almacenamiento. La creación del catálogo varía en función de las funcionalidades seleccionadas. Por lo tanto, un catálogo que emplea un disco personal vDisk o AppDisks necesitará más espacio que un simple catálogo aleatorio agrupado.
- **La actualización del catálogo** permite crear un disco base adicional en cada ubicación de almacenamiento. Las actualizaciones de catálogos también experimentan un pico temporal de almacenamiento donde cada máquina virtual en el catálogo tiene 2 discos de diferenciación (Diff) durante un cierto período de tiempo.

*Más consideraciones:*

- **Tamaño de la RAM:** Afecta al tamaño de ciertos archivos y discos de hipervisor, incluidos los discos de optimización de E/S, la memoria caché de escritura, y archivos de instantáneas.
- **Aprovisionamiento fijo/dinámico:** se prefiere el almacenamiento NFS debido a las prestaciones del aprovisionamiento dinámico.

### **Optimización del almacenamiento de Machine Creation Services (MCS)**

Con la función de optimización del almacenamiento de Machine Creation Services (MCS), denominada E/S de MCS:

- El contenedor de la memoria caché de escritura *se basa en los archivos*; es la misma funcionalidad que se encuentra en Citrix Provisioning. Por ejemplo, el nombre de archivo en la memoria caché de escritura de Citrix Provisioning es `D:\vdiskdiff.vhdx`, y el nombre de archivo en la memoria caché de escritura de E/S de MCS es `D:\mcsdiff.vhdx`.
- Las mejoras de diagnóstico se consiguen al permitir un archivo de volcado de errores de Windows escrito en el disco de la memoria caché de escritura.
- E/S de MCS conserva la tecnología de *memoria caché en la RAM con desbordamiento al disco duro* para proporcionar la mejor solución de memoria caché de escritura a varios niveles. Esta funcionalidad permite a los administradores equilibrar el coste en cada nivel, RAM y disco, y también el rendimiento para satisfacer las expectativas deseadas de carga de trabajo.

Actualizar el método de memoria caché de escritura de la opción *por disco* a la opción *por archivo* requiere los siguientes cambios:

1. E/S de MCS ya no admite la memoria caché solo en RAM. Especifique un tamaño de disco en Citrix Studio durante la creación del catálogo de máquinas.

2. El disco de la memoria caché de escritura de una VM se crea y se formatea automáticamente al arrancar la VM por primera vez. Cuando la VM ya está activa, el archivo de la memoria caché de escritura `mcsdif.vhdx` se escribe en el volumen formateado `MCSWCDisk`.
3. A excepción de los entornos de Microsoft Azure, el archivo de paginación se redirige a este volumen formateado, `MCSWCDisk`. Como resultado, este tamaño de disco tiene en cuenta el espacio total en disco, incluida la diferencia entre el tamaño del disco y la carga de trabajo generada más el tamaño del archivo de paginación, normalmente asociado al tamaño de la RAM de la VM. El archivo de paginación de Microsoft Azure está preconfigurado para utilizar un disco temporal local y no se redirige a `MCSWCDisk` a través de la funcionalidad de E/S de optimización de almacenamiento de MCS.

**Habilitar actualizaciones de optimización del almacenamiento de MCS** Para habilitar esta funcionalidad de optimización del almacenamiento de E/S de MCS, actualice la versión del Delivery Controller y de los VDA a la versión más reciente de Citrix Virtual Apps and Desktops.

**Nota:**

Si actualiza una implementación existente que tiene habilitada E/S de MCS, no se necesita ninguna configuración adicional. El VDA y la actualización de Delivery Controller gestionan la actualización de E/S de MCS.

Cuando habilite la actualización de optimización del almacenamiento de MCS, tenga en cuenta lo siguiente:

- Al crear un catálogo de máquinas, el administrador puede configurar la RAM y el tamaño del disco.

**Machine Catalog Setup**

**Studio**

- ✓ Operating System
- ✓ Machine Management
- ✓ Desktop Experience
- ✓ Master Image
- Virtual Machines**
- Computer Accounts
- Summary

**Virtual Machines**

How many virtual machines do you want to create?

1 - +

Configure your machines.

Total memory (MB) on each machine: 4096 - +

Configure a cache for temporary data on each machine.

Memory allocated to cache (MB): 256 - +

Disk cache size (GB): 10 - +

**i** Caching should not be enabled if you intend to use this catalog to create AppDisks.  
If you clear both check boxes, temporary data is not cached; it is written to the OS storage for each VM. (This is the provisioning action in releases earlier than 7.9.)

Back Next Cancel

- Al actualizar un catálogo de máquinas existente en función de la nueva instantánea de una VM que contiene un VDA con la versión 1903 de Citrix Virtual Apps and Desktops, se sigue mediante la configuración de E/S de MCS del catálogo existente sobre RAM y tamaño del disco. El disco existente sin procesar se formatea.

### Importante:

La optimización del almacenamiento MCS cambió con Citrix Virtual Apps and Desktops 1912 LTSR. Esta versión es compatible con la tecnología de caché de escritura basada en archivos, lo que proporciona un mejor rendimiento y estabilidad. La nueva funcionalidad proporcionada por MCS E/S podría requerir un mayor requisito de almacenamiento de caché de escritura, en comparación con versiones anteriores de Citrix Virtual Apps and Desktops. Citrix recomienda volver a evaluar el tamaño del disco para asegurarse de que tiene suficiente espacio en disco para el flujo de trabajo y el archivo de paginación asignados. El tamaño del archivo de paginación suele estar relacionado con la cantidad de RAM del sistema. Si el tamaño del disco del catálogo existente es insuficiente, cree un catálogo de máquinas y asigne un disco de caché de escritura más grande.

**Acerca de los entornos de Microsoft Azure** De forma predeterminada, el disco de la memoria caché de escritura de E/S de MCS se aprovisiona durante el arranque inicial de la VM y se elimina al

apagar la VM. Aunque esta es la configuración más rentable, el tiempo de arranque de la VM es mayor porque conlleva formatear el disco de la memoria caché de escritura y un reinicio adicional. Para entornos que contienen cargas de trabajo con tiempos de arranque confidenciales, Citrix recomienda usar PowerShell para crear una VM con disco de caché persistente para E/S de MCS. Aunque el disco de caché persistente no se elimina durante el evento de ciclo de energía, hay que tener en cuenta el coste de los cargos por cuenta de almacenamiento de Azure.

**Usar PowerShell para crear un catálogo de Azure con disco de caché persistente de reescritura** Para configurar un catálogo de Azure con disco de caché persistente de reescritura, utilice el parámetro de PowerShell `New-ProvScheme CustomProperties`. Este parámetro ofrece una propiedad adicional, `PersistWBC`, que se utiliza para determinar cómo el disco de caché de reescritura persiste en máquinas aprovisionadas con MCS alojadas en Azure Resource Manager. La propiedad `PersistWBC` solo se utiliza cuando se especifica el parámetro `UseWriteBackCache` y cuando se establece el parámetro `WriteBackCacheDiskSize` para indicar que se ha creado un disco.

#### Sugerencia:

Dado que Azure presenta varias propiedades específicas para el aprovisionamiento, el campo `CustomProperties` se utiliza para muchos parámetros.

He aquí unos cuantos ejemplos de propiedades que se encuentran en el parámetro `CustomProperties` antes de optar por la propiedad `PersistWBC`:

```
1 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
2   <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
3   <Property xsi:type="StringProperty" Name="StorageAccountType" Value="Premium_LRS" />
4   <Property xsi:type="StringProperty" Name="ResourceGroups" Value="benva1dev5RG3" />
5 </CustomProperties>
6 <!--NeedCopy-->
```

Al utilizar estas propiedades, tenga en cuenta que contienen valores predeterminados si las propiedades se omiten del parámetro `CustomProperties`. La propiedad `PersistWBC` tiene dos valores posibles: **true** o **false**.

Cuando la propiedad `PersistWBC` es **true**, el disco de caché de reescritura no se elimina cuando el administrador de Citrix Virtual Apps and Desktops apaga la máquina mediante Citrix Studio.

Cuando la propiedad `PersistWBC` es **false**, el disco de caché de reescritura se elimina cuando el administrador de Citrix Virtual Apps and Desktops apaga la máquina mediante Citrix Studio.

**Nota:**

Si se omite la propiedad `PersistWBC`, su valor predeterminado es **false**, y la memoria caché de reescritura se elimina cuando la máquina se apaga mediante Citrix Studio.

Por ejemplo, así se usa el parámetro `CustomProperties` para configurar `PersistWBC` en “true” :

```

1 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
  machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
  instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
  />
3 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
  Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="ResourceGroups" Value="
  benva1dev5RG3" />
5 <Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
6 </CustomProperties>
7 <!--NeedCopy-->

```

**Importante:**

La propiedad `PersistWBC` solo se puede configurar mediante el cmdlet de PowerShell `New-ProvScheme`. Si se intenta modificar `CustomProperties` de un esquema de aprovisionamiento después de la creación, esto no afecta al catálogo de máquinas ni a la persistencia del disco de caché con reescritura cuando se apaga una máquina. El valor `PersistWBC` solo se utiliza para catálogos implementados en Azure Resource Manager.

Por ejemplo, configure `New-ProvScheme` para utilizar la memoria caché de reescritura mientras configura la propiedad `PersistWBC` en “true”:

```

1 New-ProvScheme
2 -CleanOnBoot
3 -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
  /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
  XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
  UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
  StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
  /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
  Value=`"benva1dev5RG3`" /><Property xsi:type=`"StringProperty`" Name
  =`"PersistWBC`" Value=`"true`" /></CustomProperties>"
4 -HostingUnitName "adSubnetScale1"
5 -IdentityPoolName "BV-WBC1-CAT1"
6 -MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
  GoldImages.resourcegroup\W10MCSI0-01
  _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
7 -NetworkMapping @{
8   "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
  CloudScale02.resourcegroup\adVNET.virtualprivatecloud\

```

```
    adSubnetScale1.network" }  
9  
10 -ProvisioningSchemeName "BV-WBC1-CAT1"  
11 -ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.  
    folder\Standard_D2s_v3.serviceoffering"  
12 -UseWriteBackCache  
13 -WriteBackCacheDiskSize 127  
14 -WriteBackCacheMemorySize 256  
15 <!--NeedCopy-->
```

## Compatibilidad con el arrendamiento de host AWS dedicado

Puede utilizar MCS para aprovisionar hosts AWS dedicados. Un administrador puede crear un catálogo de máquinas con el arrendamiento del host definido a través de PowerShell.

Un host dedicado Amazon [EC2] es un servidor físico con una capacidad de instancia [EC2] totalmente dedicada, lo que permite utilizar licencias de software por socket o por máquina virtual existente.

Los hosts dedicados tienen una utilización predeterminada basada en el tipo de instancia. Por ejemplo: un único host dedicado asignado de los tipos de instancia C4 Large está limitado a ejecutar 16 instancias. Consulte el [sitio de AWS](#) para obtener más información.

Los requisitos para el aprovisionamiento a los hosts AWS son:

- Una imagen (AMI) importada de BYOL (bring your own license). Con hosts dedicados, puede usar y administrar sus licencias existentes.
- Una asignación de hosts dedicados con suficiente utilización para abarcar las solicitudes de aprovisionamiento.
- Habilite **auto-placement**.

Para aprovisionar a un host AWS dedicado mediante PowerShell, utilice el cmdlet **New-ProvScheme** con el parámetro "TenancyType" establecido en *Host*.

Consulte la [documentación para desarrolladores de Citrix](#) para obtener más información.

## Preparar una imagen maestra en el hipervisor o servicio de nube

Para obtener más información sobre cómo crear conexiones a hipervisores y proveedores en la nube, consulte [Conexiones y recursos](#).

La imagen maestra contiene el sistema operativo, las aplicaciones no virtualizadas, el VDA y otro software.

Información útil:

- Una imagen maestra también se conoce como imagen clon, imagen dorada, VM base o imagen base. Los proveedores de host y los proveedores de servicios en la nube usan otros nombres.

- Al usar Citrix Provisioning, se puede usar una imagen maestra o un equipo físico como dispositivo de destino maestro. Citrix Provisioning utiliza una terminología diferente de MCS para referirse a las imágenes. Para obtener información detallada, consulte la documentación de [Citrix Provisioning](#).
- Compruebe que el hipervisor o el servicio de nube tienen procesadores, memoria y capacidad de almacenamiento suficientes para admitir la cantidad de máquinas creadas.
- Configure la cantidad necesaria de espacio en disco duro para los escritorios y las aplicaciones. Ese valor no se puede cambiar más adelante o en el catálogo de la máquina.
- Los catálogos de máquinas de acceso con Remote PC no utilizan imágenes maestras.
- Consideraciones acerca de la activación de KMS de Microsoft al utilizar Machine Creation Services: Si la implementación incluye agentes VDA con la versión 7.x y un host de XenServer 6.1 o 6.2, vSphere o Microsoft System Center Virtual Machine Manager, no tendrá que rearmar manualmente Microsoft Windows ni Microsoft Office.

Instale y configure el siguiente software en la imagen maestra:

- Herramientas de integración para el hipervisor (como Citrix VM Tools, Servicios de integración de Hyper-V o VMware Tools). Si omite este paso, es posible que las aplicaciones y los escritorios no funcionen correctamente.
- Un agente VDA. Citrix recomienda instalar la última versión para poder disponer de las funciones más recientes. Un error en la instalación del VDA en la imagen maestra provoca un error en la creación de catálogos.
- Si fuera necesario, herramientas de terceros, como el software antivirus o agentes de distribución electrónica de software. Configure los servicios con los parámetros adecuados para los usuarios y el tipo de máquina (como, por ejemplo, la actualización de las funciones).
- Aplicaciones de terceros que no va a virtualizar. Citrix recomienda virtualizar las aplicaciones. La virtualización reduce costes, ya que desaparece la necesidad de actualizar la imagen maestra después de agregar o volver a configurar una aplicación. Además, al tener menos aplicaciones instaladas, se reduce el tamaño de los discos duros de la imagen maestra, lo que ahorra costes de almacenamiento.
- Clientes App-V con la configuración recomendada, si se van a publicar aplicaciones de App-V. El cliente de App-V está disponible en Microsoft.
- Si utiliza Machine Creation Services y va a localizar Microsoft Windows, instale las configuraciones regionales y los paquetes de idioma. Durante el aprovisionamiento, cuando se crea una instantánea, las máquinas virtuales aprovisionadas usan las configuraciones regionales y los paquetes de idioma instalados.

**Importante:**

Si utiliza Citrix Provisioning o Machine Creation Services, no debe ejecutar Sysprep en imágenes maestras.

Para preparar una imagen maestra:

1. Mediante la herramienta de administración del hipervisor, cree una imagen maestra y, a continuación, instale el sistema operativo, además de todos los Service Pack y las actualizaciones. Especifique la cantidad de CPU virtuales. También puede especificar el valor de la CPU virtual si crea el catálogo de máquinas mediante PowerShell. No se puede especificar la cantidad de CPU virtuales si crea el catálogo con Studio. Configure la cantidad necesaria de espacio en disco duro para los escritorios y las aplicaciones. Ese valor no se puede cambiar más adelante o en el catálogo.
2. Compruebe que el disco duro está conectado a la ubicación de dispositivo 0. La mayoría de las plantillas de imagen maestra estándar configuran esta ubicación de manera predeterminada, pero es posible que no suceda lo mismo con algunas plantillas personalizadas.
3. Instale y configure el software anterior en la imagen maestra.
4. Si utiliza Citrix Provisioning, cree un archivo VHD para el disco virtual del dispositivo de destino maestro antes de unir el dispositivo de destino maestro a un dominio. Para obtener información detallada, consulte la documentación de Citrix Provisioning.
5. Si no utiliza Machine Creation Services, debe unir la imagen maestra al dominio al que pertenecen las aplicaciones y los escritorios. Compruebe que la imagen maestra está disponible en el host donde se crearán las máquinas. Si utiliza Machine Creation Services, no es necesario unir la imagen maestra a un dominio. Las máquinas aprovisionadas se unen al dominio especificado en el Asistente para la creación de catálogos.
6. Citrix recomienda que cree y dé nombre a una instantánea de la imagen maestra, para que se pueda identificar más tarde. Si especifica una imagen maestra en lugar de una instantánea al crear un catálogo de máquinas, Studio crea una instantánea, pero no se le podrá asignar ningún nombre.

## Crear un catálogo de máquinas mediante Studio

Antes de iniciar el asistente de creación de catálogos, revise esta sección.

Si utiliza una imagen maestra, compruebe que hay instalado un VDA en la imagen antes de crear el catálogo de máquinas.

Desde Studio:

- Si ya ha creado un sitio, pero aún no ha creado un catálogo de máquinas, Studio le guiará hacia el punto de partida idóneo para crear un catálogo de máquinas.
- Si ya ha creado un catálogo de máquinas y quiere crear otro, seleccione **Catálogos de máquinas** en el panel de navegación de **Studio**. A continuación, seleccione **Crear catálogo de máquinas** en el panel **Acciones**.

El asistente le guiará a través de los siguientes elementos. Las páginas del asistente varían según las opciones que escoja.

## Sistema operativo

Cada catálogo contiene máquinas de un solo tipo. Seleccione uno.

- **SO multisesión:** Un catálogo de SO multisesión proporciona escritorios compartidos alojados. Las máquinas pueden ejecutar versiones compatibles de sistemas operativos Windows o Linux, pero el catálogo no puede contener ambos a la vez. (Consulte la documentación de Linux Virtual Delivery Agent para obtener más información sobre ese sistema operativo.)
- **SO de sesión única:** Un catálogo de SO de sesión única ofrece escritorios VDI que se pueden asignar a varios usuarios diferentes.
- **Acceso con Remote PC:** Un catálogo de acceso con Remote PC ofrece a los usuarios acceso remoto a sus escritorios físicos de oficina. El acceso con Remote PC no requiere una VPN para proporcionar seguridad.

## Administración de máquinas

Esta página no aparece cuando se crean catálogos de acceso con Remote PC.

La página **Administración de máquinas** indica cómo se administran las máquinas y con qué herramienta se implementan.

Elija si la administración de energía de las máquinas del catálogo se llevará a cabo a través de Studio.

- Las opciones de energía de las máquinas se administran a través de Studio o se aprovisionan mediante un entorno de nube (por ejemplo, máquinas virtuales o equipos Blade). Esta opción solo está disponible si ya dispone de una conexión configurada a un hipervisor o servicio de nube.
- Las opciones de energía de las máquinas no se administran a través de Studio (por ejemplo, máquinas físicas).

Si ha indicado que las opciones de energía de las máquinas se administran a través de Studio o se aprovisionan mediante un entorno de nube, elija la herramienta que se va a utilizar para crear las máquinas virtuales.

- **Citrix Machine Creation Services (MCS):** Utiliza una imagen maestra para crear y administrar máquinas virtuales. Los catálogos de máquinas en entornos de nube usan MCS. MCS no está disponible para máquinas físicas.

- **Citrix Provisioning:** (antes Provisioning Services) Administra los dispositivos de destino como una colección de dispositivos. Un disco virtual de Citrix Provisioning creado a partir de un dispositivo de destino maestro entrega escritorios y aplicaciones.

**Nota:**

Esta opción ya no está disponible. Para importar un dispositivo de destino de Citrix Provisioning en un catálogo de Citrix Virtual Apps and Desktops, utilice el **asistente para exportar dispositivos de Citrix Provisioning**.

- **Otros:** Una herramienta que administra máquinas que ya se encuentran en el centro de datos. Citrix recomienda usar Microsoft System Center Configuration Manager u otra aplicación de terceros para una mayor uniformidad entre las máquinas del catálogo.

## Tipos de escritorio (experiencia de escritorio)

Esta página solo aparece cuando se crea un catálogo que contiene máquinas con SO de sesión única.

La página **Experiencia de escritorio** determina lo que ocurre cada vez que un usuario inicia sesión. Seleccione una de las siguientes opciones:

- Los usuarios se conectan a un escritorio nuevo (aleatorio) cada vez que inician sesión.
- Los usuarios se conectan al mismo escritorio (estático) cada vez que inician sesión.

Si elige la segunda opción y usa MCS para aprovisionar las máquinas, puede definir qué pasará con los cambios que los usuarios realicen en el escritorio:

- Guardar en un disco Personal vDisk aparte los cambios que los usuarios efectúen en el escritorio. (Personal vDisk ha sido [retirado](#).)
- Guardar en el disco local los cambios que los usuarios efectúen en el escritorio.
- Descartar los cambios del usuario y limpiar el escritorio virtual cuando el usuario cierre sesión. Seleccione esta opción si está utilizando la capa de personalización de usuarios.

## Imagen maestra

Esta página solo aparece cuando se utiliza Machine Creation Services para crear máquinas virtuales.

En la página **Imagen maestra**, seleccione la conexión al hipervisor de host o el servicio de nube y, a continuación, seleccione la instantánea o máquina virtual creada anteriormente. Si está creando el primer catálogo de máquinas, la única conexión disponible es la configurada al crear el sitio.

Recuerde:

- Cuando utilice MCS o Citrix Provisioning, no ejecute Sysprep en imágenes maestras.
- Si especifica una imagen maestra en lugar de una instantánea, Studio creará una instantánea, pero usted no le podrá asignar ningún nombre.

Para que pueda utilizar las funciones más recientes del producto, compruebe que la imagen maestra tiene instalada la versión más reciente de VDA. No cambie la selección predeterminada de VDA mínimo. No obstante, si debe usar una versión anterior de VDA, consulte Niveles funcionales y versiones de VDA.

Aparecerá un mensaje de error si selecciona una instantánea o máquina virtual que no sea compatible con la tecnología de administración de la máquina que haya seleccionado antes en el asistente.

## Entornos de servicios y plataformas de nube

Si utiliza un servicio o una plataforma de nube (como Azure Resource Manager, Nutanix o Amazon Web Services) para alojar máquinas virtuales, el asistente para la creación de catálogos de máquinas contiene páginas específicas para ese host.

Para obtener más información, consulte [Dónde encontrar información acerca de los tipos de conexión](#).

## Colección de dispositivos

Esta página solo aparece cuando se utiliza Citrix Provisioning para crear máquinas virtuales.

En la página **Colección de dispositivos**, se muestran los conjuntos de dispositivos y aquellos dispositivos que aún no se han agregado a los catálogos.

Seleccione las colecciones de dispositivos que va a usar.

## Máquinas

Esta página no aparece cuando se crean catálogos de acceso con Remote PC.

El título de esta página depende de lo seleccionado en la página **Administración de máquinas: Máquinas, Máquinas virtuales o Máquinas virtuales y usuarios**.

### Si utiliza MCS:

- Especifique la cantidad de máquinas virtuales que se van a crear.
- Seleccione la cantidad de memoria (en MB) que tendrá cada máquina virtual.
- Cada máquina virtual creada tendrá un disco duro. El tamaño de este se configura en la imagen maestra. No se puede cambiar el tamaño del disco duro en el catálogo.

- Si indicó en la página **Experiencia de escritorio** que los cambios que los usuarios efectúen en los escritorios estáticos se guardan en un disco Personal vDisk aparte, especifique el tamaño del disco virtual en GB y la letra de su unidad.
- Si la implementación contiene más de una zona, puede seleccionar una zona para el catálogo.
- Si quiere crear máquinas virtuales de escritorio estático, seleccione un modo de copia para la máquina virtual. Consulte Modo de copia para la máquina virtual.
- Si quiere crear máquinas virtuales de escritorio aleatorio que no usan discos Personal vDisk, puede configurar una memoria caché que se va a usar para los datos temporales de cada máquina. Consulte Configurar la caché de datos temporales.

### **Al usar Citrix Provisioning:**

La página **Dispositivos** ofrece una lista de las máquinas que hay en la colección de dispositivos que haya seleccionado en la página anterior. No se puede agregar ni quitar máquinas en esta página.

### **Si utiliza otras herramientas:**

Agregue o importe una lista de los nombres de cuentas de máquina de Active Directory. Puede cambiar el nombre de la cuenta de Active Directory que tenga una máquina virtual después de agregarla o importarla. Si indicó máquinas estáticas en la página **Experiencia de escritorio**, puede especificar el nombre de usuario de Active Directory para cada máquina virtual que agregue.

Después de agregar o importar los nombres, puede hacer clic en el botón **Quitar** para eliminar nombres de la lista, sin salir de esta página.

### **Si utiliza Citrix Provisioning u otras herramientas (pero no MCS):**

Un icono y un cuadro de información emergente acerca de cada máquina agregada (o importada o proveniente de una colección de dispositivos de Citrix Provisioning) pueden ayudarle a identificar aquellas máquinas que no sean aptas para agregarse al catálogo o no puedan registrarse en un Delivery Controller. Para obtener más información, consulte Niveles funcionales y versiones de VDA.

### **Modo de copia para la máquina virtual**

El modo de copia que especifique en la página **Máquinas** determina si MCS crea clones ligeros (copia rápida) o pesados (copia completa) a partir de la imagen maestra. (La opción predeterminada es clones ligeros.)

- Puede optar por los clones de copia rápida para un uso más eficiente del almacenamiento y una creación de máquinas más rápida.
- En cambio, puede utilizar los clones de copia completa para mejorar la recuperación de datos y la asistencia a la migración de datos, con IOPS potencialmente reducidas una vez creadas las máquinas.

## Niveles funcionales y versiones de VDA

Con el nivel funcional de un catálogo, decide qué funciones de producto están disponibles para las máquinas del catálogo. Para poder usar las funciones introducidas en las nuevas versiones de producto, se necesita un nuevo VDA. Establecer un nivel funcional permite que todas las funcionalidades introducidas en esa versión (y versiones posteriores, si el nivel funcional no cambia) estén disponibles para las máquinas del catálogo. Sin embargo, las máquinas de ese catálogo que tengan una versión anterior de VDA no podrán registrarse.

Un menú situado cerca de la parte inferior de la página **Máquinas** (o **Dispositivos**) le permite seleccionar el nivel mínimo de VDA. Esto establece el nivel funcional mínimo del catálogo. De forma predeterminada, el nivel funcional de versión más reciente se selecciona para implementaciones locales. Si sigue la recomendación de Citrix de siempre instalar y actualizar los VDA y los componentes principales a la versión más reciente, no es necesario cambiar esta selección. Sin embargo, si debe seguir usando versiones anteriores de VDA, seleccione el valor correcto.

Una versión de Citrix Virtual Apps and Desktops puede no incluir una nueva versión de VDA, o el nuevo VDA puede no afectar al nivel funcional. En estos casos, el nivel funcional puede indicar una versión de VDA anterior a la versión de los componentes instalados o actualizados. Por ejemplo: aunque la versión 7.17 contiene un VDA 7.17, el nivel funcional predeterminado (“7.9 y versiones posteriores”) sigue siendo el más actual. Por lo tanto, después de instalar o actualizar los componentes desde 7.9-7.16 a 7.17, no es necesario cambiar el nivel funcional predeterminado.

En las implementaciones de Citrix Cloud, Studio usa un nivel funcional predeterminado que puede ser anterior a la versión más reciente.

El nivel funcional seleccionado determina la lista anterior de máquinas. En la lista, un cuadro de información situado junto a cada entrada indica si el VDA de la máquina es compatible con el catálogo en ese nivel funcional.

Aparecen mensajes en la página si el VDA de las máquinas no cumple o excede el nivel funcional mínimo seleccionado. Puede continuar con el asistente. Seguramente las máquinas no podrán registrarse en un Controller. De forma alternativa, puede:

- Quitar de la lista las máquinas que contengan agentes VDA antiguos, actualizar sus VDA y, a continuación, agregarlas de nuevo al catálogo.
- Elija un nivel funcional más bajo que impida el acceso a las funciones más recientes del producto.

También aparece un mensaje si una máquina no puede agregarse al catálogo porque no sea el tipo de máquina adecuado. Por ejemplo: si intenta agregar un servidor a un catálogo de SO de sesión única, o bien, si intenta agregar una máquina de SO de sesión única creada en su momento para la asignación aleatoria a un catálogo de máquinas estáticas.

**Importante:**

Para la versión 1811, se ha agregado un nivel funcional adicional: **1811 (o posterior)**. Ese nivel está pensado para las funciones futuras de Citrix Virtual Apps and Desktops. La selección **7.9 (o posterior)** sigue siendo la predeterminada. Ese valor predeterminado ahora es válido para todas las implementaciones.

Si selecciona **1811 (o posterior)**, ningún VDA de versión anterior en ese catálogo podrá registrarse en ningún Controller o Cloud Connector. Sin embargo, si el catálogo solo contiene VDA 1811 o versiones posteriores admitidas, todos podrán registrarse.

### Configurar la caché de datos temporales

El almacenamiento en caché de datos temporales localmente en la VM es optativo. Puede habilitar el uso de la memoria caché de datos temporal en la máquina cuando se usa MCS para administrar máquinas agrupadas (no dedicadas) en un catálogo. Si el catálogo utiliza una conexión que especifica un espacio de almacenamiento para datos temporales, puede habilitar y configurar la información de caché de datos temporales al crear el catálogo.

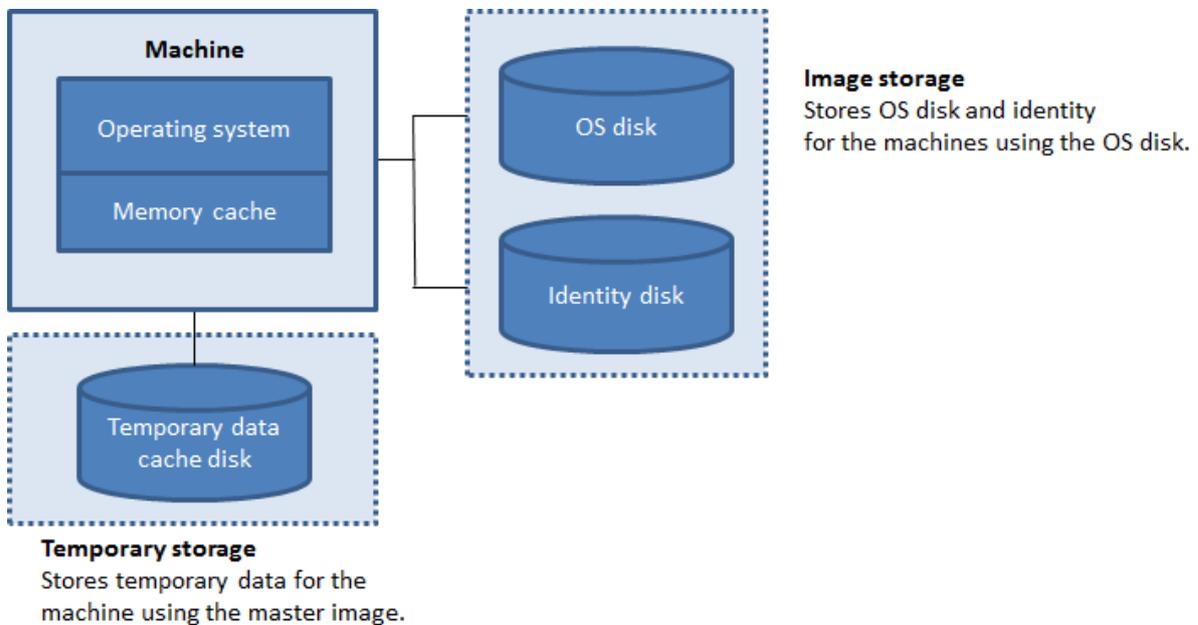
**Importante:**

Esta función requiere un controlador actualizado de E/S de MCS. La instalación de este controlador es una opción cuando instala o actualiza un VDA. De forma predeterminada, ese controlador no se instala.

Puede especificar si los datos temporales utilizarán un almacenamiento local o compartido cuando cree la conexión que utilizará el catálogo. Para obtener más información, consulte [Conexiones y recursos](#). Para configurar una memoria caché para datos temporales en cada máquina, puede utilizar las dos opciones siguientes: **Memoria asignada para caché (MB)** y **Tamaño de caché de disco (GB)**. De forma predeterminada, ninguna de las dos opciones está seleccionada. Para habilitar la opción Memoria asignada para caché (MB), marque la casilla de verificación Tamaño de caché de disco (GB). Si la casilla **Tamaño de caché de disco** no está marcada, la opción Memoria asignada a la caché aparecerá atenuada. En función del tipo de conexión, los valores predeterminados de estas opciones pueden diferir. Generalmente, los valores predeterminados son suficientes para la mayoría de los casos. Sin embargo, tenga en cuenta el espacio necesario para:

- Archivos de datos temporales creados por Windows, incluido el archivo de paginación de Windows.
- Datos de perfil de usuario.
- Datos de ShareFile que se sincronizan en las sesiones de usuario.
- Datos que pueden crear o copiar los usuarios de las sesiones, o aplicaciones que los usuarios pueden instalar dentro de la sesión.

Windows no permitirá que una sesión use una cantidad de caché de disco que sea mayor que la cantidad de espacio libre en la imagen maestra original desde la cual se aprovisionaron las máquinas de catálogo. Por ejemplo, no se consigue ningún beneficio especificando una caché de disco de 20 GB si solo hay 10 GB de espacio disponible en la imagen maestra.



Para configurar una memoria caché para datos temporales en cada máquina, tenga en cuenta los tres escenarios siguientes:

- Si no marca las casillas “Tamaño de caché de disco” y “Memoria asignada para caché”, los datos temporales no se almacenan en la memoria caché. Se escriben directamente en el disco de diferenciación (ubicado en el almacenamiento de SO) de cada VM (esta es la acción de aprovisionamiento en la versión 7.8 y en las anteriores).
- Si marca la casilla “Tamaño de caché de disco” y deja sin marcar la casilla “Memoria asignada para caché”, los datos temporales se escriben directamente en la memoria caché de disco y emplean una cantidad mínima de la memoria caché.
- Si marca las casillas “Tamaño de caché de disco” y “Memoria asignada para caché”, los datos temporales se escriben inicialmente en la memoria caché. Cuando la memoria caché alcanza su límite configurado (el valor de Memoria asignada para caché), los datos más antiguos se transfieren al disco de caché de datos temporales.

#### Importante:

- Si la memoria caché de disco se queda sin espacio, la sesión del usuario se vuelve inutilizable.
- No habilite el almacenamiento en caché si va a usar este catálogo para crear AppDisks.
- Esta función no está disponible cuando se usa una conexión de host Nutanix.

- No puede cambiar los valores de caché de un catálogo de máquinas después de haber creado la máquina.

**Nota:**

- La memoria caché es parte de la memoria total de cada máquina. Por lo tanto, si habilita la opción “Memoria asignada para caché”, considere la opción de aumentar la memoria total de cada máquina.
- Cambiar el valor predeterminado del tamaño de la caché del disco puede afectar al rendimiento. El tamaño debe coincidir con los requisitos de los usuarios y la carga que se coloca en la máquina.

## Tarjetas de interfaz de red (NIC)

Esta página no aparece cuando se crean catálogos de acceso con Remote PC.

En la página **Tarjetas de interfaz de red**, si quiere utilizar varias tarjetas NIC, asocie una red virtual a cada tarjeta. Por ejemplo, puede asignar una tarjeta para el acceso a una red segura concreta y otra para el acceso a una red más habitual. También puede agregar o quitar tarjetas NIC desde esta página.

## Cuentas de máquina

Esta página solo aparece cuando se crean catálogos de acceso con Remote PC.

En la página **Cuentas de máquina**, especifique las cuentas de máquina de Active Directory o unidades organizativas (OU) para agregarlas a usuarios o grupos de usuarios. No use barras diagonales (/) en el nombre de una unidad organizativa.

Puede elegir una conexión de administración de energía que haya configurado previamente o puede optar por no usar la administración de energía. Si quiere usar la administración de energía, pero aún no se ha configurado la conexión correspondiente, puede crear dicha conexión más tarde y posteriormente modificar el catálogo de máquinas para actualizar la configuración de la administración de energía.

## Cuentas de equipo

Esta página solo aparece cuando se utiliza Machine Creation Services para crear máquinas virtuales.

Cada máquina del catálogo debe tener una cuenta de equipo de Active Directory correspondiente. En la página **Cuentas de equipo**, indique si se van a crear cuentas o si se van a utilizar cuentas existentes, además de la ubicación de estas.

- Si crea cuentas, debe tener permiso para crear cuentas de equipo en la unidad organizativa donde residen las máquinas.

Especifique el esquema de nombres de cuenta para las máquinas que se van a crear con marcas hash para indicar dónde aparecerán los números o las letras secuenciales. No use barras diagonales (/) en el nombre de una unidad organizativa. Un nombre no puede empezar con un número. Por ejemplo, un esquema de denominación PC-Ventas-## (con números del 0 al 9 seleccionados) da como resultado cuentas de equipo llamadas PC-Ventas-01, PC-Ventas-02, PC-Ventas-03, etc.

- Si usa cuentas existentes, vaya a esas cuentas o haga clic en **Importar** y especifique un archivo CSV que contenga los nombres de cuenta. El contenido del archivo importado debe tener el formato:

```
1 [ADComputerAccount]
2 ADcomputeraccountname.domain
3 ...
4 <!--NeedCopy-->
```

Compruebe que hay cuentas suficientes para las máquinas que está agregando. Como Studio es el responsable de administrar estas cuentas, permita que Studio restablezca las contraseñas de todas las cuentas, o bien especifique la contraseña de la cuenta (que debe ser la misma para todas las cuentas).

Para catálogos que contienen máquinas físicas o máquinas existentes, seleccione o importe las cuentas existentes y asigne cada máquina a una cuenta de equipo de Active Directory y a una cuenta de usuario.

Para máquinas creadas con Citrix Provisioning, las cuentas de equipo de los dispositivos de destino se administran de forma diferente. Para obtener más información al respecto, consulte la documentación de Citrix Provisioning.

## Resumen, nombre y descripción

En la página **Resumen**, revise la configuración especificada. Introduzca un nombre y una descripción para el catálogo. Esta información se mostrará en Studio.

Cuando termine, haga clic en **Finalizar** para iniciar la creación del catálogo.

## Solución de problemas

### Importante:

Después de crear el catálogo de máquinas con Citrix Studio, ya no puede utilizar el comando

`Get-ProvTask` de PowerShell para obtener las tareas asociadas a la creación de catálogos de máquinas. Esta restricción se debe al hecho de que Studio elimina esas tareas después de la creación del catálogo de máquinas, independientemente de si el catálogo se ha creado correctamente.

Citrix recomienda recopilar registros para ayudar al equipo de asistencia a ofrecer soluciones. Si utiliza Citrix Provisioning, siga el procedimiento de esta sección para generar archivos de registros:

1. En la imagen maestra, cree la siguiente clave de Registro con el valor 1 (como un valor DWORD de 32 bits): `HKLM\Software\Citrix\MachineIdentityServiceAgent\LOGGING`.
2. Apague la imagen maestra y cree una instantánea.
3. Ejecute el siguiente comando de PowerShell en el Delivery Controller: `Set-ProvServiceConfiguration -Name ImageManagementPrep_NoAutoShutdown -Value $True`.
4. Cree un catálogo basado en esa instantánea.
5. Cuando se cree la VM de preparación en el hipervisor, inicie sesión y extraiga los archivos `Image-prep.log` y `PvsVmAgentLog.txt` desde la raíz `C:\`.
6. Apague la máquina; en ese momento la máquina informará del fallo.
7. Ejecute el siguiente comando de PowerShell para volver a habilitar el apagado automático de las máquinas de preparación de imágenes: `Remove-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown`.

## Qué hacer a continuación

Si este es el primer catálogo creado, Studio le guiará para [crear un grupo de entrega](#).

## Administrar catálogos de máquinas

May 5, 2023

### Introducción

Puede agregar o quitar máquinas de un catálogo de máquinas; también puede cambiarlo de nombre, modificar su descripción o administrar sus cuentas de equipo de Active Directory.

Asimismo, el mantenimiento de catálogos puede incluir la comprobación de que cada máquina tenga los últimos cambios de configuración y las actualizaciones más recientes del sistema operativo o del software antivirus.

- Los catálogos que contienen máquinas agrupadas aleatorias que se han creado con Machine Creation Services (MCS) pueden mantener las máquinas mediante la actualización de la imagen maestra utilizada en el catálogo y, luego, de las máquinas en sí. Este método permite actualizar de forma eficiente una gran cantidad de máquinas de usuario.
- Para máquinas creadas con Citrix Provisioning, las actualizaciones a las máquinas se propagan mediante discos virtuales. Para obtener información detallada, consulte la documentación de Citrix Provisioning.
- Para catálogos que contengan máquinas estáticas asignadas permanentemente y para catálogos de máquinas de acceso con Remote PC, se administran las actualizaciones de las máquinas de los usuarios fuera de Studio. Puede realizar esta tarea de forma individual o colectiva mediante herramientas de distribución de software de terceros.

Para obtener información sobre la creación y la administración de conexiones con hosts de hipervisores y servicios de nube, consulte [Conexiones y recursos](#).

**Nota:**

MCS no es compatible con Windows 10 IoT Core ni Windows 10 IoT Enterprise. Consulte el [sitio de Microsoft](#) para obtener más información.

### **Acerca de las instancias persistentes**

Al actualizar un catálogo MCS creado con instancias persistentes o dedicadas, cualquier máquina nueva creada para el catálogo utiliza la imagen actualizada. Las instancias preexistentes continúan mediante la instancia original. El proceso de actualización de una imagen se realiza de la misma manera que cuando se trata de cualquier otro tipo de catálogo. Se deben tener en cuenta las siguientes cuestiones:

- Con catálogos de discos persistentes, las máquinas preexistentes no se actualizan a la nueva imagen. Sin embargo, todas las máquinas nuevas que se agreguen al catálogo utilizan la nueva imagen.
- Para catálogos de discos no persistentes, la imagen de la máquina se actualiza la próxima vez que se restablezca la máquina.
- Con catálogos de máquinas persistentes, actualizar la imagen también implica actualizar las instancias de catálogo que la utilizan.
- En el caso de catálogos no persistentes, si quiere utilizar imágenes diferentes para máquinas diferentes, las imágenes deben residir en catálogos separados.

### **Agregar máquinas a un catálogo**

Antes de comenzar:

- Compruebe que el host de virtualización (hipervisor o proveedor de servicios en la nube) contenga procesadores, memoria y capacidad de almacenamiento suficientes para dar cabida a las máquinas adicionales.
- Compruebe que tiene suficientes cuentas de equipo de Active Directory sin usar. Si utiliza cuentas existentes, tenga en cuenta que la cantidad de máquinas que puede agregar se limita a la cantidad de cuentas disponibles.
- Si usa Studio con el fin de crear cuentas de equipo de Active Directory para las máquinas adicionales, debe tener los permisos de administrador de dominio apropiados.

Para agregar máquinas a un catálogo:

1. Seleccione **Catálogos de máquinas** en el panel de navegación de **Studio**.
2. Seleccione un catálogo de máquinas y, a continuación, seleccione **Agregar máquinas** en el panel **Acciones**.
3. Seleccione la cantidad de máquinas virtuales que se van a agregar.
4. Si no hay suficientes cuentas existentes de Active Directory para la cantidad de máquinas virtuales que quiere agregar, seleccione el dominio y la ubicación donde se crearán las cuentas. Especifique un esquema de nombres de cuenta con marcas hash para indicar dónde aparecerán los números o las letras secuenciales. No use barras diagonales (/) en el nombre de una unidad organizativa. Un nombre no puede empezar con un número. Por ejemplo: un esquema de nombres de PC-Ventas-## (con números del 0 al 9 seleccionados) tiene como resultado cuentas de equipo llamadas PC-Ventas-01, PC-Ventas-02, PC-Ventas-03, etc.
5. Si usa cuentas existentes de Active Directory, vaya a esas cuentas o haga clic en **Importar** y especifique un archivo CSV que contenga los nombres de cuenta. Compruebe que hay cuentas suficientes para las máquinas que está agregando. Studio es el responsable de administrar estas cuentas. Por eso, permita que Studio restablezca las contraseñas de todas las cuentas, o bien, especifique la contraseña de la cuenta (que debe ser la misma para todas las cuentas).

Las máquinas se crean en un proceso en segundo plano, que puede tardar mucho tiempo si se crea una gran cantidad de máquinas. La creación de máquinas continúa, aunque se cierre Studio.

## Eliminar máquinas de un catálogo

Después de eliminar una máquina de un catálogo, los usuarios ya no podrán acceder a ella. Por eso, antes de eliminar una máquina, compruebe que:

- Existe una copia de seguridad de los datos del usuario, si fueran útiles.
- Todos los usuarios han cerrado la sesión. La activación del modo de mantenimiento impide nuevas conexiones a una máquina.
- Las máquinas se apagan.

Para eliminar máquinas de un catálogo:

1. Seleccione **Catálogos de máquinas** en el panel de navegación de **Studio**.
2. Seleccione un catálogo y, a continuación, seleccione **Ver máquinas** en el panel **Acciones**.
3. Seleccione una o varias máquinas y, a continuación, seleccione **Eliminar** en el panel **Acciones**.

Elija si se eliminarán las máquinas que se van a quitar. Si opta por eliminar máquinas, indique si las cuentas de Active Directory de esas máquinas deben conservarse, inhabilitarse o eliminarse.

Cuando se elimina un catálogo de máquinas de Azure Resource Manager, las máquinas y los grupos de recursos asociados se eliminan de Azure, incluso aunque indique que deben conservarse.

### **Cambiar la descripción de un catálogo o cambiar la configuración de acceso con Remote PC**

1. Seleccione **Catálogos de máquinas** en el panel de navegación de **Studio**.
2. Seleccione un catálogo y, a continuación, seleccione **Modificar catálogo de máquinas** en el panel **Acciones**.
3. (Solo para catálogos de acceso con Remote PC) En la página **Administración de energía**, puede cambiar la configuración de administración de energía y seleccionar una conexión de administración de energía. En la página **Unidades organizativas**, agregue o quite unidades organizativas de Active Directory.
4. En la página **Descripción**, cambie la descripción del catálogo.

### **Cambiar el nombre de un catálogo**

1. Seleccione **Catálogos de máquinas** en el panel de navegación de **Studio**.
2. Seleccione un catálogo y, a continuación, seleccione **Cambiar nombre de catálogo de máquinas** en el panel **Acciones**.
3. Introduzca el nuevo nombre.

### **Mover un catálogo a otra zona**

Si la implementación tiene más de una zona, puede mover un catálogo de una zona a otra.

Tenga en cuenta que mover un catálogo a otra zona que el hipervisor o el servicio de nube que contiene las máquinas virtuales de ese catálogo puede afectar el rendimiento.

1. Seleccione **Catálogos de máquinas** en el panel de navegación de **Studio**.
2. Seleccione un catálogo y, a continuación, seleccione **Mover** en el panel **Acciones**.
3. Seleccione la zona a la que quiere mover el catálogo.

## Eliminar un catálogo

Antes de eliminar un catálogo, asegúrese de que:

- Todos los usuarios han cerrado sesión y no hay sesiones desconectadas en ejecución.
- El modo de mantenimiento se activa para todas las máquinas del catálogo, de modo que no se pueden establecer conexiones nuevas.
- Todas las máquinas del catálogo se apagan.
- El catálogo no está asociado a ningún grupo de entrega. Es decir, que el grupo de entrega no contiene máquinas procedentes del catálogo.

Para eliminar un catálogo:

1. Seleccione **Catálogos de máquinas** en el panel de navegación de **Studio**.
2. Seleccione un catálogo y, a continuación, seleccione **Eliminar catálogo de máquinas** en el panel **Acciones**.
3. Indique si las máquinas del catálogo deberían eliminarse. Si opta por eliminar máquinas, indique si las cuentas de equipo de Active Directory de esas máquinas deben conservarse, inhabilitarse o eliminarse.

## Administrar cuentas de equipo de Active Directory en un catálogo

Para administrar cuentas de Active Directory en un catálogo de máquinas, puede:

- Liberar cuentas de máquina sin utilizar eliminando cuentas de equipo de Active Directory que haya en catálogos de máquinas de SO de sesión única y SO multisesión. Estas cuentas se pueden usar para otras máquinas.
- Agregar cuentas de modo que, cuando se agreguen más máquinas al catálogo, las cuentas de equipo ya estén listas. No use barras diagonales (/) en el nombre de una unidad organizativa.

Para administrar cuentas de Active Directory:

1. Seleccione **Catálogos de máquinas** en el panel de navegación de **Studio**.
2. Seleccione un catálogo y, a continuación, seleccione **Administrar cuentas de AD** en el panel **Acciones**.
3. Elija si quiere agregar o eliminar las cuentas de equipo. Si agrega cuentas, deberá especificar qué hacer con las contraseñas de cuenta: restablecerlas todas o escribir una contraseña para todas ellas.

Puede restablecer contraseñas si no conoce las contraseñas de cuenta actuales. Debe tener permisos específicos para realizar el restablecimiento de contraseñas. Si introduce una contraseña, se cambiará la contraseña en las cuentas a medida que se importan. Si elimina una cuenta, se le solicitará que elija si la cuenta de Active Directory debe mantenerse, inhabilitarse o eliminarse.

También puede indicar si las cuentas de Active Directory se deberían conservar, inhabilitar o eliminar cuando quite máquinas de un catálogo o elimine un catálogo.

## **Actualizar un catálogo**

Citrix recomienda guardar copias o instantáneas de las imágenes maestras antes de actualizar las máquinas de un catálogo. La base de datos conserva un registro histórico de las imágenes maestras utilizadas con cada catálogo de máquinas. Reverta las máquinas de un catálogo para utilizar la versión anterior de la imagen maestra. Realice esta tarea si los usuarios tienen problemas con las actualizaciones implementadas en sus escritorios para, así, minimizar el tiempo de inactividad de los usuarios. No elimine, mueva o cambie el nombre de las imágenes maestras. Si lo hace, no podrá usarlas para revertir las máquinas de un catálogo.

En caso de catálogos de máquinas que utilizan Citrix Provisioning (antes Provisioning Services), debe publicar un disco virtual nuevo para aplicar los cambios al catálogo. Para obtener información más detallada, consulte la documentación de Citrix Provisioning.

Una vez actualizada la máquina, se reinicia automáticamente.

## **Actualizar o crear una imagen maestra**

Antes de actualizar un catálogo de máquinas, actualice la imagen maestra existente o cree una en el hipervisor de host.

1. En el hipervisor o proveedor del servicio de nube, tome una instantánea de la VM actual y dele un nombre significativo. Esta instantánea se puede usar para revertir (deshacer) los cambios en las máquinas del catálogo, si fuera necesario.
2. Si es necesario, encienda la máquina virtual de la imagen maestra e inicie sesión.
3. Instale las actualizaciones o realice los cambios necesarios en la imagen maestra.
4. Si la imagen maestra usa un disco Personal vDisk, actualice el inventario.
5. Apague la máquina virtual.
6. Tome una instantánea de la VM y dele un nombre significativo fácilmente reconocible cuando el catálogo se actualice en Studio. Aunque Studio puede crear una instantánea, Citrix recomienda crear la instantánea desde la consola de administración del hipervisor y, a continuación, seleccionarla en Studio. Este método le permite asignar un nombre y una descripción significativos para la instantánea, en lugar de recibir un nombre generado automáticamente. Para imágenes maestras de GPU, puede cambiar la imagen maestra solo a través de la consola de Citrix Hypervisor.

## Actualizar el catálogo

Para preparar y aplicar la actualización a todas las máquinas de un catálogo:

1. Seleccione **Catálogos de máquinas** en el panel de navegación de **Studio**.
2. Seleccione un catálogo y, a continuación, seleccione **Actualizar máquinas** en el panel **Acciones**.
3. En la página **Imagen maestra**, seleccione el host y la imagen que quiere implantar.
4. En la página **Estrategia de implantación**, elija cuándo se actualizan las máquinas del catálogo con la nueva imagen maestra (en el siguiente apagado o inmediatamente).
5. En la página **Resumen**, revise la información y haga clic en **Finalizar**. Cada máquina se reiniciará automáticamente después de actualizarse.

Si está actualizando un catálogo directamente mediante el SDK de PowerShell, en lugar de Studio, puede especificar una plantilla de hipervisor (VMTemplates), como alternativa a una imagen o una instantánea de la imagen.

### Estrategia de implantación:

La actualización de la imagen la próxima vez que se apague la máquina afectará inmediatamente a las máquinas que no estén en uso en ese momento, es decir, a las máquinas que no tengan una sesión de usuario activa. Un sistema que está en uso recibe la actualización cuando finaliza la sesión activa actual. Se deben tener en cuenta las siguientes cuestiones:

- Las sesiones nuevas no se pueden iniciar hasta que la actualización se haya completado en las máquinas correspondientes.
- Las máquinas con sistema operativo de escritorio se actualizan inmediatamente, si no están en uso o los usuarios no han iniciado sesión en ellas.
- Para un sistema operativo de servidor con máquinas secundarias, los reinicios no se producen automáticamente. Deben apagarse y reiniciarse manualmente.

#### *Sugerencia:*

Limite la cantidad de máquinas que se reinician mediante la configuración avanzada de una conexión de host. Utilice esta configuración para modificar las acciones realizadas para un catálogo determinado; la configuración avanzada varía en función del hipervisor.

Si quiere actualizar la imagen de inmediato, configure una hora concreta para la distribución y las notificaciones pertinentes.

- **Hora de distribución:** Puede optar por actualizar todas las máquinas al mismo tiempo o especificar el período total de tiempo durante el que se debe comenzar a actualizar todas las máquinas que contiene el catálogo. Un algoritmo interno determina cuándo se actualiza y se reinicia cada máquina durante ese intervalo.

- **Notificación:** En la lista desplegable “Notificación”, situada a la izquierda, elija si mostrar un mensaje de notificación en las máquinas antes de empezar una actualización. De forma predeterminada, no se muestra ningún mensaje. Si elige mostrar un mensaje 15 minutos antes de empezar una actualización, también puede decidir (en la lista desplegable de la derecha) si repetir el mensaje cada cinco minutos después del primer mensaje. De forma predeterminada, el mensaje no se repite. A menos que elija actualizar todas las máquinas a la vez, el mensaje de notificación se mostrará en cada máquina en el momento correspondiente antes de que empiece la actualización, calculada por un algoritmo interno.

### Revertir una actualización

Después de aplicar una imagen maestra nueva o actualizada, puede revertirla. Puede ser necesario si surgen problemas con las máquinas recién actualizadas. Cuando revierte una actualización, las máquinas del catálogo vuelven a la última imagen funcional. Las nuevas funciones que requieran la nueva imagen ya no estarán disponibles. Al igual que en la implantación, la reversión de una máquina implica un reinicio.

1. Seleccione **Catálogos de máquinas** en el panel de navegación de **Studio**.
2. Seleccione el catálogo de máquinas y, a continuación, seleccione **Revertir actualización de máquinas** en el panel **Acciones**.
3. Puede especificar cuándo se aplicará la versión anterior de la imagen maestra a las máquinas de la manera que se describe más arriba, en la operación de implantación.

La reversión solo se aplica a máquinas que deben revertirse. En caso de máquinas que no se hayan actualizado con la imagen maestra nueva o actualizada (por ejemplo, máquinas con usuarios que no han cerrado sesión), los usuarios no reciben mensajes de notificación y no se ven obligados a cerrar sesión.

### Actualizar la versión de un catálogo o revertir una actualización

Actualice el catálogo de máquinas después de actualizar los VDA de las máquinas a una versión más reciente. Citrix recomienda actualizar todos los VDA a la versión más reciente para permitir el acceso a todas las funciones nuevas.

Antes de actualizar un catálogo de máquinas:

- Si utiliza Citrix Provisioning, debe actualizar la versión del VDA. La consola de Provisioning no conserva la versión del VDA. Citrix Provisioning se comunica directamente con el asistente para la instalación de Citrix Virtual Apps and Desktops para establecer la versión del VDA en el catálogo creado.

- Inicie las máquinas actualizadas para que se registren con el Controller. Esto permite a Studio determinar si las máquinas del catálogo necesitan actualización.

Para actualizar un catálogo de máquinas:

1. Seleccione **Catálogos de máquinas** en el panel de navegación de **Studio**.
2. Seleccione el catálogo. En la ficha **Detalles** del panel inferior, se muestra la información de versión.
3. Seleccione **Actualizar catálogo**. Si Studio detecta que el catálogo necesita actualización, se le informará mediante un mensaje. Siga las indicaciones. Si una o varias máquinas no se pueden actualizar, aparecerá un mensaje en el que se le explicará el motivo. Citrix recomienda resolver los problemas de máquinas antes de actualizar el catálogo para que todas las máquinas funcionen correctamente.

Después de completar la actualización del catálogo, puede revertir las máquinas a sus versiones anteriores de VDA. Para ello, seleccione el catálogo y, a continuación, seleccione **Deshacer** en el panel **Acciones**.

## Solución de problemas

- Para máquinas que presentan un “Estado de energía desconocido”, consulte [CTX131267](#) para obtener instrucciones.
- Para reparar máquinas virtuales que muestran continuamente un estado de energía desconocido, consulte [How to fix VMs that continuously show an unknown power state](#).

## Crear grupos de entrega

September 22, 2021

Un grupo de entrega es un conjunto de máquinas seleccionadas de uno o varios catálogos de máquinas. El grupo de entrega especifica los usuarios que pueden usar esas máquinas y las aplicaciones y/o escritorios disponibles para esos usuarios.

Crear un grupo de entrega es el siguiente paso de la configuración de la implementación después de crear un sitio y de crear un catálogo de máquinas. Posteriormente, puede cambiar los parámetros iniciales del primer grupo de entrega y crear otros. Sin embargo, existen funciones y configuraciones que se pueden definir solo cuando se modifica un grupo de entrega, no cuando se crea.

Para el acceso con Remote PC, cuando se crea un sitio, se crea automáticamente un grupo de entrega llamado “Escritorios de acceso con Remote PC”.

Para crear un grupo de entrega:

1. Si ya ha creado un sitio y un catálogo de máquinas, pero aún no ha creado ningún grupo de entrega, Studio le dirige al punto de partida para crear uno. En cambio, si ya ha creado un grupo de entrega y quiere crear otro, seleccione **Grupos de entrega** en el panel de navegación de Studio y, a continuación, seleccione **Crear grupo de entrega** en el panel Acciones.
2. El asistente Crear grupo de entrega se inicia con la página **Introducción**, que se puede eliminar de futuros inicios de este asistente.
3. El asistente le guiará a través de las páginas que se describen a continuación. Cuando haya terminado en cada página, haga clic en **Siguiente** para llegar a la página final.

## Paso 1. Máquinas

En la página **Máquinas**, seleccione un catálogo y especifique la cantidad de máquinas que quiere usar de ese catálogo.

Información útil:

- Al menos una máquina debe permanecer sin uso en el catálogo de máquinas seleccionado.
- Se puede especificar el mismo catálogo de máquinas en más de un grupo de entrega; sin embargo, una máquina solo se puede usar en un grupo de entrega.
- Un grupo de entrega puede usar más de un catálogo de máquinas. Sin embargo, esos catálogos deben contener los mismos tipos de máquina (SO de servidor, SO de escritorio o acceso con Remote PC). En otras palabras, no se pueden mezclar tipos de máquinas en un grupo de entrega. Del mismo modo, si la implementación contiene catálogos de máquinas Windows y Linux, un grupo de entrega puede contener máquinas de un tipo de sistema operativo, pero no ambos.
- Citrix recomienda instalar o actualizar todas las máquinas a la versión más reciente de VDA y, a continuación, actualizar los catálogos de máquinas y grupos de entrega según sea necesario. Al crear un grupo de entrega, si selecciona máquinas que tienen instaladas versiones diferentes de VDA, el grupo de entrega será compatible con la versión más antigua de VDA (Esto es el *nivel funcional* del grupo.) Por ejemplo, si una de las máquinas que seleccione tiene instalada la versión 7.1 de VDA y otras máquinas tienen la versión actual, todas las máquinas del grupo podrán usar únicamente las funciones que se admitían en la versión 7.1 de VDA. Esto significa que algunas funciones que requieran de versiones posteriores de VDA podrían no estar disponibles en ese grupo de entrega. Por ejemplo, para usar la funcionalidad AppDisks, los agentes VDA (y, por tanto, el nivel funcional del grupo) debe ser una versión mínima de 7.8.
- Todas las máquinas de un catálogo de acceso con Remote PC se asocian automáticamente a un grupo de entrega. Por eso, al crear un sitio de acceso con Remote PC, se crea automáticamente un catálogo denominado “Máquinas de acceso con Remote PC” y un grupo de entrega llamado “Escritorios de acceso con Remote PC”.
- Se realizan estas comprobaciones de compatibilidad:

- MinimumFunctionalLevel debe ser compatible
- SessionSupport debe ser compatible
- AllocationType debe ser compatible con SingleSession
- ProvisioningType' debe ser compatible
- PersistChanges debe ser compatible con MCS y Citrix Provisioning
- El catálogo RemotePC solo es compatible con el catálogo RemotePC
- Comprobación relacionada con AppDisk

## Paso 2. Tipo de entrega

Esta página solo aparece si ha seleccionado un catálogo que contiene máquinas estáticas (asignadas) de SO de escritorio.

Elija **Aplicaciones** o **Escritorios** en la página **Tipo de entrega**. No se puede habilitar ambas opciones.

Si ha seleccionado máquinas de un catálogo de máquinas aleatorias (agrupadas) de SO de servidor o SO de escritorio, se entiende que el tipo de entrega serán aplicaciones y escritorios, por lo que podrá entregar aplicaciones, escritorios o ambos.

## Paso 3. AppDisks

AppDisks ha sido [retirado](#).

Para agregar un AppDisk, haga clic en **Agregar**. En el cuadro de diálogo Seleccionar AppDisks, se ofrece una lista de todos los AppDisks disponibles de la columna izquierda. En la columna derecha, se ofrece una lista de las aplicaciones presentes en el AppDisk. Al seleccionar la ficha **Aplicaciones** situada encima de la columna derecha, se muestran aplicaciones en un formato similar al del menú Inicio. Al seleccionar la ficha **Paquetes instalados**, se muestran aplicaciones en un formato similar al de la lista "Programas y características".

Marque una o varias casillas de verificación.

## Paso 4. Usuarios

Especifique los usuarios y los grupos de usuarios que pueden utilizar las aplicaciones y los escritorios del grupo de entrega.

### Dónde se especifican las listas de usuarios

Las listas de usuarios de Active Directory se especifican al crear o modificar lo siguiente:

- Una lista de acceso de usuarios a un sitio no configurada mediante Studio. La regla predeterminada de la directiva que rige los derechos a las aplicaciones incluye a todos los usuarios. Consulte los cmdlets `BrokerAppEntitlementPolicyRule` del SDK de PowerShell para obtener más información.
- Grupos de aplicaciones (si se han configurado).
- Grupos de entrega.
- Aplicaciones.

La lista de usuarios que pueden acceder a una aplicación a través de StoreFront está formada por la intersección de las listas de usuarios indicadas arriba. Por ejemplo, para configurar el uso de una aplicación A para un departamento específico, sin restringir innecesariamente el acceso por parte de otros grupos:

- Use la regla predeterminada de directiva de derechos de aplicaciones que incluye a todos los usuarios.
- Configure la lista de usuarios del grupo de entrega para permitir que todos los usuarios de las oficinas centrales usen cualquiera de las aplicaciones especificadas en el grupo de entrega.
- (Si hay grupos de aplicaciones configurados) Configure la lista de usuarios del grupo de aplicaciones para permitir que los miembros de la unidad de negocio de Administración y Finanzas accedan a las aplicaciones con nombres desde la A a la L.
- Configure las propiedades de la aplicación A para restringir su visibilidad únicamente al personal de Cuentas por cobrar en el departamento de Administración y Finanzas.

### Usuarios autenticados y no autenticados

Hay dos tipos de usuarios: los autenticados y los no autenticados (también llamados anónimos). Puede configurar uno o ambos tipos en un grupo de entrega.

- **Autenticado:** Para acceder a aplicaciones y escritorios, los usuarios y miembros del grupo cuyo nombre especifique deben introducir credenciales (como la tarjeta inteligente o el nombre de usuario y contraseña) en StoreFront o la aplicación Citrix Workspace. Para grupos de entrega que contengan máquinas de SO de escritorio, puede importar más tarde los datos de usuario (una lista de usuarios), al modificar el grupo de entrega.
- **No autenticado (anónimo):** Para grupos de entrega que contienen máquinas de SO de servidor, puede permitir a los usuarios acceder a sus aplicaciones y escritorios sin presentar credenciales a StoreFront o la aplicación Citrix Workspace. Por ejemplo, en máquinas quiosco, es posible que la aplicación requiera credenciales, mientras que el portal de acceso o las herramientas de Citrix no las requieran. Se crea un grupo de usuarios anónimos al instalar el primer Delivery Controller.

Para conceder acceso a usuarios no autenticados, cada máquina del grupo de entrega debe

tener instalado un VDA para SO de servidor Windows (versión mínima 7.6). Cuando los usuarios no autenticados están habilitados, se debe disponer de un almacén de StoreFront no autenticado.

Las cuentas de usuarios no autenticados se crean a demanda cuando se inicia una sesión. El nombre que reciben es AnonXYZ, donde XYZ es un valor único de tres dígitos.

Las sesiones de usuarios no autenticados tienen un valor predeterminado de tiempo de inactividad de 10 minutos, y se cierran automáticamente cuando el cliente se desconecta. No se admiten funciones como la reconexión, la itinerancia entre clientes y el control del espacio de trabajo.

En la siguiente tabla, se describen las opciones de la página **Usuarios**:

Habilitar acceso para	¿Agregar o asignar usuarios y grupos de usuarios?	¿Marcar la casilla “Dar acceso a usuarios no autenticados”?
Solo usuarios autenticados	Sí	No
Solo usuarios no autenticados	No	Sí
Usuarios autenticados y no autenticados	Sí	Sí

## Paso 5. Aplicaciones

Información útil:

- No se pueden agregar aplicaciones a grupos de entrega de acceso con Remote PC.
- De forma predeterminada, las nuevas aplicaciones que agregue se colocan en una carpeta denominada Applications. Puede especificar otra carpeta. Para obtener más información, consulte el artículo Administración de aplicaciones.
- Puede cambiar las propiedades de una aplicación cuando la agregue a un grupo de entrega o más tarde. Para obtener más información, consulte el artículo Administración de aplicaciones.
- Si intenta agregar una aplicación y ya existe una con el mismo nombre en la carpeta, se le pedirá cambiar el nombre de la aplicación que está agregando. Si rechaza la solicitud, la aplicación se agregará con un sufijo que hará su nombre único en la carpeta de aplicaciones.
- Al agregar una aplicación a más de un grupo de entrega, puede producirse un problema de visibilidad si no dispone de permisos suficientes para ver la aplicación en todos esos grupos de entrega. En tales casos, consulte a un administrador con más permisos o amplíe el ámbito para incluir todos los grupos de entrega a los que se haya agregado la aplicación.
- Si publica dos aplicaciones con el mismo nombre para los mismos usuarios, cambie la propiedad Nombre de la aplicación (para el usuario) en Studio; de lo contrario, los usuarios verán nombres duplicados en la aplicación Citrix Workspace.

Haga clic en **Agregar** para ver los orígenes de aplicación.

- **Desde el menú Inicio:** Se trata de las aplicaciones que se detectan en una máquina creada a partir de la imagen maestra en un catálogo de máquinas seleccionado. Cuando se selecciona este origen, se abre una nueva página con una lista de las aplicaciones detectadas; seleccione las que quiera agregar y, a continuación, haga clic en **Aceptar**.
- **Definidas manualmente:** Se trata de las aplicaciones que se encuentran en el sitio o en la red. Cuando se selecciona este origen, se abre una nueva página donde se escribe la ruta al archivo ejecutable, al directorio de trabajo, los argumentos de línea de comandos opcionales y los nombres simplificados para administradores y usuarios. Después de introducir la información, haga clic en **Aceptar**.
- **Existentes:** Se trata de aplicaciones agregadas anteriormente al sitio, existentes posiblemente en otro grupo de entrega. Cuando se selecciona este origen, se abre una nueva página con una lista de las aplicaciones detectadas; seleccione las que quiera agregar y, a continuación, haga clic en **Aceptar**.
- **App-V:** Se trata de las aplicaciones presentes en paquetes de App-V. Cuando se selecciona este origen, se abre una nueva página donde se puede seleccionar el servidor de App-V o la biblioteca de aplicaciones. Seleccione las aplicaciones que quiera agregar y, a continuación, haga clic en **Aceptar**. Para obtener más información, consulte [App-V](#).

Si una aplicación o su origen no están disponibles o no son válidos, no serán visibles o no se podrán seleccionar. Por ejemplo, el origen **Existentes** no está disponible si no hay aplicaciones que se hayan agregado al sitio. O bien, una aplicación podría no ser compatible con el tipo de sesiones admitidas en las máquinas del catálogo seleccionado.

## Paso 6. Escritorios

El título de esta página depende del catálogo de máquinas que haya elegido anteriormente en la página **Máquinas**:

- Si eligió un catálogo que contiene máquinas agrupadas, esta página se llamará **Escritorios**.
- Si eligió un catálogo que contiene máquinas asignadas y especificó “Escritorios” en la página **Tipo de entrega**, esta página se llamará **Asignaciones de usuarios de escritorios**.
- Si eligió un catálogo que contiene máquinas asignadas y especificó “Aplicaciones” en la página **Tipo de entrega**, esta página se llamará **Asignaciones de usuarios de máquinas de aplicaciones**.

Haga clic en **Add**. En el cuadro de diálogo:

- En los campos Nombre simplificado y Descripción, escriba la información que se verá en la aplicación Citrix Workspace.

- Para agregar una restricción de etiqueta a un escritorio, elija **Restringir inicios a máquinas con la etiqueta** y, a continuación, seleccione la etiqueta en el menú desplegable. (Para obtener más información, consulte [Etiquetas](#).)
- Mediante los botones de radio, indique quién puede iniciar un escritorio (para grupos con máquinas agrupadas) o a quién se asignará una máquina cuando inicie el escritorio (para grupos con máquinas asignadas). Los usuarios pueden ser todos los usuarios que puedan acceder a ese grupo de entrega, o bien grupos de usuarios y usuarios específicos.
- Si el grupo contiene máquinas asignadas, especifique la cantidad máxima de escritorios por usuario. Este debe ser un valor de uno o más.
- Habilite o inhabilite el escritorio (para máquinas agrupadas) o la regla de asignación de escritorios (para máquinas asignadas). Si inhabilita un escritorio, este deja de entregar escritorios; inhabilitar una regla de asignación de escritorios detiene la asignación automática de escritorios a los usuarios.
- Cuando haya finalizado con el cuadro de diálogo, haga clic en **Aceptar**.

### Instancias máximas de un escritorio en un sitio (solo PowerShell)

Para configurar la cantidad máxima de instancias en un escritorio del sitio (solo PowerShell):

- En PowerShell, use el cmdlet `BrokerEntitlementPolicyRule` adecuado con el parámetro `MaxPerEntitlementInstances`. Por ejemplo, el siguiente cmdlet modifica la regla “tsvda-desktop” para establecer en dos la cantidad máxima de instancias simultáneas de un escritorio permitidas en el sitio. Cuando hay dos instancias de escritorio en ejecución, se produce un error si un tercer suscriptor intenta iniciar un escritorio.

```
Set-BrokerEntitlementPolicyRule -Name tsvda-desktop -MaxPerEntitlementInstances 2
```

- Para obtener ayuda, use el cmdlet `Get-Help`. Por ejemplo, `Get-Help Set-BrokerEntitlementPolicyRule -Parameter MaxPerEntitlementInstances`.

### Paso 7. Resumen

Escriba un nombre para el grupo de entrega. También puede especificar una descripción (opcional), que aparecerá en Studio y en la aplicación Citrix Workspace.

Revise la información de resumen y, a continuación, haga clic en **Finalizar**. Si no ha seleccionado ninguna aplicación ni ha especificado escritorios a entregar, se le preguntará si quiere continuar.

## Administrar grupos de entrega

November 15, 2022

### Introducción

Este artículo describe los procedimientos para la administración de los grupos de entrega desde la consola de administración. Además de cambiar los parámetros especificados en el momento de crear el grupo, puede configurar otros parámetros que no estaban disponibles al crear el grupo de entrega.

Los procedimientos se organizan por categorías: general, usuarios, máquinas y sesiones. Algunas tareas abarcan más de una categoría. Por ejemplo, “Impedir que los usuarios se conecten a una máquina” se describe en la categoría de máquinas, pero también afecta a los usuarios. Si no puede encontrar una tarea en una categoría, compruebe otra categoría relacionada.

Hay otros artículos que también contienen información relacionada:

- [Aplicaciones](#) contiene información sobre cómo administrar aplicaciones en los grupos de entrega.
- La administración de grupos de entrega requiere permisos correspondientes al rol integrado de Administrador de grupos de entrega. Para obtener más información, consulte [Administración delegada](#).

### General

- Cambiar el método de entrega
- Cambiar direcciones de StoreFront
- Actualización de un grupo de entrega
- Administrar grupos de entrega de acceso con Remote PC

### Cambiar el tipo de entrega de un grupo de entrega

El tipo de entrega indica lo que puede entregar el grupo: aplicaciones, escritorios o ambos.

Antes de cambiar de un tipo de grupo que entrega **solo aplicaciones** o **escritorios y aplicaciones** a un tipo de grupo que entrega **solo escritorios**, elimine todas las aplicaciones que haya en el grupo.

1. Seleccione **Grupos de entrega** en el panel de navegación.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en el panel Acciones.

3. En la página **Tipo de entrega**, seleccione el tipo de entrega que quiere.
4. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta. También puede hacer clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

### **Cambiar direcciones de StoreFront**

1. Seleccione **Grupos de entrega** en el panel de navegación.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en el panel Acciones.
3. En la página **StoreFront**, seleccione o agregue direcciones URL de StoreFront que utiliza la aplicación Citrix Workspace instalada en cada máquina del grupo de entrega.
4. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta. También puede hacer clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

También puede especificar las direcciones de servidor de StoreFront tras seleccionar **Configuración > StoreFront** en el panel de navegación.

### **Actualizar o revertir la versión de un grupo de entrega**

Actualice un grupo de entrega después de actualizar la versión de los VDA de sus máquinas y los catálogos de máquinas que contengan las máquinas que se usan en ese grupo de entrega.

Antes de iniciar la actualización del grupo de entrega:

- Si utiliza Citrix Provisioning (antes Provisioning Services), debe actualizar la versión de VDA en la consola de Citrix Provisioning.
- Inicie las máquinas que contienen el VDA actualizado para que se registren con un Delivery Controller. Este proceso indica a la consola los elementos del grupo de entrega cuya versión necesita actualizarse.
- Si debe seguir mediante versiones anteriores de VDA, es posible que las funciones más recientes del producto no estén disponibles. Para obtener más información, consulte la documentación de la actualización de versiones.

Para actualizar un grupo de entrega:

1. Seleccione **Grupos de entrega** en el panel de navegación.
2. Seleccione un grupo de entrega y haga clic en **Actualizar grupo de entrega** en el panel Acciones. La acción **Actualizar grupo de entrega** aparece solo si se detectan agentes VDA actualizados.

La pantalla le indica qué máquinas, si las hay, no pueden actualizarse y por qué. A continuación, puede cancelar la actualización, resolver los problemas de las máquinas y, luego, iniciar de nuevo el proceso de actualización.

Después de completar la actualización, puede revertir las máquinas a su estado anterior. Para ello, seleccione el grupo de entrega y, a continuación, haga clic en **Deshacer** en el panel Acciones.

### **Administrar grupos de entrega de acceso con Remote PC**

Si una máquina del catálogo de acceso con Remote PC no está asignada a ningún usuario, se asigna temporalmente una máquina a un grupo de entrega asociado a ese catálogo de máquinas. Esta asignación temporal permite que la máquina se asigne más tarde a un usuario.

La asociación de grupo de entrega a catálogo de máquinas tiene un valor de prioridad. La prioridad determina a qué grupo de entrega se asigna la máquina cuando esta se registra en el sistema o cuando un usuario necesita que se le asigne una máquina: cuanto menor sea el valor, mayor será la prioridad. Si un catálogo de máquinas de acceso con Remote PC tiene varias asignaciones de grupos de entrega, el software selecciona la de prioridad más alta. Use el SDK de PowerShell para configurar este valor de prioridad.

Nada más crearse, los catálogos de máquinas de acceso con Remote PC se asocian a un grupo de entrega. Esto significa que las cuentas de máquina o unidades organizativas que se agreguen al catálogo de máquinas más adelante se pueden agregar al grupo de entrega. Esta asociación se puede activar o desactivar.

Para agregar o quitar una asociación de catálogo de máquinas de acceso con Remote PC a un grupo de entrega:

1. Seleccione **Grupos de entrega** en el panel de navegación.
2. Seleccione un grupo de acceso con Remote PC.
3. En la sección **Detalles**, seleccione la ficha **Catálogos de máquinas** y, a continuación, seleccione un catálogo de acceso con Remote PC.
4. Para agregar o restaurar una asociación, seleccione **Agregar escritorios**. Para quitar una asociación, seleccione **Quitar asociación**.

### **Usuarios**

- Cambiar los parámetros del usuario
- Agregar o quitar usuarios

### **Cambiar la configuración de usuario en un grupo de entrega**

El nombre de esta página puede aparecer como **Parámetros de usuario** o **Parámetros básicos**.

1. Seleccione **Grupos de entrega** en el panel de navegación.

2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en el panel Acciones.
3. En la página **Parámetros de usuario** (o **Parámetros básicos**), puede cambiar los parámetros de la tabla siguiente.
4. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta. También puede hacer clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

Parámetro	Descripción
Descripción	El texto que utiliza Citrix Workspace (o StoreFront) y que verán los usuarios.
Habilitar grupo de entrega	Indica si el grupo de entrega está habilitado o no.
Zona horaria	La zona horaria en la que deben residir las máquinas de este grupo de entrega. La opción muestra las zonas horarias admitidas por el sitio.
Habilitar Secure ICA	Oculto todas las comunicaciones que tienen lugar desde y hacia las máquinas del grupo de entrega mediante la funcionalidad SecureICA, que cifra el protocolo ICA. El nivel predeterminado es 128 bits. Este nivel se puede cambiar mediante el SDK. Citrix recomienda el uso de métodos de cifrado adicionales como el cifrado TLS cuando se trabaje en redes públicas. Asimismo, SecureICA no comprueba la integridad de los datos.

### Agregar o eliminar usuarios de un grupo de entrega

Para obtener más información acerca de los usuarios, consulte [Usuarios](#).

1. Seleccione **Grupos de entrega** en el panel de navegación.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en el panel Acciones.
3. En la página **Usuarios**:
  - Para agregar usuarios, haga clic en **Agregar** y especifique los usuarios que quiere agregar.
  - Para quitar usuarios, seleccione uno o varios usuarios y, a continuación, haga clic en **Quitar**.
  - Marque o desmarque la casilla para permitir el acceso a usuarios no autenticados.

4. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta. También puede hacer clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

**Importar o exportar listas de usuarios** Para grupos de entrega que contengan máquinas físicas con SO de sesión única, puede importar la información de usuarios desde un archivo CSV después de crear el grupo de entrega. También es posible exportar información de usuarios a un archivo CSV. El archivo CSV puede contener datos de una versión anterior del producto.

La primera línea del archivo CSV debe contener encabezados de columna separados por comas (no necesariamente por orden), que pueden ser: `ADComputerAccount`, `AssignedUser`, `VirtualMachine` y `HostId`. Las siguientes líneas del archivo deben contener datos separados por comas. Las entradas `ADComputerAccount` pueden ser nombres comunes, direcciones IP, nombres distintivos o pares de nombres de dominios y equipos.

Para importar o exportar la información de usuarios:

1. Seleccione **Grupos de entrega** en el panel de navegación.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en el panel Acciones.
3. En la página **Asignación de máquinas**, seleccione el botón **Importar lista** o **Exportar lista** y, a continuación, vaya a la ubicación del archivo.
4. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta. También puede hacer clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

## Máquinas

- Cambio de asignaciones de máquinas a usuarios
- Cambiar la cantidad máxima de máquinas por usuario
- Actualización de una máquina
- Agregar, modificar o eliminar una restricción por etiquetas para un escritorio
- Quitar una máquina
- Restricción del acceso a las máquinas
- Impedir que los usuarios se conecten a una máquina (modo de mantenimiento)
- Apagado y reiniciado de las máquinas
- Crear y administrar programaciones de reinicios para las máquinas
- Administrar la carga de las máquinas
- Administrar la energía de las máquinas

## Cambiar asignaciones de máquinas a usuarios en un grupo de entrega

Puede cambiar las asignaciones de las máquinas de SO de sesión única aprovisionadas con MCS. No puede cambiar las asignaciones para máquinas de SO multisesión o máquinas aprovisionadas con Citrix Provisioning.

1. Seleccione **Grupos de entrega** en el panel de navegación.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en el panel Acciones.
3. En la página **Escritorios** o **Reglas de asignación de escritorio** (el título de la página depende del tipo de catálogo que utilice el grupo de entrega), especifique los nuevos usuarios.
4. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta. También puede hacer clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

## Cambio de la cantidad máxima de máquinas por usuario en un grupo de entrega

1. Seleccione **Grupos de entrega** en el panel de navegación.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en el panel Acciones.
3. En la página **Reglas de asignación de escritorio**, establezca los escritorios máximos por usuario.
4. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta. También puede hacer clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

## Actualizar una máquina en un grupo de entrega

1. Seleccione **Grupos de entrega** en el panel de navegación.
2. Seleccione un grupo y, a continuación, seleccione **Ver máquinas** en el panel Acciones.
3. Seleccione una máquina y, a continuación, seleccione **Actualizar máquinas** en el panel Acciones.

Para elegir otra imagen maestra, seleccione **Imagen maestra** y, a continuación, seleccione una instantánea.

Para aplicar cambios y notificar a los usuarios de la máquina, seleccione **Notificación de implantación para usuarios finales**. A continuación, especifique:

- El momento de la actualización de la imagen maestra: ahora o en el próximo reinicio
- La hora de la distribución de reinicios (el tiempo total para comenzar a actualizar todas las máquinas del grupo)
- Si se notifica a los usuarios del reinicio
- El mensaje que los usuarios recibirán

## Agregar, modificar o eliminar una restricción por etiquetas para un escritorio

Agregar, modificar o eliminar restricciones por etiqueta puede tener efectos no esperados en los escritorios que se tengan en cuenta para el inicio. Consulte las precauciones y los aspectos a tener en cuenta en [Etiquetas](#).

1. Seleccione **Grupos de entrega** en el panel de navegación.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en el panel Acciones.
3. En la página **Escritorios**, seleccione el escritorio y haga clic en **Modificar**.
4. Para agregar una restricción por etiquetas, elija **Restringir inicios a máquinas con la etiqueta** y, a continuación, seleccione la etiqueta.
5. Para cambiar o eliminar una restricción por etiquetas, ya sea:
  - Seleccione otra etiqueta.
  - Puede eliminar la restricción por etiquetas al desmarcar la casilla **Restringir inicios a máquinas con esta etiqueta**.
6. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta. También puede hacer clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

## Quitar una máquina de un grupo de entrega

Al quitar una máquina, se elimina de un grupo de entrega. No se eliminará del catálogo de máquinas que el grupo de entrega utiliza. Por lo tanto, esa máquina está disponible para la asignación a otro grupo de entrega.

Las máquinas deben estar apagadas antes de poder eliminarlas. Para impedir temporalmente que los usuarios se conecten a una máquina mientras se procede a quitarla, ponga la maquina en modo de mantenimiento antes de apagarla.

Las máquinas pueden contener datos personales, así que actúe con precaución a la hora de asignar una máquina a otro usuario. Considere restablecer la imagen inicial de la máquina.

1. Seleccione **Grupos de entrega** en el panel de navegación.
2. Seleccione un grupo y, a continuación, seleccione **Ver máquinas** en el panel Acciones.
3. Compruebe que la máquina esté apagada.
4. Seleccione la máquina y, a continuación, haga clic en **Quitar del grupo de entrega** en el panel Acciones.

También puede quitar una máquina de un grupo de entrega a través de la [conexión](#) que usa la máquina.

## Restringir el acceso a máquinas en un grupo de entrega

Todos los cambios que realice para restringir el acceso a las máquinas de un grupo de entrega anulan los parámetros anteriores, independientemente del método que utilice. Puede hacer lo siguiente:

- **Restringir el acceso de los administradores mediante los ámbitos de administración delegada:** Puede crear y asignar un ámbito que permita el acceso de los administradores a todas las aplicaciones, y otro ámbito que conceda acceso solamente a determinadas aplicaciones. Para obtener más información, consulte [Administración delegada](#).
- **Restringir el acceso de los usuarios a través de las expresiones de directiva SmartAccess:** Use las expresiones de la directiva para filtrar las conexiones de usuario realizadas a través de Citrix Gateway.
  1. Seleccione **Grupos de entrega** en el panel de navegación.
  2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en el panel Acciones.
  3. En la página **Directiva de acceso**, seleccione **Conexiones a través de NetScaler Gateway**.
  4. Para elegir un subconjunto de esas conexiones, seleccione **Conexiones que cumplan cualquiera de estos filtros**. Ahora defina el sitio de Citrix Gateway y agregue, modifique o quite las expresiones de directiva SmartAccess para las situaciones de acceso autorizado de los usuarios. Para obtener información más detallada, consulte la documentación de Citrix Gateway.
  5. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta. También puede hacer clic en **Aceptar** para aplicar los cambios y cerrar la ventana.
- **Restringir el acceso de los usuarios a través de los filtros de exclusión:** Use los filtros de exclusión incluidos en las directivas de acceso que usted estableció en el SDK. Las directivas de acceso se aplican a grupos de entrega para limitar las conexiones. Por ejemplo, puede restringir el acceso a las máquinas por parte de un subconjunto de usuarios. También puede especificar los dispositivos de usuario permitidos. El uso de filtros de exclusión permite definir más detalladamente las directivas de acceso. Por ejemplo, por razones de seguridad, puede negar el acceso a un subconjunto de usuarios o dispositivos. De forma predeterminada, los filtros de exclusión están inhabilitados.

Por ejemplo: en el caso de un laboratorio escolar ubicado en una subred dentro de la red corporativa, para impedir el acceso desde ese laboratorio a un determinado grupo de entrega, independientemente del usuario que utilice las máquinas del laboratorio, use el comando: `Set-BrokerAccessPolicy -Name VPDesktops_Direct -ExcludedClientIPFilterEnabled $True -`

Puede utilizar el asterisco (\*) como comodín para hacer coincidir todas las etiquetas

que comienzan por la misma expresión de directiva. Por ejemplo, si agrega la etiqueta `VPDesktops_Direct` a una máquina y `VPDesktops_Test` a otra, al configurar la etiqueta en el script `Set-BrokerAccessPolicy` como `VPDesktops_*`, se aplica el filtro a las dos máquinas.

Si se conecta mediante un explorador web o con la funcionalidad de experiencia de usuario de la aplicación Citrix Workspace habilitada en el almacén, no puede usar un filtro de exclusión de nombres de clientes.

### **Impedir que los usuarios se conecten a una máquina (modo de mantenimiento) en un grupo de entrega**

Cuando tenga que detener temporalmente las conexiones nuevas a las máquinas, puede activar el modo de mantenimiento para una o todas las máquinas de un grupo de entrega. Puede hacerlo antes de aplicar revisiones o mediante herramientas de administración.

- Cuando una máquina con SO multisesión está en modo de mantenimiento, los usuarios pueden conectarse a las sesiones existentes, pero no pueden iniciar sesiones nuevas.
- Cuando una máquina con SO de sesión única (o un PC de acceso con Remote PC) está en modo de mantenimiento, los usuarios no pueden conectarse o volver a conectarse. Las conexiones actuales permanecen conectadas hasta que se desconectan o cierran sesión.

Para activar o desactivar el modo de mantenimiento:

1. Seleccione **Grupos de entrega** en el panel de navegación.
2. Seleccione un grupo.
3. Para activar el modo de mantenimiento en todas las máquinas de un grupo de entrega, seleccione **Activar modo de mantenimiento** en el panel Acciones.

Para activar el modo de mantenimiento en una máquina, seleccione **Ver máquinas** en el panel Acciones. Seleccione una máquina y, a continuación, seleccione **Activar modo de mantenimiento** en el panel Acciones.

4. Para desactivar el modo de mantenimiento en una o todas las máquinas de un grupo de entrega, siga las instrucciones anteriores, pero seleccione **Desactivar modo de mantenimiento** en el panel Acciones.

La configuración de la Conexión a Escritorio remoto (RDC) de Windows también afecta a si una máquina con SO multisesión está en modo de mantenimiento o no. El modo de mantenimiento se activa en cualquiera de las siguientes circunstancias:

- Cuando el modo de mantenimiento se activa, como se ha descrito anteriormente.

- Cuando la conexión a Escritorio remoto se establece en **No permitir las conexiones a este equipo**.
- Cuando la conexión a Escritorio remoto no se establece en **No permitir las conexiones a este equipo** y el parámetro “Modo de inicio de sesión de usuario en la Configuración de host remoto” es **Permitir reconexiones, pero impedir nuevos inicios de sesión** o **Permitir reconexiones, pero impedir nuevos inicios de sesión hasta que el servidor se reinicie**.

También puede activar o desactivar el modo de mantenimiento de:

- Una conexión, que afecta a las máquinas que usan esa conexión.
- Un catálogo de máquinas, que afecta a las máquinas en ese catálogo.

### Apagar y reiniciar máquinas en un grupo de entrega

No se admite este procedimiento en las máquinas de acceso con Remote PC.

1. Seleccione **Grupos de entrega** en el panel de navegación.
2. Seleccione un grupo y, a continuación, seleccione **Ver máquinas** en el panel Acciones.
3. Seleccione la máquina y, a continuación, seleccione una de las siguientes entradas del panel Acciones (es posible que, según el estado de la máquina, algunas opciones no estén disponibles):
  - **Forzar apagado:** Apaga la máquina y actualiza la lista de máquinas.
  - **Reiniciar:** Solicita al sistema operativo que se apague y que, a continuación, vuelva a iniciar la máquina. Si el sistema operativo no puede hacerlo, esta permanece en su estado actual.
  - **Forzar reinicio:** Obliga al sistema operativo a apagarse y, a continuación, reinicia la máquina.
  - **Suspender:** Pausa la máquina sin apagarla y actualiza la lista de máquinas.
  - **Apagar:** Solicita al sistema operativo de la máquina que se apague.

Para acciones no forzadas, si la máquina no se apaga en un plazo de 10 minutos, se le obliga a apagarse. Si Windows intenta instalar actualizaciones durante el apagado, existe el riesgo de que la máquina se apague antes de que se completen las actualizaciones.

Citrix recomienda impedir que los usuarios de máquinas de SO de sesión única seleccionen **Apagar** mientras estén en sesión. Para obtener información más detallada, consulte la documentación acerca de directivas de Microsoft.

También puede apagar y reiniciar las máquinas en una [conexión](#).

## Crear y administrar programaciones de reinicios para las máquinas de un grupo de entrega

Una programación de reinicios especifica cuándo se reinician periódicamente las máquinas de un grupo de entrega. Puede crear una o varias programaciones para un grupo de entrega. Una programación puede afectar a:

- Todas las máquinas del grupo.
- Una o varias máquinas (pero no todas) del grupo. Las máquinas se identifican mediante una etiqueta que se les aplica. Esta operación se denomina restricción por etiquetas, porque la etiqueta restringe una acción solo a los elementos (en este caso, máquinas) que tienen la etiqueta.

Por ejemplo: todas las máquinas están en un solo grupo de entrega y quiere reiniciarlas todas al menos una vez por semana, salvo las máquinas que utiliza el departamento de contabilidad, que deben reiniciarse todos los días. Quiere reiniciar todas las máquinas al menos una vez por semana, salvo las máquinas que utiliza el departamento de contabilidad, que deben reiniciarse todos los días. Para ello, configure una programación para todas las máquinas y otra para las máquinas del departamento de contabilidad.

Una programación incluye el día y la hora en que comienza el reinicio, así como la duración de este. La duración es “iniciar todas las máquinas afectadas al mismo tiempo” o el tiempo que debe tardarse en reiniciar todas las máquinas afectadas.

Puede activar o desactivar una programación. Inhabilitar una programación puede ser útil durante la realización de pruebas, durante intervalos especiales o cuando se preparan programaciones antes de necesitarlas.

No puede usar programaciones para el encendido o el apagado automáticos desde la consola de administración; solo para reiniciar.

**Superposición de programaciones** Es posible que las programaciones se solapen. En el ejemplo anterior, ambas programaciones afectan a las máquinas utilizadas por el equipo de contabilidad. Esas máquinas podrían reiniciarse dos veces el domingo. Ahora bien, la programación está diseñada para evitar tener que reiniciar la misma máquina con más frecuencia de la necesaria, pero eso no puede garantizarse.

- Si las programaciones se solapan en la hora de inicio y la duración, es más probable que las máquinas se reinicien una sola vez.
- Por tanto, cuanto más difieran las programaciones en la hora de inicio y la duración, más probable será que haya varios reinicios.
- La cantidad de máquinas que se vean afectadas por los reinicios programados también puede influir en las posibilidades de superposición. En el ejemplo, la programación semanal que afecta a todas las máquinas podría iniciar los reinicios mucho más rápidamente que el reini-

cio diario programado para las máquinas de contabilidad (según la duración configurada para cada reinicio).

Para obtener información exhaustiva sobre las programaciones de reinicios, consulte [Datos internos de programación de reinicios](#).

### Ver programaciones de reinicios

1. Seleccione **Grupos de entrega** en el panel de navegación.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en el panel Acciones.
3. Seleccione la página **Programación de reinicios**.

La página **Programación de reinicios** contiene la siguiente información para cada programación configurada:

- Nombre de la programación.
- Restricción por etiquetas utilizada, si la hay.
- La frecuencia con se producen los reinicios de las máquinas.
- Si los usuarios de la máquina reciben una notificación.
- Si la programación está habilitada. Inhabilitar una programación puede ser útil durante la realización de pruebas, durante intervalos especiales o cuando se preparan programaciones antes de necesitarlas.

**Agregar (aplicar) etiquetas** Si configura una programación de reinicios que usa una restricción de etiqueta, compruebe que esa etiqueta se ha agregado (aplicado) a las máquinas a las que esa programación debería afectar. En el ejemplo anterior, cada una de las máquinas utilizadas por el equipo de contabilidad tiene una etiqueta aplicada. Para obtener más información, consulte [Etiquetas](#).

Aunque puede aplicar más de una etiqueta a una máquina, solo se puede especificar una etiqueta en una programación de reinicios.

1. Seleccione **Grupos de entrega** en el panel de navegación.
2. Seleccione el grupo de entrega que contiene las máquinas a las que afectará la programación.
3. Haga clic en **Ver máquinas** y, a continuación, seleccione las máquinas a las que agregará la etiqueta.
4. Haga clic en **Administrar etiquetas** en el panel Acciones.
5. Si la etiqueta ya existe, marque la casilla situada junto al nombre de la etiqueta. Si la etiqueta no existe, haga clic en **Crear** y especifique el nombre de la etiqueta. Una vez creada, marque la casilla situada junto al nombre de la etiqueta recién creada.
6. Haga clic en **Guardar** en el cuadro de diálogo **Administrar etiquetas**.

## Crear una programación de reinicios

1. Seleccione **Grupos de entrega** en el panel de navegación.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en el panel Acciones.
3. En la página **Programación de reinicios**, haga clic en **Agregar**.
4. En la página **Agregar programación de reinicios**:
  - Escriba un nombre y una descripción para la programación.
  - Si utiliza una restricción por etiquetas, seleccione la etiqueta.
  - En **Frecuencia de reinicio**, seleccione la frecuencia con que se produce el reinicio (diariamente, de lunes a viernes, los días del fin de semana o un día concreto cada semana).
  - Con el reloj de 24 horas, especifique la hora del día para comenzar el reinicio.
  - Para la **Duración de reinicio**, elija si todas las máquinas deben reiniciarse al mismo tiempo, o bien elija la franja total del tiempo necesario para empezar a reiniciar todas las máquinas afectadas. Un algoritmo interno determina cuándo se reinicia cada máquina durante ese intervalo.
  - En **Enviar notificación a los usuarios**, elija si mostrar un mensaje de notificación en las máquinas correspondientes antes de empezar un reinicio. De forma predeterminada, no se muestra ningún mensaje.
  - Si elige mostrar un mensaje 15 minutos antes de empezar el reinicio, puede decidir (en Frecuencia de notificaciones) si repetir el mensaje cada cinco minutos después del primer mensaje. De forma predeterminada, el mensaje no se repite.
  - Escriba el título y el texto de la notificación. No hay texto predeterminado.

Si quiere que el mensaje incluya la cantidad de minutos que quedan antes del reinicio, incluya la variable **%m%**. Por ejemplo: “Advertencia: Su equipo se reiniciará automáticamente dentro de %m% minutos”. El valor disminuye cinco minutos en cada mensaje repetido. A menos que haya optado por reiniciar todas las máquinas a la vez, el mensaje de notificación se mostrará en cada máquina en el momento correspondiente antes de que empiece el reinicio, calculado por un algoritmo interno.
  - Para habilitar la programación, marque la casilla. Para inhabilitar la programación, desmarque la casilla.
5. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta. También puede hacer clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

## Modificar, quitar, habilitar o inhabilitar una programación de reinicios

1. Seleccione **Grupos de entrega** en el panel de navegación.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en el panel Acciones.
3. En la página **Programación de reinicios**, marque la casilla de una programación.
  - Para modificar una programación, haga clic en **Modificar**. Actualice los parámetros de la programación siguiendo las instrucciones indicadas en Crear una programación de reinicios.
  - Para habilitar o inhabilitar una programación, haga clic en **Modificar**. Marque o desmarque la casilla **Habilitar programación de reinicios**.
  - Para eliminar una programación, haga clic en **Quitar**. Confirme la eliminación. La eliminación de una programación no afecta a las etiquetas aplicadas a las máquinas afectadas.

## Reinicios programados que se retrasan por una interrupción de la base de datos

### Nota:

Esta función solo está disponible mediante PowerShell.

Si se produce una interrupción de la base de datos del sitio antes de que comience un reinicio programado para las máquinas (VDA) de un grupo de entrega, los reinicios comienzan cuando finaliza la interrupción. Esto puede provocar resultados inesperados.

Por ejemplo, supongamos que ha programado reinicios de un grupo de entrega para que se produzcan durante las horas que no son de producción (a partir de las 3:00). Se produce una interrupción de la base de datos del sitio una hora antes de que comience el reinicio programado (2:00). La interrupción dura 6 horas (hasta las 8:00). La programación de reinicios comienza cuando se restaura la conexión entre el Delivery Controller y la base de datos del sitio. Ahora el VDA se reinicia cinco horas después de su programación original. Esto podría provocar que los VDA se reinicien durante las horas de producción.

Para evitar esta situación, puede usar el parámetro `MaxOvertimeStartMins` para los cmdlets `New-BrokerRebootScheduleV2` y `Set-BrokerRebootScheduleV2`. El valor especifica el máximo de minutos transcurridos a partir de la hora de inicio programada a la que puede comenzar una programación de reinicios.

Si la conexión a la base de datos se restaura antes de que haya transcurrido ese tiempo (hora programada + `MaxOvertimeStartMins`), los VDA se reinician.

Si la conexión a la base de datos no se restaura antes de que haya transcurrido ese tiempo, los VDA no se reinician.

Si se omite este parámetro, la programación de reinicios comienza cuando se restablece la conexión a la base de datos, independientemente de la duración de la interrupción.

Para obtener más información, consulte la ayuda de los cmdlets. Esta función solo está disponible en PowerShell. No se puede establecer este valor al configurar una programación de reinicios en Studio.

### Administrar la carga de las máquinas de un grupo de entrega

Solo puede administrar la carga de las máquinas con sistema operativo multisesión.

La administración de carga mide la carga del servidor y determina el servidor que quiere seleccionar en el entorno actual. Esta selección se basa en:

- **Estado del modo de mantenimiento del servidor:** Una máquina de SO multisesión se tiene en cuenta para el equilibrio de carga solo cuando el modo de mantenimiento está desactivado.
- **Índice de carga de servidor:** Este índice determina con qué probabilidad recibirá conexiones un servidor que entrega máquinas de SO multisesión. El índice es una combinación de patrones de carga: la cantidad de sesiones y la configuración de las mediciones de rendimiento (como la CPU, el disco y el uso de memoria). Los patrones de carga se especifican en las configuraciones de la directiva Administración de carga.

Un índice de carga del servidor de 10000 indica que la carga del servidor es total. Si no hay otros servidores disponibles, es posible que los usuarios reciban un mensaje en el que se les notifica que el escritorio o la aplicación no están disponibles cuando intentan iniciar sesión.

Puede supervisar el índice de carga en el SDK, en Director (Supervisión) y en la búsqueda de Studio (Administración).

En las pantallas de la consola, para mostrar la columna **Índice de carga del servidor** (que está oculta de forma predeterminada), seleccione una máquina, haga clic con el botón secundario en el encabezado de una columna y, a continuación, elija **Seleccionar columna**. En la categoría **Máquina**, seleccione **Índice de carga**.

En el SDK, use el cmdlet `Get-BrokerMachine`. Para obtener más información, consulte [CTX202150](#).

- **Parámetro de directiva Tolerancia de inicios de sesión simultáneos:** La cantidad máxima de solicitudes simultáneas para iniciar sesión en el servidor. (esta opción es equivalente a la regulación de carga en las versiones 6.x de XenApp).

Cuando todos los servidores superan o se encuentran en el límite definido por el parámetro Tolerancia de inicios de sesión simultáneos, la siguiente solicitud de inicio de sesión se asigna al servidor que tenga el menor número de inicios de sesión pendientes. Si hay más de un servidor que cumple esos criterios, se selecciona el servidor que presenta el menor índice de carga.

## Administrar la energía de las máquinas de un grupo de entrega

Solo es posible administrar las opciones de energía de las máquinas virtuales con SO de sesión única, no las máquinas físicas (incluidas las máquinas de acceso con Remote PC). Las máquinas de SO de sesión única y con capacidad de GPU no se pueden suspender, por lo que las operaciones de apagado dan error. Para máquinas con sistema operativo multisesión, puede crear una programación de reinicios.

En grupos de entrega que contengan máquinas agrupadas, las máquinas virtuales con SO de sesión única pueden estar en uno de los siguientes estados:

- En uso y de asignación aleatoria
- No asignadas y no conectadas

En grupos de entrega que contengan máquinas estáticas, las máquinas virtuales con SO de sesión única pueden ser:

- De asignación permanente y en uso
- De asignación permanente y no conectadas (pero listas)
- No asignadas y no conectadas

Durante el uso habitual, los grupos de entrega estáticos normalmente contienen máquinas asignadas de forma permanente y máquinas sin asignar. Al principio, todas las máquinas se presentan sin asignar (excepto las máquinas asignadas manualmente al crearse el grupo de entrega). Cuando los usuarios se conectan, las máquinas pasan a estar asignadas de forma permanente. Puede administrar la totalidad de las opciones de energía de las máquinas sin asignar en esos grupos de entrega. En cambio, la administración de energía de las máquinas de asignación permanente solo es parcial.

- **Agrupaciones y búferes:** Para grupos de entrega agrupados y grupos de entrega estáticos con máquinas sin asignar, una agrupación (en este caso) es un conjunto de máquinas no asignadas o asignadas temporalmente que se mantienen en estado activo y listas para que se conecten los usuarios. El usuario obtiene una máquina inmediatamente después de iniciar sesión. El tamaño de la agrupación (la cantidad de máquinas que se mantienen activas) se puede configurar en función del momento del día. En caso de grupos de entrega estáticos, utilice el SDK para configurar la agrupación.

Un búfer es un conjunto adicional de máquinas sin asignar que se mantienen en modo de espera. Estas se inician cuando la cantidad de dichas máquinas en la agrupación se encuentra por debajo de un umbral. El umbral es un porcentaje del tamaño del grupo de entrega. Para grupos de entrega grandes, se puede encender una cantidad significativa de máquinas cuando se excede el umbral. Por lo tanto, planifique con cuidado los tamaños del grupo de entrega o use el SDK para ajustar el tamaño predeterminado del búfer.

- **Temporizadores de estado de energía:** Puede usar temporizadores de estado de energía para suspender máquinas después de que los usuarios se hayan desconectado durante un período

de tiempo especificado. Por ejemplo, las máquinas se suspenderán automáticamente fuera del horario de oficina si los usuarios han estado desconectados durante, al menos, 10 minutos. Las máquinas aleatorias o las máquinas con discos Personal vDisk se apagan automáticamente cuando los usuarios cierran sesión, a menos que se configure la propiedad de grupo de entrega `ShutdownDesktopsAfterUse` en el SDK.

Se pueden configurar temporizadores para los días de la semana y para los fines de semana, para intervalos de horas punta y viceversa.

- **Administración parcial de energía en máquinas de asignación permanente:** En caso de máquinas de asignación permanente, se pueden configurar temporizadores de estado de energía, pero no agrupaciones o búferes. Las máquinas se encienden al comienzo de cada período de mayor actividad (hora punta) y se apagan al comienzo de cada período de actividad normal. De modo que no se tiene un control preciso (como con las máquinas sin asignar) sobre la cantidad de máquinas que pasan a estar disponibles para compensar las máquinas consumidas.

### Administrar la energía de las máquinas virtuales con SO de sesión única

1. Seleccione **Grupos de entrega** en el panel de navegación.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en el panel Acciones.
3. En la página **Administración de energía**, seleccione **Lunes a Viernes** en la lista desplegable **Administrar energía de las máquinas**. De manera predeterminada, se consideran los días de lunes a viernes como los días de la semana.
4. Para grupos de entrega aleatorios, en **Máquinas para iniciar**, seleccione **Modificar** y especifique el tamaño de la agrupación de lunes a viernes. A continuación, seleccione la cantidad de máquinas que quiere iniciar.
5. En **Horas punta**, establezca las horas punta y las horas normales para cada día.
6. Establezca los temporizadores de estado de energía para las horas punta y las horas normales durante los días de la semana. Para ello, en **Durante horas punta > Cuando está desconectado**, especifique la demora (en minutos) que deben transcurrir antes de suspender una máquina desconectada del grupo de entrega y seleccione **Suspender**. En **Durante horas normales > Cuando está desconectado**, especifique la demora que debe transcurrir antes de apagar una máquina del grupo de entrega con la sesión cerrada y seleccione **Apagar**. Este temporizador no está disponible para grupos de entrega con máquinas aleatorias.
7. Seleccione **Fin de semana** en la lista desplegable **Administrar energía de las máquinas** y, a continuación, configure las horas de mayor actividad y los temporizadores de estado de energía para los fines de semana.
8. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta. También puede hacer clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

Use el SDK para:

- Apagar (en lugar de suspender) las máquinas en respuesta a los temporizadores de estado de energía, o si prefiere que los temporizadores se basen en los cierres de sesión en lugar de basarse en las desconexiones.
- Cambiar las definiciones predeterminadas de días de la semana y días de fin de semana.
- Inhabilitar la administración de energía. Consulte [CTX217289](#).

### Administrar la energía de máquinas VDI que pasan a otro período de tiempo con sesiones desconectadas

#### Importante:

Esta mejora solo se aplica a máquinas VDI con sesiones desconectadas. No se aplica a máquinas VDI con sesiones que el usuario ha cerrado.

En versiones anteriores, las máquinas VDI que pasaban a un período de tiempo en el que se requería una acción (acción de desconexión="Suspender" o "Apagar") permanecían encendidas. Este caso se producía si la máquina se desconectaba durante un período de tiempo (horas punta u horas normales) donde no se requería ninguna acción (acción de desconexión="Nada").

A partir de Citrix Virtual Apps and Desktops 7 1909, las máquinas quedan suspendidas o se apagan cuando transcurre el tiempo de desconexión especificado, en función de la acción de desconexión configurada para el período de tiempo de destino.

Por ejemplo, configure las siguientes directivas de energía para un grupo de entrega de VDI:

- Establecer `PeakDisconnectAction` en "Nada"
- Establecer `OffPeakDisconnectAction` en "Apagar"
- Establezca `OffPeakDisconnectTimeout` en "10"

#### Nota:

Para obtener más información sobre la directiva de energía para las acciones de desconexión, consulte [https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about\\_Broker\\_PowerManagement/#power-policy](https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy) y <https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/>.

En versiones anteriores, una máquina VDI con una sesión desconectada durante horas punta permanecía encendida cuando pasaba del período de horas punta al de horas normales. A partir de Citrix Virtual Apps and Desktops 7 1909, las acciones de directiva `OffPeakDisconnectAction` y `OffPeakDisconnectTimeout` se aplican a la máquina VDI al cambiar de período. Como resultado, la máquina se apaga 10 minutos después de pasar a las horas normales.

En caso de que quiera volver al comportamiento anterior (es decir, no realizar ninguna acción en máquinas que pasen de horas punta a horas normales o de horas normales a horas punta con sesiones desconectadas), dispone de varias opciones:

- Establezca el valor del Registro “LegacyPeakTransitionDisconnectedBehaviour” en 1 (true; habilita el comportamiento anterior). De forma predeterminada, el valor es 0 (false; desencadena acciones de directiva de energía para desconexiones al cambiar de período).
  - Ruta: HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\DesktopServer
  - Nombre: LegacyPeakTransitionDisconnectedBehaviour
  - Tipo: REG\_DWORD
  - Datos: 0x00000001 (1)
- Configure el parámetro mediante el comando `Set-BrokerServiceConfigurationData` de PowerShell. Por ejemplo:
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

Las máquinas deben cumplir los siguientes criterios antes de que se puedan aplicar acciones de directiva de energía al cambiar de período:

- Tiene una sesión desconectada.
- No tiene acciones de energía pendientes.
- Pertenece a un grupo de entrega de VDI (sesión única) que pasa a otro período de tiempo.
- Tiene una sesión que se desconecta durante un período de tiempo determinado (horas pico u horas normales) y pasa a un período en el que se asigna una acción de energía.

### **Cambiar el porcentaje de agentes VDA en un estado de energía para catálogos**

1. Ajuste las horas punta del grupo de entrega desde la sección **Administración de energía del grupo de entrega**.
2. Tome nota del nombre del grupo de escritorios.
3. Con privilegios de administrador, inicie PowerShell y ejecute los siguientes comandos. Reemplace “Nombre del grupo de escritorios” con el nombre del grupo de escritorios que tiene un porcentaje cambiado de los VDA en ejecución.

```
asnp Citrix*
```

```
# Set-BrokerDesktopGroup "Desktop Group Name"-PeakBufferSizePercent 100
```

Un valor de 100 significa que el 100% de los VDA están listos.

4. Verifique la solución ejecutando:

```
#Get-BrokerDesktopGroup "Desktop Group Name"
```

```

PS C:\Program Files\Citrix\Desktop Studio> Get-BrokerDesktopGroup "win 7 pvd pol
led"

AdministratorNames           : {}
AutomaticPowerOnForAssigned  : True
ColorDepth                   : TwentyFourBit
Description                   :
DesktopKind                   : Private
DesktopsAvailable            : 0
DesktopsDisconnected         : 0
DesktopsInUse                : 0
DesktopsNeverRegistered      : 0
DesktopsPreparing           : 0
DesktopsUnregistered         : 0
Enabled                       : True
IconUId                      : 1
InMaintenanceMode           : False
Name                          : Win 7 PvD Polled
OffPeakBuffer$izePercent     : 10
OffPeakDisconnectAction      : Nothing
OffPeakDisconnectTimeout     : 0
OffPeakExtendedDisconnectAction : Nothing
OffPeakExtendedDisconnectTimeout : 0
OffPeakLogOffAction         : Nothing
OffPeakLogOffTimeout        : 0
PeakBuffer$izePercent        : 100
PeakDisconnectAction         : Nothing
PeakDisconnectTimeout        : 0
PeakExtendedDisconnectAction : Nothing
PeakExtendedDisconnectTimeout : 0
PeakLogOffAction             : Nothing
PeakLogOffTimeout           : 0
ProtocolPriority              : {}
PublishedName                 : Win 7 PvD Polled
SecureIcaRequired            : False
ShutdownDesktopsAfterUse     : False
Tags                          : {}
TimeZone                     : Eastern Standard Time
TotalDesktops                 : 3
UUID                          : e3854918-420e-4fab-a2b8-1dfb08416d4b
UId                           : 3

PS C:\Program Files\Citrix\Desktop Studio>

```

Puede tardar hasta una hora hasta que los cambios surtan efecto.

Para que se apaguen los VDA después de que el usuario cierre sesión, introduzca:

```
# Set-BrokerDesktopGroup "Desktop Group Name"-ShutdownDesktopsAfterUse
$True
```

Para reiniciar los VDA durante las horas punta y que estén disponibles para los usuarios después de cerrar sesión, introduzca:

```
# Set-BrokerDesktopGroup "Desktop Group Name"-AutomaticPowerOnForAssignedDurin
$True
```

## Sesiones

- [Cerrar o desconectar una sesión, o enviar un mensaje a los usuarios](#)
- Configurar el preinicio y la persistencia de sesiones

### Cerrar sesión o desconectar una sesión

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo de entrega y, a continuación, seleccione **Ver máquinas** en el panel **Acciones**.
3. En el panel central, seleccione la máquina, seleccione **Ver sesiones** en el panel **Acciones** y, a continuación, seleccione una sesión.
  - Alternativamente, en el panel central, seleccione la ficha **Sesión** y, a continuación, seleccione una sesión.
4. Para cerrar la sesión de un usuario, seleccione **Cerrar sesión** en el panel **Acciones**. La sesión se cierra y se cierra también la sesión del usuario. La máquina queda disponible para otros usuarios, a menos que esté asignada a un usuario concreto.
5. Para desconectar una sesión, seleccione **Desconectar** en el panel **Acciones**. Las aplicaciones siguen ejecutándose en la sesión y la máquina permanece asignada a ese usuario. El usuario puede volver a conectarse a la misma máquina.

Puede configurar temporizadores de estado de energía para que las máquinas con SO de sesión única gestionen automáticamente las sesiones que no se estén utilizando. Para obtener información más detallada, consulte Administrar energía de las máquinas.

### Enviar un mensaje a un grupo de entrega

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo de entrega y, a continuación, seleccione **Ver máquinas** en el panel **Acciones**.
3. En el panel central, seleccione una máquina a la que quiera enviar un mensaje.
4. En el panel **Acciones**, seleccione **Ver sesiones**.
5. En el panel central, seleccione todas las sesiones y, a continuación, seleccione **Enviar mensaje** en el panel **Acciones**.
6. Escriba su mensaje y haga clic en **Aceptar**. Puede especificar el nivel de gravedad si es necesario. Las opciones incluyen **Grave**, **Pregunta**, **Advertencia** e **Información**.

También puede enviar un mensaje mediante Citrix Director. Para obtener más información, consulte [Enviar mensajes a usuarios](#).

### Configurar el preinicio de sesiones y la persistencia de sesiones en un grupo de entrega

Estas funciones solo se admiten en máquinas con sistema operativo multisesión.

Las funciones de preinicio de sesiones y persistencia de sesiones ayudan a usuarios concretos a acceder a las aplicaciones con rapidez, al iniciar sesiones antes de solicitarlas (preinicio de sesiones) y al mantener las sesiones de aplicaciones activas después de que un usuario cierra todas las aplicaciones (persistencia de sesiones).

De forma predeterminada, no se usa el preinicio de sesiones ni la persistencia de sesiones. Una sesión comienza cuando el usuario abre una aplicación y permanece activa hasta que la última aplicación abierta en la sesión se cierra.

Consideraciones:

- El grupo de entrega debe admitir aplicaciones, y las máquinas deben estar ejecutando un VDA para SO multisesión, al menos con la versión 7.6.
- Estas funciones se admiten solamente cuando se usa la aplicación Citrix Workspace para Windows, y también necesitan una configuración adicional de la aplicación Citrix Workspace. Para obtener instrucciones, busque preinicio de sesiones en la documentación de producto correspondiente a la versión de la aplicación Citrix Workspace para Windows de que dispone.
- No se admite la aplicación Citrix Workspace para HTML5.
- La función de preinicio de sesiones no funcionará si la máquina de un usuario se pone en los modos suspensión o hibernación (independientemente de la configuración de esa función). Los usuarios pueden bloquear sus máquinas/sesiones. Sin embargo, si un usuario cierra la sesión de la aplicación Citrix Workspace, esa sesión finaliza y la función de preinicio deja de aplicarse.
- Cuando se usa el preinicio de sesiones, las máquinas de clientes físicos no pueden usar las funciones de suspensión o hibernación. Los usuarios de máquinas cliente pueden bloquear sus sesiones, pero no deben cerrarlas.
- Las sesiones preiniciadas y las persistentes utilizan una licencia simultánea, pero solo cuando están conectadas. Si utiliza una licencia de usuario por dispositivo, la licencia dura 90 días. De manera predeterminada y si no se están utilizando, las sesiones preiniciadas y las persistentes se desconectan pasados 15 minutos. Este valor se puede configurar en PowerShell (con el cmdlet `New/Set-BrokerSessionPreLaunch`).
- Una planificación y una supervisión minuciosas de los patrones de actividad de los usuarios son esenciales para adaptar estas funciones y que se complementen entre sí. Una configuración óptima equilibra las ventajas de una disponibilidad más rápida de aplicaciones para los usuarios, por un lado, y el coste del mantenimiento de licencias en uso y recursos asignados, por el otro.
- También puede configurar el preinicio de sesiones para un momento programado del día en la aplicación Citrix Workspace.

**Cuánto tiempo permanecen activas las sesiones preiniciadas y las persistentes** Existen varios métodos para especificar cuánto tiempo se mantiene activa una sesión si el usuario no inicia ninguna aplicación: un tiempo de espera configurado y varios umbrales de carga del servidor. Puede configurarlos todos. El primer evento que tenga lugar pondrá fin a la sesión no utilizada.

- **Tiempo de espera:** El tiempo de espera configurado especifica la cantidad de minutos, horas o días que una sesión preiniciada o persistente permanece activa. Si configura un tiempo de espera demasiado corto, las sesiones preiniciadas terminarán antes de que el usuario se pueda beneficiar de un acceso más rápido a las aplicaciones. Si configura un tiempo de espera demasiado largo, es posible que se denieguen las conexiones entrantes del usuario porque el servidor no tiene recursos suficientes.

Puede habilitar este tiempo de espera solamente desde el SDK (cmdlet `New/Set-BrokerSessionPreLaunch`), no desde la consola de administración. Si inhabilita el tiempo de espera, este no aparece en la pantalla de la consola de ese grupo de entrega ni en las páginas de **Modificar grupo de entrega**.

- **Umbrales:** Finalizar de forma automática sesiones preiniciadas y sesiones persistentes en función de la carga del servidor garantiza que las sesiones permanezcan abiertas el mayor tiempo posible, siempre que el servidor tenga recursos disponibles. Las sesiones preiniciadas y persistentes que no se utilicen no provocan conexiones denegadas porque ambas finalizan de forma automática cuando los recursos sean necesarios para sesiones de usuario nuevas.

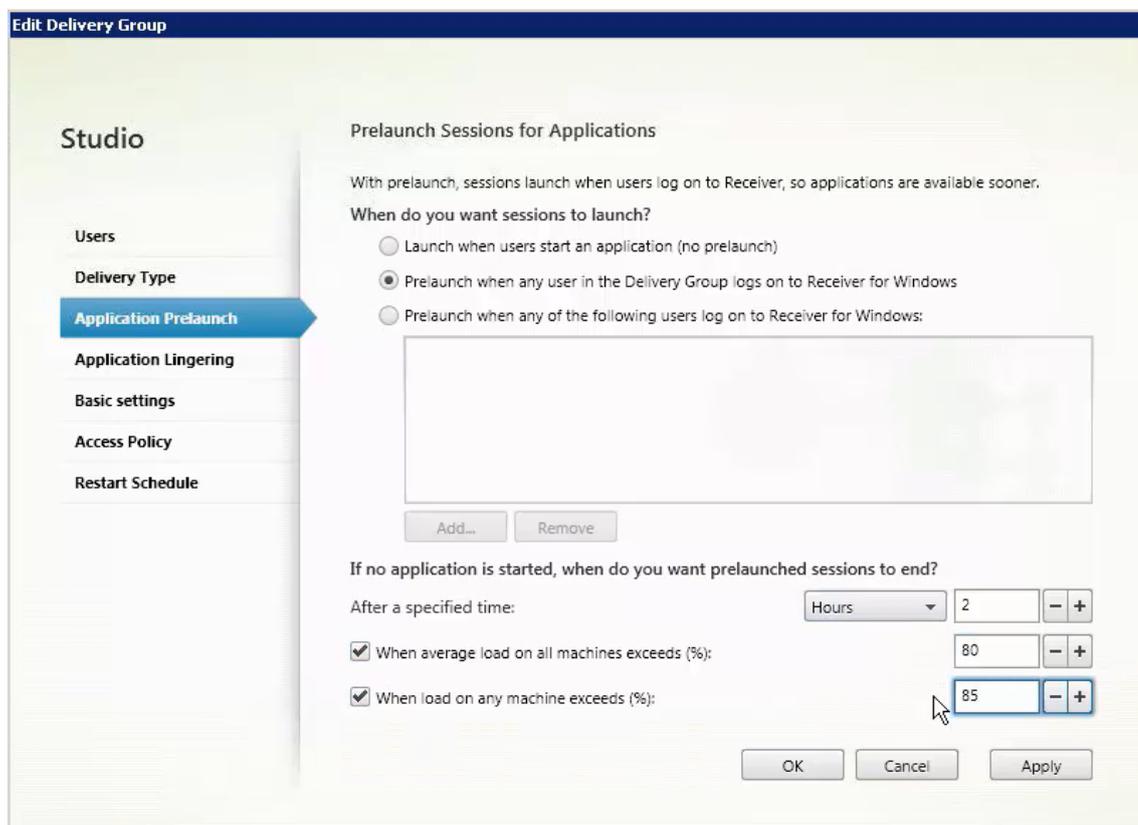
Puede configurar dos umbrales: el porcentaje medio de carga para todos los servidores del grupo de entrega y el porcentaje máximo de carga para un servidor único del grupo de entrega. Cuando se supera un umbral, se finalizan aquellas sesiones que hayan tenido el estado de preinicio o persistente durante más tiempo. Las sesiones se finalizan una a una con intervalos de minutos entre cada cierre hasta que la carga se halle por debajo del umbral. Mientras el umbral permanezca rebasado, no se iniciará ninguna sesión de preinicio.

Los servidores con VDA que no se hayan registrado con el Controller y los servidores en el modo de mantenimiento se consideran servidores con carga completa. Una interrupción no planificada tendrá como consecuencia la finalización automática de sesiones de preinicio y sesiones persistentes para liberar capacidad.

### Para habilitar la función de preinicio de sesiones

1. Seleccione **Grupos de entrega** en el panel de navegación.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en el panel Acciones.
3. En la página **Preinicio de aplicaciones**, habilite el preinicio de sesiones. Para ello, elija cuándo deben iniciarse estas:
  - Cuando un usuario inicia una aplicación. Esta es la opción predeterminada. El preinicio de sesiones está inhabilitado.
  - Cuando un usuario del grupo de entrega inicia sesión en la aplicación Citrix Workspace para Windows.

- Cuando alguien de una lista de usuarios y grupos de usuarios inicia sesión en la aplicación Citrix Workspace para Windows. Si elige esta opción, compruebe que ha especificado también los usuarios o los grupos de usuarios.



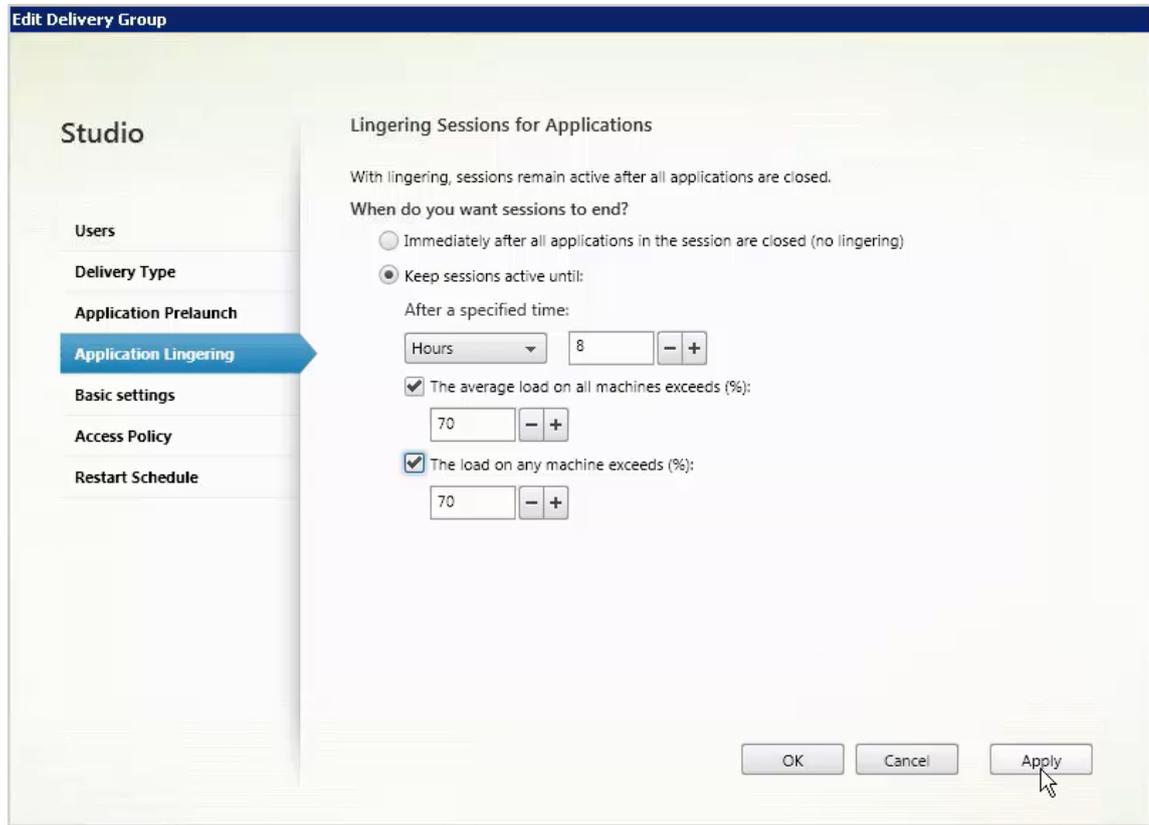
4. Una sesión preiniciada se reemplaza por una sesión habitual cuando el usuario inicia una aplicación. Si el usuario no inicia una aplicación (es decir, la sesión preiniciada no se llega a utilizar), la siguiente configuración afecta a la cantidad de tiempo que esta sesión permanece activa.
  - Cuando se agota un intervalo de tiempo especificado. Puede cambiar el intervalo de tiempo (de 1-99 días, de 1-2376 horas, o de 1-142 560 minutos).
  - Cuando el promedio de carga de todas las máquinas del grupo de entrega supera un porcentaje especificado (del 1-99%).
  - Cuando la carga de una máquina del grupo de entrega supera un porcentaje especificado (del 1-99%).

En resumen, una sesión preiniciada permanece activa hasta que se da uno de los siguientes eventos: un usuario inicia una aplicación, se agota el tiempo especificado, o se supera un umbral de carga especificado.

### Para habilitar la persistencia de sesiones

1. Seleccione **Grupos de entrega** en el panel de navegación.

2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en el panel Acciones.
3. En la página **Persistencia de aplicaciones**, habilite la persistencia de sesiones seleccionando la opción **Mantener las sesiones activas hasta**.



4. Algunos parámetros influyen en la cantidad de tiempo que las sesiones persistentes pueden permanecer activas si el usuario no inicia otra aplicación.
  - Cuando se agota un intervalo de tiempo especificado. Puede cambiar el intervalo de tiempo: de 1-99 días, de 1-2376 horas, o de 1-142 560 minutos.
  - Cuando el promedio de carga de todas las máquinas del grupo de entrega supera un porcentaje especificado: 1-99%.
  - Cuando la carga de una máquina del grupo de entrega supera un porcentaje especificado: del 1-99%.

En resumen, una sesión persistente permanece activa hasta que se da uno de los siguientes eventos: un usuario inicia una aplicación, se agota el tiempo especificado, o se supera un umbral de carga especificado.

## Solución de problemas

- Los VDA no registrados en un Delivery Controller no se tienen en cuenta cuando se inicien sesiones con intermediario. Esto provoca una infrutilización de los recursos disponibles. Existen diversos motivos por los que un VDA puede no registrarse, y un administrador puede solucionar muchos de ellos. Para solucionar problemas, los detalles proporcionan información en el Asistente para la creación de catálogos y después de agregar el catálogo a un grupo de entrega.

Tras crear un grupo de entrega, el recuadro Detalles de dicho grupo indica la cantidad de máquinas que deberían estar registradas pero no se han registrado. Por ejemplo, una o varias máquinas que están activadas y no están en modo de mantenimiento, pero no están actualmente registradas en el Controller. Al ver una máquina que “no está registrada, pero debería estarlo”, consulte la ficha **Solución de problemas** del panel de detalles para buscar las posibles causas y las acciones correctivas recomendadas.

Para ver los mensajes sobre el nivel funcional, consulte [Niveles funcionales y versiones de VDA](#).

Para obtener información sobre la solución de problemas de registro de VDA, consulte [CTX136668](#).

- En la pantalla de un grupo de entrega, la **versión instalada de VDA** del recuadro Detalles puede ser diferente de la versión real instalada en las máquinas. La pantalla Programas y características de la máquina Windows muestra la versión real del VDA.
- Para máquinas que presentan un **Estado de energía desconocido**, consulte [CTX131267](#) para obtener instrucciones.

## Crear grupos de aplicaciones

September 22, 2021

### Introducción

Los grupos de aplicaciones permiten administrar colecciones de aplicaciones. Puede crear grupos de aplicaciones para las aplicaciones compartidas entre varios grupos de entrega o que son utilizadas por un subconjunto de usuarios dentro de un grupo de entrega. Los grupos de aplicaciones son optativos: ofrecen una alternativa para no tener que agregar las mismas aplicaciones a varios grupos de entrega. Los grupos de entrega se pueden asociar a varios grupos de aplicaciones, y un grupo de aplicaciones puede estar asociado a varios grupos de entrega.

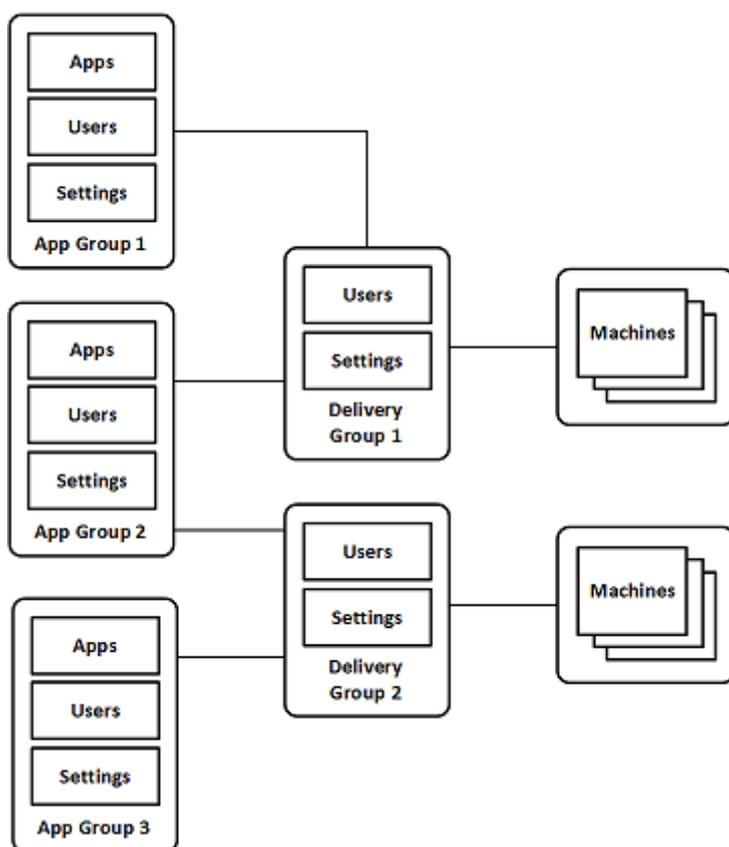
El uso de grupos de aplicaciones puede proporcionar ventajas para la administración de aplicaciones y para el control de los recursos frente a la opción de grupos de entrega:

- La agrupación lógica de las aplicaciones y sus parámetros permite administrar esas aplicaciones como una sola unidad. Por ejemplo, no tiene que agregar (publicar) la misma aplicación en grupos de entrega individuales de uno en uno.
- Compartir sesiones entre grupos de aplicaciones puede reducir el consumo de los recursos. En otros casos, la inhabilitación del uso compartido de sesiones entre grupos de aplicaciones puede ser beneficioso.
- Puede usar la función de restricción por etiquetas para publicar aplicaciones desde un grupo de aplicaciones, con lo que solo se tiene en cuenta un subconjunto de las máquinas que contienen los grupos de entrega seleccionados. Con una restricción por etiquetas, puede usar las máquinas existentes para más de una tarea de publicación, con lo que se ahorran los costes asociados a la implementación y la administración de máquinas adicionales. La restricción de etiqueta puede entenderse como una subdivisión (o partición) de las máquinas de un grupo de entrega. Usar un grupo de aplicaciones o escritorios con una restricción de etiqueta puede ser útil para aislar un subconjunto de las máquinas de un grupo de entrega y solucionar los problemas que presentan.

## **Ejemplos de configuración**

### **Ejemplo 1:**

El gráfico siguiente muestra una implementación de Citrix Virtual Apps and Desktops que incluye grupos de aplicaciones:



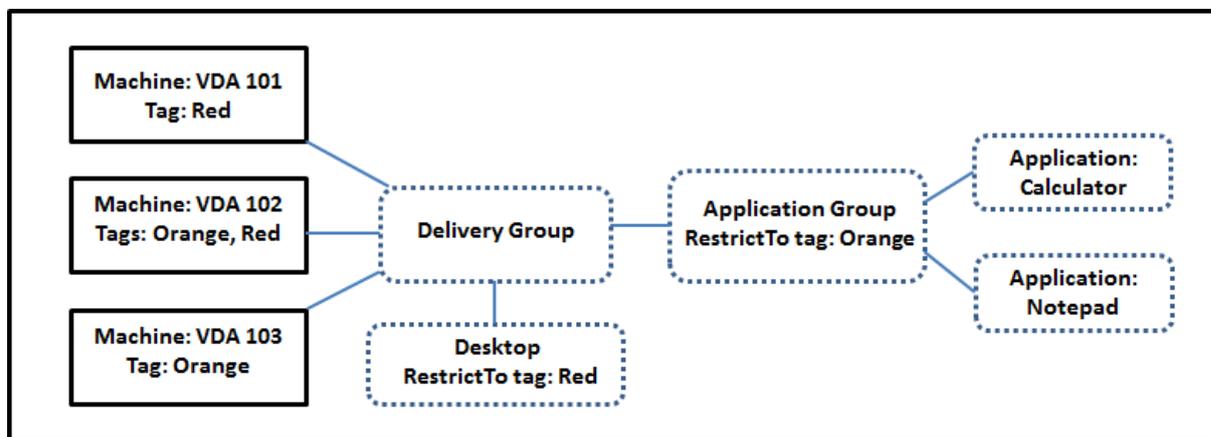
En esta configuración, las aplicaciones se agregan a los grupos de aplicaciones no a los grupos de entrega. Los grupos de entrega especifican qué máquinas se usarán. (Aunque no se muestra, las máquinas se encuentran en catálogos de máquinas.)

El grupo de aplicaciones 1 está asociado al grupo de entrega 1. A las aplicaciones del Grupo de aplicaciones 1 tienen acceso los usuarios especificados en el Grupo de aplicaciones 1, siempre y cuando también estén en la lista de usuarios del Grupo de entrega 1. Esto es conforme a la recomendación de que la lista de usuarios de un grupo de aplicaciones debe ser un subconjunto (una restricción) de la lista de usuarios del grupo de entrega asociado. Los parámetros del Grupo de aplicaciones 1 (tales como el uso compartido de sesiones entre grupos de aplicaciones y los grupos de entrega asociados) se aplican a las aplicaciones y los usuarios de ese grupo. Los parámetros del Grupo de entrega 1 (tales como la funcionalidad para usuarios anónimos) se aplican a los usuarios de los grupos de aplicaciones 1 y 2, porque esos grupos de aplicaciones se han asociado a ese grupo de entrega.

El Grupo de aplicaciones 2 está asociado a dos grupos de entrega: 1 y 2. Se puede asignar una prioridad a cada uno de esos grupos de entrega en el Grupo de aplicaciones 2, para indicar el orden en que se comprobarán los grupos de entrega cuando se inicie una aplicación. Si los grupos de entrega tienen la misma prioridad, se les aplica el equilibrio de carga. A las aplicaciones del Grupo de aplicaciones 2 tienen acceso los usuarios especificados en el Grupo de aplicaciones 2, siempre y cuando también estén en la lista de usuarios de los grupos de entrega 1 y 2.

**Ejemplo 2:**

En esta sencilla distribución, se usan restricciones por etiqueta para limitar las máquinas que se tendrán en cuenta para ciertos inicios de aplicaciones y escritorios. El sitio tiene un grupo de entrega compartido, un escritorio publicado, y un grupo de aplicaciones configurado con dos aplicaciones.



Se han agregado etiquetas a cada una de las tres máquinas (VDA 101, 102 y 103).

El grupo de aplicaciones se creó con la restricción de etiqueta “Naranja”, por lo que cada una de sus aplicaciones (Calculadora y Bloc de notas) solo se pueden iniciar en las máquinas de ese grupo de entrega que tengan la etiqueta “Naranja”: VDA 102 y 103.

Para ver instrucciones y ejemplos más detallados sobre cómo usar las restricciones de etiqueta en los grupos de aplicaciones (y escritorios), consulte [Etiquetas](#).

**Información orientativa y consideraciones**

Citrix recomienda agregar aplicaciones a grupos de aplicaciones o grupos de entrega, pero no a ambos. De lo contrario, la complejidad de tener las aplicaciones asignadas a dos tipos de grupos puede complicar la administración de estas.

De forma predeterminada, hay un grupo de aplicaciones habilitado. Después de crear un grupo de aplicaciones, puede modificar el grupo para cambiar este parámetro. Consulte [Administrar grupos de aplicaciones](#).

De forma predeterminada, se pueden compartir sesiones entre grupos de aplicaciones. Consulte [Compartir sesiones entre grupos de aplicaciones](#).

Citrix recomienda que los grupos de entrega se actualicen a la versión actual. Eso requiere:

1. Actualizar la versión de los VDA de las máquinas utilizadas en el grupo de entrega.
2. Actualizar la versión de los catálogos que contienen esas máquinas.
3. Actualizar la versión del grupo de entrega.

Para obtener más información, consulte [Administrar grupos de entrega](#).

Para utilizar grupos de aplicaciones, los componentes principales deben tener la versión 7.9 como mínimo.

La creación de grupos de aplicaciones requiere el permiso de administración delegada correspondiente al rol integrado de Administrador de grupos de entrega. Para obtener información más detallada, consulte [Administración delegada](#).

Este artículo se refiere a la “asociación” de una aplicación con varios grupos de aplicaciones para diferenciarla de la acción de agregar una nueva instancia de esa aplicación desde algún origen disponible. Del mismo modo, los grupos de entrega se asocian a grupos de aplicaciones (y viceversa), en lugar de ser agregados como componentes unos de otros.

## Compartir sesiones con grupos de aplicaciones

Cuando se habilita la capacidad de compartir sesiones de aplicación, todas las aplicaciones se inician en la misma sesión de aplicación. Lo que reduce los costes asociados al inicio de aplicaciones adicionales y permite las funciones de aplicación que hacen uso del Portapapeles, como las operaciones de copiar y pegar contenido. Sin embargo, podría interesarle desactivar el uso compartido de sesiones en algunas situaciones.

Cuando se usan grupos de aplicaciones, se puede configurar el uso compartido de las sesiones de aplicación de las siguientes tres maneras (que amplían el comportamiento estándar del uso compartido de sesiones que solo está disponible cuando se usan grupos de entrega):

- Uso compartido de sesiones habilitado entre grupos de aplicaciones.
- Uso compartido de sesiones habilitado solamente entre las aplicaciones de un mismo grupo de aplicaciones.
- Uso compartido de sesiones inhabilitado.

## Compartir sesiones entre grupos de aplicaciones

Puede permitir que las sesiones de aplicaciones se compartan entre los grupos de aplicaciones, o bien, puede inhabilitarlo para limitar la capacidad de compartir sesiones solo a las aplicaciones que se encuentren en el mismo grupo de aplicaciones.

- **Este es un ejemplo de cuándo puede ser útil habilitar el uso compartido de sesiones entre los grupos de aplicaciones:**

El grupo de aplicaciones 1 contiene aplicaciones de Microsoft Office como Word y Excel. El grupo de aplicaciones 2 contiene otras aplicaciones (como el Bloc de notas y la Calculadora), y ambos grupos de aplicaciones están conectados al mismo grupo de entrega. Un usuario que tiene

acceso a ambos grupos de aplicaciones inicia una sesión de aplicación mediante Word y, a continuación, el Bloc de notas. Si el Controller cree que la sesión existente del usuario que ejecuta Word es adecuada para ejecutar el Bloc de notas, el Bloc de notas se iniciará dentro de la sesión existente. En cambio, si el Bloc de notas no se puede ejecutar en la sesión existente (por ejemplo, si la restricción por etiquetas excluye la máquina donde se ejecuta la sesión), se crea una nueva sesión en otra máquina, en lugar de compartir sesiones.

- **Este es un ejemplo de cuándo puede ser útil inhabilitar el uso compartido de sesiones entre los grupos de aplicaciones:**

Tiene un conjunto de aplicaciones que no pueden interactuar correctamente con otras aplicaciones instaladas en las mismas máquinas: por ejemplo, dos versiones diferentes de una misma suite de software o dos versiones diferentes del mismo explorador web. Usted prefiere no permitir que un usuario inicie ambas versiones en una misma sesión.

Puede crear un grupo de aplicaciones para cada versión de la suite de software y agregar las aplicaciones para cada versión de la suite al grupo de aplicaciones correspondiente. Si el uso compartido de sesiones entre los grupos se inhabilita para cada uno de esos grupos de aplicaciones, un usuario especificado en esos grupos puede ejecutar las aplicaciones de la misma versión en la misma sesión, y puede ejecutar otras aplicaciones al mismo tiempo, pero no en la misma sesión. Si el usuario inicia una de las aplicaciones de diferente versión (que se encuentra en un grupo de aplicaciones distinto) o inicia cualquier aplicación que no está contenida en un grupo de aplicaciones, esa aplicación se inicia en una nueva sesión.

Compartir sesiones entre los grupos de aplicaciones no es una función de seguridad de un espacio aislado. No es totalmente segura y no puede impedir que los usuarios inicien aplicaciones en sus sesiones por otros medios (por ejemplo, a través del Explorador de Windows).

Si una máquina alcanza su capacidad máxima, no se inician nuevas sesiones en ella. Las nuevas aplicaciones se inician en las sesiones existentes en la máquina compartiendo sesiones si fuera necesario (siempre que eso concuerde con las restricciones respecto a compartir sesiones que se describen aquí).

Solo se pueden ofrecer las sesiones preiniciadas a los grupos de aplicaciones que tienen permitido compartir sesiones (Las sesiones que usan la funcionalidad Persistencia de sesiones están disponibles a todos los grupos de aplicaciones.) Esas funciones deben habilitarse y configurarse en cada uno de los grupos de entrega asociados al grupo de aplicaciones; no se pueden configurar en los grupos de aplicaciones.

De forma predeterminada, se pueden compartir sesiones entre grupos de aplicaciones cuando se crea un grupo de aplicaciones. No puede cambiar esto cuando crea el grupo. Después de crear un grupo de aplicaciones, puede modificar el grupo para cambiar este parámetro. Consulte [Administrar grupos de aplicaciones](#).

## Inhabilitar el uso compartido de sesiones en un grupo de aplicaciones

Puede impedir que las aplicaciones que se encuentran en el mismo grupo compartan sesiones.

- **Este es un ejemplo de cuándo puede ser útil impedir que se compartan sesiones entre los grupos de aplicaciones:**

Si quiere que los usuarios accedan a varias sesiones simultáneas de pantalla completa de una aplicación en varios monitores.

Cree un grupo de aplicaciones y agréguele las aplicaciones. Si las aplicaciones de ese grupo no pueden compartir sesiones, cuando un usuario especificado en el grupo inicia una aplicación y después otra, las aplicaciones se inician en sesiones distintas y el usuario puede mover cada una a un monitor aparte.

De forma predeterminada, se pueden compartir sesiones entre grupos de aplicaciones cuando se crea un grupo de aplicaciones. No puede cambiar esto cuando crea el grupo. Después de crear un grupo de aplicaciones, puede modificar el grupo para cambiar este parámetro. Consulte [Administrar grupos de aplicaciones](#).

## Crear un grupo de aplicaciones

Para crear un grupo de aplicaciones:

1. Seleccione **Aplicaciones** en el panel de navegación de Studio y, a continuación, seleccione **Crear grupo de aplicaciones** en el panel Acciones.
2. El asistente Crear grupo de aplicaciones se inicia con la página **Introducción**, que se puede eliminar de futuros inicios de este asistente.
3. El asistente le guiará a través de las páginas que se describen a continuación. Cuando haya terminado con cada página, haga clic en **Siguiente** hasta llegar a la página Resumen.

### Paso 1. Grupos de entrega

La página **Grupos de entrega** muestra todos los grupos de entrega, con la cantidad de máquinas que contiene cada grupo.

- La lista **Grupos de entrega compatibles** contiene los grupos de entrega que puede seleccionar. Los grupos de entrega compatibles contienen máquinas aleatorias (no asignadas de forma permanente o estática) de SO multisesión o de sesión única.
- La lista **Grupos de entrega incompatibles** contiene grupos de entrega que no puede seleccionar. Cada entrada explica por qué no es compatible, como, por ejemplo, porque contienen máquinas asignadas estáticas.

Un grupo de aplicaciones se puede asociar a grupos de entrega que contengan máquinas compartidas (no privadas) que puedan entregar aplicaciones.

También puede seleccionar grupos de entrega que contengan máquinas compartidas que solo entregan escritorios, siempre que se cumplan las dos condiciones siguientes:

- El grupo de entrega contiene máquinas compartidas y se creó con una versión de XenDesktop anterior a 7.9.
- Usted tiene el permiso Modificar grupo de entrega.

El tipo de grupo de entrega se convierte automáticamente a “escritorios y aplicaciones” cuando se confirma el asistente Crear grupo de aplicaciones.

Aunque puede crear un grupo de aplicaciones que no tenga grupos de entrega asociados (por ejemplo, para organizar aplicaciones o para servir de almacenamiento para las aplicaciones que no se están utilizando en ese momento), el grupo de aplicaciones no se puede usar para entregar aplicaciones hasta que se especifica al menos un grupo de entrega. Además, no se pueden agregar aplicaciones al grupo de aplicaciones desde la opción de origen **Desde el menú Inicio** si no hay grupos de entrega especificados.

Los grupos de entrega que seleccione especifican las máquinas que se usarán para entregar aplicaciones. Marque las casillas que aparecen junto a los grupos de entrega que quiere asociar al grupo de aplicaciones.

Para agregar una restricción por etiquetas, elija **Restringir inicios a máquinas con la etiqueta** y, a continuación, seleccione la etiqueta en el menú desplegable.

## **Paso 2. Usuarios**

Especifique quién puede usar las aplicaciones del grupo de aplicaciones. Puede permitir todos los usuarios y los grupos de usuarios de los grupos de entrega seleccionados en la página anterior, o puede seleccionar un grupo específico de usuarios y grupos de usuarios de los grupos de entrega. Si restringe el uso a unos cuantos usuarios especificados, solo los usuarios especificados en el grupo de entrega y el grupo de aplicaciones pueden acceder a las aplicaciones de este grupo de aplicaciones. Básicamente, la lista de usuarios del grupo de aplicaciones proporciona un filtro en las listas de usuarios de los grupos de entrega.

El uso de las aplicaciones por parte de usuarios no autenticados solo puede habilitarse o inhabilitarse en los grupos de entrega, no en los grupos de aplicaciones.

Para obtener información sobre dónde se especifican las listas de usuarios en una implementación, consulte [Dónde se especifican las listas de usuarios](#).

### Paso 3. Aplicaciones

Información útil:

- De forma predeterminada, las nuevas aplicaciones que agregue se colocan en una carpeta denominada **Applications**. Puede especificar otra carpeta. Si intenta agregar una aplicación y ya existe una con el mismo nombre en la carpeta, se le pedirá cambiar el nombre de la aplicación que está agregando. Si acepta el nombre único sugerido, la aplicación se agrega con ese nombre. De lo contrario, cambie el nombre antes de agregarla. Para obtener más información, consulte [Administrar carpetas de aplicaciones](#).
- Puede cambiar las propiedades de una aplicación (parámetros) al agregarla, o más tarde. Consulte [Cambiar las propiedades de la aplicación](#). Si publica dos aplicaciones con el mismo nombre para los mismos usuarios, cambie la propiedad **Nombre de la aplicación (para el usuario)** en Studio. De lo contrario, los usuarios verán nombres duplicados en la aplicación Citrix Workspace.
- Al agregar una aplicación a más de un grupo de entrega, puede haber un problema de visibilidad si no dispone de permisos suficientes para ver la aplicación en todos esos grupos de entrega. En tales casos, consulte a un administrador con más permisos o amplíe su ámbito para incluir todos los grupos a los que se haya agregado la aplicación.

Haga clic en la lista desplegable **Agregar** para ver los orígenes de aplicación.

- **Desde el menú Inicio:** Se trata de las aplicaciones que se detectan en una máquina de los grupos de entrega seleccionados. Cuando se selecciona este origen, se abre una nueva página con una lista de aplicaciones detectadas. Marque las casillas de verificación de las aplicaciones que quiere agregar y, a continuación, haga clic en **Aceptar**.

Este origen no se puede seleccionar si seleccionó una de estas opciones:

- Grupos de aplicaciones que no tienen grupos de entrega asociados.
  - Grupos de aplicaciones con grupos de entrega asociados que no contienen máquinas.
  - Un grupo de entrega que no contiene máquinas.
- **Definidas manualmente:** Se trata de las aplicaciones que se encuentran en el sitio o en la red. Cuando se selecciona este origen, se abre una nueva página donde se escribe la ruta al archivo ejecutable, al directorio de trabajo, los argumentos de línea de comandos opcionales y los nombres simplificados para administradores y usuarios. Después de introducir la información, haga clic en **Aceptar**.
  - **Existentes:** Se trata de aplicaciones agregadas anteriormente al sitio. Cuando se selecciona este origen, se abre una nueva página con una lista de aplicaciones detectadas. Marque las casillas de verificación de las aplicaciones que quiere agregar y, a continuación, haga clic en **Aceptar**. Este origen no se puede seleccionar si el sitio no contiene ninguna aplicación.

- **App-V:** Se trata de las aplicaciones presentes en paquetes de App-V. Cuando se selecciona este origen, se abre una nueva página donde se puede seleccionar el servidor de App-V o la biblioteca de aplicaciones. En la pantalla resultante, marque las casillas de las aplicaciones que quiere agregar y, a continuación, haga clic en **Aceptar**. Para obtener más información, consulte [App-V](#). Este origen no se puede seleccionar (o no aparece) si App-V no está configurado en el sitio.

Como se ha indicado, algunas de las entradas de la lista desplegable **Agregar** no se pueden seleccionar si no existe ningún origen válido de ese tipo. Los orígenes que son incompatibles no aparecen (por ejemplo, no se pueden agregar grupos de aplicaciones a grupos de aplicaciones, por lo que ese origen no aparece en la lista cuando se crea un grupo de aplicaciones).

#### Paso 4. Ámbitos

Esta página aparecerá solo si se ha creado antes un ámbito personalizado. De forma predeterminada, está seleccionado el ámbito **Todo**. Para obtener más información, consulte [Administración delegada](#).

#### Paso 5. Resumen

Escriba un nombre para el grupo de aplicaciones. También puede especificar una descripción (opcativa).

Revise la información de resumen y, a continuación, haga clic en **Finalizar**.

## Administrar grupos de aplicaciones

September 22, 2021

Nota:

Cuando se utilizan grupos de aplicaciones con Citrix Virtual Apps and Desktops Service, la función de restricción por etiqueta no está disponible por el momento.

### Introducción

En este artículo, se describe cómo administrar grupos de aplicaciones después de [crearlos](#).

Consulte el artículo [Aplicaciones](#) para obtener información sobre cómo administrar aplicaciones en los grupos de entrega o los grupos de aplicaciones, incluido cómo:

- Agregar o quitar aplicaciones en un grupo de aplicaciones.

- Cambiar asociaciones de grupos de aplicaciones.

La administración de grupos de aplicaciones requiere los permisos de administración delegada correspondientes al rol integrado de Administrador de grupos de entrega. Para obtener información más detallada, consulte [Administración delegada](#).

## Habilitar o inhabilitar un grupo de aplicaciones

Cuando se habilita un grupo de aplicaciones, este grupo puede distribuir las aplicaciones que se hayan agregado a él. Cuando se inhabilita un grupo de aplicaciones, se inhabilitan las aplicaciones incluidas en él. Sin embargo, si esas aplicaciones también están asociadas a otros grupos de aplicaciones que sí están habilitados, esas aplicaciones pueden seguir siendo entregadas desde esos otros grupos. Del mismo modo, si las aplicaciones se agregaron explícitamente a grupos de entrega asociados al grupo de aplicaciones (además de agregarlas al grupo de aplicaciones), cuando se inhabilita el grupo de aplicaciones esto no afecta a esas aplicaciones agregadas a esos grupos de entrega.

Un grupo de aplicaciones está habilitado cuando se crea. No puede cambiar esto cuando crea el grupo.

1. Seleccione **Aplicaciones** en el panel de navegación de Studio.
2. Seleccione el grupo de aplicaciones en el panel central y, a continuación, seleccione **Modificar grupo de aplicaciones** en el panel Acciones.
3. En la página **Parámetros**, marque o desmarque la casilla **Habilitar grupo de aplicaciones**.
4. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta, o bien haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

## Habilitar o inhabilitar el uso compartido de sesiones de aplicación entre grupos de aplicaciones

Se pueden compartir sesiones entre grupos de aplicaciones cuando se crea un grupo de aplicaciones. No puede cambiar esto cuando crea el grupo. Para obtener más información, consulte [Compartir sesiones con grupos de aplicaciones](#).

1. Seleccione **Aplicaciones** en el panel de navegación de Studio.
2. Seleccione el grupo de aplicaciones en el panel central y, a continuación, seleccione **Modificar grupo de aplicaciones** en el panel Acciones.
3. En la página **Parámetros**, marque o desmarque la casilla **Habilitar uso compartido de sesiones de aplicaciones entre grupos de aplicaciones**.
4. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta, o bien haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

## Inhabilitar el uso compartido de sesiones de aplicación en un grupo de aplicaciones

De forma predeterminada, se pueden compartir sesiones de aplicaciones en el mismo grupo de aplicaciones cuando se crea un grupo de aplicaciones. Aunque inhabilite la posibilidad de compartir sesiones de aplicaciones entre grupos de aplicaciones, se podrán compartir sesiones entre aplicaciones del mismo grupo.

Puede usar el SDK de PowerShell para configurar grupos de aplicaciones con el uso compartido de sesiones inhabilitado entre las aplicaciones que contienen. En algunas circunstancias, esto puede ser conveniente. Por ejemplo, si quiere que los usuarios inicien aplicaciones no integradas en ventanas de aplicación de pantalla completa en monitores diferentes.

Cuando se inhabilita el uso compartido de sesiones dentro de un grupo de aplicaciones, cada aplicación de ese grupo se inicia en una nueva sesión de aplicación. Si está disponible una sesión desconectada adecuada (que ejecuta la misma aplicación), se vuelve a conectar a esa sesión. Por ejemplo, si se inicia el Bloc de notas y hay una sesión desconectada que ejecuta el Bloc de notas, se reconecta a esa sesión en lugar de crear una nueva. Si están disponibles varias sesiones desconectadas adecuadas, se elige una de ellas para reconectarse de forma aleatoria pero determinante. En otras palabras, si se vuelve a dar la situación en las mismas circunstancias, se selecciona la misma sesión, pero la elección no es necesariamente predecible en otras circunstancias.

Puede usar el SDK de PowerShell para inhabilitar el uso compartido de sesiones de aplicación para todas las aplicaciones de un grupo de existente, o bien, para crear un grupo de aplicaciones con el uso compartido de sesiones inhabilitado.

### Ejemplos de cmdlets de PowerShell

Para inhabilitar el uso compartido de sesiones, use los cmdlets de Broker PowerShell `New-BrokerApplicationGroup` o `Set-BrokerApplicationGroup` con el parámetro `SessionSharingEnabled` establecido en `False` y el parámetro `SingleAppPerSession` establecido en `True`.

- Por ejemplo, para crear un grupo de aplicaciones con el uso compartido de sesiones de aplicación inhabilitado para todas las aplicaciones del grupo:

```
New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False -SingleAppPerSession $True
```

- Por ejemplo, para inhabilitar el uso compartido de sesiones de aplicación entre todas las aplicaciones de un grupo de aplicaciones existente:

```
Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False -SingleAppPerSession $True
```

## Consideraciones

- Para habilitar la propiedad `SingleAppPerSession`, debe establecer la propiedad `SessionSharingEnabled` en `False`. No se deben habilitar las dos propiedades al mismo tiempo. El parámetro `SessionSharingEnabled` hace referencia a compartir sesiones entre grupos de aplicaciones.
- Compartir sesiones solo funciona para aplicaciones que están asociadas a grupos de aplicaciones, pero no están asociadas a grupos de entrega. (Todas las aplicaciones asociadas directamente a un grupo de entrega comparten sesiones de forma predeterminada.)
- Si una aplicación se asigna a varios grupos de aplicaciones, compruebe que los grupos no tienen parámetros en conflicto. Por ejemplo, un grupo tiene la opción establecida en `True`, mientras que el otro en `False`, lo que resulta en un comportamiento inesperado.

## Cambiar el nombre de un grupo de aplicaciones

1. Seleccione **Aplicaciones** en el panel de navegación de Studio.
2. Seleccione el grupo de aplicaciones en el panel central y, a continuación, seleccione **Cambiar nombre de grupo de aplicaciones** en el panel Acciones.
3. Especifique un nuevo nombre único y, a continuación, haga clic en **Aceptar**.

## Agregar, quitar o cambiar la prioridad de las asociaciones de grupos de entrega con un grupo de aplicaciones

Un grupo de aplicaciones se puede asociar a grupos de entrega que contengan máquinas compartidas (no privadas) que puedan entregar aplicaciones.

También puede seleccionar grupos de entrega que contengan máquinas compartidas que solo entregan escritorios, siempre que se cumplan las dos condiciones siguientes:

- El grupo de entrega contiene máquinas compartidas y se creó con una versión anterior a 7.9.
- Usted tiene el permiso Modificar grupo de entrega.

El tipo de grupo de entrega se convierte automáticamente a “escritorios y aplicaciones” cuando se confirma el cuadro de diálogo Modificar grupo de aplicaciones.

1. Seleccione **Aplicaciones** en el panel de navegación de Studio.
2. Seleccione el grupo de aplicaciones en el panel central y, a continuación, seleccione **Modificar grupo de aplicaciones** en el panel Acciones.
3. Seleccione la página **Grupos de entrega**.
4. Para agregar grupos de entrega, haga clic en **Agregar**. Marque las casillas de los grupos de entrega disponibles (los grupos de entrega incompatibles no se pueden seleccionar). Cuando termine de seleccionarlos, haga clic en **Aceptar**.

5. Para eliminar grupos de entrega, marque las casillas de los grupos que quiere eliminar y luego haga clic en **Eliminar**. Confirme la eliminación cuando se le solicite.
6. Para cambiar la prioridad de un grupo de entrega, seleccione ese grupo y, a continuación, haga clic en **Modificar prioridad**. Especifique una prioridad (0 = máxima prioridad) y, a continuación, haga clic en **Aceptar**.
7. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta, o bien haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

### **Agregar, modificar o quitar una restricción de etiqueta en un grupo de aplicaciones**

Agregar, modificar o quitar restricciones por etiqueta puede tener efectos no esperados en las máquinas que se tengan en cuenta para iniciar las aplicaciones. Consulte las precauciones y los aspectos a tener en cuenta en [Etiquetas](#).

1. Seleccione **Aplicaciones** en el panel de navegación de Studio.
2. Seleccione el grupo de aplicaciones en el panel central y, a continuación, seleccione **Modificar grupo de aplicaciones** en el panel Acciones.
3. Seleccione la página **Grupos de entrega**.
4. Para agregar una restricción por etiquetas, elija **Restringir inicios a máquinas con la etiqueta** y, a continuación, seleccione la etiqueta en el menú desplegable.
5. Para cambiar o quitar una restricción de etiqueta, seleccione otra etiqueta de la lista desplegable o quite la restricción de etiqueta por completo desmarcando **Restringir inicios a máquinas con la etiqueta**.
6. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta, o bien haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

### **Agregar o quitar usuarios de un grupo de aplicaciones**

Para obtener más información acerca de los usuarios, consulte [Crear grupos de aplicaciones](#).

1. Seleccione **Aplicaciones** en el panel de navegación de Studio.
2. Seleccione el grupo de aplicaciones en el panel central y, a continuación, seleccione **Modificar grupo de aplicaciones** en el panel Acciones.
3. Seleccione la página **Usuarios**. Indique si quiere permitir que todos los usuarios de los grupos de entrega asociados usen las aplicaciones del grupo de aplicaciones, o si solo quiere que la usen grupos y usuarios específicos. Para agregar usuarios, haga clic en **Agregar** y especifique los usuarios que quiere agregar. Para quitar usuarios, seleccione uno o varios usuarios y, a continuación, haga clic en **Quitar**.
4. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta, o bien haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

## Cambiar ámbitos en un grupo de aplicaciones

Puede cambiar un ámbito solo si usted lo ha creado (no puede modificar el ámbito Todo). Para obtener más información, consulte [Administración delegada](#).

1. Seleccione **Aplicaciones** en el panel de navegación de Studio.
2. Seleccione el grupo de aplicaciones en el panel central y, a continuación, seleccione **Modificar grupo de aplicaciones** en el panel Acciones.
3. Seleccione la página **Ámbitos**. Marque o deje sin marcar la casilla correspondiente a un ámbito.
4. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta, o bien haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

## Eliminar un grupo de aplicaciones

La aplicación debe estar asociada con, al menos, un grupo de entrega o un grupo de aplicaciones. Si eliminar un grupo de aplicaciones provocará que una o varias aplicaciones dejen de pertenecer a un grupo, se le advertirá que, al eliminar el grupo, también se eliminarán esas aplicaciones. Entonces, puede confirmar o cancelar la eliminación.

Eliminar una aplicación aquí no la elimina de su lugar de origen. Sin embargo, si quiere que la aplicación vuelva a estar disponible, tendrá que volver a agregarla.

1. Seleccione **Aplicaciones** en el panel de navegación de Studio.
2. Seleccione el grupo de aplicaciones en el panel central y, a continuación, seleccione **Eliminar grupo** en el panel Acciones.
3. Confirme la eliminación cuando se le solicite.

## Acceso con Remote PC

June 27, 2024

Acceso con Remote PC es una funcionalidad de Citrix Virtual Apps and Desktops, gracias a la cual las organizaciones pueden hacer que sus empleados accedan fácilmente a los recursos corporativos de forma remota y segura. La plataforma Citrix hace posible este acceso seguro al proporcionar a los usuarios acceso a sus PC físicos de oficina. Si los usuarios pueden acceder a sus PC de oficina, pueden acceder a todas las aplicaciones, datos y recursos que necesitan para hacer su trabajo. Acceso con Remote PC elimina la necesidad de introducir y proporcionar otras herramientas para adaptarse al teletrabajo. Por ejemplo, aplicaciones o escritorios virtuales y su infraestructura asociada.

Acceso con Remote PC utiliza los mismos componentes de Citrix Virtual Apps and Desktops que facilitan aplicaciones y escritorios virtuales. Como resultado, los requisitos y el proceso de implementación y configuración de Acceso con Remote PC son los mismos que los necesarios para implementar Citrix Virtual Apps and Desktops para la entrega de recursos virtuales. Esta uniformidad ofrece una experiencia de administración homogénea y unificada. Los usuarios disfrutan de la mejor experiencia posible al utilizar Citrix HDX para la entrega de sesiones de PC de oficina.

La función consta de un catálogo de máquinas de tipo **Acceso con Remote PC** que proporciona esta funcionalidad:

- Posibilidad de agregar máquinas especificando unidades organizativas. Esta capacidad facilita la agregación de PC en bloque.
- Asignación automática de usuarios basada en el usuario que inicia sesión en el PC de oficina con Windows. La funcionalidad es compatible con asignaciones de un solo usuario y de múltiples usuarios.

Citrix Virtual Apps and Desktops puede acomodar otros casos de uso de PC físicos si se utilizan otros tipos de catálogos de máquinas. Entre los casos de uso, se incluyen:

- PC Linux físicos
- PC físicos agrupados (es decir, asignados aleatoriamente, no dedicados)

#### **Notas:**

Para obtener información detallada sobre las versiones de sistema operativo compatibles, consulte los requisitos del sistema para VDA de [SO de sesión única](#) y [Linux VDA](#).

Para implementaciones locales, el acceso con Remote PC solo es válido para licencias de Citrix Virtual Apps and Desktops Advanced o Premium. Las sesiones consumen licencias del mismo modo que otras sesiones de Citrix Virtual Desktops. Para Citrix Cloud, el acceso con Remote PC es válido para Citrix Virtual Apps and Desktops Service y Workspace Premium Plus.

## **Consideraciones**

Aunque todos los requisitos técnicos y consideraciones aplicables a Citrix Virtual Apps and Desktops en general también son aplicables a acceso con Remote PC, algunos pueden ser más relevantes o específicos para el caso de uso de PC físico.

#### **Importante:**

Los sistemas físicos Windows 11 (y algunos que ejecutan Windows 10) incluyen funciones de seguridad basadas en virtualización que hacen que el software VDA los detecte incorrectamente como máquinas virtuales. Para mitigar este problema, tiene las siguientes opciones:

- Utilice la opción “/physicalmachine” junto con la opción “/remotepc” como parte de la instalación mediante línea de comandos del VDA

- Agregue este valor del Registro después de instalar el VDA si no se utilizó la opción antes mencionada

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\PortICA

- Nombre: ForceEnableRemotePC

- Tipo: DWORD

- Datos: 1

## Consideraciones sobre la implementación

Mientras planifica la implementación de Acceso con Remote PC, debe adoptar algunas decisiones generales.

- Puede agregar Acceso con Remote PC a una implementación existente de Citrix Virtual Apps and Desktops. Antes de elegir esta opción, considere lo siguiente:
  - ¿Tienen los Delivery Controllers o Cloud Connectors actuales el tamaño adecuado para acomodar la carga adicional asociada a los VDA de acceso con Remote PC?
  - ¿Tienen las bases de datos locales del sitio y los servidores de bases de datos el tamaño adecuado para acomodar la carga adicional asociada a los VDA de acceso con Remote PC?
  - ¿Superarán los VDA existentes y los nuevos VDA de acceso con Remote PC el número máximo de VDA admitidos por sitio?
- Deberá implementar el VDA en los PC de oficina mediante un proceso automatizado. A continuación, se indican dos opciones disponibles:
  - Herramientas de distribución electrónica de software (ESD) como SCCM: [Instalar agentes VDA mediante SCCM](#).
  - Scripts de implementación: [Instalar agentes VDA mediante scripts](#).
- Consulte las [consideraciones de seguridad sobre el acceso con Remote PC](#).

## Consideraciones acerca del catálogo de máquinas

El tipo de catálogo de máquinas requerido depende del caso de uso:

- Acceso con Remote PC
  - PC Windows dedicados
  - PC multiusuario Windows dedicados
- SO de sesión única

- Estático: PC Linux dedicados
- Aleatorio: PC Windows y Linux agrupados

Una vez que haya identificado el tipo de catálogo de máquinas, tenga en cuenta lo siguiente:

- Una máquina solo se puede asignar a un catálogo de máquinas a la vez.
- Para facilitar la administración delegada, considere la posibilidad de crear catálogos de máquinas basados en la ubicación geográfica, el departamento o cualquier otra agrupación que facilite la delegación de la administración de cada catálogo a los administradores correspondientes.
- Al elegir las unidades organizativas en las que residen las cuentas de máquina, seleccione unidades organizativas de nivel inferior para lograr una mayor granularidad. Si no se requiere una granularidad tan estricta, puede elegir unidades organizativas de nivel superior. Por ejemplo, en el caso de bancos, funcionarios o cajeros, seleccione **cajeros**. De lo contrario, puede seleccionar **funcionarios** o **bancos**, en función de los requisitos.
- Mover o eliminar unidades organizativas después de que se hayan asignado a un catálogo de máquinas de acceso con Remote PC afecta a las asociaciones de VDA y genera problemas con futuras asignaciones. Por lo tanto, asegúrese de planificar convenientemente, de manera que la actualización de asignaciones de unidades organizativas para catálogos de máquinas se tenga en cuenta en el plan de cambios de Active Directory.
- Si la estructura de las unidades organizativas no facilita la selección de estas a la hora de agregar máquinas al catálogo de máquinas, no es necesario que seleccione ninguna unidad organizativa. Puede usar PowerShell para agregar las máquinas al catálogo más tarde. Las asignaciones automáticas de usuario continúan funcionando si la asignación de escritorios está configurada correctamente en el grupo de entrega. Hay disponible un script de ejemplo para agregar máquinas al catálogo de máquinas, junto con las asignaciones de usuario, en [GitHub](#).
- Wake on LAN integrada solo está disponible con el catálogo de máquinas de tipo **acceso con Remote PC**.

## Consideraciones acerca de Linux VDA

Estas consideraciones son específicas de Linux VDA:

- Utilice Linux VDA en máquinas físicas solo en modo no 3D. Debido a las limitaciones del controlador de NVIDIA, la pantalla local del PC no se puede oscurecer completamente y muestra las actividades de la sesión cuando el modo HDX 3D está habilitado. Mostrar esta pantalla representa un riesgo para la seguridad.
- Con máquinas Linux físicas, utilice catálogos de máquinas de tipo SO de sesión única.
- La funcionalidad Wake on LAN integrada no está disponible para máquinas Linux.

## Requisitos técnicos y consideraciones

En esta sección, se incluyen los requisitos técnicos y consideraciones para PC físicos.

- Estas opciones no se admiten:
  - Los conmutadores KVM u otros componentes que pueden desconectar una sesión.
  - Los equipos híbridos, incluidos los equipos portátiles y de sobremesa todo en uno y con NVIDIA Optimus.
- Conecte el teclado y el mouse directamente al PC. La conexión al monitor u otros componentes que se pueden apagar o desconectar puede hacer que estos periféricos no estén disponibles. Si tiene que conectar los dispositivos de entrada a componentes como monitores, no apague esos componentes.
- Los PC deben unirse a un dominio de Active Directory Domain Services.
- La funcionalidad Arranque seguro solo es compatible con Windows 10.
- El PC debe tener una conexión de red activa. Se recomienda una conexión por cable para una mayor fiabilidad y ancho de banda.
- Si utiliza Wi-Fi, haga lo siguiente:
  1. Configure los parámetros de energía para dejar encendido el adaptador inalámbrico.
  2. Configure el adaptador inalámbrico y el perfil de red para permitir la conexión automática a la red inalámbrica antes de que el usuario inicie sesión. De lo contrario, el VDA no se registra hasta que el usuario inicia sesión. El PC no está disponible para acceso remoto hasta que un usuario haya iniciado sesión.
  3. Asegúrese de que se pueda acceder a los Delivery Controllers o a los Cloud Connectors desde la red Wi-Fi.
- Puede utilizar el acceso con Remote PC en equipos portátiles. Asegúrese de que el portátil esté conectado a una fuente de alimentación, en lugar de funcionar con batería. Configure las opciones de energía del portátil de manera que coincidan con las de un PC de escritorio. Por ejemplo:
  1. Inhabilite la función de hibernación.
  2. Inhabilite la función de suspensión.
  3. Establezca la opción **No hacer nada** en la acción de cierre de tapa.
  4. Establezca la opción **Apagar** en la acción al presionar el botón de encendido.
  5. Inhabilite las funciones de ahorro de energía de las tarjetas de vídeo y de las tarjetas de interfaz de red.
- Acceso con Remote PC es compatible con dispositivos Surface Pro con Windows 10. Siga las mismas pautas para los portátiles mencionados anteriormente.

- Si utiliza una base de acoplamiento, puede desacoplar y reacoplar portátiles. Al desacoplar un portátil, el VDA vuelve a registrarse con los Delivery Controllers o los Cloud Connectors a través de Wi-Fi. Sin embargo, al reacoplarlo, el VDA no pasa a usar la conexión por cable a menos que desconecte el adaptador inalámbrico. Algunos dispositivos ofrecen una funcionalidad integrada para desconectar el adaptador inalámbrico al establecerse una conexión por cable. Los demás dispositivos requieren soluciones personalizadas o utilidades de terceros para desconectar el adaptador inalámbrico. Consulte las consideraciones mencionadas anteriormente acerca de las redes Wi-Fi.

Para habilitar el acoplamiento y el desacoplamiento de dispositivos de acceso con Remote PC, haga lo siguiente:

1. En el menú **Inicio**, seleccione **Configuración > Sistema > Inicio/apagado y suspensión** y establezca **Suspend** en **Nunca**.
  2. En **Administrador de dispositivos > Adaptadores de red > Adaptador Ethernet**, vaya a **Administración de energía** y desmarque la opción **Permitir que el equipo apague este dispositivo para ahorrar energía**. Asegúrese de que la opción **Permitir que este dispositivo reactive el equipo** está marcada.
- Varios usuarios con acceso al mismo PC de oficina ven el mismo icono de Citrix Workspace. Cuando un usuario inicia sesión en Citrix Workspace, ese recurso aparece como no disponible si otro usuario ya lo está utilizando.
  - Instale la aplicación Citrix Workspace en cada dispositivo cliente (por ejemplo, un equipo casero) que acceda al PC de la oficina.

## Secuencia de configuración

Esta sección contiene una descripción general de cómo configurar el acceso con Remote PC cuando se utiliza el catálogo de máquinas de tipo **Acceso con Remote PC**. Para obtener información sobre cómo crear otros tipos de catálogos de máquinas, consulte [Crear catálogos de máquinas](#).

1. Solo para un sitio local: Para utilizar la función Wake on LAN integrada, configure los requisitos previos descritos en [Wake on LAN](#).
2. Si se creó un nuevo sitio de Citrix Virtual Apps and Desktops para el acceso con Remote PC:
  - a) Seleccione el tipo de sitio del **acceso con Remote PC**.
  - b) En la página **Administración de energía**, habilite o inhabilite la administración de energía del catálogo de máquinas predeterminado de acceso con Remote PC. Puede cambiar esta configuración más adelante modificando las propiedades del catálogo de máquinas. Para obtener más información sobre la configuración de Wake on LAN, consulte [Wake on LAN](#).
  - c) Complete la información en las páginas **Usuarios** y **Cuentas de máquina**.

Al completar estos pasos, se crea un catálogo de máquinas llamado **Máquinas de acceso con Remote PC** y un grupo de entrega llamado **Escritorios de acceso con Remote PC**.

3. Si se agrega a un sitio existente de Citrix Virtual Apps and Desktops:
  - a) Cree un catálogo de máquinas de tipo **Acceso con Remote PC** (página Sistema operativo del asistente). Para obtener información detallada sobre cómo crear un catálogo de máquinas, consulte [Crear catálogos de máquinas](#). Asegúrese de asignar la unidad organizativa correcta para que los equipos de destino estén disponibles para uso con acceso con Remote PC.
  - b) Cree un grupo de entrega para proporcionar a los usuarios acceso a los equipos del catálogo de máquinas. Para obtener información detallada sobre cómo crear un grupo de entrega, consulte [Crear grupos de entrega](#). Asegúrese de asignar el grupo de entrega a un grupo de Active Directory que contenga los usuarios que requieren acceso a sus equipos.
4. Implemente el VDA en los PC de oficina.
  - Se recomienda utilizar el instalador básico de VDA de SO de sesión única (VDAWorkstation-CoreSetup.exe).
  - También puede utilizar el instalador completo de VDA de SO de sesión única (VDAWorkstationSetup.exe) con la opción `/remotepc`, que ofrece el mismo resultado que usar el instalador básico de VDA.
  - Considere la posibilidad de habilitar la Asistencia remota de Windows para que los equipos del servicio de asistencia puedan proporcionar asistencia remota a través de Citrix Director. Para ello, utilice la opción `/enable_remote_assistance`. Para obtener más información, consulte [Instalación desde la línea de comandos](#).
  - Para poder ver la información sobre la duración del inicio de sesión en Director, debe utilizar el instalador completo de VDA de SO de sesión única e incluir el componente **Citrix User Profile Manager WMI Plugin**. Para incluir este componente, utilice la opción `/includeadditional`. Para obtener más información, consulte [Instalación desde la línea de comandos](#).
  - Para obtener información sobre cómo implementar el VDA con SCCM, consulte [Instalar agentes VDA mediante SCCM](#).
  - Para obtener información sobre cómo implementar el VDA con scripts de implementación, consulte [Instalar agentes VDA mediante scripts](#).

Después de completar correctamente los pasos 2 a 4, los usuarios se asignan automáticamente a sus propias máquinas cuando inician sesión localmente en los PC.

5. Indique a los usuarios que descarguen e instalen la aplicación Citrix Workspace en cada dispositivo cliente que utilicen para acceder al equipo de oficina de forma remota. La aplicación Citrix Workspace está disponible en <https://www.citrix.com/downloads/> o en los almacenes de aplicaciones para los dispositivos móviles a los que se ofrece soporte.

## Funciones administradas a través del Registro

### Precaución:

Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

## Inhabilitar asignaciones automáticas de varios usuarios

En cada Delivery Controller, agregue el siguiente parámetro de Registro:

`HKEY_LOCAL_MACHINE\Software\Citrix\DesktopServer`

- Nombre: AllowMultipleRemotePCAssignments
- Tipo: DWORD
- Datos: 0

## Modo de suspensión (versión mínima 7.16)

Para permitir que un equipo de acceso con Remote PC entre en el modo de suspensión, agregue este parámetro al Registro en el VDA y reinicie la máquina. Después del reinicio, se respetan los parámetros de ahorro de energía del sistema operativo. La máquina entra en el modo de suspensión pasado el tiempo preconfigurado en el temporizador de inactividad. Después de que la máquina despierte, vuelve a registrarse en el Delivery Controller.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nombre: DisableRemotePCSleepPreventer
- Tipo: DWORD
- Datos: 1

## Administrar sesiones

De forma predeterminada, la sesión de un usuario remoto se desconecta automáticamente cuando un usuario local inicia una sesión en esa máquina (al presionar CTRL + ALT + SUPR). Para evitar esta acción automática, agregue la siguiente entrada de Registro en el PC de la oficina y, a continuación, reinícielo.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Nombre: SasNotification

- Tipo: DWORD
- Datos: 1

De forma predeterminada, el usuario remoto tiene preferencia sobre el usuario local cuando el mensaje de conexión no se reconoce dentro del plazo de tiempo de espera. Para configurar el comportamiento, utilice este parámetro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Nombre: RpgaMode
- Tipo: DWORD
- Datos:
  - 1: El usuario remoto siempre tiene preferencia si no responde a los mensajes de la interfaz de usuario en el tiempo de espera especificado. Este comportamiento es el predeterminado si este parámetro no está configurado.
  - 2: El usuario local tiene preferencia.

De forma predeterminada, el tiempo de espera para aplicar el modo de acceso con Remote PC es de 30 segundos. Puede configurar este tiempo de espera, pero no lo establezca en menos de 30 segundos. Para configurar el tiempo de espera, utilice este parámetro de Registro:

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- Nombre: RpgaTimeout
- Tipo: DWORD
- Datos: número de segundos de tiempo de espera en valores decimales

Cuando el usuario local quiera forzar el acceso a la consola, puede presionar Ctrl + Alt + Supr dos veces en 10 segundos para obtener el control local sobre una sesión remota y forzar la desconexión.

Después de cambiar el Registro y reiniciar la máquina, si un usuario local presiona Ctrl + Alt + Supr para iniciar sesión en ese PC mientras está siendo utilizado por un usuario remoto, el usuario remoto recibe un mensaje. En el mensaje, se le pregunta si quiere permitir o denegar la conexión del usuario local. Si permite la conexión, la sesión del usuario remoto se desconecta.

## Wake on LAN

Wake on LAN integrada solo está disponible en instancias de Citrix Virtual Apps and Desktops locales y requiere Microsoft System Center Configuration Manager (SCCM).

La función de acceso con Remote PC admite Wake on LAN, el cual ofrece a los usuarios la capacidad de encender equipos físicos de forma remota. Esta función permite a los usuarios mantener apagados sus equipos de oficina cuando no estén en uso, lo que disminuye costes de energía. También permite

el acceso remoto cuando una máquina se ha apagado inadvertidamente. Por ejemplo, debido a un corte de energía.

La funcionalidad Wake on LAN de acceso con Remote PC es compatible con equipos que tienen habilitada la opción Wake on LAN en BIOS/UEFI.

### **SCCM y Wake on LAN de acceso con Remote PC**

Para configurar la función Wake on LAN de acceso con Remote PC, complete los siguientes pasos antes de implementar el VDA.

- Configure SCCM 2012 R2, 2016 o 2019 dentro de la organización. A continuación, implemente el cliente de SCCM en todas las máquinas de acceso con Remote PC. Debe dejar tiempo suficiente para que se ejecute el ciclo de inventario de SCCM programado (o fuerce uno manualmente, si es necesario).
- Para habilitar Magic Packet o el proxy de reactivación de SCCM:
  - Configure la función Wake on LAN en los ajustes de BIOS/UEFI de cada equipo.
  - Para habilitar el proxy de reactivación, habilite la opción en SCCM. Asegúrese de que haya tres o más máquinas que puedan utilizarse como centinelas para cada subred de la organización que contiene los equipos que usan la función Wake on LAN del acceso con Remote PC.
  - Para habilitar Magic Packet, configure los firewalls y los enrutadores de red para que permitan el envío de ese tipo de paquetes mediante una difusión o unidifusión dirigidas a las subredes.

Después de instalar el VDA en los equipos de oficina, habilite o inhabilite la administración de energía cuando cree la conexión y el catálogo de máquinas.

- Si habilita la administración de energía en el catálogo, especifique los datos de conexión: el nombre, la dirección y las credenciales de acceso de SCCM. Las credenciales de acceso deben conceder acceso a las colecciones en el ámbito y al rol de **operador de herramientas remotas**.
- Si no habilita la administración de energía, puede agregar más tarde una conexión de administración de energía (Configuration Manager) y luego modificar un catálogo de máquinas de acceso con Remote PC para habilitar la administración de energía.

Puede modificar una conexión de administración de energía para configurar opciones de configuración avanzadas. Puede habilitar:

- Proxy de reactivación entregado por SCCM.
- Paquetes Wake on LAN (Magic Packets). Si habilita paquetes Wake on LAN, puede seleccionar un método de transmisión Wake on LAN: unidifusión o difusiones dirigidas a subredes.

El equipo usa los comandos de encendido AMT (si se admiten), además de cualquier configuración avanzada que esté habilitada. Si el equipo no utiliza comandos de encendido AMT, recurre a la configuración avanzada.

## Solución de problemas

### La puesta en blanco del monitor no funciona

Si el monitor local del PC con Windows no se pone en blanco mientras hay una sesión HDX activa (el monitor local muestra lo que está sucediendo en la sesión) es probable que se deba a problemas con el controlador del proveedor de la GPU. Para resolver el problema, asigne a Citrix Indirect Display Driver (IDD) una prioridad mayor que al controlador del proveedor de la tarjeta gráfica estableciendo el siguiente valor del Registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- Nombre: CitrixIDD
- Tipo: DWORD
- Datos: 3

Para obtener más información acerca de las prioridades del adaptador de pantalla y la creación de monitores, consulte el artículo [CTX237608](#) de Knowledge Center.

### La sesión se desconecta cuando se selecciona Ctrl+Alt+Supr en la máquina que tiene habilitada la notificación de administración de sesiones

La notificación de administración de sesiones, controlada por el valor de Registro **SasNotification**, solo funciona cuando el modo acceso con Remote PC está habilitado en el VDA. Si el PC físico tiene habilitado el rol Hyper-V o alguna otra función de seguridad basada en la virtualización, el PC informa como una máquina virtual. Si el VDA detecta que se está ejecutando en una máquina virtual, inhabilita automáticamente el modo acceso con Remote PC. Para habilitar el modo acceso con Remote PC, agregue el siguiente valor de Registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nombre: ForceEnableRemotePC
- Tipo: DWORD
- Datos: 1

Reinicie el PC para que la configuración surta efecto.

## Información de diagnóstico

El diagnóstico sobre el acceso con Remote PC se escribe en el registro de eventos de aplicación que ofrece Windows. Los mensajes informativos no tienen limitaciones. Los mensajes de error se limitan mediante el descarte de mensajes duplicados.

- 3300 (informativo): Máquina agregada al catálogo
- 3301 (informativo): Máquina agregada al grupo de entrega
- 3302 (informativo): Máquina asignada al usuario
- 3303 (error): Excepción

## Administración de energía

Cuando se habilita la administración de energía para el acceso con Remote PC, es posible que las difusiones dirigidas a subredes no puedan iniciar las máquinas que se encuentran en una subred diferente a la del Controller. Si necesita la administración de energía en las subredes que utilicen difusiones dirigidas a subredes y la tecnología AMT no está disponible, pruebe el método de unidifusión o de proxy de reactivación. Compruebe que estos parámetros están habilitados en las propiedades avanzadas de la administración de energía de la conexión.

## La sesión remota activa graba la entrada de la pantalla táctil local

Cuando el VDA habilita el modo acceso con Remote PC, la máquina ignora la entrada de la pantalla táctil local durante una sesión activa. Si el PC físico tiene habilitado el rol Hyper-V o alguna otra función de seguridad basada en la virtualización, el PC informa como una máquina virtual. Si el VDA detecta que se está ejecutando en una máquina virtual, inhabilita automáticamente el modo acceso con Remote PC. Para habilitar el modo acceso con Remote PC, agregue el siguiente parámetro de Registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nombre: ForceEnableRemotePC
- Tipo: DWORD
- Datos: 1

Reinicie el PC para que la configuración surta efecto.

## Más recursos

A continuación, se muestran otros recursos para acceso con Remote PC:

- Guía de diseño de soluciones: [Remote PC Access Design Decisions](#).

- Ejemplos de arquitecturas de acceso con Remote PC: [Reference Architecture for Citrix Remote PC Access Solution](#).

## App-V

September 22, 2021

### Usar App-V con Citrix Virtual Apps and Desktops

Microsoft Application Virtualization (App-V) permite implementar, actualizar y admitir aplicaciones como si fueran servicios. Los usuarios acceden a las aplicaciones sin instalarlas en sus dispositivos. App-V y Microsoft User State Virtualization (USV) ofrecen acceso a aplicaciones y datos, independientemente de la ubicación y de la conexión a Internet.

La tabla siguiente muestra las versiones admitidas.

App-V	Delivery Controller de Citrix Virtual Apps and Desktops	VDA de Citrix Virtual Apps and Desktops
5.0 y 5.0 SP1	Desde XenDesktop 7 hasta la versión actual, desde XenApp 7.5 hasta la versión actual	Desde 7.0 hasta la versión actual
5.0 SP2	Desde XenDesktop 7 hasta la versión actual, desde XenApp 7.5 hasta la versión actual	Desde 7.1 hasta la versión actual
5.0 SP3 y 5.1	Desde XenDesktop 7.6 hasta la versión actual, desde XenApp 7.6 hasta la versión actual	Desde 7.6.300 hasta la versión actual
App-V en Windows Server 2016	Desde XenDesktop 7.12 hasta la versión actual, desde XenApp 7.12 hasta la versión actual	Desde 7.12 hasta la versión actual

El cliente de App-V no admite el acceso sin conexión a las aplicaciones. En la compatibilidad con la integración de App-V se incluye el uso de recursos compartidos SMB para aplicaciones. El protocolo HTTP no se admite.

Si no conoce App-V, consulte la documentación de Microsoft. A continuación, se ofrece una recapitulación de los componentes de App-V mencionados en este artículo:

- **Servidor de administración.** Ofrece una consola centralizada para administrar la infraestructura de App-V y entrega aplicaciones virtuales tanto a un cliente App-V de escritorio como a

un cliente de Servicios de escritorio remoto. El servidor de administración de App-V autentica, solicita y proporciona la seguridad, las métricas, la supervisión y la recopilación de datos que necesita el administrador. El servidor utiliza Active Directory y herramientas adicionales para administrar a usuarios y aplicaciones.

- **Servidor de publicación.** Proporciona clientes de App-V con aplicaciones para usuarios específicos y aloja el paquete de aplicaciones virtuales para distribuirlo por streaming. Obtiene los paquetes del servidor de administración.
- **Cliente.** Recupera aplicaciones virtuales, publica aplicaciones en el cliente, y automáticamente establece y administra entornos virtuales en el momento de la ejecución en dispositivos Windows. El cliente de App-V se instala en el VDA, donde almacena parámetros de aplicaciones virtuales específicos de los usuarios, tales como los cambios en el Registro y en los archivos de cada perfil de usuario.

Las aplicaciones están siempre disponibles sin tener que definir o cambiar previamente la configuración del sistema operativo. Puede iniciar aplicaciones de App-V desde grupos de entrega con SO de servidor y con SO de escritorio:

- A través de la aplicación Citrix Workspace
- A través del cliente de App-V y la aplicación Citrix Workspace
- Varios usuarios simultáneos en varios dispositivos
- A través de Citrix StoreFront

Las propiedades modificadas de las aplicaciones de App-V se implementan al iniciar las aplicaciones. Por ejemplo, para las aplicaciones con un nombre simplificado modificado o un icono personalizado, la modificación aparece cuando los usuarios inician la aplicación. Las personalizaciones de aplicaciones que se guardan en los archivos de configuración dinámica también se aplican cuando se inicia la aplicación.

## Métodos de administración

Puede usar los paquetes de App-V y los archivos de configuración dinámica que se crearon con el secuenciador de App-V y se encuentran en servidores de App-V o recursos compartidos de red.

- **Servidores App-V:** Para poder usar las aplicaciones de los paquetes en servidores de App-V, se requiere una comunicación continua entre Studio y los servidores de App-V para la detección, la configuración y la descarga a los VDA. Lo que resulta en una sobrecarga de hardware, infraestructura y administración. Studio y los servidores de App-V deben estar sincronizados, especialmente para los permisos de usuario.

Esto se conoce como el método de *administración dual* porque el paquete de App-V y el acceso a la aplicación requieren tanto la consola de Studio como la consola del servidor de App-V. Este método funciona mejor en implementaciones de App-V y Citrix estrechamente ligadas. En

este método, el servidor de administración gestiona los archivos de configuración dinámica. Cuando se utiliza el método de administración dual, los componentes de Citrix App-V administran el registro del servidor de publicación apropiado que se necesita para el lanzamiento de aplicaciones. Así, se garantiza que, en un momento dado, el servidor de publicación esté sincronizado para el usuario. El servidor de publicación conserva otros aspectos del ciclo de vida del paquete (como la actualización en los inicios de sesión y los grupos de conexión) mediante su configuración.

- **Recurso compartido de red:** Los paquetes y los archivos XML de configuración para implementación colocados en un recurso compartido de red eliminan la dependencia que tiene Studio del servidor de App-V y de la infraestructura de la base de datos, por lo que se reduce la sobrecarga (necesita instalar el cliente de App-V de Microsoft en cada VDA).

Esto se conoce como el método de *administración única* porque el paquete de App-V y la aplicación solo necesitan la consola de Studio. Puede ir al recurso compartido de red y agregar uno o varios paquetes de App-V desde esa ubicación a la biblioteca de aplicaciones que se encuentre al nivel del sitio [1]. En este método, los componentes App-V de Citrix procesan los archivos de configuración de la implementación cuando se inicia la aplicación (no se admiten los archivos de configuración de usuario). Cuando se utiliza el método de administración única, los componentes de Citrix App-V administran todos los aspectos del ciclo de vida del paquete en la máquina host. Los paquetes se agregan a la máquina al iniciar el broker o cuando se detecta un cambio de configuración (que también puede ser al iniciar una sesión). Los paquetes se publican por primera vez para los usuarios “a petición” cuando se recibe una solicitud de lanzamiento de la aplicación Citrix Workspace.

La administración única también administra el ciclo de vida de los grupos de conexión necesarios para cumplir con las definiciones de configuración del grupo de aislamiento realizadas en Studio.

La [1] *biblioteca de aplicaciones* es un término de Citrix para designar un repositorio de almacenamiento en caché que guarda información sobre paquetes de App-V. La biblioteca de aplicaciones también almacena información acerca de otras tecnologías de Citrix para la entrega de aplicaciones.

En los dos métodos de administración, si el VDA está configurado para descartar datos de usuario, la publicación (o sincronización) debe volver a realizarse en el inicio de la siguiente sesión.

Puede usar uno o ambos métodos de administración de forma simultánea. En otras palabras, al agregar aplicaciones a grupos de entrega, esas aplicaciones pueden proceder de paquetes de App-V ubicados en servidores de App-V o en un recurso compartido de red.

**Nota:**

Si utiliza simultáneamente ambos métodos de administración, y el paquete de App-V tiene un

archivo de configuración dinámica en ambas ubicaciones, se utiliza el archivo que se encuentra en el servidor de App-V (administración dual).

Cuando se seleccione **Configuración > Publicación de App-V** en el panel de navegación de Studio, aparecerán los orígenes y los nombres de los paquetes de App-V. La columna de origen indica si los paquetes se encuentran en el servidor de App-V o en la memoria caché de la biblioteca de aplicaciones. Al seleccionar un paquete, el panel de detalles muestra las aplicaciones y los accesos directos que contiene ese paquete.

## Archivos de configuración dinámica

**Descripción general** Los paquetes de App-V se pueden personalizar mediante archivos de configuración dinámica. Cuando esos archivos se aplican al paquete, se pueden cambiar las funciones de este. Por ejemplo, puede usarlos para definir comportamientos y accesos directos adicionales de la aplicación. Citrix App-V admite ambos tipos de archivo de configuración dinámica. Los parámetros que contiene el archivo se aplican cuando se inicia la aplicación:

- Los archivos de configuración de la implementación proporcionan una configuración de toda la máquina para todos los usuarios. Estos archivos se suelen denominar `<NombreDeArchivoDePaquete>_Deploy` y suelen estar en la misma carpeta que el paquete de App-V al que se aplican. Se admiten en la administración única y dual.
- Los archivos de configuración de usuario proporcionan una configuración específica del usuario que admite personalizaciones por usuario para el paquete. La administración única admite archivos de configuración de usuario nombrados en el siguiente formato: `<NombreDeArchivoDePaquete>[SIDdelUsuario | NombreDeUsuario | SIDdelGrupo | NombreDelGrupo]UserConfig.xml`, ubicados en la misma carpeta que el paquete App-V al que se aplican.

Cuando existen varios archivos de configuración de usuario para un paquete en particular, se aplican con la siguiente prioridad:

1. SID del usuario
2. Nombre de usuario
3. SID del grupo de AD (el primero encontrado prevalece)
4. Nombre del grupo de AD (el primero encontrado prevalece)
5. Predeterminado

### Por ejemplo

- 1 MyAppVPackage\_S-1-5-21-000000001-0000000001-000000001-001\_UserConfig.xml
- 2 MyAppVPackage\_joeblogs\_UserConfig.xml
- 3 MyAppVPackage\_S-1-5-32-547\_UserConfig.xml

```
4 MyAppVPackage_Power Users_UserConfig.xml
5 MyAppVPackage_UserConfig.xml
```

**Nota:**

La parte específica del usuario en el nombre del archivo también puede aparecer opcionalmente al final (por ejemplo, MyAppVPackage\_UserConfig\_**joeblogs**.xml).

**Ubicación de los archivos de configuración dinámica** En la administración única, los componentes de Citrix App-V solo procesan los archivos de configuración dinámica que se encuentran en la misma carpeta que su paquete de App-V. Cuando se inician las aplicaciones que contiene el paquete, se vuelven a aplicar los cambios a los archivos de configuración dinámica correspondientes. Si sus archivos de configuración dinámica no comparten ubicación con sus paquetes, use un archivo de asignación para vincular los paquetes a sus archivos de configuración de la implementación.

**Para crear un archivo de asignación**

1. Abra un nuevo archivo de texto.
2. Para cada archivo de configuración dinámica, agregue una línea que especifique la ruta al paquete con el formato <GUIDPaquete> : ruta.

Por ejemplo:

```
F1f4fd78ef044176aad9082073a0c780 : c:\windows\file\packagedeploy.xml
```

3. Guarde el archivo como ctxAppVDynamicConfigurations.cfg en la misma carpeta que el paquete. Toda la jerarquía de directorios que haya en el mismo recurso compartido UNC que el paquete de App-V se examina de forma recurrente hacia arriba para buscar este archivo cada vez que se inicia una aplicación del paquete.

**Nota**

No puede aplicar cambios a la configuración de una implementación dinámica cuando hay sesiones de usuario que tienen abierta una aplicación del paquete. Puede aplicar cambios a los archivos de configuración dinámica del usuario si otros usuarios, *pero no el usuario actual*, tienen abierta una aplicación del paquete.

**Grupos de aislamiento**

Cuando se usa el método de administración única de App-V, crear grupos de aislamiento permite especificar grupos interdependientes de aplicaciones que deben ejecutarse en el sandbox. Esta funcionalidad es similar (pero no idéntica) a los grupos de conexión de App-V. En lugar de la terminología

“paquetes obligatorios” y “paquetes optativos” que utiliza el servidor de administración de App-V, Citrix utiliza los términos “automática” y “explícita” cuando se refiere a las opciones de implementación de paquetes.

- Así, cuando un usuario inicia una aplicación de App-V (la aplicación principal), se buscan en los grupos de aislamiento otros paquetes de aplicación que estén marcados para la inclusión automática. Esos paquetes se descargan y se incluyen automáticamente en el grupo de aislamiento. No es necesario que los agregue al grupo de entrega que contiene la aplicación principal.
- En cambio, un paquete de aplicación que esté marcado para la inclusión explícita en el grupo de aislamiento se descarga solo si agrega explícitamente esa aplicación al mismo grupo de entrega que contiene la aplicación principal.

Esto permite crear grupos de aislamiento que contengan una mezcla de aplicaciones incluidas automáticamente que están disponibles globalmente para todos los usuarios. Además, el grupo puede contener un conjunto de plug-ins y otras aplicaciones (que pueden tener restricciones concretas de licencias), que puede limitar a un determinado grupo de usuarios (identificado a través de grupos de entrega) sin necesidad de crear más grupos de aislamiento.

Por ejemplo, la aplicación A requiere JRE 1.7 para ejecutarse. Puede crear un grupo de aislamiento que contenga la aplicación A (con un tipo de implementación explícito) y JRE 1.7 (con un tipo de implementación automático). A continuación, agregue esos paquetes de App-V a uno o varios grupos de entrega. Cuando un usuario inicie la aplicación A, JRE 1.7 se implementará automáticamente con ella.

Puede agregar una aplicación a más de un grupo de aislamiento de App-V. No obstante, cuando un usuario inicia una aplicación, siempre se utiliza el primer grupo de aislamiento al que se agregó la aplicación. No se puede ordenar ni priorizar a los demás grupos de aislamiento que contengan dicha aplicación.

### **Servidores de equilibrio de carga de App-V**

Los servidores de administración y publicación de equilibrio de carga que utilizan el sistema de nombres de dominio round robin son compatibles si está utilizando el método de administración “Administración dual”. El equilibrio de carga del servidor de administración detrás de NetScaler, IP virtual F5 (o similar) no se admite debido a la forma en que Studio necesita comunicarse con el servidor de administración a través de PowerShell remoto. Para obtener más información, consulte este artículo del [blog de Citrix](#).

## Configurar

En la siguiente tabla, se resume la secuencia de las tareas de configuración a realizar para utilizar App-V en Citrix Virtual Apps and Desktops cuando se utilizan los métodos de administración única y dual.

Administración única	Administración dual	Tarea
X	X	Implementar App-V
X	X	Empaquetar y seleccionar ubicación
	X	Configurar direcciones de servidor de App-V en Studio
X	X	Instalar software en máquinas VDA
X		Agregar paquetes de App-V a la biblioteca de aplicaciones
X		Agregar grupos de aislamiento de App-V (opcional)
X	X	Agregar aplicaciones de App-V a grupos de entrega

## Implementar Microsoft App-V

Para obtener las instrucciones de implementación de App-V, consulte <https://docs.microsoft.com/en-us/microsoft-desktop-optimization-pack/>.

Si lo prefiere, puede cambiar la configuración del servidor de publicación de App-V. Citrix recomienda usar los cmdlets del SDK presente en el Controller. Consulte la documentación del SDK para obtener más información.

- Para ver la configuración del servidor de publicación, escriba **Get-CtxAppvServerSetting -AppVPublishingServer <pubServer>**.
- Para asegurarse de que las aplicaciones de App-V se inicien correctamente, escriba **Set-CtxAppvServerSetting -UserRefreshonLogon 0**.

Si ya utilizó configuraciones de GPO para administrar parámetros del servidor de publicación, estas configuraciones de GPO supeditan todos los parámetros de integración de App-V, incluidos los parámetros de cmdlets. Esto puede dar lugar a fallos de inicio de la aplicación de App-V. Citrix recomienda quitar todos los parámetros de directiva de grupo (GPO) y utilizar el SDK para definir esa configuración.

## **Empaquetar y seleccionar ubicación**

Puede crear paquetes de aplicación mediante el secuenciador de App-V para ambos métodos de administración. Consulte la documentación de Microsoft para obtener más detalles.

- Para la administración única, ponga los paquetes (y sus archivos de configuración dinámica correspondientes) a disposición en una ubicación de red compartida UNC o SMB. Compruebe que el administrador de Studio que agregue las aplicaciones a los grupos de entrega tenga al menos el acceso de lectura a esa ubicación.
- Para la administración dual, publique los paquetes en el servidor de administración de App-V desde una ruta UNC. (No se admite la publicación desde direcciones URL de HTTP.)

Independientemente de si los paquetes están en el servidor de App-V o en un recurso compartido de red, compruebe que tienen los permisos de seguridad adecuados para que el administrador de Studio acceda a ellos. Los recursos compartidos de red deben compartirse con “Usuarios autenticados” para garantizar que el VDA y Studio tienen el acceso de lectura de forma predeterminada.

## **Configurar direcciones de servidor de App-V en Studio**

### **Importante:**

Citrix recomienda usar los cmdlets de PowerShell en el Controller para especificar las direcciones de servidores de App-V si esos servidores utilizan valores de propiedad no predeterminados. Consulte la documentación del SDK para obtener más información. Si cambia las direcciones de servidor de App-V en Studio, algunas propiedades de conexiones de servidor que especifique pueden restablecerse a los valores predeterminados. Estas propiedades se utilizan en los VDA para conectarse a los servidores de publicación de App-V. Si eso ocurriera, vuelva a configurar en los servidores los valores no predeterminados de las propiedades restablecidas.

Este procedimiento solo es válido para la administración dual.

Puede especificar las direcciones de los servidores de administración y publicación de App-V para la administración dual durante o después de la creación de sitios. Puede hacerlo durante o después de crear el sitio.

Durante la creación de sitio:

- En la página **App-V** del asistente, escriba la URL del servidor de administración de App-V, así como la URL y el número de puerto del servidor de publicación de App-V.
- Pruebe la conexión antes de continuar con el asistente. Si se produce un error en la prueba, consulte la sección “Solucionar problemas” que se presenta más adelante en este artículo.

Después de la creación de sitio:

1. Seleccione **Configuración > Publicación de App-V** en el panel de navegación de Studio.
2. Si no ha especificado previamente direcciones de servidor de App-V, seleccione **Agregar servidor de Microsoft** en el panel Acciones.
3. Para cambiar las direcciones del servidor de App-V, seleccione **Modificar servidor de Microsoft** en el panel Acciones.
4. Escriba la URL del servidor de administración de App-V, así como la URL y el número de puerto del servidor de publicación de App-V.
5. Pruebe la conexión a esos servidores antes de cerrar el cuadro de diálogo. Si se produce un error en la prueba, consulte la sección “Solucionar problemas” que se presenta más adelante en este artículo.

Más adelante, si quiere eliminar todos los enlaces a los servidores de administración y publicación de App-V y evitar que Studio detecte los paquetes de App-V de esos servidores, seleccione **Quitar servidor de Microsoft** en el panel Acciones. Esta acción solo se permite si ninguna de las aplicaciones que se encuentran en los paquetes de esos servidores está publicada en los grupos de entrega. Si lo están, debe quitar esas aplicaciones de los grupos de entrega antes de poder quitar los servidores de App-V.

### Instalar software en máquinas VDA

Las máquinas que contienen los VDA deben tener dos conjuntos de software instalados para admitir App-V: uno de Microsoft y otro de Citrix.

**Cliente de Microsoft App-V** Este software recupera aplicaciones virtuales, publica aplicaciones en el cliente, y automáticamente establece y administra entornos virtuales en el momento de la ejecución en dispositivos Windows. El cliente de App-V almacena parámetros de aplicaciones virtuales específicos de los usuarios, tales como los cambios en el Registro y en los archivos de cada perfil de usuario.

El cliente de App-V está disponible en Microsoft. Instale un cliente en todas las máquinas que contienen agentes VDA o en la imagen maestra que se usa en el catálogo de máquinas para crear las máquinas virtuales. **Nota:** Windows 10 (1607 o posterior) y Windows Server 2016 ya incluyen el cliente de App-V. Solo en esos sistemas operativos, habilite el cliente de App-V. Para ello, ejecute el cmdlet **Enable-AppV** (sin parámetros) de PowerShell. El cmdlet **Get-AppVStatus** obtiene el estado actual (habilitado o no habilitado).

#### Sugerencia:

Después de instalar el cliente de App-V, con permisos de administrador, ejecute el cmdlet **Get-AppVClientConfiguration** de PowerShell y verifique que `EnablePackageScripts` esté establecido en 1. Si no está establecido en 1, ejecute **Set-AppVClientConfiguration -EnablePackageScripts**

**\$true.**

**Componentes de Citrix App-V** El software del componente Citrix App-V se excluye de manera predeterminada cuando se instala un VDA.

Se puede controlar este comportamiento predeterminado durante la instalación del VDA. En la interfaz gráfica, marque la casilla **Citrix Personalization para App-V: VDA** en la página **Componentes adicionales**. En la interfaz de línea de comandos, use la opción **/includeadditional "Citrix Personalization para App-V: VDA"**.

Si no incluye los componentes de App-V desarrollados por Citrix durante la instalación de VDA, pero más tarde quiere usar aplicaciones de App-V: En la lista "Programas y características" de la máquina Windows, haga clic con el botón secundario en la entrada **Citrix Virtual Delivery Agent** y, a continuación, seleccione **Cambiar**. Se iniciará un asistente. En el asistente, habilite la opción que instala y habilita los componentes de publicación de App-V.

### **Agregar o eliminar paquetes de App-V de la biblioteca de aplicaciones**

Estos procedimientos solo son válidos para el método de administración única.

Debe tener al menos el acceso de lectura al recurso compartido de red que contiene los paquetes de App-V.

### **Agregar un paquete de App-V a la biblioteca de aplicaciones**

1. Seleccione **Configuración > Publicación de App-V** en el panel de navegación de Studio.
2. Seleccione **Agregar paquetes** en el panel Acciones.
3. Vaya al recurso compartido que contiene los paquetes de App-V y seleccione uno o varios paquetes.
4. Haga clic en **Add**.

**Eliminar un paquete de App-V de la biblioteca de aplicaciones** Si quita un paquete de App-V que hubiera en la biblioteca de aplicaciones, este se quita del nodo de publicación de App-V en Studio. Sin embargo, esta acción no elimina, de los grupos de entrega, las aplicaciones que contenía el paquete, por lo que esas aplicaciones aún se pueden iniciar. El paquete sigue en su ubicación de red física. (Este efecto difiere de la eliminación de una aplicación de App-V de un grupo de entrega.)

1. Seleccione **Configuración > Publicación de App-V** en el panel de navegación de Studio.
2. Seleccione uno o varios paquetes que se van a quitar.
3. Seleccione **Quitar paquete** en el panel Acciones.

## Agregar, modificar o eliminar grupos de aislamiento de App-V

### Agregar un grupo de aislamiento de App-V

1. Seleccione **Publicación de App-V** en el panel de navegación de Studio.
2. Seleccione **Agregar grupo de aislamiento** en el panel Acciones.
3. En el cuadro de diálogo **Agregar parámetros del grupo de aislamiento**, escriba un nombre y una descripción para el grupo de aislamiento.
4. En la lista Paquetes disponibles, seleccione las aplicaciones a agregar al grupo de aislamiento y, a continuación, haga clic en la flecha derecha. Las aplicaciones seleccionadas deberían aparecer en la lista Paquetes en grupo de aislamiento. En la lista desplegable **Implementación** situada junto a cada aplicación, seleccione **Explícita** o **Automática**. También puede usar las flechas arriba y abajo para cambiar el orden de las aplicaciones en la lista.
5. Cuando haya terminado, haga clic en **Aceptar**.

### Modificar un grupo de aislamiento de App-V

1. Seleccione **Publicación de App-V** en el panel de navegación de Studio.
2. Seleccione la ficha **Grupos de aislamiento** en el panel central y, a continuación, seleccione el grupo de aislamiento a modificar.
3. Seleccione **Modificar grupo de aislamiento** en el panel Acciones.
4. En el cuadro de diálogo **Edit Isolation Group Settings**, cambie el nombre o la descripción del grupo de aislamiento, agregue o elimine aplicaciones, cambie el tipo de implementación o cambie el orden de aplicaciones.
5. Cuando haya terminado, haga clic en **Aceptar**.

**Eliminar un grupo de aislamiento de App-V** Quitar un grupo de aislamiento no quita los paquetes de aplicaciones. Solo elimina la agrupación.

1. Seleccione **Publicación de App-V** en el panel de navegación de Studio.
2. Seleccione la ficha **Grupos de aislamiento** en el panel central y, a continuación, seleccione el grupo de aislamiento a eliminar.
3. Seleccione **Quitar grupo de aislamiento** en el panel Acciones.
4. Confirme la eliminación.

### Agregar aplicaciones de App-V a grupos de entrega

El siguiente procedimiento se centra en cómo agregar aplicaciones de App-V a grupos de entrega. Para obtener información completa sobre cómo crear un grupo de entrega, consulte [Crear grupos de entrega](#).

**Paso 1:** Elija si quiere crear un grupo de entrega o agregar aplicaciones de App-V a un grupo de entrega existente:

Para crear un grupo de entrega que contenga las aplicaciones de App-V:

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione **Crear grupo de entrega** en el panel Acciones.
3. En las siguientes páginas del asistente, especifique un catálogo de máquinas y unos usuarios.

Para agregar aplicaciones de App-V a grupos de entrega existentes:

1. Seleccione **Aplicaciones** en el panel de navegación de Studio.
2. Seleccione **Agregar aplicaciones** en el panel Acciones.
3. Seleccione uno o varios grupos de entrega a los que se agregarán las aplicaciones de App-V.

**Paso 2:** En la página **Aplicaciones** del asistente, haga clic en la lista desplegable **Agregar** para ver los orígenes de las aplicaciones. Seleccione **App-V**.

**Paso 3:** En la página **Agregar aplicaciones de App-V**, elija el origen de App-V: el servidor de App-V o la biblioteca de aplicaciones. La pantalla resultante contiene los nombres de las aplicaciones y sus nombres y versiones de paquete. Marque las casillas situadas junto a las aplicaciones o los accesos directos a ellas que quiera agregar. Luego haga clic en **Aceptar**.

**Paso 4:** Complete el asistente.

Información útil:

- Si cambia las propiedades de una aplicación de App-V cuando la agregue a un grupo de entrega, esos cambios se realizan cuando se inicia la aplicación. Por ejemplo, si modifica el icono o el nombre simplificado de una aplicación cuando la agregue al grupo, el cambio aparece cuando un usuario inicia la aplicación.
- Si usa archivos de configuración dinámica para personalizar las propiedades de una aplicación de App-V, esas propiedades anulan los cambios que haya hecho cuando las agregó a un grupo de entrega.
- Si, más adelante, quiere modificar un grupo de entrega que contenga aplicaciones de App-V, no habrá ningún cambio en el rendimiento de esas aplicaciones si se cambia el tipo de entrega del grupo de “escritorios y aplicaciones” a “solo aplicaciones”.
- Al quitar un paquete de App-V publicado anteriormente (administrador único) de un grupo de entrega, los componentes del cliente Citrix App-V intentan limpiar, anular la publicación y quitar todos los paquetes que ya no se utilicen por el método de administración de administrador único.
- Si utiliza una implementación híbrida (con paquetes entregados por el método de administración de administrador único y un servidor de publicación de App-V, administrado por un administrador dual o por otro mecanismo, como una directiva de grupo), no es posible determi-

nar el origen de los paquetes (ahora potencialmente redundantes). En este caso, no se intenta realizar la limpieza.

- Si publica más de 100 aplicaciones de App-V en un único grupo de entrega, es posible que las aplicaciones no se inicien. Si es así, utilice la propiedad `MaxReceivedMessageSize` en el elemento de enlace adecuado para aumentar el tamaño del mensaje Max Receivable en la configuración del Delivery Controller y/o el agente del broker en el VDA.

## Solución de problemas

Los problemas que solo pueden ocurrir cuando se utiliza el método de administración dual están marcados con “(DUAL)”.

(DUAL) Se produce un error de conexión de PowerShell cuando selecciona **Configuración > Publicación de App-V** en el panel de navegación de Studio.

- ¿El administrador de Studio es también un administrador del servidor de App-V? El administrador de Studio debe pertenecer al grupo “administradores” en el servidor de administración de App-V para que los administradores se puedan comunicar con él.

(DUAL) La operación “Probar conexión” devuelve un error cuando se especifican las direcciones de servidores de App-V en Studio.

- ¿Está encendido el servidor de App-V? Envíe un comando Ping o compruebe el Administrador de IIS; todos los servidores de App-V deben tener el estado Iniciado y En ejecución.
- ¿Está habilitada la comunicación remota de PowerShell en el servidor de App-V? Si no, consulte [https://docs.microsoft.com/en-us/previous-versions/technet-magazine/ff700227\(v=msdn.10\)](https://docs.microsoft.com/en-us/previous-versions/technet-magazine/ff700227(v=msdn.10)).
- ¿El administrador de Studio es también un administrador del servidor de App-V? El administrador de Studio debe pertenecer al grupo *administradores* en el servidor de administración de App-V para que los administradores se puedan comunicar con él.
- ¿Está habilitado el uso compartido de archivos en el servidor de App-V? Escriba `\\<App-V server FQDN>` en el Explorador de Windows o con el comando Ejecutar.
- ¿El servidor de App-V tiene los mismos permisos de uso compartido de archivos que el administrador de App-V? En el servidor de App-V, agregue una entrada para `\\<App-V server FQDN>` en “Nombres de usuarios y contraseñas almacenados”, especificando las credenciales del usuario que tiene privilegios de administrador en el servidor de App-V. Para obtener instrucciones, consulte <http://support.microsoft.com/kb/306541>
- ¿Se encuentra el servidor de App-V en Active Directory?

Si la máquina de Studio y el servidor de App-V se encuentran en dominios de Active Directory distintos que no tienen una relación de confianza, desde la consola de PowerShell en la máquina

de Studio, ejecute **winrm s winrm/Config/client '@(TrustedHosts="<FQDN del servidor de App-V>")'**.

Si TrustedHosts está administrado por un objeto de directiva de grupo (GPO), aparece un mensaje de error como el siguiente: “*El parámetro de configuración TrustedHosts no se puede cambiar porque el uso se controla mediante directivas. La directiva debe establecerse como 'No configurada' para poder cambiar el parámetro de configuración*”. En este caso, agregue una entrada para el nombre del servidor de App-V a la directiva de hosts de confianza en GPO [Plantillas administrativas > Componentes de Windows > Administración remota de Windows (WinRM) > Cliente WinRM].

(DUAL) Falla la detección cuando se agrega una aplicación de App-V a un grupo de entrega.

- ¿El administrador de Studio es también un administrador del servidor de administración de App-V? El administrador de Studio debe pertenecer al grupo *administradores* en el servidor de administración de App-V para que los administradores se puedan comunicar con él.
- ¿Se está ejecutando el servidor de administración de App-V? Envíe un comando Ping o compruebe el Administrador de IIS; todos los servidores de App-V deben tener el estado Iniciado y En ejecución.
- ¿Está habilitada la comunicación remota de PowerShell en ambos servidores de App-V? Si no, consulte [https://docs.microsoft.com/en-us/previous-versions/technet-magazine/ff700227\(v=msdn.10\)](https://docs.microsoft.com/en-us/previous-versions/technet-magazine/ff700227(v=msdn.10)).
- ¿Los paquetes tienen los permisos de seguridad adecuados para que el administrador de Studio tenga acceso a ellos?

Las aplicaciones de App-V solo se inician en una versión del explorador web.

- Si publica varias versiones en secuencia de la misma aplicación de explorador web, solo podrá iniciarse una versión de la aplicación a la vez por usuario en el VDA. Se da el mismo comportamiento incluso cuando los componentes de Citrix no intervienen y el usuario inicia las aplicaciones secuenciadas desde accesos directos de escritorio que apuntan a rutas diferentes.

La primera versión de explorador que inicie el usuario determina la versión que se ejecutará posteriormente para él. Cuando Firefox detecta un segundo inicio de sí mismo, prefiere crear una instancia del proceso ya en ejecución, en lugar de crear un nuevo proceso. Otros exploradores web pueden comportarse de la misma manera.

Puede hacer que la aplicación se inicie en la versión del explorador Firefox deseada. Para ello, agregue el parámetro de línea de comandos **-no-remote** al comando de inicio del acceso directo. Otros exploradores ofrecen el mismo recurso o uno similar.

**Nota:**

Debe usar XenApp 7.17 o posterior para poder usar la función de enumeración de acceso di-

recto. También debe cambiar el paquete en ambas versiones de la aplicación para obtener este comportamiento bidireccional.

Las aplicaciones de App-V no se inician.

- (DUAL) ¿Se está ejecutando el servidor de publicación?
- (DUAL) ¿Los paquetes de App-V tienen los permisos de seguridad adecuados para que los usuarios puedan acceder a ellos?
- (DUAL) En el agente VDA, compruebe que Temp hace referencia a la ubicación correcta y que hay espacio suficiente disponible en el directorio Temp.
- (DUAL) En el servidor de publicación de App-V, ejecute `Get-AppvPublishingServer \*` para que se muestre la lista de servidores de publicación.
- (DUAL) En el servidor de publicación de App-V, compruebe si UserRefreshonLogon está establecido en False.
- (DUAL) En el servidor de publicación de App-V, con privilegios de administrador, ejecute **Set-AppvPublishingServer** y establezca UserRefreshonLogon en “False”.
- ¿El VDA tiene instalada una versión admitida del cliente de App-V? ¿El VDA tiene habilitada la opción de **habilitar scripts de paquetes**?
- En la máquina que contiene el VDA y el cliente de App-V, desde el editor del Registro (regedit), vaya a HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Citrix\AppV. Compruebe que la clave AppVServers tiene un valor en el siguiente formato: AppVManagementServer+metadata;PublishingServer (por ejemplo: `http://xmas-demo-appv.blrstrm.com+0+0+0+1+1+1+0+1;http://xmas-demo-appv.blrstrm.com:8082`).
- En la máquina o imagen maestra que contiene el VDA y el cliente de App-V, compruebe que el parámetro ExecutionPolicy de PowerShell está establecido en RemoteSigned. El cliente de App-V suministrado por Microsoft no está firmado, y esta directiva ExecutionPolicy permite que PowerShell ejecute cmdlets y scripts locales sin firma. Utilice uno de los siguientes dos métodos para configurar ExecutionPolicy: 1) Como administrador, escriba el cmdlet **Set-ExecutionPolicy RemoteSigned** o 2) En Configuración de directivas de grupo, vaya a Configuración del equipo > Directivas > Plantillas administrativas > Componentes de Windows > Windows PowerShell > Activar la ejecución de scripts.
- Si aparece el error “RegistrationManager.AttemptRegistrationWithSingleDdc: Failed to register”, utilice la propiedad MaxReceivedMessageSize en el elemento de enlace adecuado para aumentar el tamaño del mensaje Max Receivable en la configuración del Delivery Controller y/o el agente del broker en el VDA.

Si estos pasos no resuelven el problema, habilite y examine los registros.

## Registros

Los registros relacionados con la configuración de App-V están ubicados en C:\CtxAppvLogs. Los registros de inicio de aplicaciones se encuentran en: %LOCALAPPDATA%\Citrix\CtxAppvLogs. LOCALAPPDATA es la carpeta local del usuario que ha iniciado sesión. Consulte la carpeta local del usuario para el que falló el inicio de la aplicación.

Para habilitar los registros de Studio y VDA que se utilizan para App-V, debe tener privilegios de administrador. También necesitará un editor de texto, como el Bloc de notas.

Para habilitar los registros de Studio:

1. Cree la carpeta C:\CtxAppvLogs.
2. Vaya a C:\Archivos de programa\Citrix\StudioAppVIntegration\SnapIn\Citrix.Appv.Admin.V1. Abra CtxAppvCommon.dll.config en un editor de texto y quite la marca de comentario de la línea siguiente: `<add key="LogFileName" value="C:\CtxAppvLogs\log.txt"/>`
3. Reinicie el servicio de Broker para comenzar la captura de registros.

Para habilitar los registros del VDA:

1. Cree la carpeta C:\CtxAppvLogs.
2. Vaya a C:\Archivos de programa\Citrix\Virtual Desktop Agent. Abra CtxAppvCommon.dll.config en un editor de texto y quite la marca de comentario de la línea siguiente: `<add key="LogFileName" value="C:\CtxAppvLogs\log.txt"/>`
3. Quite la marca de comentario de la línea y establezca el valor en 1: `<add key="EnableLauncherLogs" value="1"/>`
4. Reinicie la máquina para comenzar a capturar registros.

## AppDisks

December 13, 2022

### Nota:

AppDisks ha sido [retirado](#).

## Información general

Administrar las aplicaciones y, a su vez, las imágenes en que esas aplicaciones están instaladas puede ser complejo. En estos casos, la función Citrix AppDisks puede solucionar el problema. AppDisks separa, por un lado, el sistema operativo y, por el otro, las aplicaciones y los grupos de aplicaciones, lo que permite administrarlos de forma independiente.

Puede crear varios AppDisks que contengan aplicaciones diseñadas para los distintos grupos de usuarios y, a continuación, puede combinar esos AppDisks en la imagen maestra que decida. Agrupar y administrar las aplicaciones de esta forma permite controlar de manera más precisa las aplicaciones que utilice. Además, permite reducir la cantidad de imágenes maestras que mantener. Esto simplifica la administración de TI y permite responder mejor a las necesidades del usuario. Las aplicaciones contenidas en AppDisks se entregan por medio de grupos de entrega.

Si su implementación incluye la función Citrix AppDNA, puede integrar AppDisks en ella, ya que AppDNA permite que Citrix Virtual Apps and Desktops analicen automáticamente las aplicaciones presentes en cada AppDisk. Usar AppDNA ayuda a sacar el máximo provecho de la función AppDisks. Sin ella, la compatibilidad de las aplicaciones no se prueba ni se notifica.

Dos funciones distinguen AppDisks de otras tecnologías de aprovisionamiento de aplicaciones: la administración de cambios y la administración de aislamientos.

- Microsoft App-V permite que existan aplicaciones no compatibles aislándolas. La función AppDisks no aísla las aplicaciones. Las separa (a ellas y a sus archivos auxiliares y claves del Registro) del sistema operativo. Para el sistema operativo y el usuario, los AppDisks aparecen y se comportan como si estuvieran instalados directamente en la imagen maestra.
- La administración de cambios (actualizar las imágenes maestras y probar la compatibilidad de las actualizaciones con las aplicaciones instaladas) puede redundar en un gasto considerable. Con los informes de AppDNA, puede identificar problemas y sugerir correcciones. Por ejemplo, AppDNA puede identificar las aplicaciones que tienen dependencias comunes (como .NET) para, así, instalarlas en una sola imagen base común. Asimismo, AppDNA puede identificar las aplicaciones que se cargan pronto en la secuencia de inicio del SO, por lo que puede comprobar si se comportan de la manera esperada.

#### Información útil:

- Después de actualizar una imagen, algunas aplicaciones no funcionan correctamente porque no se pueden verificar las licencias previamente instaladas. Por ejemplo, después de una actualización de imagen, iniciar Microsoft Office puede provocar que aparezca un mensaje de error similar al siguiente:

“Microsoft Office Professional Plus 2010 no puede verificar la licencia de esta aplicación. Se produjo un error en el intento de reparación o lo canceló el usuario. La aplicación se cerrará ahora”.

Para resolver este problema, desinstale Microsoft Office e instale la nueva versión en la imagen base.

- En algunos casos, falla la descarga de aplicaciones de Metro desde la Tienda Windows en una máquina virtual publicada después de una cantidad considerable de tiempo.

- Citrix recomienda que siempre coloque todos los componentes de Microsoft Office en el mismo AppDisk. Por ejemplo, un AppDisk con Microsoft Office y Project; otro AppDisk con Microsoft Office con Project y Visio.
- En algunos sistemas, SCCM deja de responder cuando se actualiza una imagen. Esta situación ocurre cuando se realizan y se aplican actualizaciones en la imagen base, lo que provoca fallos del cliente SCCM. Para resolver este problema, primero instale la instancia de cliente SCCM en la imagen base.
- En algunos casos, es posible que una aplicación instalada en el AppDisk no aparezca en el menú Inicio de Windows tras haber sido asignada a un grupo de entrega y a la máquina virtual de un usuario. Consulte [Cómo aparecen las aplicaciones en el menú Inicio](#) para obtener más información.
- Los usuarios no detectan la separación de aplicaciones y sistema operativo; tampoco son conscientes de ningún otro aspecto de la función AppDisks. Las aplicaciones se comportan como si estuvieran instaladas en la imagen. Los AppDisks que contienen aplicaciones complejas pueden provocar un pequeño retraso en el inicio del escritorio.
- Puede usar AppDisks solamente con escritorios alojados agrupados y compartidos.
- Asimismo, puede usar AppDisks con escritorios compartidos alojados.
- Puede compartir AppDisks entre las imágenes maestras y las plataformas de SO (por cada aplicación); sin embargo, esto no funcionará para todas las aplicaciones. Si dispone de aplicaciones con scripts de instalación para SO de escritorio que les impiden funcionar en un SO de servidor, Citrix recomienda empaquetar las aplicaciones por separado para cada sistema operativo.
- En muchos casos, AppDisks funciona en diferentes sistemas operativos. Por ejemplo, puede agregar un AppDisk, creado en una VM de Windows 7, a un grupo de entrega que contenga máquinas con Windows 2008 R2, siempre que ambos sistemas operativos tengan el mismo valor de bits (32 bits o 64 bits) y admitan la aplicación. Sin embargo, Citrix recomienda no agregar AppDisks creados en una versión posterior de sistema operativo (como Windows 10) a grupos de entrega que contengan máquinas con una versión anterior de sistema operativo (por ejemplo, Windows 7), porque es posible que no funcionen correctamente.
- Aun así, si debe conceder acceso a las aplicaciones de un AppDisk a solo un subconjunto de usuarios pertenecientes a un grupo de entrega, Citrix recomienda utilizar una directiva de grupo para ocultar a algunos usuarios las aplicaciones que corresponda de un AppDisk. El archivo ejecutable de la aplicación en cuestión sigue estando disponible, pero no se ejecutará para esos usuarios.
- En entornos en ruso y chino que ejecutan el sistema operativo Windows 7, el diálogo de reinicio no desaparece automáticamente. En estos casos, después de iniciar sesión en un escritorio entregado, el diálogo de reinicio aparece y debería desaparecer rápidamente.

- Cuando se utiliza la herramienta de script `Upload-PvDDiags`, falta información de registro relacionada con la capa de usuario PVD cuando la designación de la unidad del usuario no está establecida en “P”.
- En entornos configurados en vasco, un sistema operativo Windows 7 puede no mostrar correctamente el idioma apropiado en la pantalla de solicitud de reinicio. Antes de establecer el idioma a vasco, instale el francés o el español como idioma primario. A continuación, instale el vasco y establézcalo como idioma del sistema operativo.
- Al apagar un equipo, aparece un aviso de actualización PVD incluso aunque el disco PVD esté establecido en modo de solo lectura.
- Durante una actualización en contexto, podría suprimirse un archivo del Registro (DaFsFilter), lo que provoca error en la actualización.

#### Sugerencia:

Al crear un disco AppDisk, utilice una VM que solo tenga instalado el sistema operativo (es decir, que no incluya otras aplicaciones); el sistema operativo debe contener todas las actualizaciones correspondientes antes de crear el AppDisk.

## Introducción a la implementación

En la siguiente lista, se ofrece un resumen de los pasos a seguir para implementar AppDisks. Los detalles se proporcionan más adelante en este artículo.

1. Desde la consola de administración del hipervisor, instale un Virtual Delivery Agent (VDA) en una máquina virtual.
2. Cree un AppDisk, lo que implica completar los pasos de Studio y de la consola de administración del hipervisor.
3. Desde la consola de administración del hipervisor, instale aplicaciones en el AppDisk.
4. Selle el AppDisk (desde Studio o la consola de administración del hipervisor). El sellado permite que Citrix Virtual Apps and Desktops registren las aplicaciones y los archivos auxiliares del AppDisk en una biblioteca de aplicaciones (AppLibrary).
5. En Studio, cree o modifique un grupo de entrega y seleccione los AppDisks a incluir; esto se denomina *asignación de AppDisks* (aunque use la acción **Administrar AppDisks** en Studio). Cuando se inicien las máquinas virtuales del grupo de entrega, Citrix Virtual Apps and Desktops se coordinarán con la librería AppLibrary, interactuarán con Machine Creation Services (MCS) o Citrix Provisioning (antes Provisioning Services) y el Delivery Controller para distribuir por streaming los dispositivos de arranque después de que los AppDisks hayan sido configurados en ellos.

## Requisitos

Los requisitos de AppDisks se suman a los que se muestran en [Requisitos del sistema](#).

La función AppDisks solo se admite en implementaciones que contienen (como mínimo) las versiones de Delivery Controller y Studio suministradas en XenApp y XenDesktop 7.8, incluidos los requisitos previos que el instalador instala automáticamente (como .NET).

Los AppDisks se pueden crear en las mismas versiones de sistema operativo Windows que se admiten para los VDA. Las máquinas de los grupos de entrega que utilizarán AppDisks deben tener instalada al menos la versión 7.8 de VDA.

Citrix recomienda instalar o actualizar todas las máquinas a la versión más reciente de VDA y, a continuación, actualizar los catálogos de máquinas y los grupos de entrega si es necesario. Al crear un grupo de entrega, si selecciona máquinas que tienen instaladas versiones diferentes de VDA, el grupo de entrega será compatible con la versión más antigua de VDA. Este es el *nivel funcional* del grupo. Para obtener más información sobre el nivel funcional, consulte [Crear grupos de entrega](#).

Si quiere aprovisionar las máquinas virtuales que se usarán para crear AppDisks, puede usar:

- MCS proporcionado con Delivery Controller.
- La versión de Citrix Provisioning que se ofrece en la página de descargas junto con la versión de Citrix Virtual Apps and Desktops.
- Hipervisores compatibles:
  - XenServer
  - VMware (versión mínima 5.1)
  - Microsoft System Center Virtual Machine Manager

AppDisks no se puede utilizar con otros hipervisores de host y tipos de servicios de nube que se admiten para Citrix Virtual Apps and Desktops.

La creación de AppDisks no está disponible en las máquinas de catálogos de MCS que usan caché de datos temporales.

### Nota:

Se pueden conectar discos AppDisk a máquinas aprovisionadas con MCS mediante el caché de escritura, pero no se pueden usar para crear los discos AppDisk.

Los catálogos de Acceso con Remote PC no admiten el uso de AppDisks.

El Servicio de instantáneas de volumen de Windows debe estar habilitado en la máquina virtual donde se cree el AppDisk. Este servicio está habilitado de forma predeterminada.

Los grupos de entrega que se utilicen con AppDisks pueden contener máquinas provenientes de catálogos de máquinas agrupadas aleatorias con SO de servidor o de escritorio. No se puede usar AppDisks

con máquinas provenientes de otros tipos de catálogos, como escritorios agrupados estáticos o dedicados (asignados).

Las máquinas en que esté instalado Studio deben tener instalado .NET Framework 3.5 (además de otras versiones instaladas de .NET).

AppDisks puede afectar al almacenamiento. Para obtener más información, consulte [Consideraciones sobre rendimiento y almacenamiento](#).

Si utiliza AppDNA:

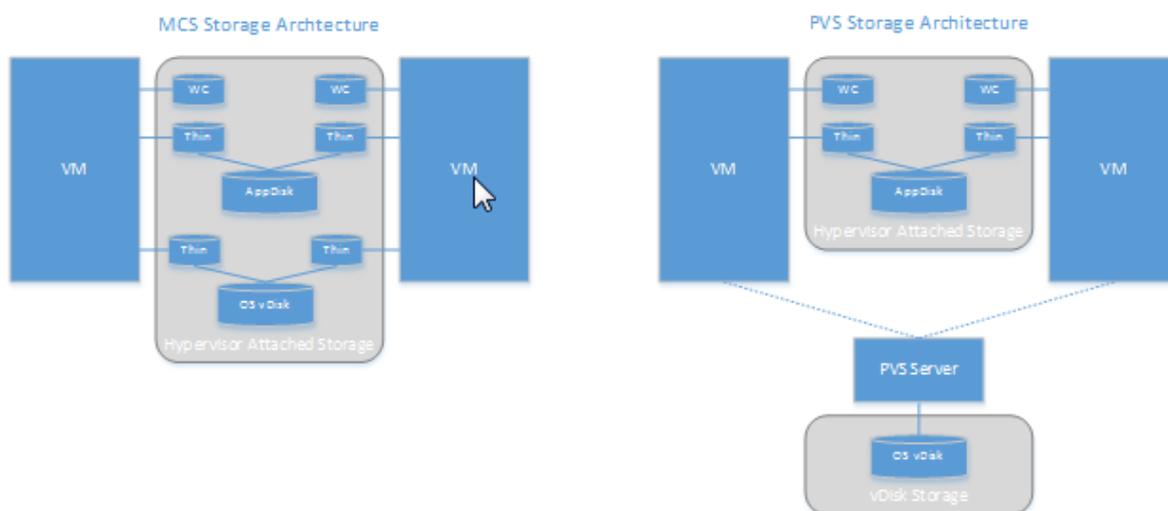
- Consulte la [documentación de AppDNA](#) y las [preguntas frecuentes de AppDisk](#).
- El software de AppDNA y Controller no deben estar instalados en el mismo servidor. Utilice la versión de AppDNA proporcionada con esta versión de Citrix Virtual Apps and Desktops. Para conocer otros requisitos de AppDNA, consulte la documentación referente a esa función.
- En el servidor AppDNA, compruebe que haya una excepción de firewall para el puerto predeterminado 8199.
- No inhabilite la conexión de AppDNA cuando cree AppDisks.
- Al crear el sitio de Citrix Virtual Apps and Desktops, puede habilitar el análisis de compatibilidad con AppDNA en la página **Funciones adicionales** del asistente para la creación de sitios. También puede habilitarlo o inhabilitarlo más adelante. Para ello, deberá seleccionar **Configuración > AppDNA** en el panel de navegación de Studio.
- En Studio, al hacer clic en el enlace “Ver informe de problemas”, aparece el informe de AppDNA. Sin embargo, las combinaciones de sistema operativo que utiliza AppDNA de forma predeterminada son Windows 7 de 64 bits para grupos de entrega de escritorios y Windows Server 2012 R2 para grupos de entrega de servidores. Si los grupos de entrega cuentan con versiones diferentes de Windows, las combinaciones predeterminadas de imagen en los informes que muestra Studio serán incorrectas. Para solucionar este problema, modifique manualmente el informe en AppDNA después de que Studio lo haya creado.
- Hay una dependencia entre las distintas versiones de servidor AppDNA y Studio.
  - Desde la versión 7.12, Studio debe ser tener la misma versión (o una posterior) que el servidor AppDNA.
  - Para las versiones 7.9 y 7.11, las versiones del servidor Studio y AppDNA deben coincidir.
  - En la siguiente tabla se resumen las versiones que pueden combinarse (Sí = versiones a combinar; - = no funcionan combinadas):

Versión del producto	Studio 7.9	Studio 7.11	Studio 7.12	Studio 7.13	Studio 7.14	Studio 7.15
AppDNA 7.9	Sí	-	-	-	-	-
AppDNA 7.11	-	Sí	-	-	-	-

Versión del producto	Studio 7.9	Studio 7.11	Studio 7.12	Studio 7.13	Studio 7.14	Studio 7.15
AppDNA 7.12	-	-	Sí	Sí	Sí	Sí
AppDNA 7.13	-	-	Sí	Sí	Sí	Sí
AppDNA 7.14	-	-	-	-	Sí	Sí
AppDNA 7.15	-	-	-	-	-	Sí

### Consideraciones sobre rendimiento y almacenamiento

Separar aplicaciones y sistema operativo mediante dos discos y almacenar esos discos en áreas diferentes puede afectar a su planificación de almacenamiento. En el gráfico siguiente, se muestran las arquitecturas de almacenamiento de Machine Creation Services y Citrix Provisioning. “WC” indica la memoria caché de escritura, mientras que “Thin” indica el disco ligero usado para almacenar las diferencias entre los discos virtuales de sistema operativo y el AppDisk de una máquina virtual.



En entornos de MCS:

- Puede seguir equilibrando el tamaño de los discos virtuales (vDisk) del sistema operativo y de los AppDisks con las directrices de tamaño de datos existentes en la empresa. Si los AppDisks se comparten entre varios grupos de entrega, se puede reducir la capacidad total de almacenamiento.
- Los AppDisks y los discos virtuales de SO se encuentran en las mismas áreas de almace-

namiento, por lo que debe planificar con cuidado sus requisitos de capacidad de almacenamiento con el fin de evitar cualquier efecto negativo en la capacidad resultante cuando implemente los AppDisks. Los AppDisks pueden sobrecargarse, por lo que su almacenamiento debe poder adaptarse a esa sobrecarga y a las aplicaciones.

- No hay ningún efecto relevante sobre IOPS porque los discos virtuales del SO y los AppDisks se encuentran en la misma área de almacenamiento. No hay aspectos a tener en cuenta sobre la memoria caché de escritura cuando se utilice Machine Creation Services.

En entornos de Citrix Provisioning:

- Debe permitir IOPS y la capacidad aumentada porque las aplicaciones se moverán desde el almacenamiento de AppDisk al almacenamiento correspondiente al hipervisor.
- Con Citrix Provisioning, los AppDisks y los discos virtuales (vDisk) del SO no comparten las áreas de almacenamiento. La capacidad de almacenamiento del disco virtual (vDisk) del sistema operativo se reduce, mientras que el almacenamiento correspondiente al hipervisor aumenta. Por lo tanto, debe dar a los entornos de Citrix Provisioning el tamaño adecuado para dar cabida a esos cambios.
- Los AppDisks del almacenamiento correspondiente al hipervisor requieren más IOPS, mientras que los discos virtuales del sistema operativo requieren menos.
- Memoria caché de escritura: Citrix Provisioning utiliza un archivo VHDX dinámico en una unidad con formato NTFS; cuando se escriben bloques en la memoria caché de escritura, el archivo VHDX se extiende dinámicamente. Cuando los AppDisks se conectan a su máquina virtual asociada, se combinan con los discos virtuales (vDisk) del sistema operativo para ofrecer una vista unificada del sistema de archivos. Por lo general, esta combinación tiene como resultado que se escriban datos adicionales en la caché de escritura, lo que aumenta el tamaño del archivo de caché de escritura. Debe tener esto en cuenta cuando planifique la capacidad necesaria.

En ambos entornos, MCS o Citrix Provisioning, no olvide reducir el tamaño del disco virtual (vDisk) del SO para aprovechar los AppDisks que cree. Si no, deberá planificar más almacenamiento.

Cuando varios usuarios de un sitio enciendan sus equipos simultáneamente (por ejemplo, al inicio de la jornada laboral), las múltiples solicitudes de inicio ejercen presión sobre el hipervisor, lo que puede afectar al rendimiento. En caso de Citrix Provisioning, las aplicaciones no se encuentran en el disco virtual (vDisk) del SO, por lo que se realizan menos solicitudes al servidor Citrix Provisioning. Con la menor carga resultante en cada dispositivo de destino, el servidor Citrix Provisioning puede transmitir a más destinos. Sin embargo, tenga en cuenta que una mayor densidad entre destino y servidor podría afectar negativamente al rendimiento cuando haya una gran cantidad de arranques de máquinas.

## Consideraciones sobre la creación de AppDisks

Hay dos formas de crear un AppDisk, instalar aplicaciones en él y sellarlo. Ambos métodos incluyen pasos a completar desde Studio y la consola de administración del hipervisor. Los métodos se diferencian en dónde se completa la mayoría de los pasos.

Independientemente del método que utilice:

- Reserve 30 minutos para la creación del AppDisk.
- No inhabilite la conexión de AppDNA cuando cree AppDisks.
- Cuando agregue aplicaciones a un AppDisk, instale aplicaciones para todos los usuarios. Rearme aquellas aplicaciones que usen la activación de Key Management Server (KMS). Para obtener más información, consulte la documentación de la aplicación.
- No se conservan los archivos, las carpetas ni las entradas de Registro que se hayan creado en ubicaciones específicas del usuario durante la creación de AppDisk. Además, algunas aplicaciones ejecutan un asistente de primer uso para crear datos de usuario durante la instalación. Use una solución de administración de perfiles para conservar esos datos y evitar que el asistente aparezca cada vez que se inicie el AppDisk.
- Si usa AppDNA, el análisis comienza automáticamente después de que se complete el proceso de creación. Durante este intervalo, el estado del AppDisk en Studio es “analizando”.

## Consideraciones sobre Citrix Provisioning

En máquinas procedentes de catálogos creados con Provisioning Services, AppDisks requiere una configuración adicional durante la creación de AppDisk. Desde la consola de Provisioning Services:

1. Cree una nueva versión del disco virtual (vDisk) asociado a la colección de dispositivos que contiene la máquina virtual.
2. Coloque la máquina virtual en el modo de mantenimiento.
3. Durante la creación de AppDisk, seleccione la versión de mantenimiento en la pantalla de inicio cada vez que se reinicie la máquina virtual.
4. Después de sellar el AppDisk, coloque la máquina virtual de nuevo en producción y elimine la versión de disco virtual (vDisk) creada.

## Crear un AppDisk principalmente en Studio

Este procedimiento incluye tres tareas: crear el AppDisk, crear las aplicaciones en el AppDisk y, a continuación, sellar el AppDisk.

### Crear un AppDisk:

1. Seleccione **AppDisks** en el panel de navegación de Studio y, a continuación, seleccione **Crear AppDisk** en el panel Acciones.
2. Revise la información en la página **Introducción** del asistente y haga clic en **Siguiente**.
3. En la página **Crear AppDisk**, seleccione el botón de opción **Crear nuevo AppDisk**. Seleccione un tamaño de disco predefinido (pequeño, mediano o grande), o bien especifique un tamaño de disco en GB; el tamaño mínimo es de 3 GB. El tamaño del disco debe ser lo suficientemente grande para alojar las aplicaciones que se vayan a agregar. Haga clic en **Siguiente**.
4. En la página **Máquina de preparación**, seleccione un catálogo de máquinas agrupadas aleatorias para que se utilicen como la imagen maestra en la que se generará el AppDisk. Nota: La pantalla muestra todos los catálogos de máquinas presentes en el sitio separados por tipo; solo se pueden seleccionar aquellos catálogos que contengan al menos una máquina disponible. Si elige un catálogo que no contiene máquinas virtuales agrupadas aleatorias, fallará la creación del AppDisk. Después de seleccionar una VM de un catálogo de máquinas virtuales agrupadas aleatorias, haga clic en **Siguiente**.
5. En la página **Resumen**, escriba un nombre y una descripción para el AppDisk. Revise la información especificada en las páginas anteriores del asistente. Haga clic en **Finalizar**.

Recuerde: Si utiliza Citrix Provisioning, siga las instrucciones de [Consideraciones sobre Citrix Provisioning](#).

Una vez cerrado el asistente, la pantalla de Studio referente al nuevo AppDisk indicará “Creando”. Después de crear el AppDisk, la pantalla cambia a “Listo para instalar aplicaciones”.

### **Instalar aplicaciones en el AppDisk:**

Desde la consola de administración del hipervisor, instale aplicaciones en el AppDisk (**Sugerencia:** Si olvida el nombre de la VM, seleccione **AppDisks** en el panel de navegación de Studio y, a continuación, seleccione **Instalar aplicaciones** en el panel “Acciones” para ver el nombre). Consulte la documentación del hipervisor para obtener información sobre cómo instalar las aplicaciones. (Recuerde: Debe instalar aplicaciones en el AppDisk desde la consola de administración del hipervisor. No use la tarea **Instalar aplicaciones** en el panel “Acciones” de Studio.)

### **Sellar el AppDisk:**

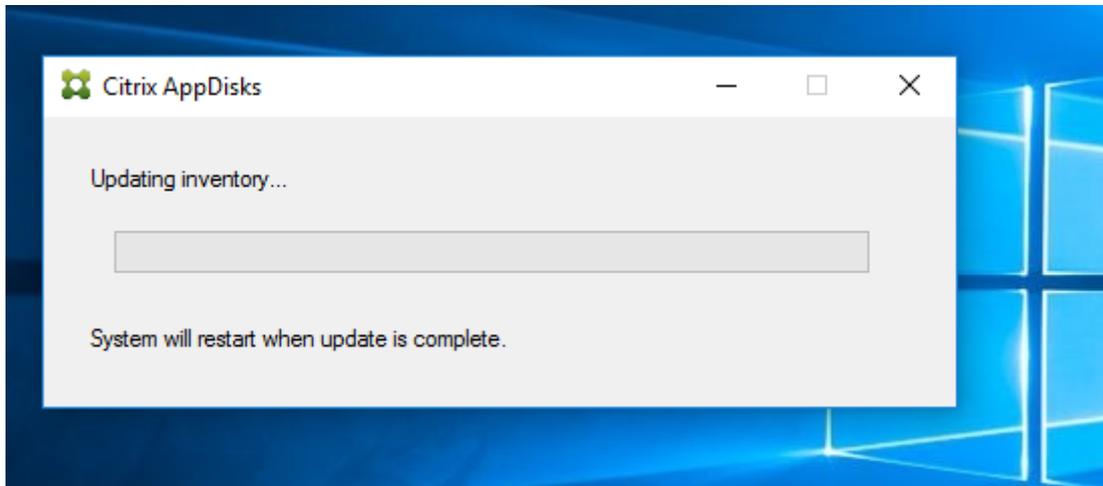
1. Seleccione **AppDisks** en el panel de navegación de Studio.
2. Seleccione el AppDisk que ha creado y seleccione **Sellar AppDisk** en el panel Acciones.

Después de crear el AppDisk, instale aplicaciones en él, séllelo y asígnelo a un grupo de entrega.

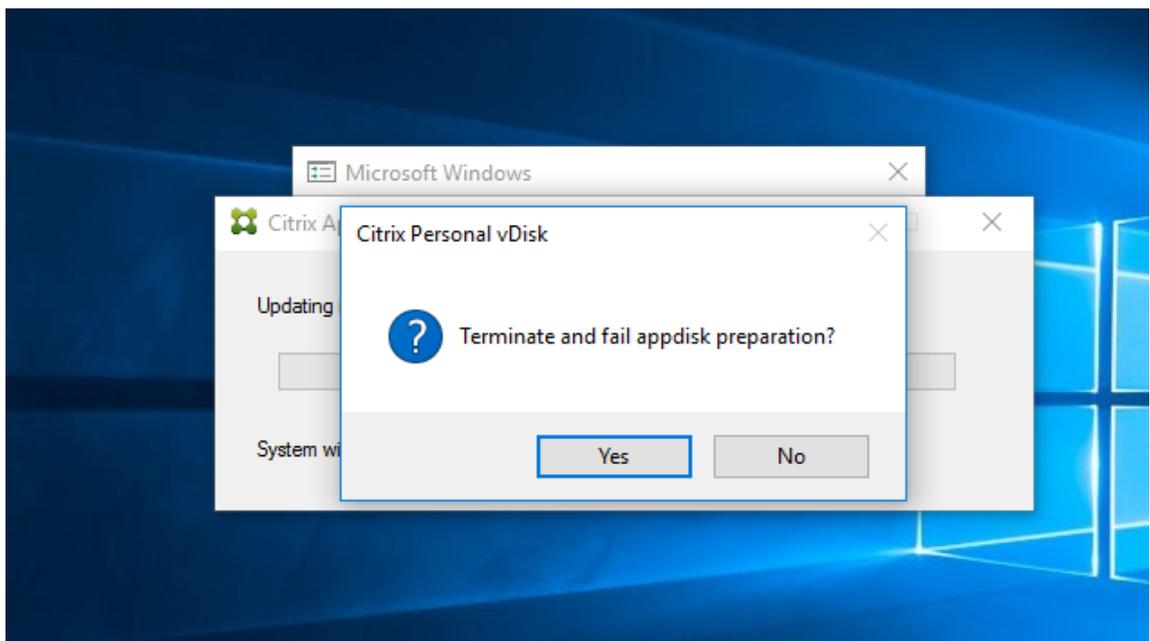
### **Cancelar la preparación y el sellado de AppDisk**

En algunos casos, puede que un administrador necesite cancelar la creación o el sellado de AppDisk:

1. Acceda a la máquina virtual.
2. Cierre el cuadro de diálogo:



3. Después de cerrar el cuadro de diálogo, aparece un mensaje emergente que solicita confirmación para cancelar la operación seleccionada. Haga clic en **Sí**.



**Nota**

Si cancela la preparación de AppDisk, reiniciar la máquina la devuelve a su estado inicial; de lo contrario, debe crear una VM limpia.

## Crear un AppDisk en el hipervisor e importarlo en Studio

En este procedimiento, se completan las tareas de creación y preparación del AppDisk desde la consola de administración del hipervisor y, a continuación, el AppDisk se importa en Studio.

### Preparar, instalar aplicaciones y sellar un AppDisk en el hipervisor:

1. Desde la consola de administración del hipervisor, cree una máquina virtual e instale un VDA en ella.
2. Apague la máquina y tome una instantánea de ella.
3. Cree una nueva máquina a partir de la instantánea y, a continuación, agréguele un disco nuevo. Ese disco (que se convertirá en el AppDisk) debe ser lo suficientemente grande como para alojar todas las aplicaciones que se instalarán en él.
4. Inicie la máquina y seleccione **Inicio > Preparar AppDisk**. Si este acceso directo al menú Inicio no está disponible en el hipervisor, abra un símbolo del sistema en C:\Archivos de programa\Citrix\personal vDisk\bin y escriba: **CtxPvD.Exe –s LayerCreationBegin**. La máquina se reiniciará y preparará el disco. Se produce un segundo reinicio después de unos minutos, cuando se complete la preparación.
5. Instale las aplicaciones que quiere poner a disposición de los usuarios.
6. Haga doble clic en el acceso directo **Paquete AppDisk** en el escritorio de la máquina. La máquina se reinicia y comienza el proceso de sellado. Cuando se cierre el cuadro de diálogo “En proceso”, apague la máquina virtual.

### Use Studio para importar el AppDisk creado en el hipervisor:

1. Seleccione **AppDisks** en el panel de navegación de Studio y, a continuación, seleccione **Crear AppDisk** en el panel Acciones.
2. Revise la información en la página **Introducción** y haga clic en **Siguiente**.
3. En la página **Crear AppDisk**, seleccione el botón de opción **Importar AppDisk existente**. Seleccione el recurso (red y almacenamiento) donde reside el AppDisk que ha creado en el hipervisor. Haga clic en **Siguiente**.
4. En la página **Máquina de preparación**, vaya a la máquina, seleccione el disco y haga clic en **Siguiente**.
5. En la página **Resumen**, escriba un nombre y una descripción para el AppDisk. Revise la información especificada en las páginas anteriores del asistente. Haga clic en **Finalizar**. Studio importa el AppDisk.

Después de importar el AppDisk en Studio, asígnelo a un grupo de entrega.

## Asignar un AppDisk a un grupo de entrega

Puede asignar uno o varios AppDisks a un grupo de entrega a la hora de crear el grupo de entrega o más adelante. La información que proporcione sobre los AppDisks es esencialmente la misma.

Si está agregando AppDisks a un grupo de entrega que está creando, use la siguiente guía para la página **AppDisks** en el asistente para crear el grupo de entrega (Para obtener información sobre otras páginas de ese asistente, consulte [Crear grupos de entrega.](#))

Para agregar (o quitar) AppDisks de un grupo de entrega existente:

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo de entrega y seleccione **Administrar AppDisks** en el panel Acciones. Consulte las siguientes instrucciones para la página **AppDisks**.
3. Al cambiar la configuración de AppDisk en un grupo de entrega, es obligatorio reiniciar las máquinas del grupo.

### Página de AppDisks:

La página **AppDisks** (en el asistente para crear grupos de entrega o en el flujo “Administrar AppDisks”) ofrece una lista de los AppDisks ya implementados para el grupo de entrega, junto con la prioridad que tienen. (Si está creando el grupo de entrega, la lista estará vacía.) Para obtener más información, consulte la sección “Prioridad de AppDisk”.

1. Haga clic en **Agregar**. En el cuadro de diálogo Seleccionar AppDisks, se ofrece una lista de todos los AppDisks de la columna izquierda. Los AppDisks que ya están asignados a ese grupo de entrega tienen las casillas marcadas y no se pueden seleccionar.
2. Marque una o varias casillas de los AppDisks disponibles en la columna izquierda. En la columna derecha, se ofrece una lista de las aplicaciones presentes en el AppDisk. (Al seleccionar la ficha **Aplicaciones** situada encima de la columna derecha, se muestran aplicaciones en un formato similar al del menú Inicio. Al seleccionar la ficha **Paquetes instalados**, se ofrece una lista de las aplicaciones en un formato similar al de la lista Programas y características.)
3. Después de seleccionar uno o varios AppDisks disponibles, haga clic en **Aceptar**.
4. Haga clic en **Siguiente** en la página de AppDisks.

### Prioridad de AppDisk en un grupo de entrega

Cuando un grupo de entrega tiene asignado más de un AppDisk, la página **AppDisks** (en las pantallas “Crear grupo de entrega”, “Modificar grupo de entrega” y “Administrar AppDisks”) muestra los AppDisks por prioridad descendente. Las entradas situadas en la parte superior de la lista tienen la prioridad más alta. La prioridad indica el orden en que se procesan los AppDisks.

Puede usar las flechas de dirección arriba y abajo ubicadas junto a la lista para cambiar la prioridad de cada AppDisk. Si está AppDNA integrado en la implementación de AppDisk, entonces analiza au-

tomáticamente las aplicaciones y establece la prioridad cuando los AppDisks se asignan al grupo de entrega. Posteriormente, si agrega o quita AppDisks del grupo, hacer clic en **Orden automático** indica al AppDNA que debe volver a analizar la lista actual de AppDisks y volver a determinar las prioridades. El análisis (y la reordenación de prioridades, si fuera necesario) puede tardar varios minutos en completarse.

## Administrar AppDisks

Después de crear y asignar AppDisks a los grupos de entrega, puede cambiar las propiedades de un AppDisk con la ayuda del nodo AppDisks en el panel de navegación de Studio. Los cambios a las aplicaciones de un AppDisk deben realizarse desde la consola de administración del hipervisor.

### Consideraciones importantes sobre Windows Update:

Puede usar el servicio Windows Update para actualizar aplicaciones (por ejemplo, el conjunto de aplicaciones Office) en un AppDisk. Sin embargo, no use el servicio Windows Update para aplicar las actualizaciones del sistema operativo a un AppDisk. Aplique las actualizaciones de sistema operativo a la imagen maestra, no al AppDisk; de lo contrario, el AppDisk no se inicializará correctamente.

- Al aplicar correcciones y otras actualizaciones a las aplicaciones de un AppDisk, aplique solo aquellas que requiera cada aplicación. No aplique actualizaciones para otras aplicaciones.
- Cuando se instalen actualizaciones de Windows, primero deseleccione todas las entradas y, a continuación, seleccione el subconjunto que necesiten las aplicaciones en los AppDisks que esté actualizando.

## Consideraciones sobre antivirus para la creación de AppDisk

En algunos casos, puede toparse con problemas si intenta crear un AppDisk cuando la VM base tiene un agente antivirus instalado. En esos casos, la creación de AppDisk puede fallar porque el antivirus marca ciertos procesos como peligrosos. Estos procesos, **CtxPvD.exe** y **CtxPvDSrv.exe**, se deben agregar a la lista de excepciones del antivirus que se utilice en la VM base.

En esta sección, se ofrece información sobre cómo agregar excepciones en las siguientes aplicaciones de antivirus:

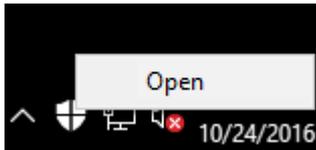
- Windows Defender (para Windows 10)
- OfficeScan (versión 11.0)
- Symantec (versión 12.1.16)
- McAfee (versión 4.8)

## Windows Defender

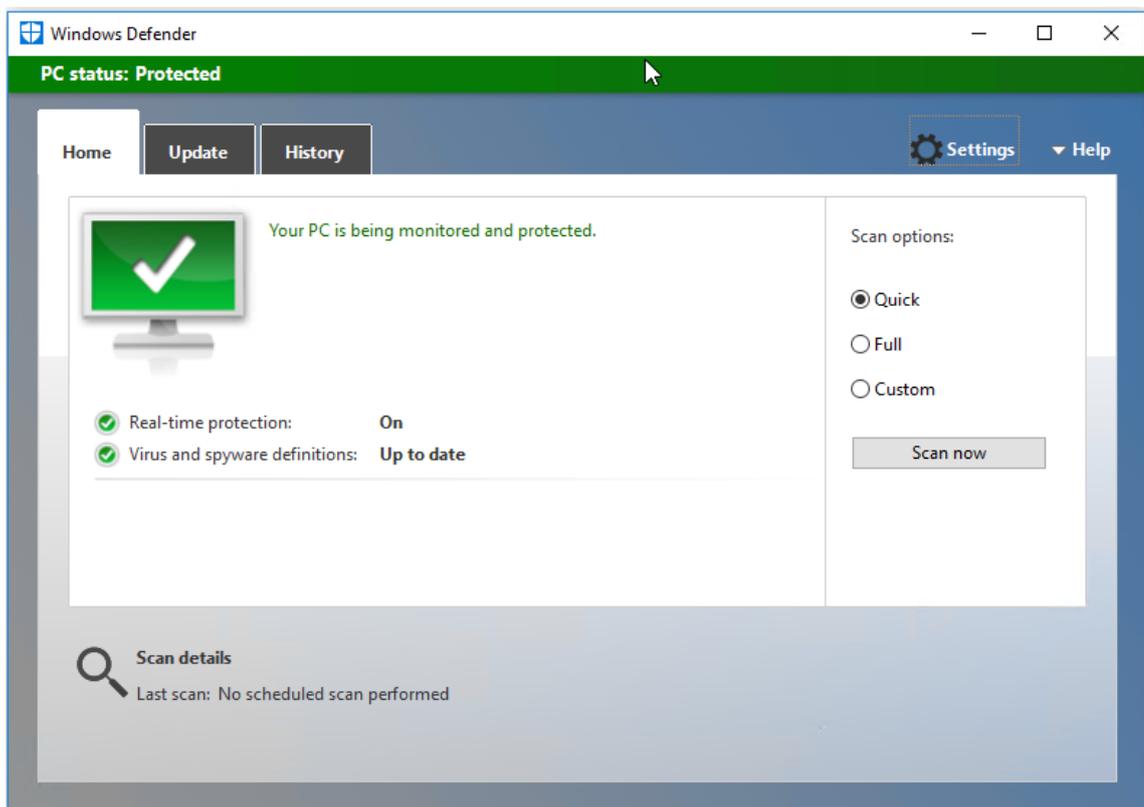
Si la VM base usa Windows Defender (versión 10):

1. Inicie sesión en el equipo con privilegios de administrador local.
2. Seleccione el icono de Windows Defender y haga clic con el botón secundario para ver el botón

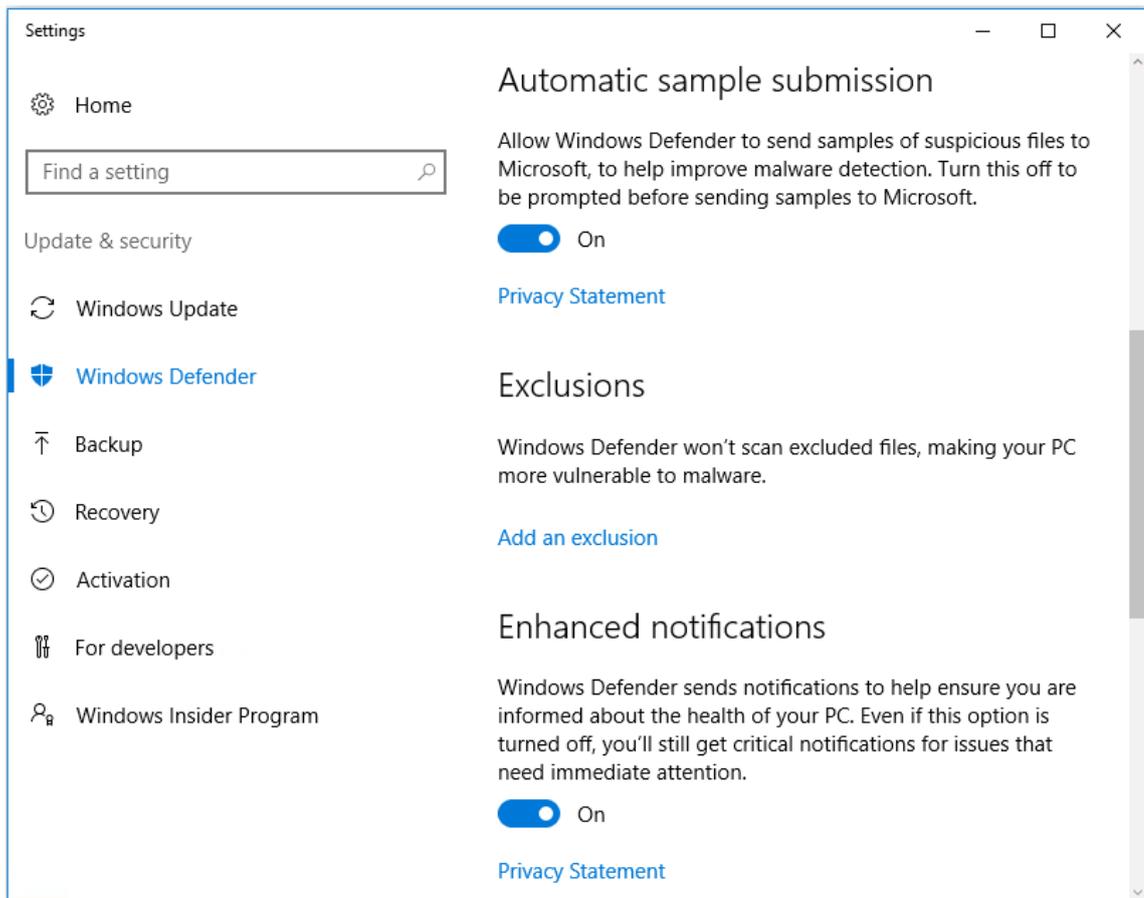
**Abrir:**



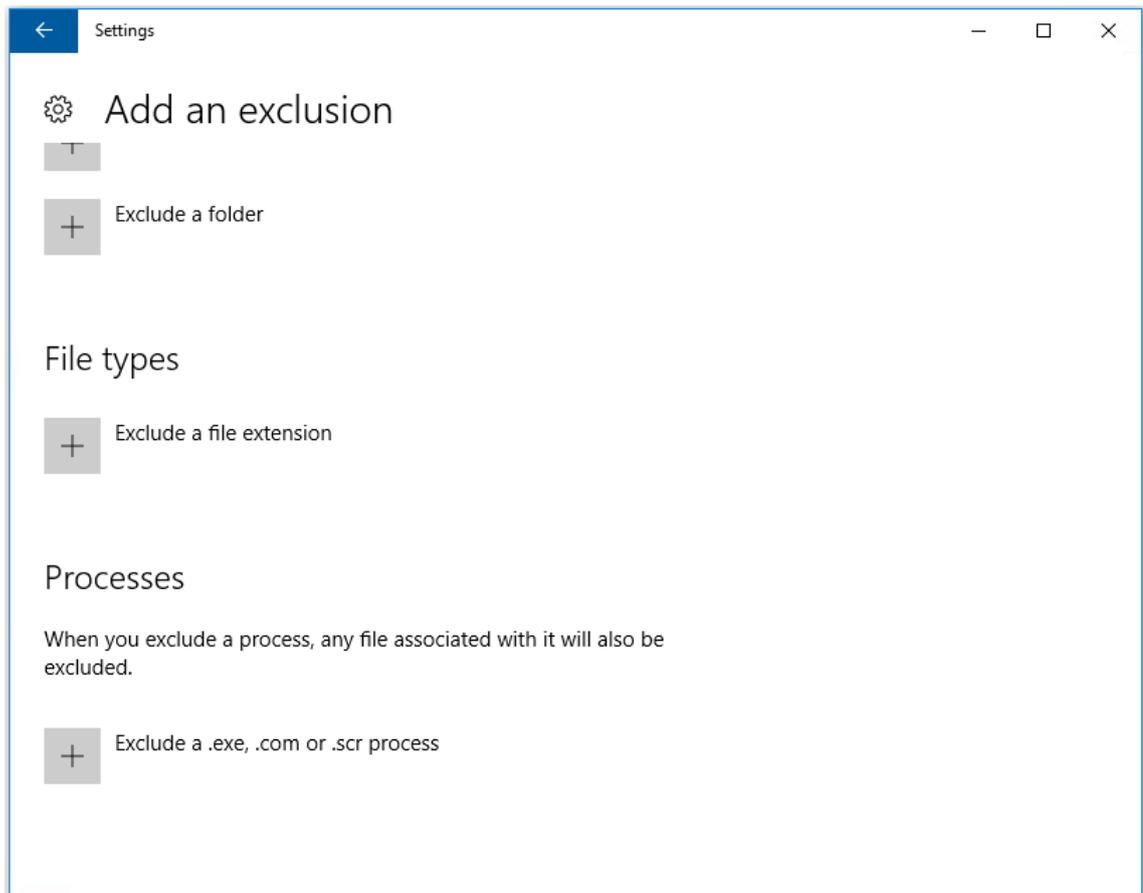
3. En la consola de Windows Defender, seleccione **Configuración** en la parte superior derecha de la interfaz:



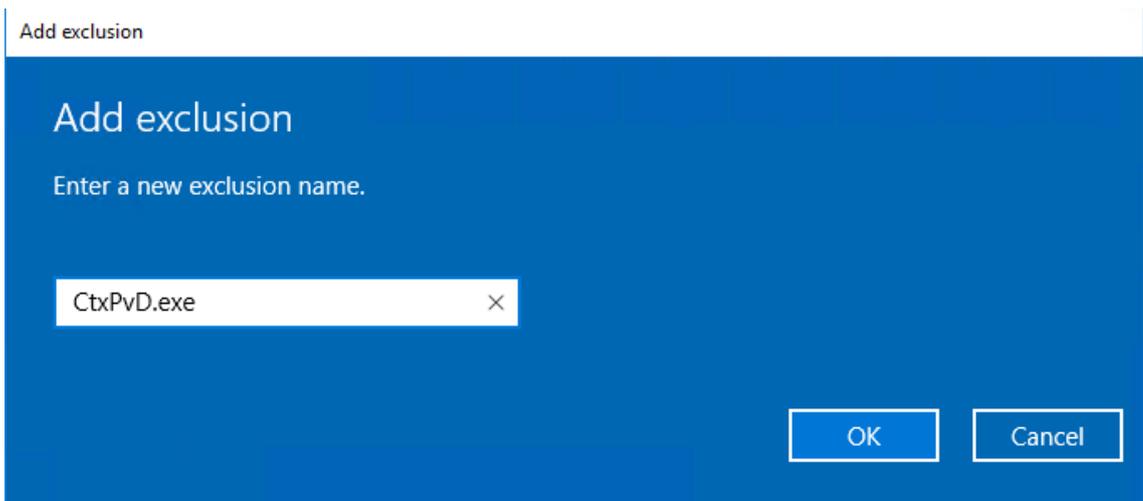
4. En la sección **Exclusiones** de la pantalla “Configuración”, haga clic en **Agregar exclusión**:



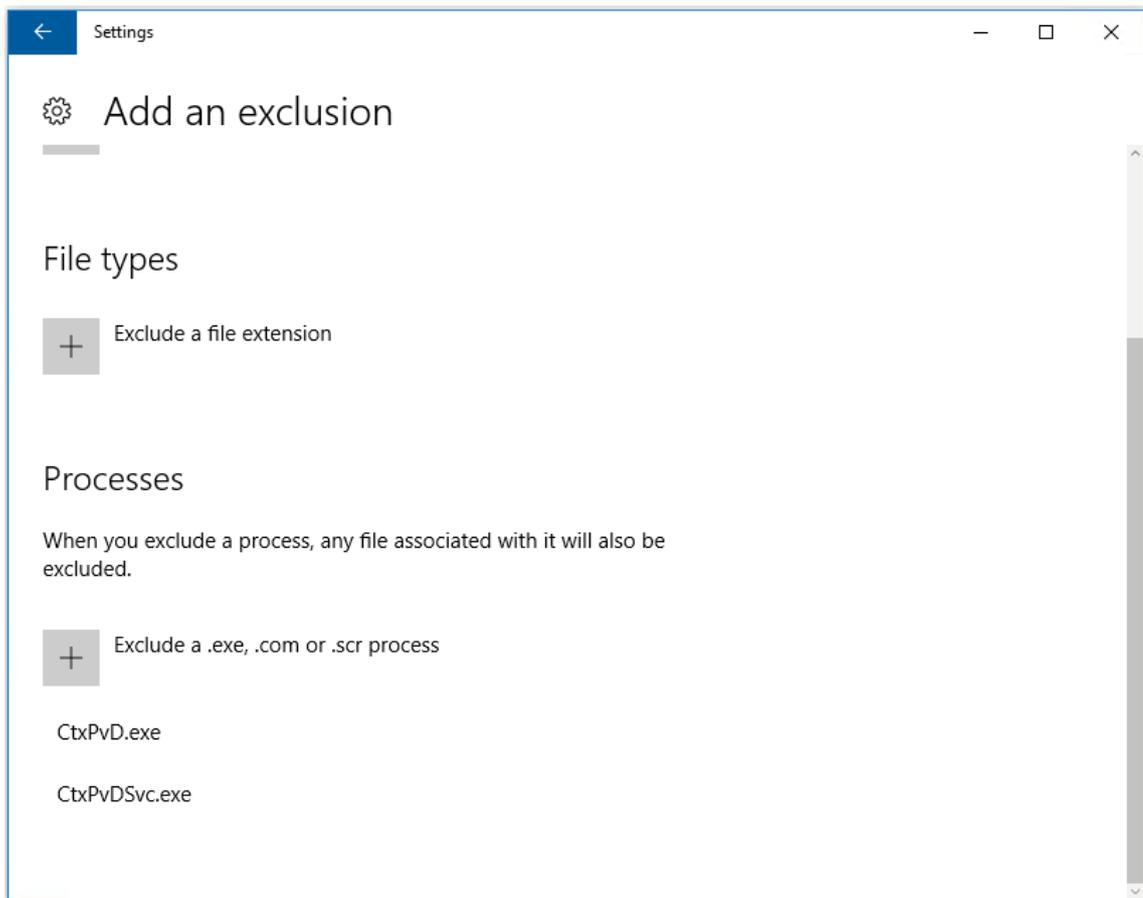
5. En la pantalla **Agregar exclusión**, seleccione **Excluir un proceso EXE, COM o SCR**:



6. En la pantalla **Agregar exclusión**, escriba el nombre de la exclusión; deben agregarse **Ctx-PvD.exe** y **CtxPvDSvc.exe** a fin de evitar conflictos en el momento de crear un AppDisk. Después de escribir el nombre de la exclusión, haga clic en **Aceptar**:



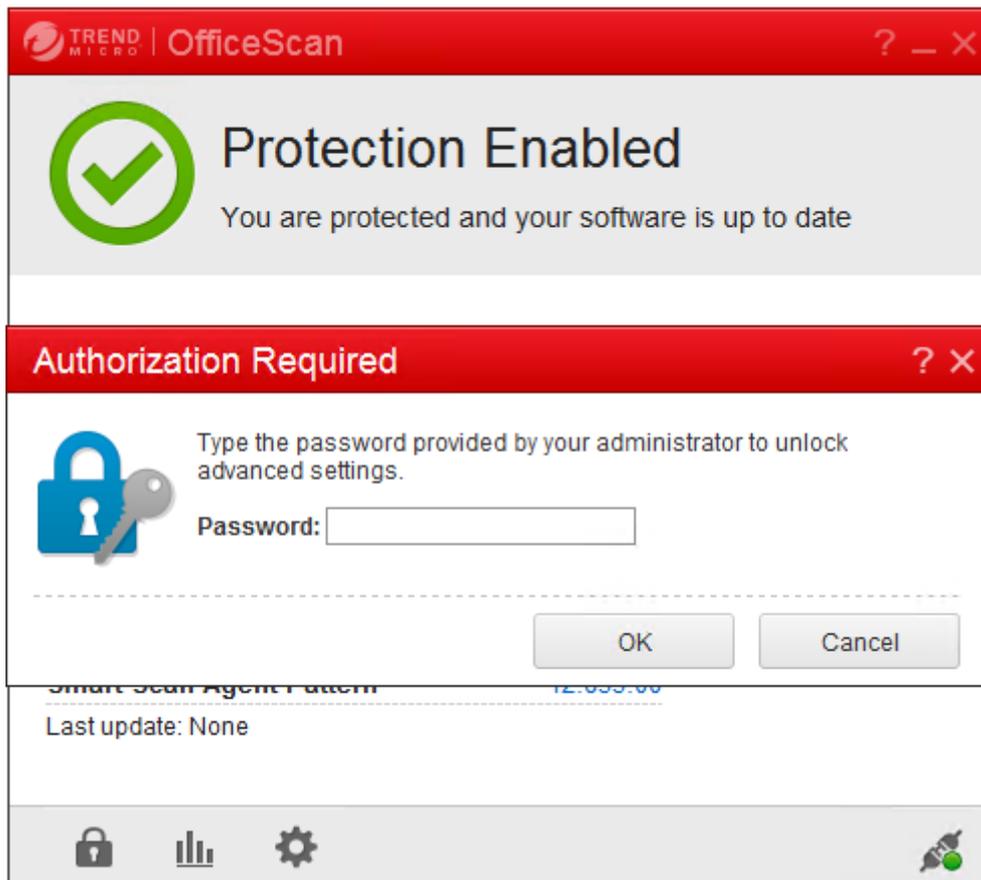
Después de agregar las exclusiones, aparecen en la lista de procesos excluidos en la pantalla **Configuración**:



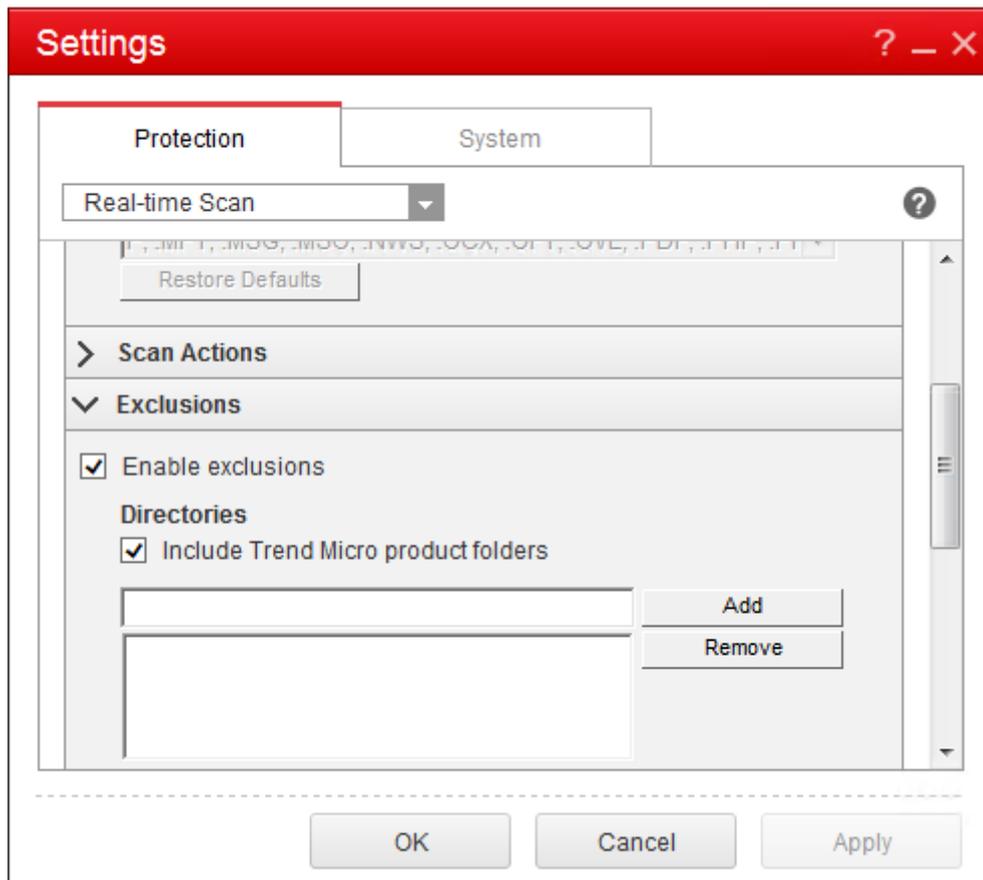
## OfficeScan

Si la VM base usa OfficeScan (versión 11):

1. Inicie la consola de OfficeScan.
2. Haga clic en el icono de bloqueo en la parte inferior izquierda de la interfaz y escriba la contraseña:



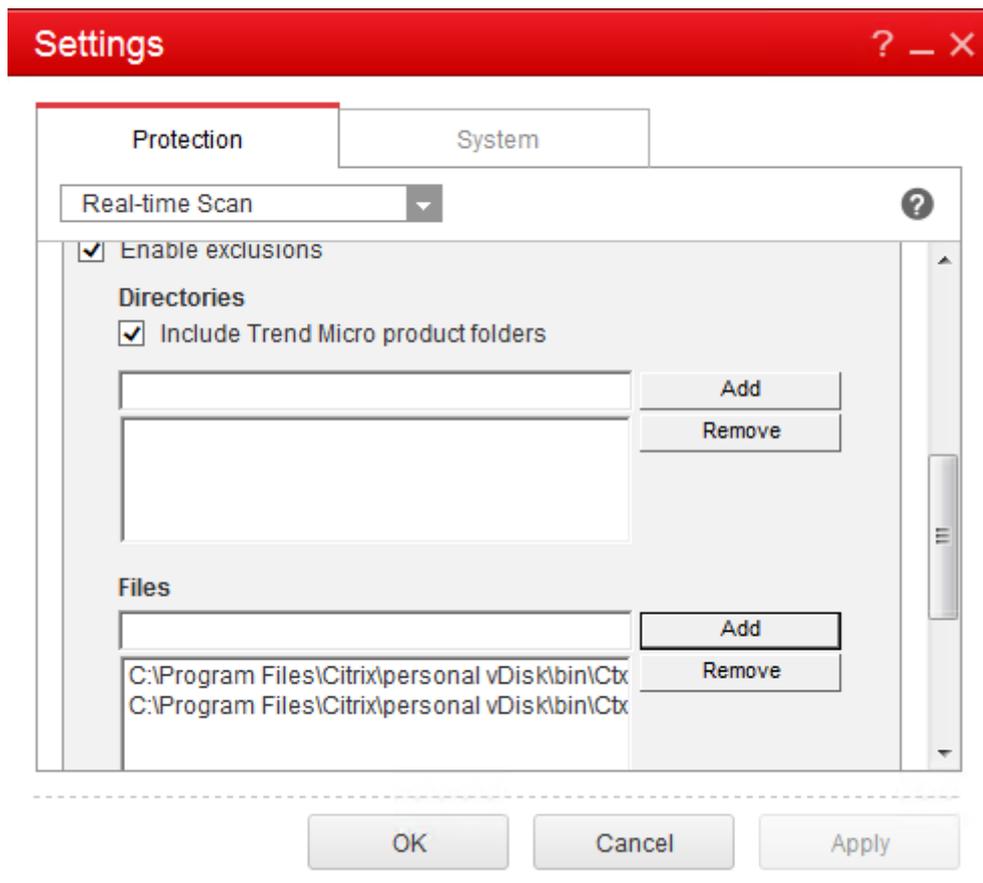
3. Haga clic en el icono **Settings** para ver las opciones de configuración.
4. En la pantalla “Settings”, seleccione la ficha **Protection**.
5. En la ficha de protección, desplácese hasta encontrar la sección **Exclusions**.



6. En la sección **Files**, haga clic en **Add** y, a continuación, introduzca los siguientes procesos de AppDisk a la lista de excepciones:

`C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe`

`C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe`

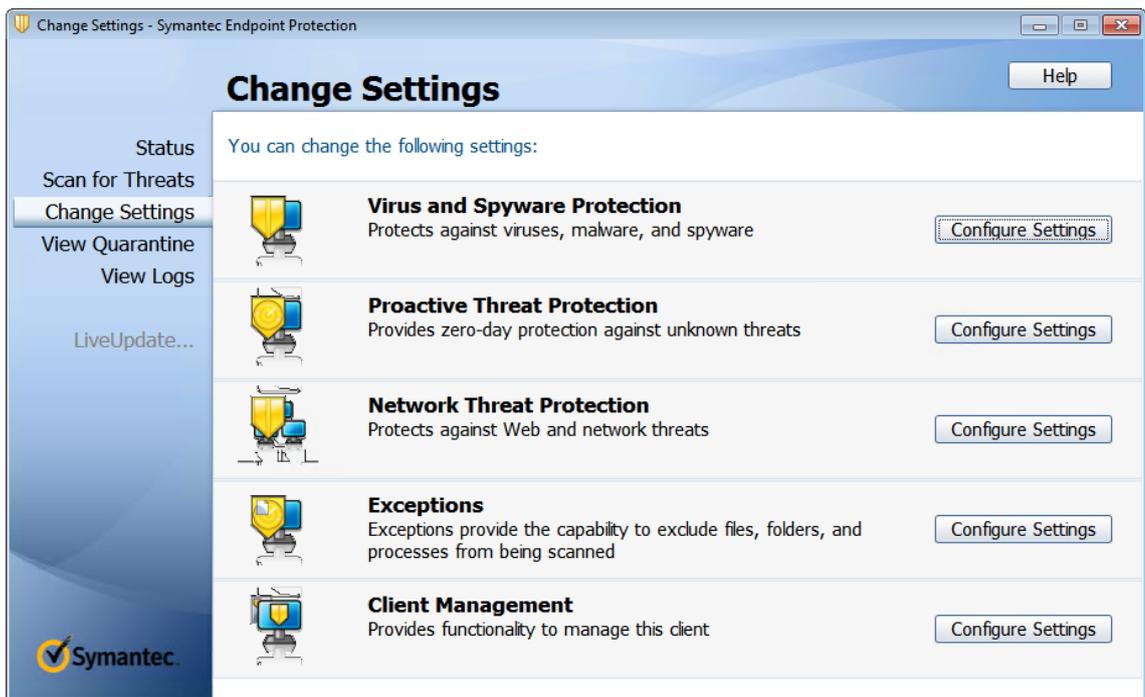


7. Haga clic en **Apply** y, a continuación, en **OK** para agregar las exclusiones.

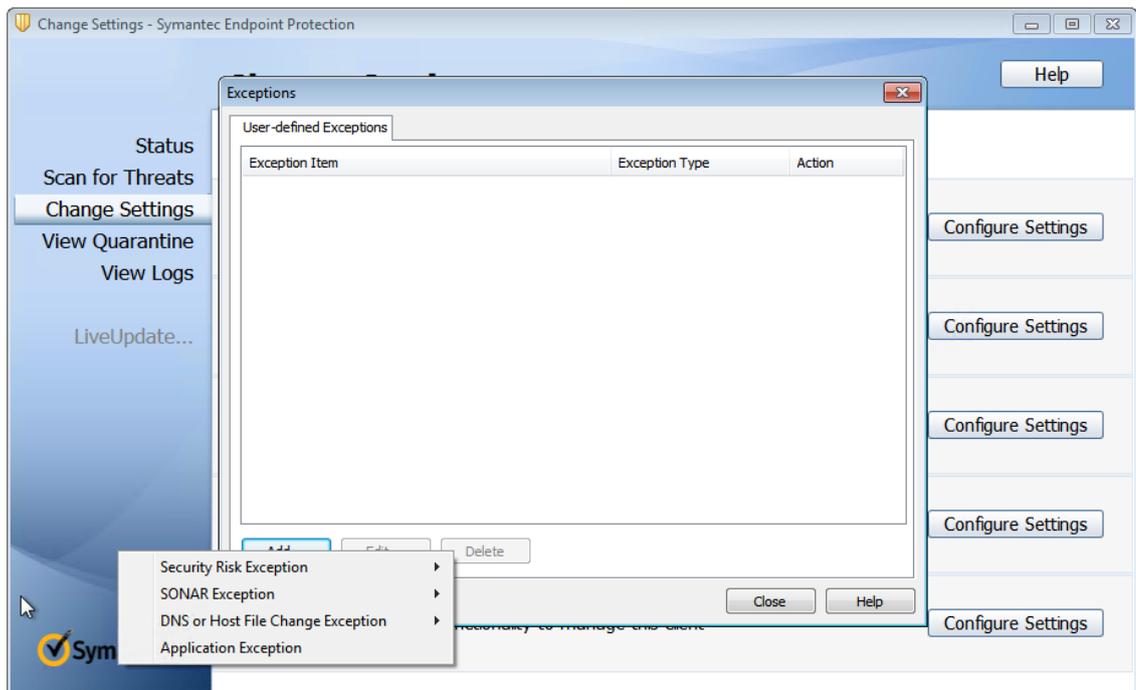
## Symantec

Si la VM base usa Symantec (versión 12.1.16):

1. Inicie la consola de Symantec.
2. Haga clic en **Change Settings**.
3. En la sección **Exceptions**, haga clic en **Configure Settings**:



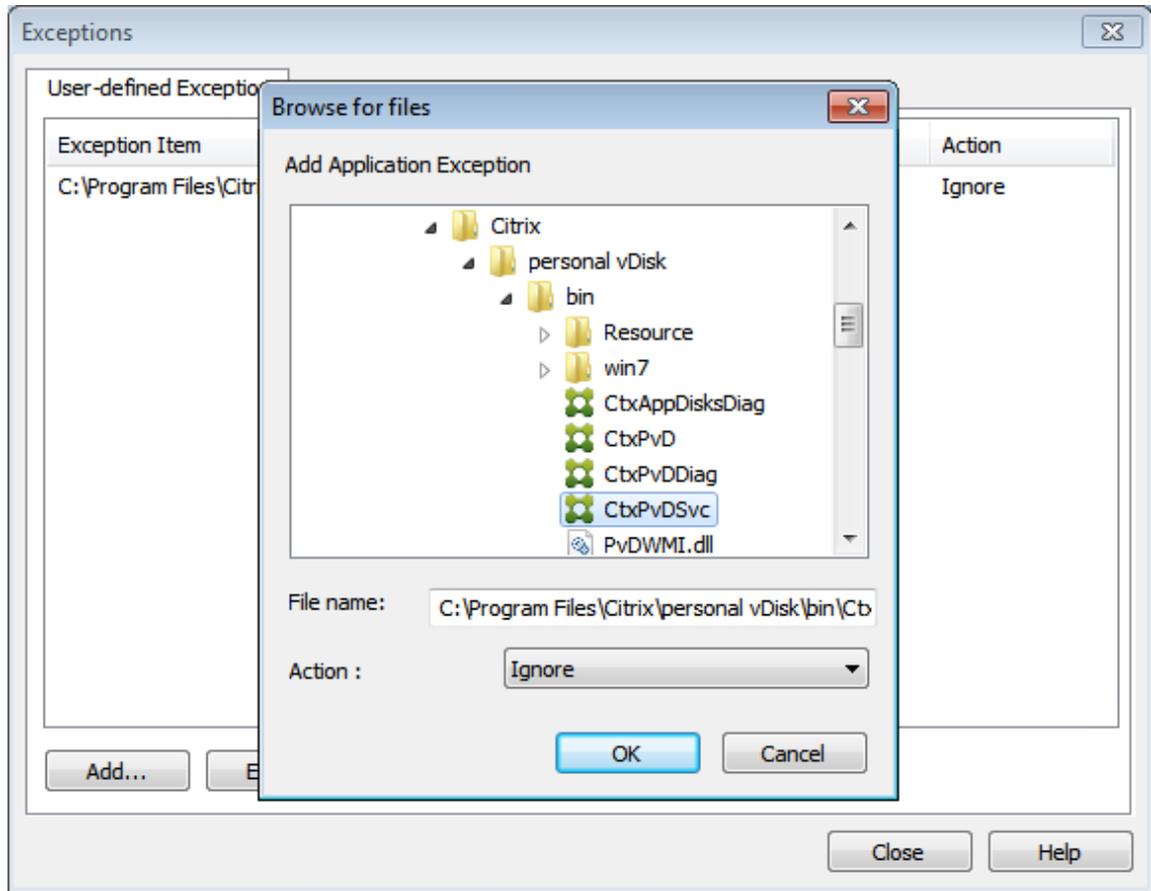
4. En la pantalla de configuración, haga clic en **Add**.
5. Después de hacer clic en la opción de agregar, aparecerá el menú contextual, que permite especificar el tipo de aplicación. Seleccione **Application Exception**:



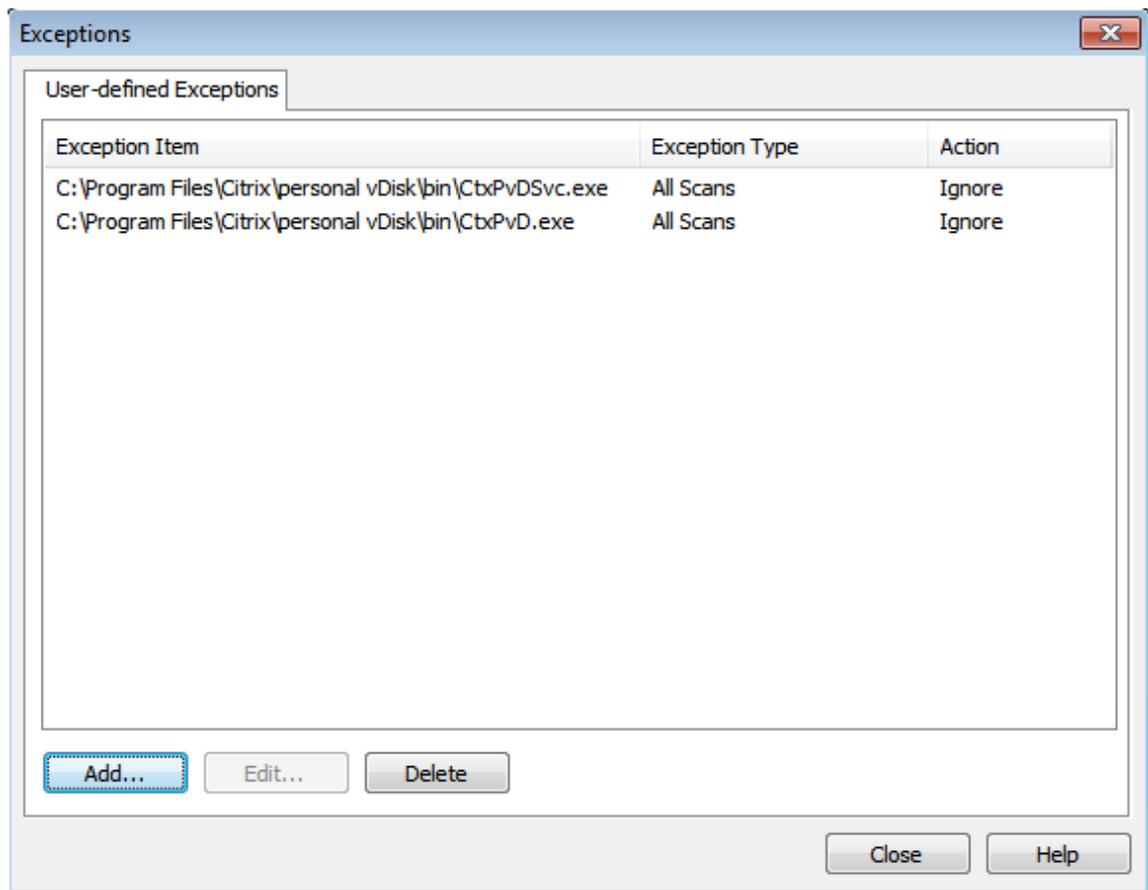
6. En la pantalla de excepciones, introduzca las siguientes rutas de archivo de AppDisk y establezca la acción en **Ignore**:

C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe

C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe



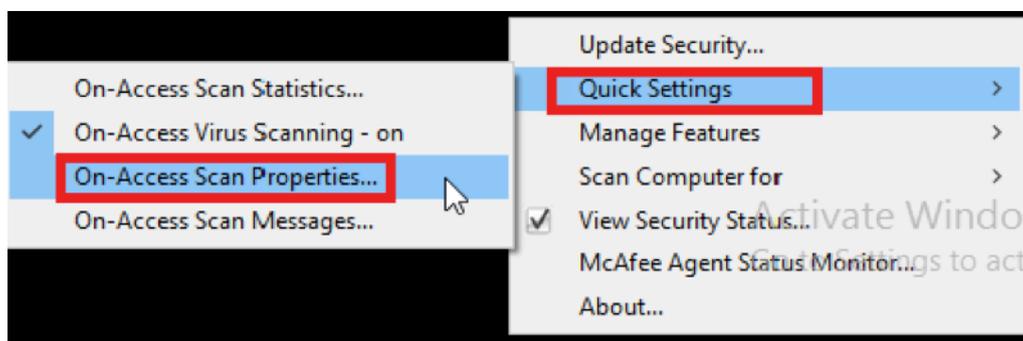
Las excepciones indicadas se agregan a la lista. Cierre la ventana para aplicar los cambios.



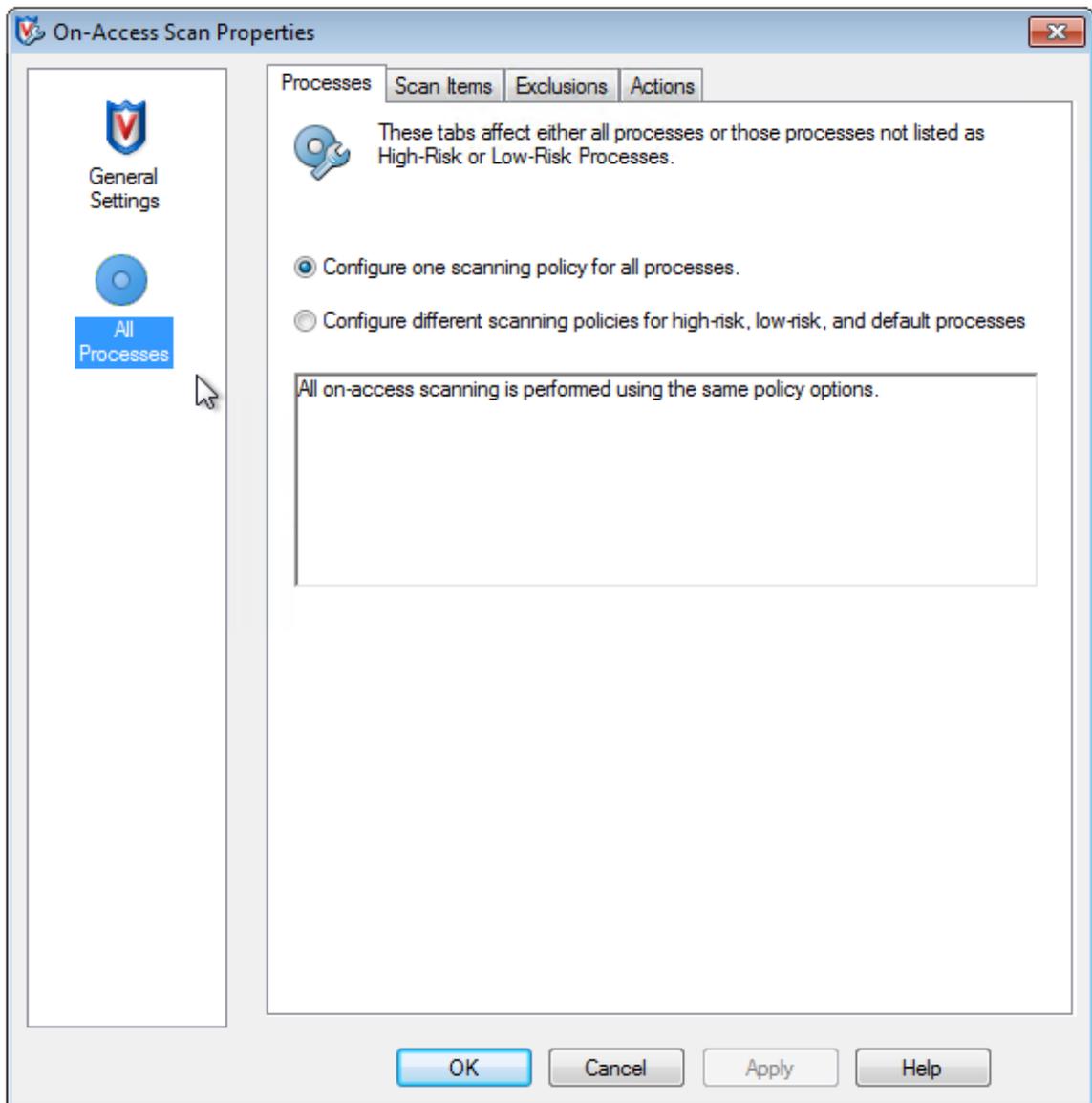
## McAfee

Si la VM base usa McAfee (versión 4.8):

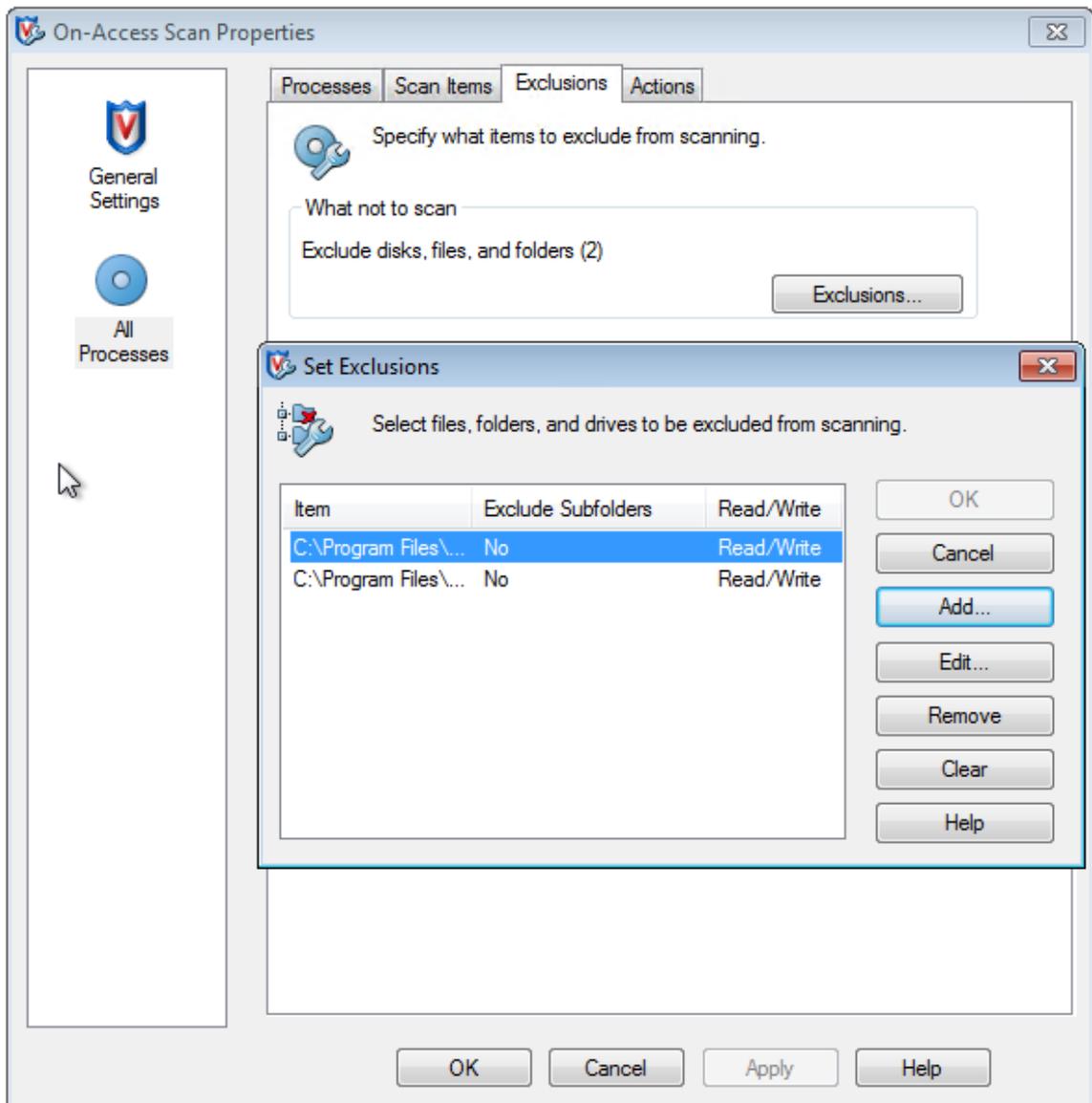
1. Haga clic con el botón secundario en el icono de McAfee y expanda la opción **Quick Settings**.
2. En el menú expandido, seleccione **On-Access Scan Properties**:



3. En la pantalla **On-Access Scan Properties**, haga clic en **All Processes**:



4. Seleccione la ficha **Exclusions**.
5. Haga clic en el botón **Exclusions**.
6. En la pantalla **Set exclusions**, haga clic en **Add**:

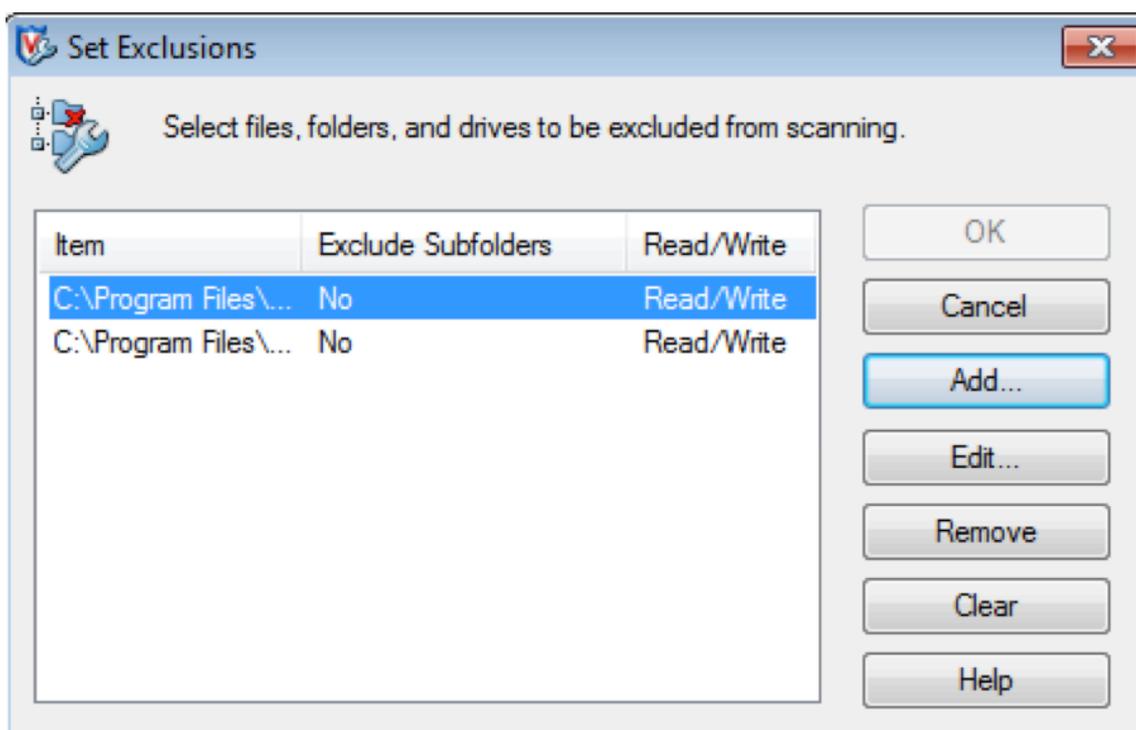


7. En la pantalla **Add Exclusion Item**, seleccione **By name/location (can include wildcards \* or ?)**. Haga clic en **Browse** para buscar los archivos ejecutables de exclusión:

C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe

C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe

8. Haga clic en **Aceptar**.
9. Ahora, la pantalla **Set Exclusions** muestra las exclusiones agregadas. Haga clic en **OK** para aplicar los cambios:



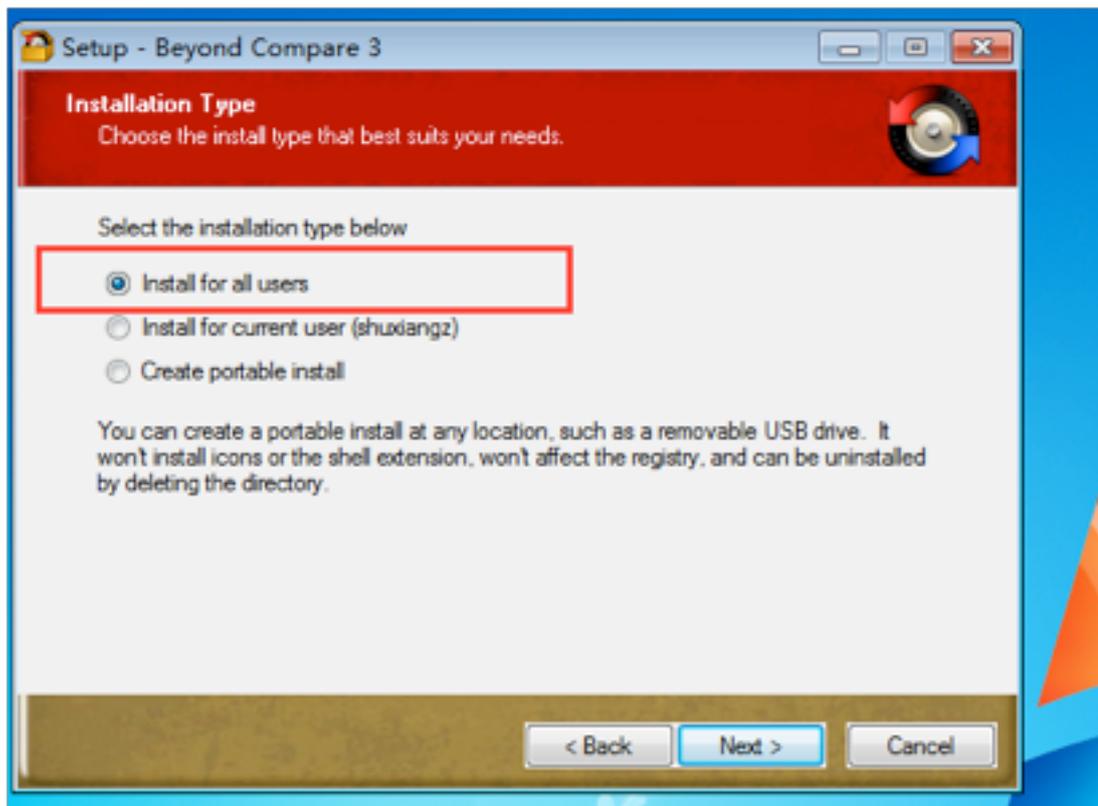
Después de la configuración de estas exclusiones, cree el AppDisk.

### Cómo aparecen las aplicaciones en el menú Inicio

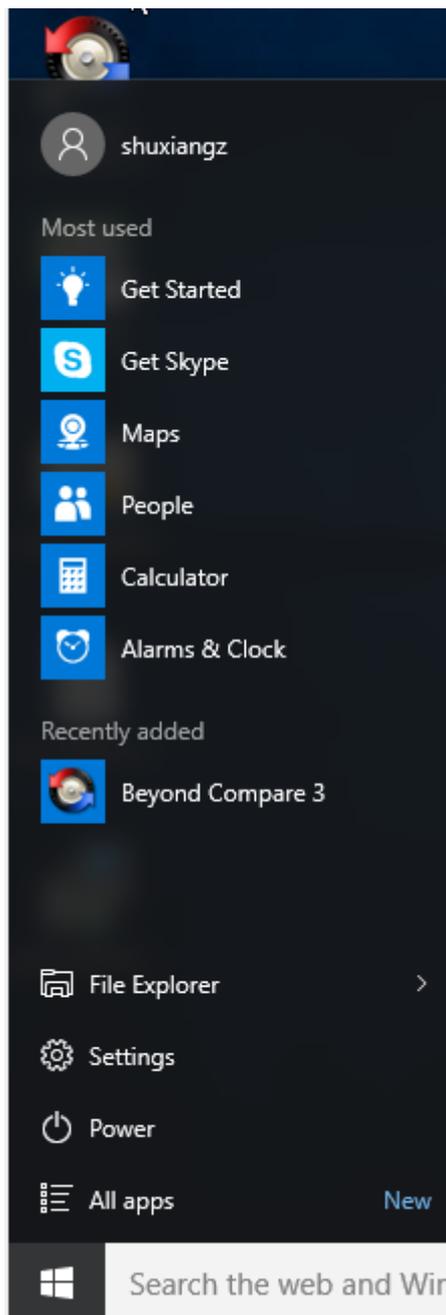
Si se crea un nuevo AppDisk y una aplicación se pone a disposición de todos los usuarios a los que está conectado el disco del escritorio, aparece un acceso directo de la aplicación en el menú Inicio. Si se crea un AppDisk y se instala solo para el usuario actual, y el disco está conectado al escritorio, el acceso directo de la aplicación no aparece en el menú Inicio.

Por ejemplo, cree una nueva aplicación y póngala a disposición de todos los usuarios:

1. Instale una aplicación en el AppDisk (por ejemplo, *Beyond Compare*):

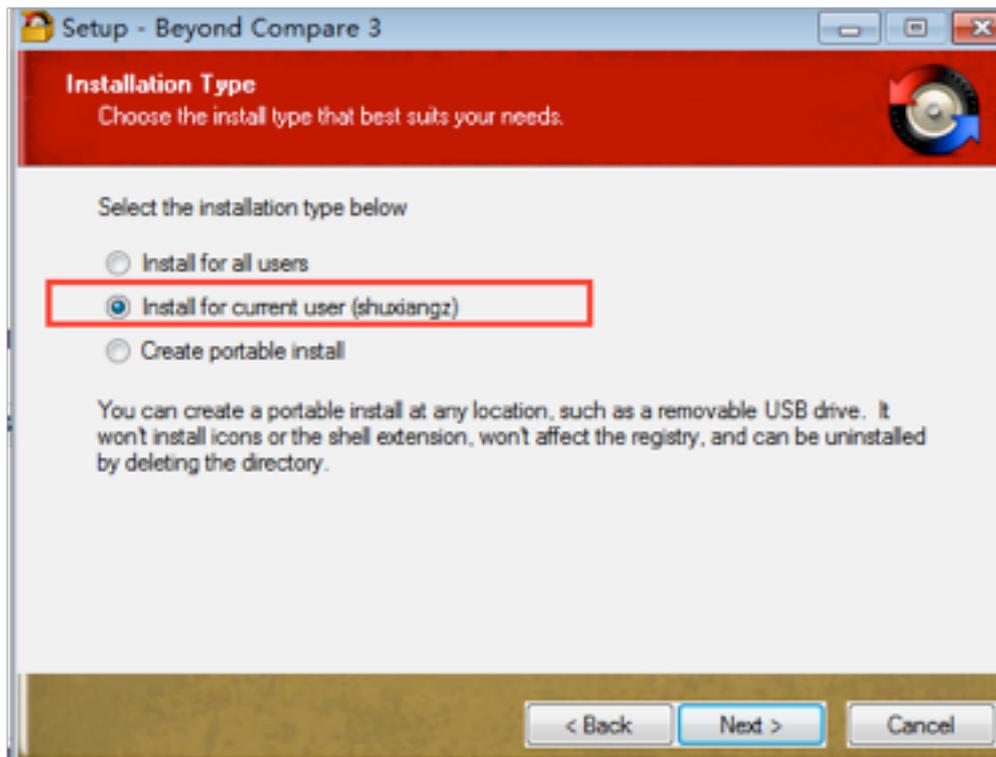


2. Conecte el disco al escritorio y el acceso directo de la aplicación recién instalada (*Beyond Compare*) aparecerá en el menú Inicio:

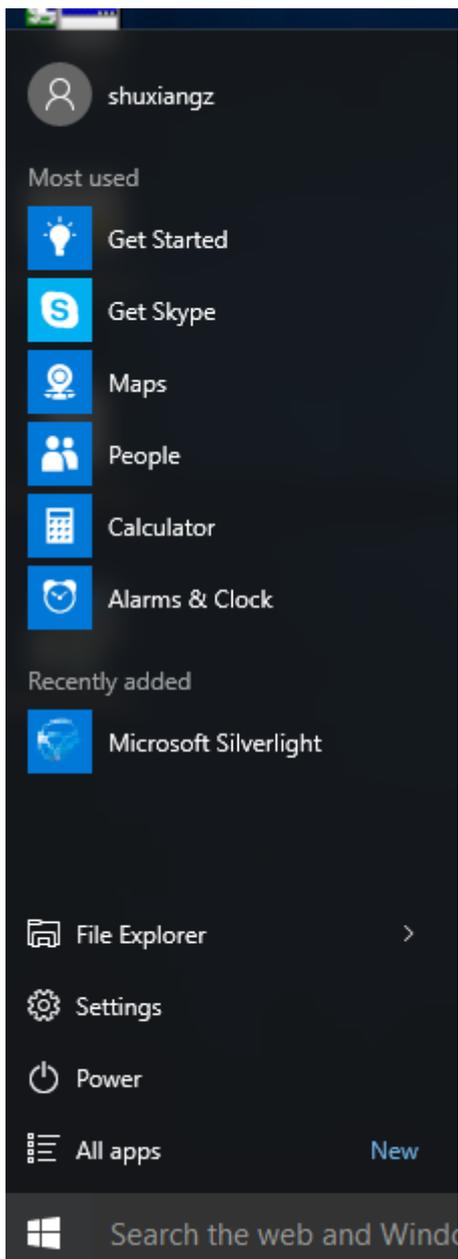


Para instalar una aplicación solo para el usuario actual:

1. Instale una aplicación en el AppDisk y póngala a disposición del usuario actual:



2. Conecte el disco al escritorio; tenga en cuenta que el acceso directo no aparecerá en el menú Inicio:



## Registros de AppDisk

Los usuarios de AppDisk pueden obtener información de diagnóstico y cargarla en el [sitio web de Citrix Insight Services \(CIS\)](#).

## Cómo funciona

En esta funcionalidad, se utiliza una herramienta de scripts de PowerShell que identifica todos los archivos de registro creados por AppDisk o PVD, recopila los resultados de los comandos de Power-

Shell que contienen información sobre el sistema (y los procesos), lo comprime todo en un archivo único y organizado y, finalmente, ofrece la opción de guardar la carpeta comprimida localmente o cargarla en CIS (Citrix Insight Services).

**Nota:**

CIS recopila información anónima de diagnóstico que usa para mejorar la funcionalidad de AppDisk o PVD. Debe acceder al [sitio web de Citrix CIS](#) para cargar manualmente el paquete de diagnóstico. Necesita sus credenciales de Citrix para iniciar sesión en este sitio.

### Usar scripts de PowerShell para recopilar archivos de registro de AppDisk o PVD

El instalador de AppDisk o PVD agrega dos scripts para la recopilación de datos de diagnóstico:

- `Upload-AppDDiags.ps1`: Lleva a cabo la recopilación de datos de diagnóstico de AppDisk.
- `Upload-PvDDiags.ps1`: Lleva a cabo la recopilación de datos de diagnóstico de PVD.

Estos archivos se agregan a `C:\Archivos de programa\Citrix\personal vDisk\bin\scripts`. Estos scripts de PowerShell se deben ejecutar como administrador.

**Upload-AppDDiags.ps1** Use este script para iniciar la recopilación de datos de diagnóstico de AppDisk y cargar manualmente los datos en el sitio web de CIS.

```
Upload-AppDDiags [[-OutputFile] <string>] [-help] [<CommonParameters>]
```

`-OutputFile`: Ruta local al archivo ZIP en lugar de cargarlo en CIS. Cuando se omita `-OutputFile`, se realiza la carga. En cambio, cuando se especifica `-OutputFile`, el script crea un archivo ZIP que usted puede cargar manualmente más tarde.

Ejemplos:

- `Upload-AppDDiags`: Carga datos de diagnóstico en el sitio web de Citrix CIS mediante las credenciales que haya escrito el usuario interactivo.
- `Upload-AppDDiags -OutputFile C:\MyDiags.zip`: Guarda los datos de diagnóstico de AppDisk en el archivo ZIP especificado. Puede acceder a <https://cis.citrix.com/> para cargarlo más tarde.

**Upload-PvDDiags.ps1** Use este script para iniciar la recopilación de datos de diagnóstico de PVD y cargar manualmente los datos en el sitio web de CIS.

```
Upload-PvDDiags [[-OutputFile] <string>] [-help] [<CommonParameters>]
```

`-OutputFile`: Ruta local al archivo ZIP en lugar de cargarlo en CIS. Cuando se omite `-OutputFile`, se realiza la carga. En cambio, cuando se especifica `-OutputFile`, el script crea un archivo ZIP que usted puede cargar manualmente más tarde.

Ejemplos:

- `Upload-PvDDiags`: Carga datos de diagnóstico de PvD en el sitio web de Citrix CIS mediante las credenciales que haya escrito el usuario interactivo.
- `Upload-PvDDiags -OutputFile C:\MyDiags.zip`: Guarda los datos de diagnóstico de PvD en el archivo ZIP especificado. Puede acceder a <https://cis.citrix.com/> para cargarlo más tarde.

## Publicar contenido

September 22, 2021

Puede publicar una aplicación que sea una ruta UNC o una dirección URL a un recurso (por ejemplo, un documento de Microsoft Word o un enlace web). Esta función se conoce como Contenido publicado. La capacidad para publicar contenido flexibiliza la entrega de contenido a los usuarios. Le permite aprovechar las aplicaciones existentes de administración y control del acceso. Además, puede especificar qué se debe utilizar para abrir el contenido: aplicaciones locales o publicadas.

El contenido publicado aparece como las demás aplicaciones en StoreFront y la aplicación Citrix Workspace. Los usuarios acceden a él de la misma forma que acceden a las aplicaciones. En el cliente, el recurso se abre como es habitual.

- Si existe una aplicación instalada localmente que sea adecuada, ésta se inicia para abrir el recurso.
- Si se ha definido una asociación de tipos de archivo, se inicia una aplicación publicada para abrir el recurso.

Puede publicar contenido con el SDK de PowerShell. (No se puede utilizar Studio para publicar contenido. No obstante, puede usar Studio para modificar posteriormente las propiedades de las aplicaciones, una vez publicadas.)

## Preparación y resumen de configuración

Para publicar contenido, use el cmdlet `New-BrokerApplication` con las siguientes propiedades de clave. (Consulte la ayuda de cmdlets para ver una descripción de las propiedades de todos los cmdlets.)

```
1 New-BrokerApplication -ApplicationType PublishedContent -  
  CommandLineExecutable location -Name app-name -DesktopGroup delivery  
  -group-name  
2 <!--NeedCopy-->
```

La propiedad `ApplicationType` debe ser `PublishedContent`.

La propiedad `CommandLineExecutable` indica la ubicación del contenido publicado. Se admiten los formatos siguientes, con un límite de 255 caracteres.

- Dirección del sitio web HTML (por ejemplo, <http://www.citrix.com>)
- Archivo de documento en un servidor web (por ejemplo, <https://www.citrix.com/press/pressrelease.doc>)
- Directorio en un servidor FTP (por ejemplo, <ftp://ftp.citrix.com/code>)
- Archivo de documento en un servidor FTP (por ejemplo, <ftp://ftp.citrix.com/code/Readme.txt>)
- Ruta de directorio UNC (por ejemplo, <file://myServer/myShare> or `\\\\myServer\\myShare`)
- Ruta de archivo UNC (por ejemplo, <file://myServer/myShare/myFile.asf> o `\\\\myServer\\myShare\\myFile.asf`)

Compruebe que cuenta con el SDK correcto.

- Para las implementaciones de servicios de Citrix Virtual Apps and Desktops, [descargue](#) e instale Citrix Virtual Apps and Desktops Remote PowerShell SDK.
- Para implementaciones locales de Citrix Virtual Apps and Desktops, use el SDK de PowerShell que se instala con el Delivery Controller. Agregar una aplicación de contenido publicado requiere como mínimo la versión 7.11 de Delivery Controller.

Se usan ejemplos en los siguientes procedimientos. En los ejemplos:

- Se ha creado un catálogo de máquinas.
- Se ha creado un grupo de entrega llamado `PublishedContentApps`. El grupo utiliza una máquina de SO de servidor proveniente del catálogo. Se ha agregado la aplicación WordPad al grupo.
- Se han hecho asignaciones para el nombre del grupo de entrega, la ubicación `CommandLineExecutable` y el nombre de la aplicación.

## Introducción

En la máquina que contiene el SDK de PowerShell, abra PowerShell.

El cmdlet siguiente agrega el complemento adecuado del SDK de PowerShell y asigna el registro devuelto del grupo de entrega.

```
Add-PsSnapin Citrix\* $dg = Get-BrokerDesktopGroup -Name PublishedContentApps
```

Si utiliza el servicio Citrix Virtual Apps and Desktops, debe autenticarse con sus credenciales de Citrix Cloud. Si hay más de un cliente, elija uno.

### Publicar una URL

Después de asignar el nombre y la ubicación de la aplicación, el cmdlet siguiente publica la página de inicio de Citrix como una aplicación.

```
1 $citrixUrl = "https://www.citrix.com/"
2 $appName = "Citrix Home Page"
3
4 New-BrokerApplication -ApplicationType PublishedContent -
   CommandLineExecutable $citrixUrl -Name $appName -DesktopGroup $dg.
   Uid
5 <!--NeedCopy-->
```

Compruebe el resultado:

- Abra StoreFront e inicie sesión como usuario que puede acceder a las aplicaciones del grupo de entrega PublishedContentApps. La pantalla incluye la aplicación recién creada con el icono predeterminado. Para obtener información sobre cómo personalizar el icono, consulte <https://www.citrix.com/blogs/2013/08/21/xd-tipster-changing-delivery-group-icons-revisited-7/>.
- Haga clic en la aplicación Citrix Home Page. La URL se abre en una ficha nueva de una instancia ejecutada localmente de su explorador web predeterminado.

### Publicar recursos ubicados en rutas UNC

En este ejemplo, el administrador ya ha creado un recurso compartido llamado PublishedResources. Después de asignar las ubicaciones y los nombres de las aplicaciones, los siguientes cmdlets publican un archivo RTF y un archivo DOCX en ese recurso compartido.

```
1 $rtfUNC = "\\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedRTF.rtf"
2 $rtfAppName = "PublishedRTF"
3
4 New-BrokerApplication -ApplicationType PublishedContent
5 - CommandLineExecutable $rtfUNC -Name $rtfAppName
6 -DesktopGroup $dg.Uid
7
8 $docxUNC = "\\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.docx"
9
10 $docxAppName = "PublishedDOCX"
11 New-BrokerApplication -ApplicationType PublishedContent
```

```

12 - CommandLineExecutable $docxUNC -Name $docxAppName
13 -DesktopGroup $dg.Uid
14 <!--NeedCopy-->

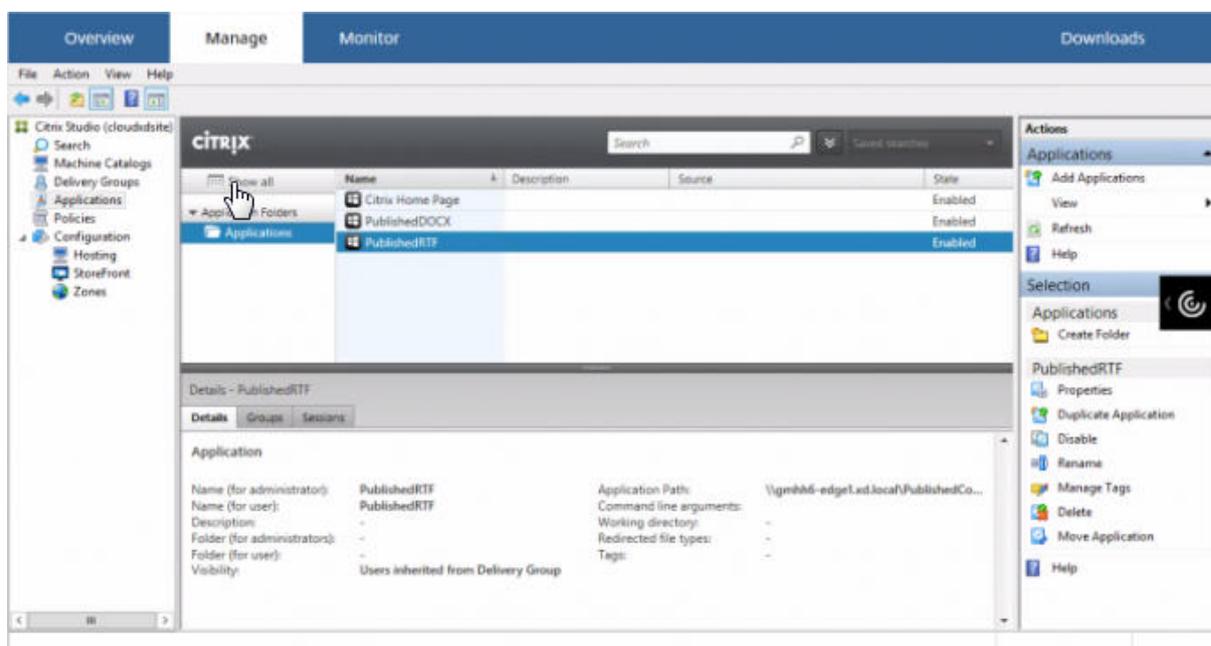
```

Compruebe el resultado:

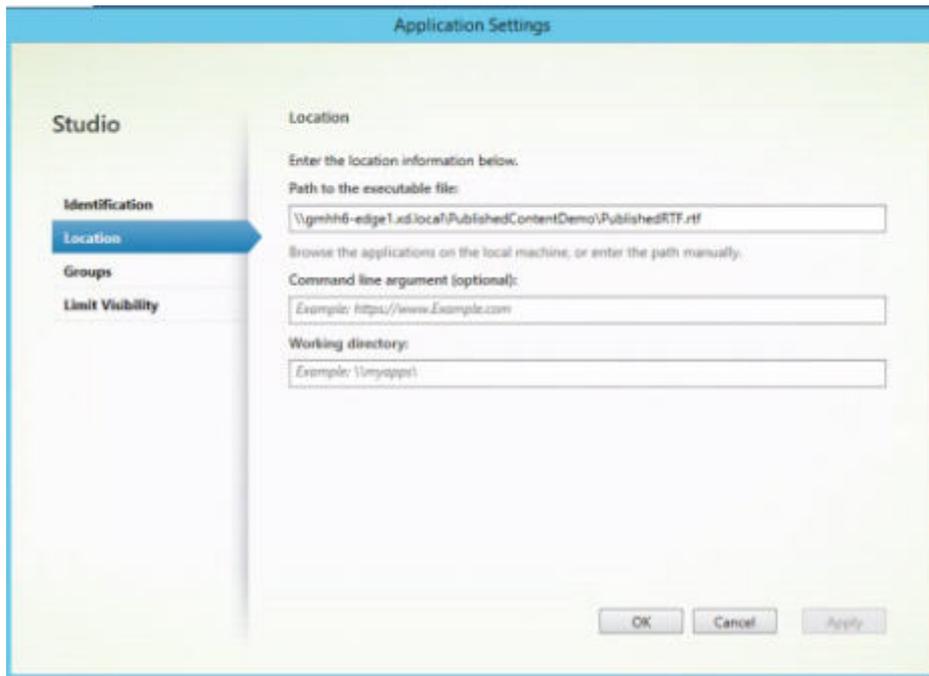
- Actualice la ventana de StoreFront para ver los documentos recién publicados.
- Haga clic en las aplicaciones **PublishedRTF** y **PublishedDOCX**. Cada documento se abre en un WordPad ejecutado localmente.

## Ver y modificar aplicaciones PublishedContent

Puede administrar el contenido publicado con los mismos métodos que se utilizan para otros tipos de aplicación. Los elementos publicados aparecerán en la lista Aplicaciones de Studio y pueden modificarse en Studio.

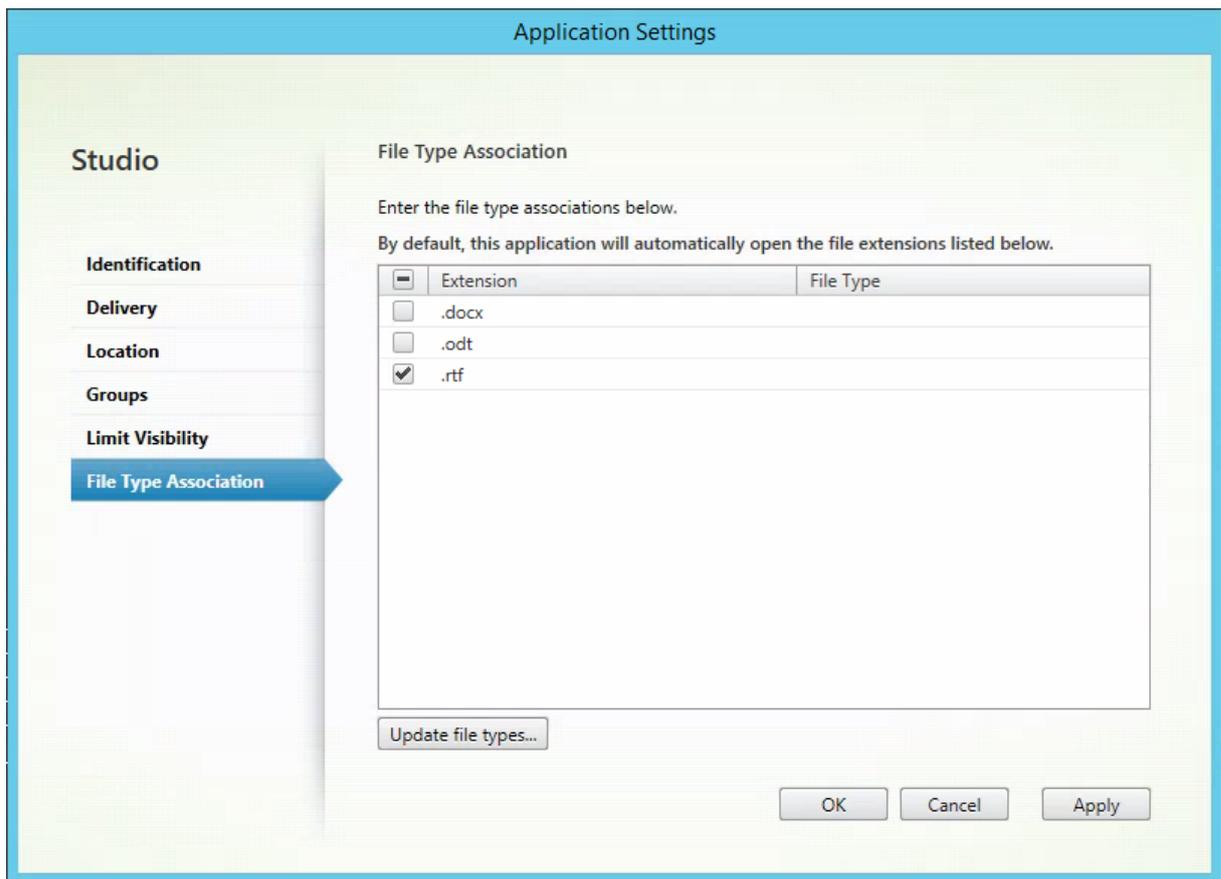


Las propiedades de aplicación (por ejemplo, la visibilidad a los usuarios, la asociación de grupo y el acceso directo) se aplican al contenido publicado. Sin embargo, no puede cambiar el argumento de la línea de comandos ni las propiedades del directorio de trabajo que se ven en la página **Ubicación**. Para cambiar el recurso, modifique el campo **Ruta del archivo ejecutable** en dicha página.

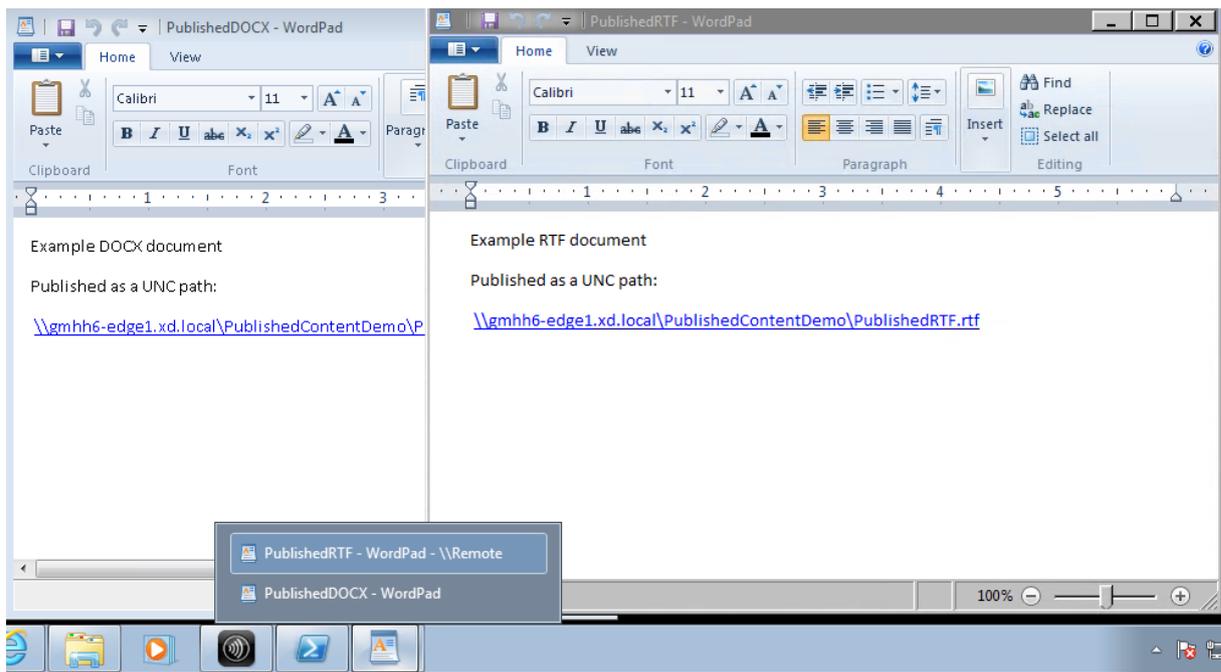


Si quiere usar una aplicación publicada para abrir una aplicación PublishedContent (en lugar de una aplicación local), modifique la propiedad **Asociación de tipos de archivo** de la aplicación publicada. En este ejemplo, la aplicación publicada de WordPad se modificó para crear una asociación de tipos de archivo para archivos RTF.

Active el modo de mantenimiento para el grupo de entrega antes de modificar la asociación de tipos de archivo. Recuerde que debe desactivar el modo de mantenimiento cuando haya terminado.



Actualice StoreFront para que cargue los cambios de asociación de tipos de archivo y, a continuación, haga clic en las aplicaciones PublishedRTF y PublishedDOCX. Compruebe el resultado. Published-DOCX aún se abre en la instancia local de WordPad. No obstante, ahora PublishedRTF se abre en la instancia publicada de WordPad debido a la nueva asociación de tipos de archivo.



## Para obtener más información

- [Crear catálogos de máquinas](#)
- [Crear grupos de entrega](#)
- [Cambiar las propiedades de la aplicación](#)

## VDI de servidor

September 22, 2021

Use la función VDI (infraestructura de escritorios virtuales) de servidor para entregar escritorios desde un sistema operativo de servidor a un solo usuario.

- Los administradores de empresa pueden entregar sistemas operativos de servidor como escritorios VDI, lo cual puede ser útil para usuarios como ingenieros y diseñadores.
- Los proveedores de servicios pueden ofrecer escritorios desde la nube; esos escritorios cumplen con el Contrato de licencia de proveedor de servicios (SPLA) de Microsoft.

Puede usar la configuración de directiva “Enhanced Desktop Experience” de Citrix para que el sistema operativo del servidor parezca un sistema operativo de escritorio.

Las siguientes funciones no se pueden usar con VDI de servidor:

- Discos Personal vDisk
- Aplicaciones alojadas
- Acceso a aplicaciones locales
- Conexiones de escritorio directas (sin broker)
- Acceso con Remote PC

Actualmente se admite VDI de servidor en máquinas Windows Server 2019 y Windows Server 2016.

Para que VDI de servidor funcione con los dispositivos TWAIN (por ejemplo, escáneres), debe instalarse la función Experiencia de escritorio de servidor Windows.

## Instalar y configurar VDI de servidor

### 1. Prepare el servidor Windows para la instalación.

- Use el Administrador del servidor de Windows para asegurarse de que los servicios de rol de los Servicios de Escritorio remoto no están instalados. Si se instalaron anteriormente, elimínelos. La instalación de VDA falla si se instalan esos servicios de rol.
- Compruebe que la propiedad “Restringir cada usuario a una sola sesión” está habilitada. En el servidor Windows, modifique el Registro y establezca el parámetro de Terminal Server:
  - HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer
  - DWORD fSingleSessionPerUser = 1

### 2. Use la interfaz de la línea de comandos que tiene el instalador de Citrix Virtual Apps and Desktops para instalar un VDA en un servidor compatible o en la imagen maestra de un servidor compatible. Debe especificar las opciones “quiet” y “servervdi” (de forma predeterminada, la interfaz gráfica del instalador impide que aparezca la opción del VDA para Windows con SO de sesión única en un sistema operativo de servidor; con la línea de comandos, se suprime este comportamiento). Use uno de los siguientes comandos:

- Implementaciones de Citrix Virtual Apps and Desktops:
  - `XenDesktopVdaSetup.exe /quiet /servervdi`
  - `VDAWorkstationSetup.exe /quiet /servervdi`
- Implementaciones de Citrix Virtual Apps and Desktops Service:
  - `VDAWorkstationSetup.exe /quiet /servervdi`

Para otras opciones:

- Puede especificar el Delivery Controller o Cloud Connector con la opción “controllers”.
- Use la opción `enable_hdx_ports` para abrir puertos en el firewall, a menos que el firewall deba configurarse manualmente.

- Agregue la opción `mastermcsimage` (o `masterimage`) si está instalando el VDA en una imagen y va a usar MCS para crear máquinas virtuales de servidor a partir de esa imagen.
  - No incluya opciones para funciones que no se admiten con VDI de servidor, como, por ejemplo, “baseimage”(para discos Personal vDisk).
  - Para obtener más información sobre todas las opciones, consulte [Instalación desde la línea de comandos](#).
3. Cree un catálogo de máquinas para VDI de servidor. En el asistente para la creación de catálogos:
- En la página **Sistema operativo**, seleccione **SO de sesión única**.
  - En la página **Resumen**, especifique un nombre del catálogo de máquinas y una descripción para los administradores que claramente lo identifique como VDI de servidor. Será lo único que indique en Studio que el catálogo admite VDI de servidor.

Al usar “Buscar” en Studio, el catálogo de VDI de servidor aparece en la ficha **Máquinas con SO de sesión única**, aunque el VDA se instalara en un servidor.

4. Cree un grupo de entrega y seleccione el catálogo de VDI de servidor que ha creado.

Si no especificó Delivery Controllers ni Cloud Connector mientras instalaba el VDA, recuerde especificarlos posteriormente. Para obtener información detallada, consulte [Registro de VDA](#).

## Capa de personalización de usuarios

September 22, 2021

La funcionalidad “capa de personalización de usuarios” para Citrix Virtual Apps and Desktops amplía las posibilidades de los catálogos de máquinas no persistentes. Las capas de personalización de usuario conservan los datos de los usuarios y las aplicaciones instaladas localmente en las distintas sesiones. Con la tecnología Citrix App Layering, esta funcionalidad sustituye a Personal vDisk (PvD).

Al igual que PvD, la funcionalidad “capa de personalización del usuario” funciona con Citrix Provisioning y Machine Creation Services (MCS) en catálogos de máquinas no persistentes. Los componentes de la funcionalidad se instalan junto con Virtual Delivery Agent (VDA) dentro de la imagen maestra de Windows 10.

Las aplicaciones y los datos que los usuarios crean se almacenan en su propio disco duro virtual de capa de usuario, en un archivo VHD montado en la imagen.

Este documento incluye instrucciones para implementar y configurar la funcionalidad “capa de personalización de usuarios”. En él, se describen los requisitos para una implementación correcta, las limitaciones y los problemas conocidos.

Para utilizar la funcionalidad “capa de personalización de usuarios”, primero debe implementarla siguiendo los pasos que se indican en el artículo. Hasta entonces, la funcionalidad no está disponible para su uso.

## Compatibilidad con aplicaciones

Aparte de las excepciones siguientes, todas las aplicaciones que un usuario instala localmente en el escritorio se admiten en la capa de personalización de usuarios.

### Excepciones

Las siguientes aplicaciones son la excepción, y *no* se admiten en la capa de personalización de usuarios:

- Aplicaciones de empresa, como MS Office y Visual Studio.
- Aplicaciones que modifican el hardware o la pila de red. Ejemplo: un cliente VPN.
- Aplicaciones que tienen controladores de nivel de arranque. Ejemplo: un antivirus.
- Aplicaciones con controladores que utilizan el almacén de controladores. Ejemplo: un controlador de impresora.

**Nota:**

Puede hacer que las impresoras estén disponibles mediante objetos de directiva de grupo (GPO) de Windows.

No permita que los usuarios instalen localmente aplicaciones no admitidas. En su lugar, instale estas aplicaciones directamente en la imagen maestra.

### Aplicaciones que requieren una cuenta de administrador o usuario local

Cuando un usuario instala una aplicación localmente (en su capa de usuario), si intenta agregar o modificar un usuario o grupo local requerido por la aplicación, los cambios de usuario o grupo *no* persisten.

**Importante:**

Agregue cualquier usuario o grupo local requerido en la imagen maestra.

## Requisitos

La funcionalidad de capa de personalización de usuarios requiere los siguientes componentes:

- Citrix Virtual Apps and Desktops 7 1909 o una versión posterior
- Virtual Delivery Agent (VDA), versión 1912
- Citrix Provisioning, versión 1909 o una posterior
- Uso compartido de archivos de Windows (SMB)
- Windows 10 Enterprise x64, versión 1607 o una posterior

### Importante:

- Si ha instalado la versión de vista previa de la funcionalidad de capa de personalización de usuarios, desinstale el software y reinicie la imagen maestra antes de instalar esta versión.
- Como se describe en los pasos siguientes, debe definir las directivas dentro de Studio y asignarlas al grupo de entrega específico vinculado a un catálogo de máquinas donde se implementa la capa de personalización de usuario. Al dejar la imagen maestra sin configuración de capa de personalización del usuario, los servicios permanecen inactivos y no pueden interferir con las actividades de creación. Si establece las directivas en la imagen maestra, los servicios de capa de personalización de usuario intentan ejecutar y montar una capa de usuario en la imagen maestra. Dado que ese entorno es para crear cambios en la imagen, esto no es ideal y podría causar comportamientos imprevistos e inestabilidad en la imagen maestra.

## Recomendaciones

Siga las recomendaciones que se indican en esta sección para implementar correctamente la capa de personalización de usuarios.

### Solución de gestión de perfiles

Se recomienda utilizar una solución de gestión de perfiles, como Citrix Profile Management, con la funcionalidad de capa de personalización del usuario.

Si utiliza Profile Management con la funcionalidad de capa de personalización del usuario, desactive la eliminación de la información de usuario al cerrar la sesión. Dependiendo de cómo esté implementando la configuración, puede desactivar la eliminación mediante un objeto de directiva de grupo (GPO) o mediante la directiva del Delivery Controller (Desktop Delivery Controller/DDC).

Para obtener más información sobre las directivas de Profile Management disponibles, consulte [Descripción y configuración predeterminada de las directivas de Profile Management](#).

## Microsoft System Center Configuration Manager (SCCM)

Si utiliza SCCM con la funcionalidad de capa de personalización del usuario, siga las prácticas recomendadas de Microsoft para preparar la imagen en un entorno VDI. Consulte este [artículo de Microsoft TechNet](#) para obtener más información.

### Tamaño máximo de capa de usuario

Recomendamos al menos 10 GB como tamaño de capa de usuario.

**Nota:**

Durante la instalación, el valor cero (0) representa el tamaño predeterminado de capa de usuario de 10 GB.

### Una cuota establecida en Windows puede invalidar el tamaño máximo de capa de usuario

Puede pasar por alto el tamaño máximo de capa de usuario establecido en Studio definiendo una cuota para el recurso compartido de archivos en la capa de usuario. Si se define una cuota, la capa de usuario se configura en el tamaño máximo de la cuota.

Para establecer una cuota fija en el tamaño de la capa de usuario, utilice cualquiera de las herramientas de configuración de cuotas de Microsoft:

- Administrador de recursos del servidor de archivos (FSRM)
- Administrador de cuotas

La cuota debe establecerse en el directorio de capa de usuario denominado Usuarios.

**Nota:**

Aumentar o reducir la cuota solo afecta a las nuevas capas de usuario. No cambia el tamaño máximo de las capas de usuario existentes. Estas permanecen sin cambios cuando se actualiza la cuota.

### Implementar una capa de personalización de usuarios

Para implementar la funcionalidad “capa de personalización de usuarios”, siga estos pasos, por orden:

- Paso 1: Verifique la disponibilidad de un entorno Citrix Virtual Apps and Desktops.
- Paso 2: Prepare la imagen maestra.
- Paso 3: Cree un catálogo de máquinas.
- Paso 4: Cree un grupo de entrega.
- Paso 5: Cree directivas personalizadas de grupo de entrega.

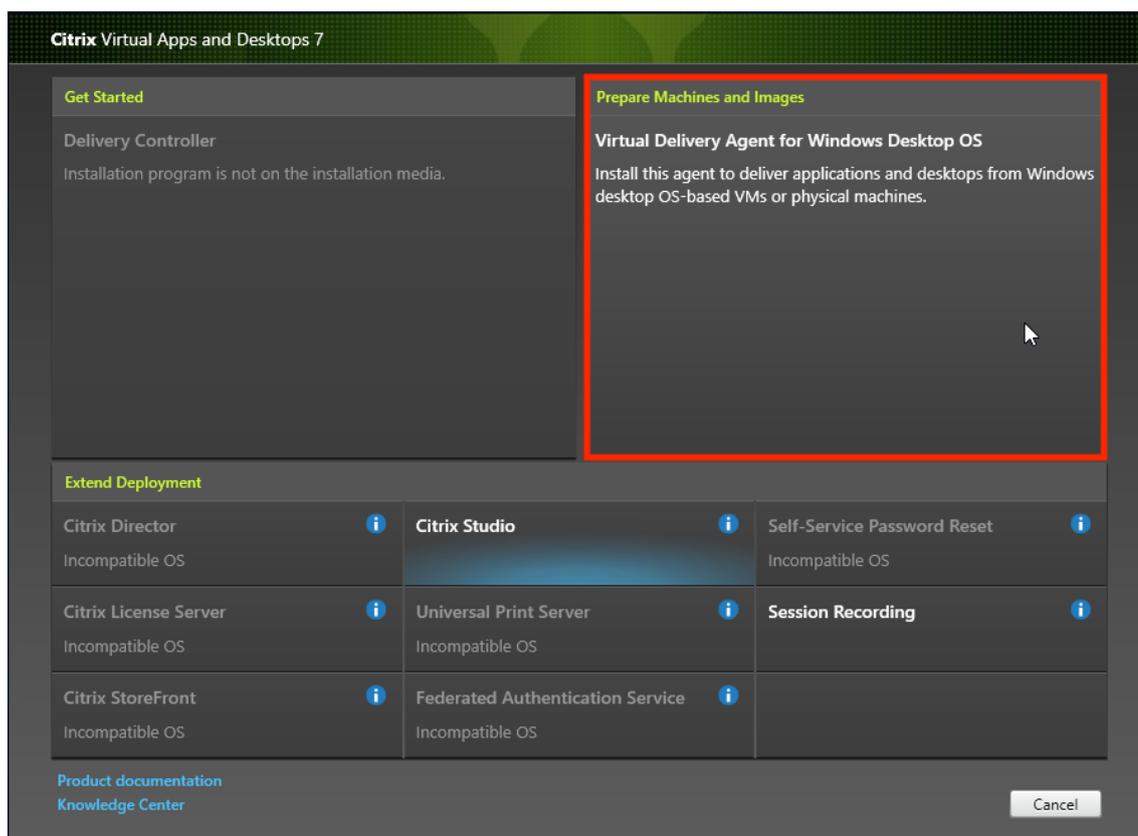
## Paso 1: Verifique la disponibilidad de un entorno Citrix Virtual Apps and Desktops

Asegúrese de que su entorno Citrix Virtual Apps and Desktops esté disponible para su uso con esta nueva función. Para obtener información detallada sobre la configuración, consulte Instalar y configurar Citrix Virtual Apps and Desktops.

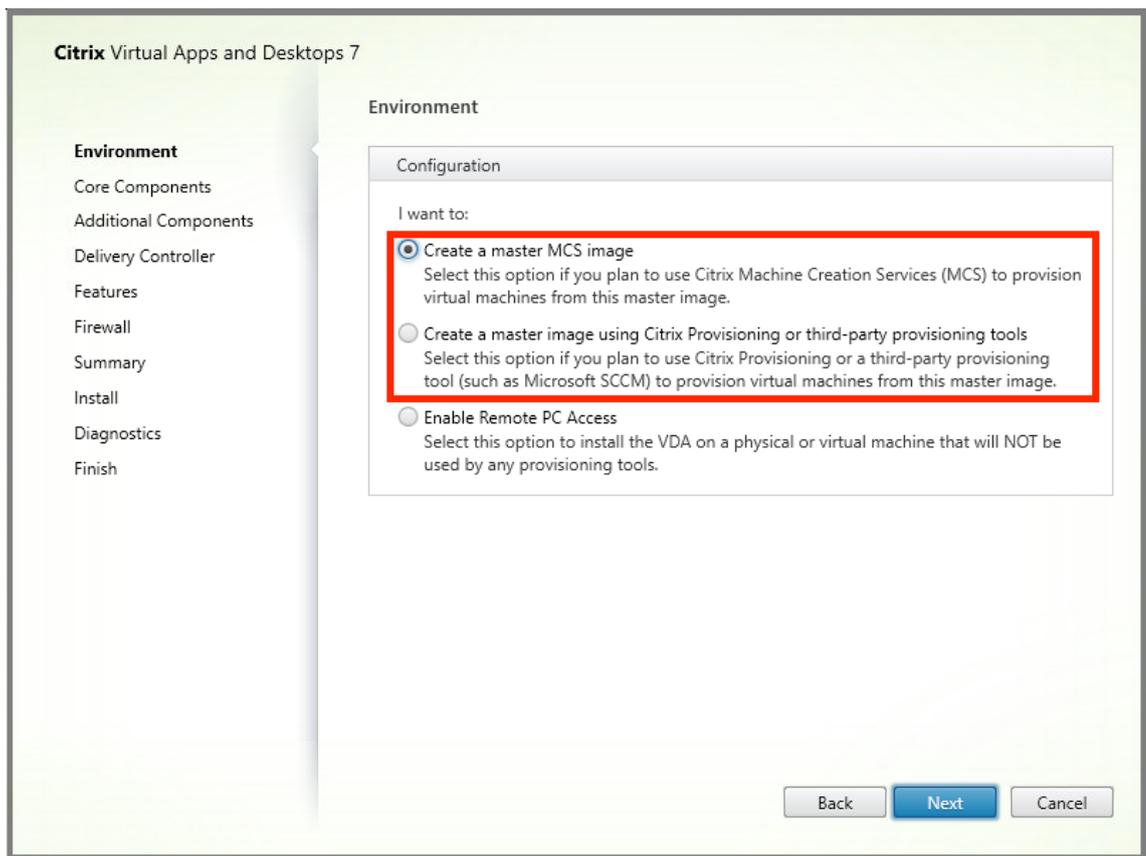
## Paso 2: Prepare la imagen maestra

Para preparar la imagen maestra:

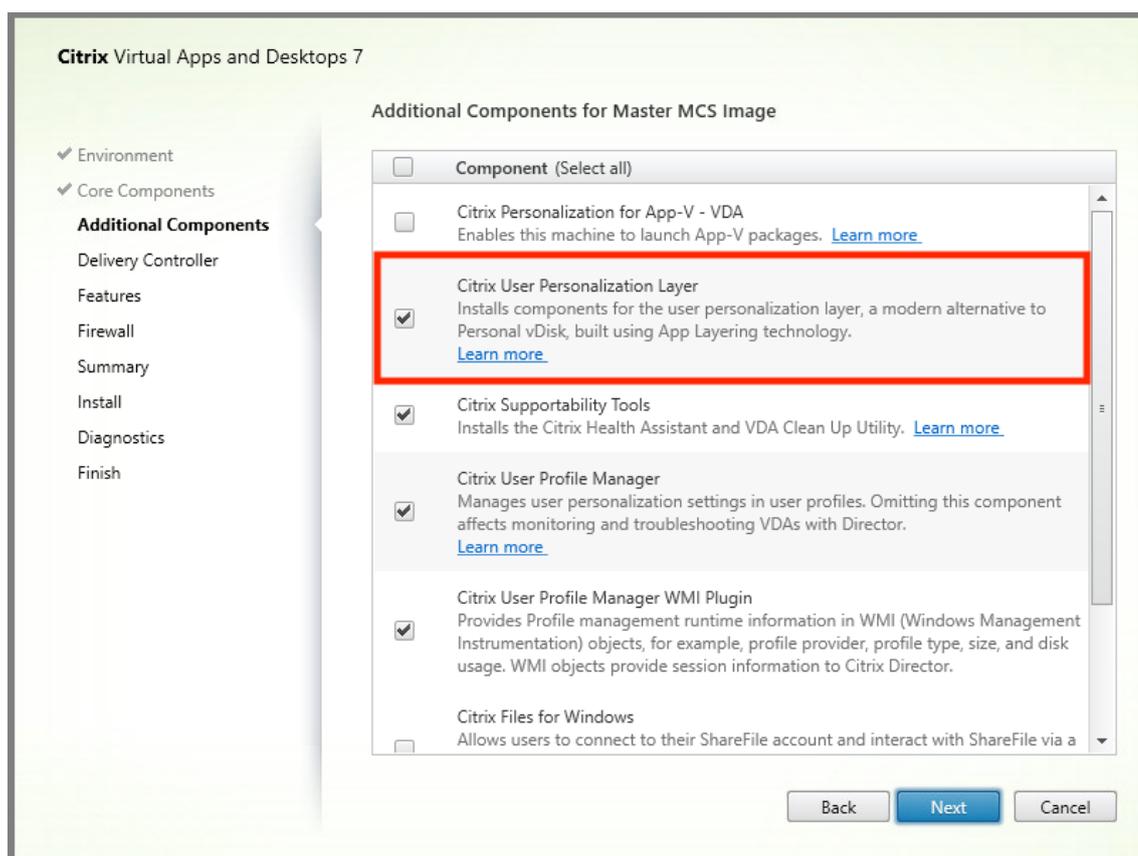
1. Localice la imagen maestra. Instale las aplicaciones de empresa de su organización y todas las demás aplicaciones que los usuarios puedan encontrar útiles.
2. Instale el agente Virtual Delivery Agent (VDA) 1912. Si ya hay instalada una versión anterior del VDA, desinstale antes la versión anterior. Al instalar la nueva versión, seleccione e instale el componente opcional, Capa de personalización de usuarios de Citrix, de esta manera:
  - a) Haga clic en el icono **Virtual Delivery Agent para SO de escritorio Windows**:



- a) **Entorno:** Seleccione Crear una imagen maestra de MCS o Crear una imagen maestra mediante Citrix Provisioning o herramientas de aprovisionamiento de terceros.



- a) **Componentes principales:** Haga clic en **Siguiente**.
- b) **Componentes adicionales:** Marque **Capa de personalización de usuarios de Citrix**.



- a) Haga clic en las pantallas de instalación restantes, configure el VDA según sea necesario y haga clic en Instalar. La imagen se reinicia una o más veces durante la instalación.
3. Deje las **actualizaciones de Windows** inhabilitadas. El instalador de la capa de personalización de usuarios inhabilitará las actualizaciones de Windows en la imagen. Deje las actualizaciones inhabilitadas.

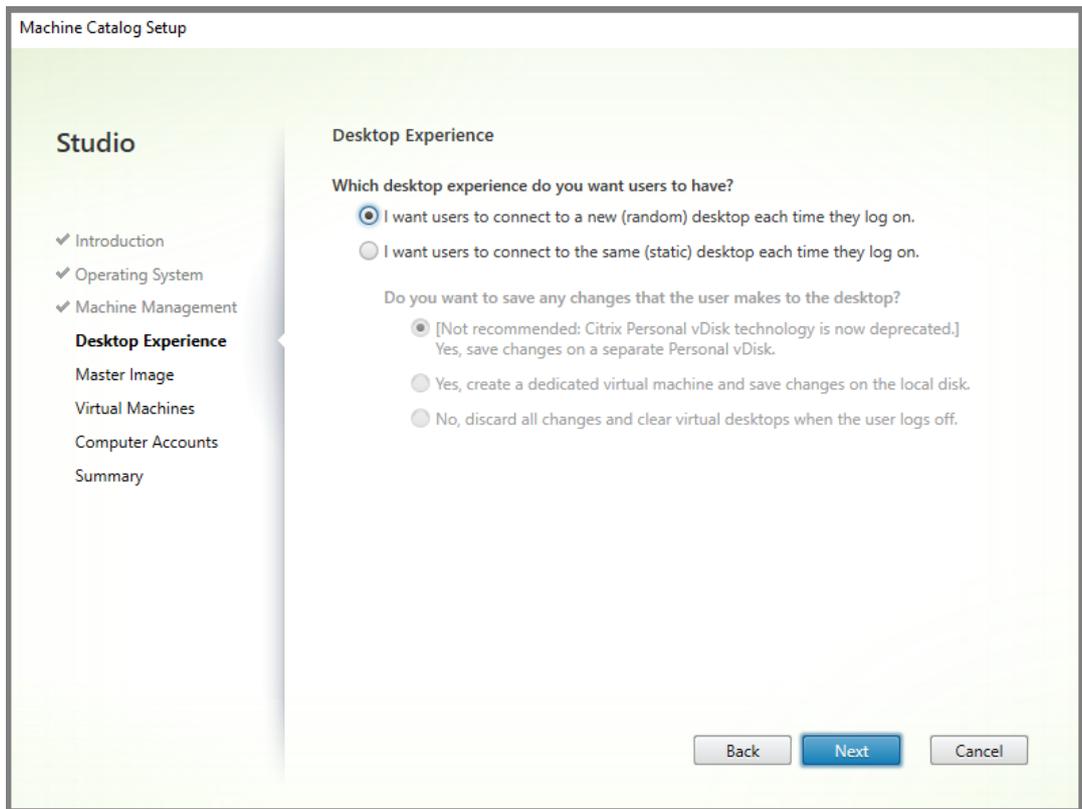
La imagen estará lista para que la cargue en Studio.

### Paso 3: Cree un catálogo de máquinas

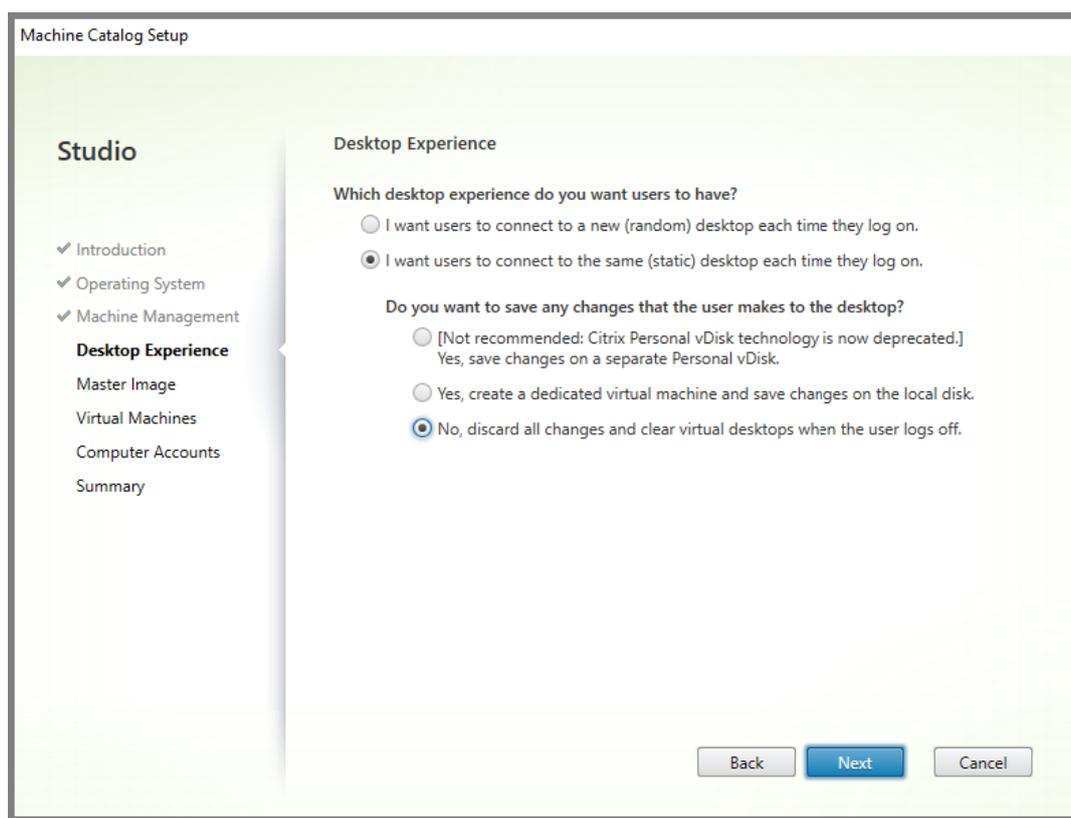
En Studio, siga los pasos para crear un catálogo de máquinas. Utilice las siguientes opciones durante la creación del catálogo:

1. Seleccione **Sistema operativo** y establezca el valor en **SO de sesión única**.
2. Seleccione **Administración de máquinas** y establezca el valor en **Máquinas con administración de energía**. (por ejemplo, máquinas virtuales o PC blade).
3. Seleccione **Experiencia de escritorio** y establezca el tipo de catálogo en **agrupadas aleatorias** o **agrupadas estáticas**, como se muestra en los ejemplos siguientes:

- **Agrupadas aleatorias:**



- **Agrupadas estáticas:** Si selecciona agrupadas estáticas, configure los escritorios para descartar todos los cambios y borrar los escritorios virtuales cuando el usuario cierre la sesión, como se muestra en la siguiente captura de pantalla:

**Nota:**

La capa de personalización de usuarios no admite catálogos de máquinas agrupadas estáticas configuradas para uso con Citrix Personal vDisk o asignadas como máquinas virtuales dedicadas.

4. Si utiliza MCS, seleccione **Imagen maestra** y la instantánea de la imagen creada en la sección anterior.
5. Configure las propiedades de catálogo restantes según sea necesario para su entorno.

**Paso 4: Cree un grupo de entrega**

Cree y configure un **grupo de entrega**, incluidas las máquinas del catálogo de máquinas que ha creado. Para obtener más información, consulte [Crear grupos de entrega](#).

**Paso 5: Cree directivas personalizadas de grupo de entrega**

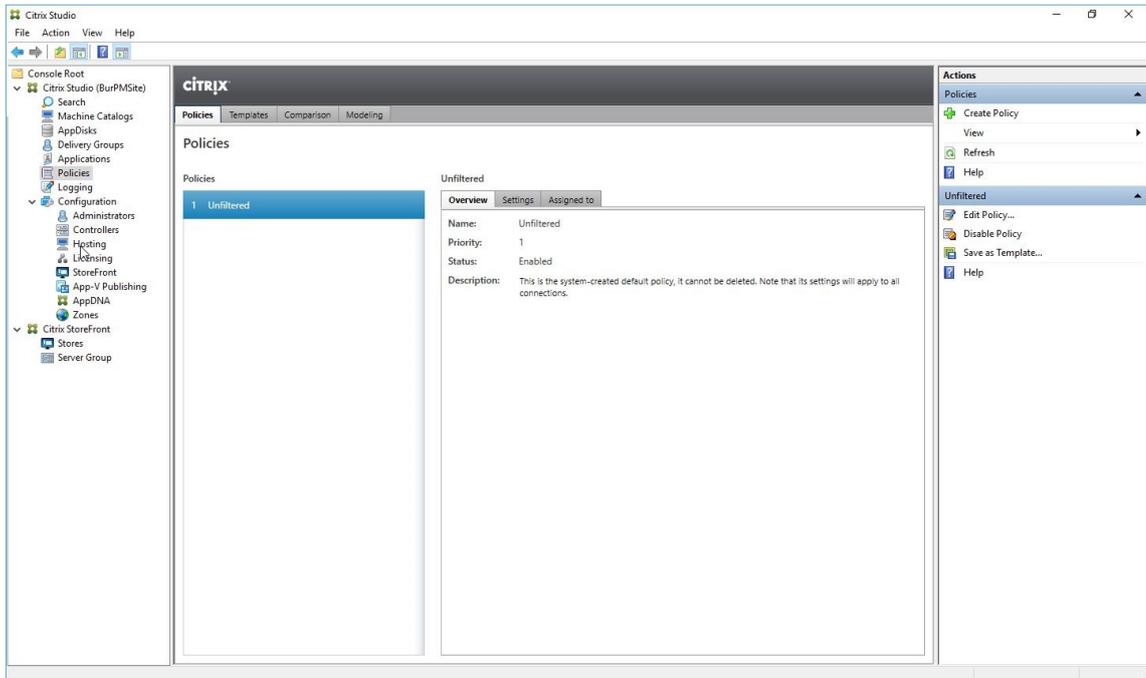
Para habilitar el montaje de capas de usuarios dentro de Virtual Delivery Agents, utilice los parámetros de configuración para especificar:

- En qué lugar de la red se accede a las capas de usuarios.

- Hasta qué tamaño puede permitir que los discos de capa de usuarios crezcan.

En los pasos siguientes, se explica cómo definir los parámetros como directivas de Citrix personalizadas en Studio y, a continuación, asignarlos al grupo de entrega.

1. Seleccione Directivas en el panel de navegación de Studio.



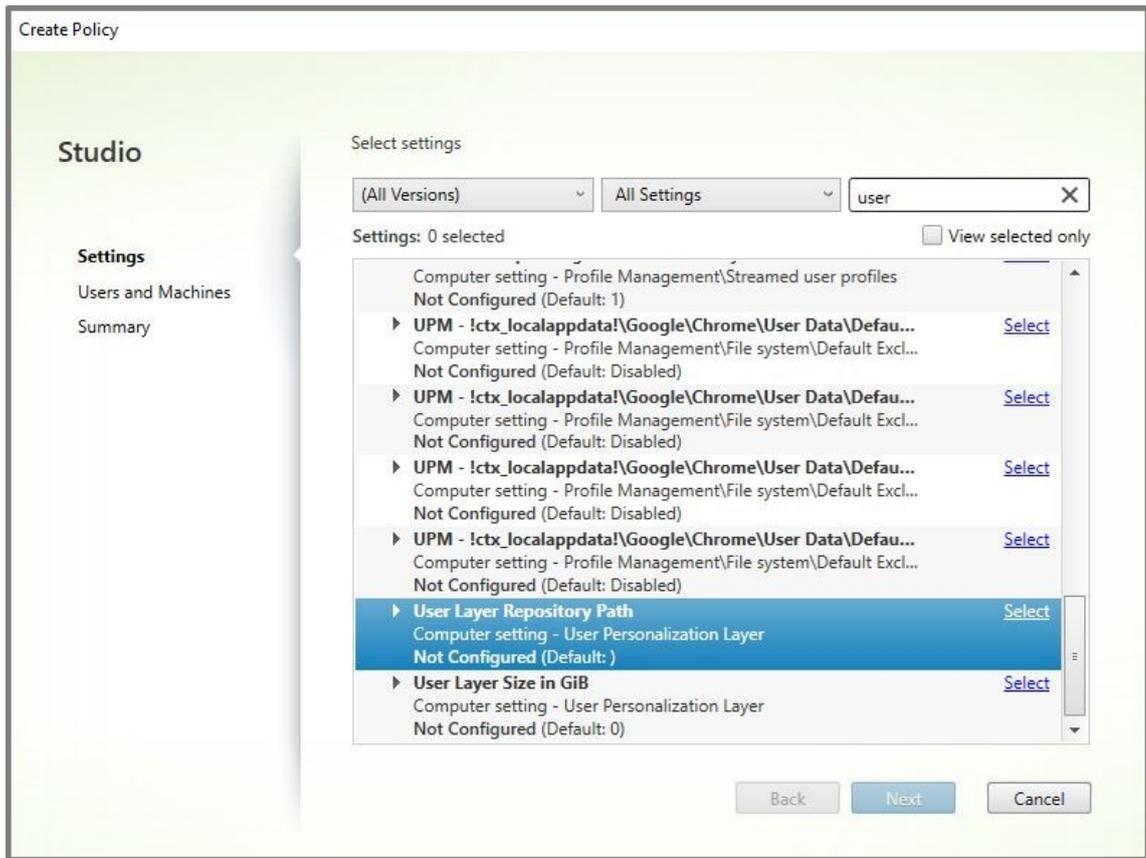
2. Seleccione Crear directiva en el panel Acciones. Aparecerá la ventana Crear directiva.
3. Escriba “capa de usuarios” en el campo de búsqueda. En la lista de directivas disponibles, aparecen las dos directivas siguientes:

- Ruta del repositorio de capas de usuarios
- Tamaño de capa de usuarios en GB

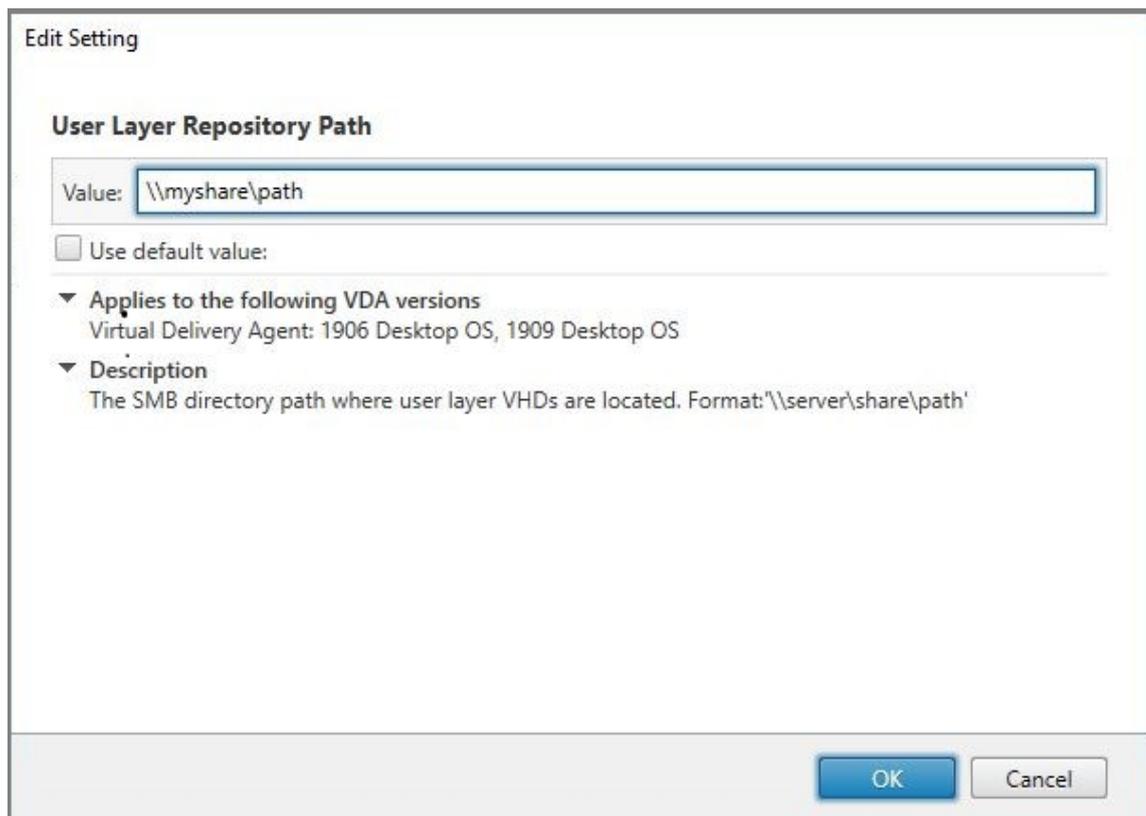
**Nota:**

El hecho de cambiar el tamaño de las capas de usuarios en la directiva no cambia el tamaño de las capas existentes.

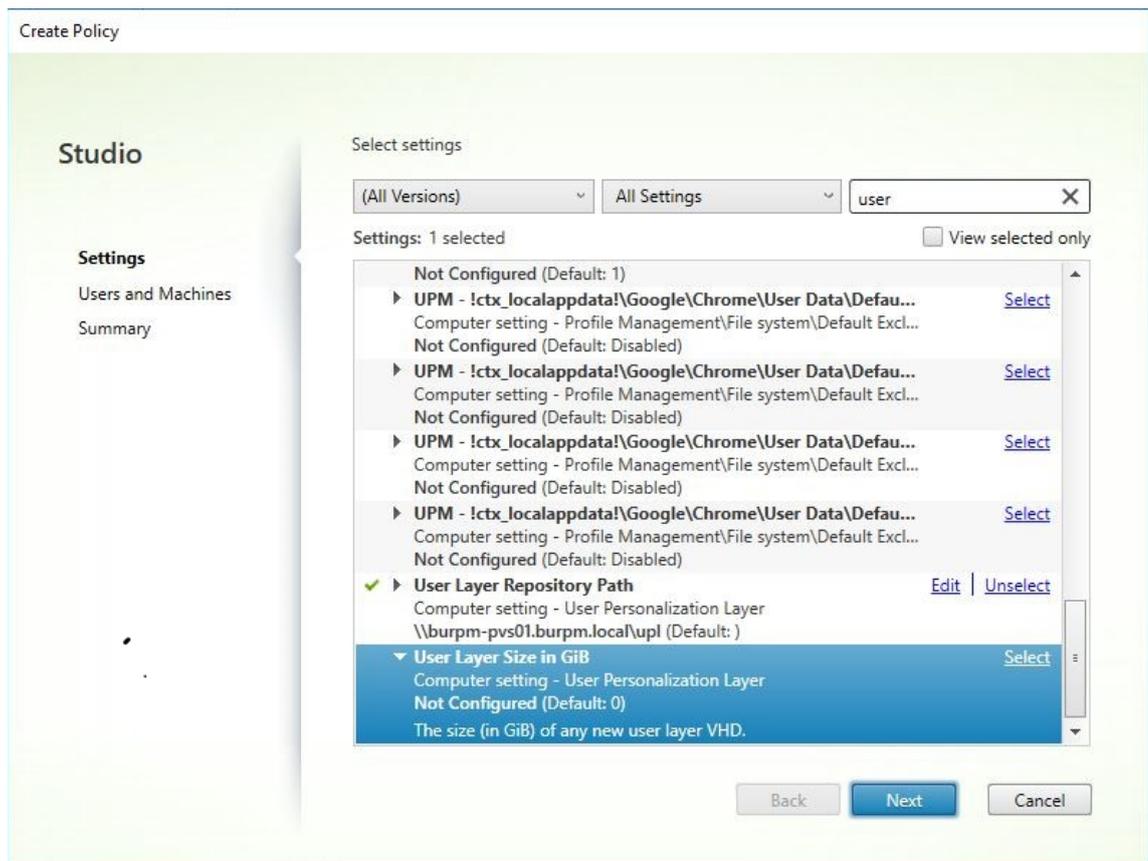
4. Haga clic en **Seleccionar** junto a Ruta del repositorio de capas de usuarios. Aparecerá la ventana Modificar configuración.



5. Escriba una ruta con el formato `\\server name or address\folder name` en el campo Valor y haga clic en **Aceptar**:



6. Opcional: Haga clic en **Seleccionar** junto a Tamaño de capa de usuarios en GB:

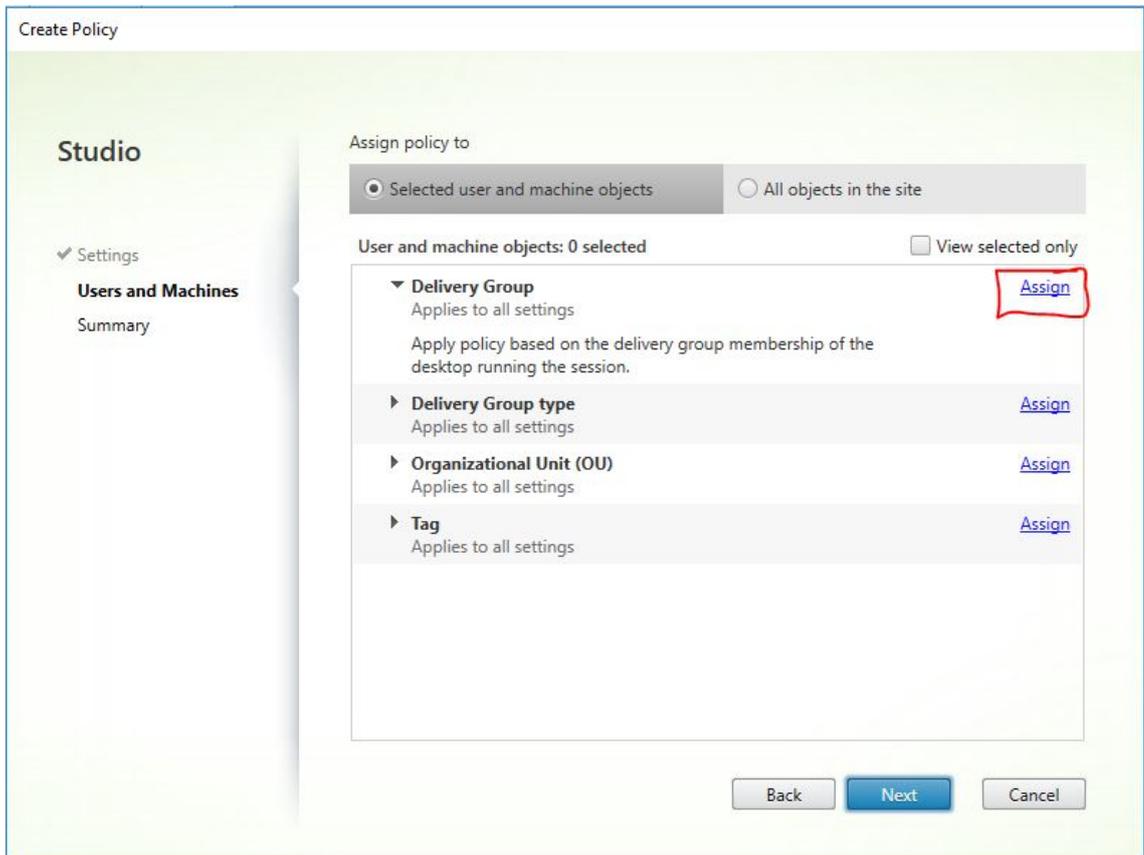


7. Aparecerá la ventana Modificar parámetros.
8. Opcional: Cambie el valor predeterminado de “0” al tamaño máximo (en GB) hasta el que puede crecer la capa de usuarios. Haga clic en OK.

**Nota:**

Si mantiene el valor predeterminado, el tamaño máximo de las capas de usuario es de 10 GB.

9. Haga clic en Siguiete para configurar Usuarios y máquinas. Haga clic en el enlace Asignar grupo de entrega resaltado en esta imagen:



10. En el menú Grupo de entrega, seleccione el grupo de entrega creado en la sección anterior. Haga clic en OK.

**Assign Policy**

**Delivery Group**

**Applies to:** Virtual Delivery Agent: 5.6, 7.0 Server OS, 7.0 Desktop OS, 7.1 Server OS, 7.1 Desktop OS, 7.5 Server OS, 7.5 Desktop OS, 7.6 Server OS, 7.6 Desktop OS, 7.7 Server OS, 7.7 Desktop OS, 7.8 Server OS, 7.8 Desktop OS, 7.9 Server OS, 7.9 Desktop OS, 7.11 Server OS, 7.11 Desktop OS, 7.12 Server OS, 7.12 Desktop OS, 7.13 Server OS, 7.13 Desktop OS, 7.14 Server OS, 7.14 Desktop OS, 7.15 Server OS, 7.15 Desktop OS, 7.16 Server OS, 7.16 Desktop OS, 7.17 Server OS, 7.17 Desktop OS, 7.18 Server OS, 7.18 Desktop OS, 1808 Server OS, 1808 Desktop OS, 1811 Server OS, 1811 Desktop OS, 1903 Server OS, 1903 Desktop OS, 1906 Server OS, 1906 Desktop OS, 1909 Server OS, 1909 Desktop OS

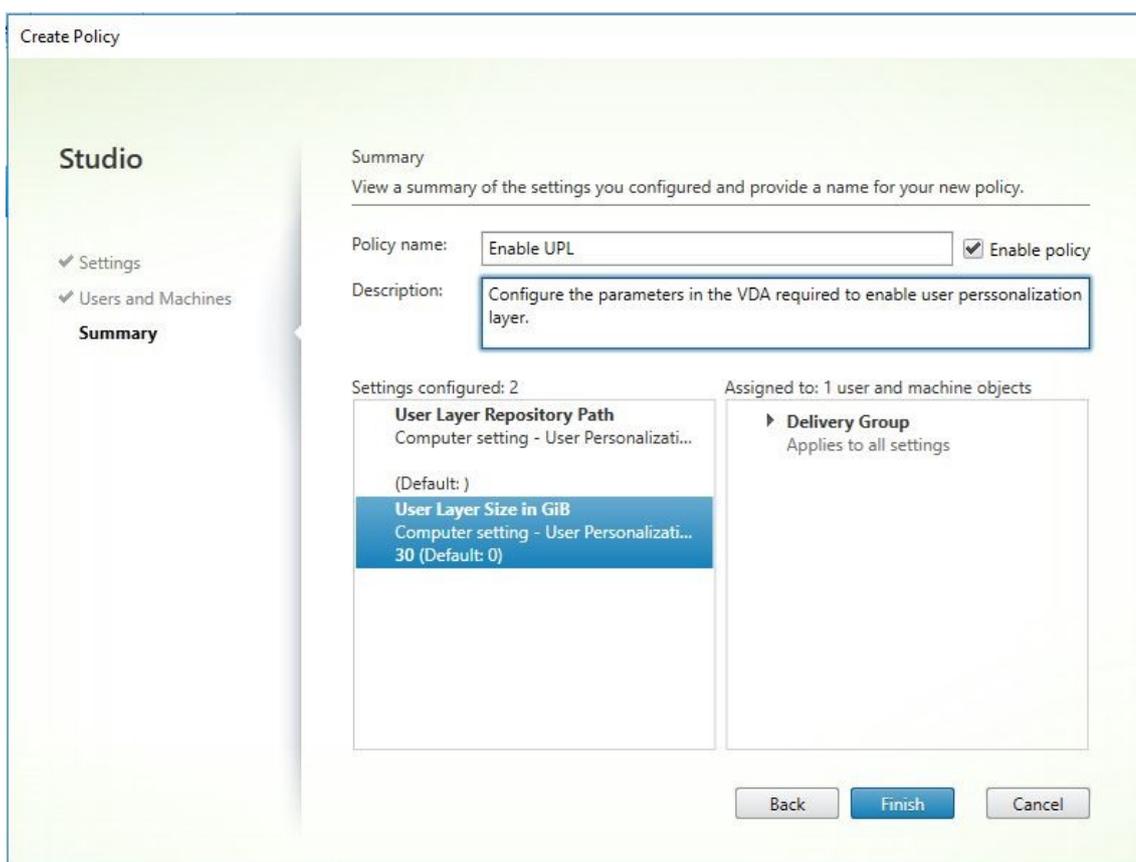
Apply policy based on the delivery group membership of the desktop running the session.

**Delivery Group elements:**

Mode	Controller	Delivery Group	
Allow		Win10 - UPL	+ -
<input checked="" type="checkbox"/> Enable			

OK Cancel

11. Introduzca un nombre para la directiva. Marque la casilla para habilitar la directiva y haga clic en Finalizar.



## Configurar los parámetros de seguridad en la carpeta de capa de usuario

Como administrador de dominios, puede especificar más de una ubicación de almacenamiento para las capas de usuarios. Para cada ubicación de almacenamiento (incluida la predeterminada), cree una subcarpeta `\Users` y proteja esa ubicación con la configuración siguiente.

Nombre del parámetro	Valor	Aplicar a
Propietario creador	Modificar	Subcarpetas y archivos únicamente
Derechos de propietario	Modificar	Subcarpetas y archivos únicamente
Usuarios o grupo	Crear carpeta/anexar datos; Atravesar la carpeta/ejecutar archivo; Mostrar lista de carpetas/leer datos; Leer atributos	Solo carpeta seleccionada
Sistema	Control total	Carpeta, subcarpetas y archivos seleccionados

---

Nombre del parámetro	Valor	Aplicar a
Administradores de dominio y grupo de administradores seleccionado	Control total	Carpeta, subcarpetas y archivos seleccionados

---

## Mensajes de capa de usuarios

Cuando un usuario no puede acceder a su capa de usuarios, recibe uno de los siguientes mensajes de notificación.

- *Capa de usuarios que se está utilizando*

No hemos podido adjuntar la capa de usuarios porque se está utilizando. Los cambios que realice en la configuración o en los datos de la aplicación no se guardarán. Asegúrese de guardar cualquier trabajo realizado en una ubicación de red compartida.

- *Capa de usuarios no disponible*

No hemos podido adjuntar la capa de usuarios. Los cambios que realice en la configuración o en los datos de la aplicación no se guardarán. Asegúrese de guardar cualquier trabajo realizado en una ubicación de red compartida.

- *El sistema no se restablece después de que el usuario haya cerrado la sesión*

Este sistema no se ha apagado correctamente. lease log off immediately and contact your system administrator.

## Archivos de registro para solución de problemas

El archivo de registro, ulayersvc.log, contiene la salida del software de capa de personalización de usuarios donde se registran los cambios.

```
1 C:\ProgramData\Unidesk\Logs\ulayersvc.log
2 <!--NeedCopy-->
```

## Limitaciones

Tenga en cuenta las siguientes limitaciones al instalar y usar la funcionalidad de capa de personalización de usuarios.

- No configure la funcionalidad de capa de personalización de usuarios con catálogos de máquinas persistentes.

- No utilice hosts de sesión.
- No actualice el catálogo de máquinas con una imagen que ejecute una nueva instalación del sistema operativo (incluso la misma versión de Windows 10). La práctica recomendada es aplicar las actualizaciones al sistema operativo dentro de la misma imagen maestra utilizada al crear el catálogo de máquinas.
- No utilice controladores de tiempo de arranque, ni ninguna otra personalización de primera fase de arranque.
- No migre datos de PvD a la capa de personalización de usuarios.
- No migre capas de usuarios existentes del producto App Layering completo a la capa de personalización de usuarios.
- No cambie la ruta SMB de capa de usuarios para acceder a las capas de usuarios creadas con una imagen maestra de un sistema operativo diferente.
- No habilite el arranque seguro en máquinas virtuales con capas de personalización de usuarios, ya que no se admite actualmente.

- Centro de software de Microsoft SCCM puede mostrar una aplicación instalada en la capa de usuarios como no disponible, incluso si se ha instalado previamente. El problema se produce cuando un usuario cierra una sesión y, a continuación, vuelve a una sesión en otra máquina del grupo. Este comportamiento es una propiedad de SCCM cuando se ejecuta en un entorno VDI. Centro de software solo muestra las aplicaciones que el usuario ha instalado en la máquina actual, pero las aplicaciones siguen estando instaladas y son completamente funcionales.

Para comprobar que una aplicación está instalada, el usuario puede seleccionarla en Centro de software y hacer clic en **Instalar**. Si la aplicación ya está instalada en su capa de usuarios, SCCM actualiza el estado a “Instalada” y la muestra con las demás aplicaciones instaladas.

- Centro de software en ocasiones se detiene inmediatamente después de iniciarse en un VDA que tiene habilitada la funcionalidad de capa de personalización de usuarios. Para evitar este problema, siga las recomendaciones de Microsoft para [Implementación de SCCM en un entorno VDI de XenDesktop](#). Además, asegúrese de que el servicio ccmexec se está ejecutando antes de iniciar Centro de software.
- Directivas de grupo (configuraciones de equipo): Los parámetros de capa de usuarios anulan los parámetros aplicables a la imagen maestra. Por consiguiente, los cambios realizados en Configuración del equipo mediante un objeto de directiva de grupo no siempre están presentes para el usuario en el inicio de sesión siguiente.

Para evitar este problema, cree un script de inicio de sesión de usuario que emita el comando:

```
gpupdate /force
```

Por ejemplo, un cliente definió el siguiente comando para que se ejecute en cada inicio de sesión de usuario:

```
gpupdate /Target:Computer /force
```

Para obtener los mejores resultados, aplique los cambios a Configuración del equipo directamente en la capa de usuarios, después de que el usuario haya iniciado sesión.

## Personal vDisk

June 4, 2020

### Nota:

Personal vDisk se ha **retirado**. La entidad de la capa de personalización del usuario controla la persistencia del usuario.

La función Personal vDisk conserva la administración de imágenes únicas para escritorios agrupados y distribuidos por streaming, al tiempo que permite a los usuarios instalar aplicaciones y cambiar la configuración de sus escritorios. A diferencia de las implementaciones de VDI (Virtual Desktop Infrastructure) tradicionales con escritorios agrupados, donde los usuarios pierden sus personalizaciones y sus aplicaciones personales cuando el administrador modifica la imagen maestra, las implementaciones con discos Personal vDisk conservan dichos cambios. Esto significa que los administradores pueden administrar de manera centralizada y sencilla las imágenes maestras, al mismo tiempo que proporcionan a los usuarios una experiencia de escritorio personalizada.

Los discos Personal vDisk permiten esta separación al redirigir todos los cambios que efectúa el usuario en la máquina virtual a un disco aparte (el disco Personal vDisk) asociado a la máquina virtual del usuario. El contenido del disco Personal vDisk se fusiona en tiempo de ejecución con el contenido de la imagen publicada para proporcionar una experiencia unificada. De este modo, los usuarios pueden seguir accediendo a las aplicaciones aprovisionadas por el administrador en la imagen maestra.

Los discos virtuales personales constan de dos partes, que utilizan letras de unidad distintas y tienen el mismo tamaño de manera predeterminada:

- Perfil de usuario: contiene los datos, los documentos y el perfil del usuario. De manera predeterminada, esta parte usa la unidad P: pero se puede seleccionar otra letra de unidad cuando se crea un catálogo de máquinas con discos Personal vDisk. La unidad usada también depende del parámetro EnableUserProfileRedirection.
- Disco duro virtual (.vhd): contiene todos los demás elementos, como, por ejemplo, las aplicaciones instaladas en C:\Archivos de programa. Esta parte no se muestra en el Explorador de Windows y, a partir de la versión 5.6.7, ya no necesita una letra de unidad.

Los discos Personal vDisk admiten el aprovisionamiento de aplicaciones específicas de cada departamento, así como el de aplicaciones descargadas e instaladas por los propios usuarios, incluidas las que necesitan controladores (excepto los controladores de fase 1), bases de datos y software de administración de máquinas. Si un cambio efectuado por un usuario entra en conflicto con otro cambio realizado por un administrador, el disco Personal vDisk ofrece un método sencillo y automático para resolver dichos cambios.

Además, también pueden aprovisionarse en el entorno del usuario aplicaciones administradas localmente (como pueden ser las aprovisionadas y administradas por departamentos de TI locales). El usuario no nota diferencia alguna en cuanto a la usabilidad; los discos virtuales personales garantizan que todos los cambios hechos y todas las aplicaciones instaladas se guardan en el disco virtual. Cuando una aplicación de un disco Personal vDisk coincide exactamente con una aplicación existente en la imagen maestra, la copia del disco Personal vDisk se descarta para ahorrar espacio, sin que el usuario pierda acceso a ella.

Físicamente, los discos Personal vDisk se almacenan en el hipervisor, pero no es necesario que residan en la misma ubicación que los otros discos conectados al escritorio virtual. Esto puede reducir los costes de almacenamiento de Personal vDisk.

Durante la creación de sitios, cuando crea una conexión, debe definir las ubicaciones de almacenamiento para los discos utilizados por las máquinas virtuales. Puede separar los discos Personal vDisk de los discos que utilice el sistema operativo. Cada máquina virtual debe tener acceso a una ubicación de almacenamiento para ambos discos. Si usa almacenamiento local para ambos, deben estar accesibles desde el mismo hipervisor. Para garantizar que se cumple este requisito, Studio ofrece únicamente ubicaciones de almacenamiento compatibles. Más adelante, también puede agregar discos Personal vDisk y almacenarlos en hosts existentes (pero no en catálogos de máquinas) desde Configuración > Alojamiento en Studio.

Haga copias de seguridad de los discos Personal vDisk con regularidad con el método que prefiera. Los discos virtuales son volúmenes estándar en el nivel de almacenamiento de un hipervisor, de modo que puede realizar copias de seguridad de ellos como de cualquier otro volumen.

### **Novedades en Personal vDisk 7.6.1**

En esta versión se incluyen las siguientes mejoras:

- Esta versión de Personal vDisk contiene mejoras de rendimiento que reducen el tiempo que lleva aplicar una actualización de imagen a un catálogo de Personal vDisk.

Se han solucionado los siguientes problemas conocidos de esta versión:

- Al intentar una actualización en contexto de una máquina virtual base desde Microsoft Office 2010 a Microsoft Office 2013, el usuario veía una ventana de reconfiguración, seguida de un mensaje de error similar al siguiente: “Error 25004. La clave de producto que escribió no se puede

usar en este equipo”. En el pasado, se recomendaba desinstalar Office 2010 de la máquina virtual base antes de instalar Office 2013. Ahora ya no es necesario desinstalar Office 2010 al llevar a cabo una actualización en contexto en la máquina virtual base (#391225).

- Durante el proceso de actualización de imagen, si existía una versión más reciente de Microsoft .NET en el disco Personal vDisk del usuario, esta versión se sobrescribía con la versión anterior existente en la imagen base. Esto provocaba problemas para los usuarios que ejecutaban ciertas aplicaciones instaladas en su disco Personal vDisk que requerían la versión posterior, tales como Visual Studio (#439009).
- Un disco creado con una imagen de Provisioning Services que tiene Personal vDisk instalado y habilitado no se puede usar para crear un catálogo de máquinas sin Personal vDisk. Esta limitación se ha eliminado (#485189).

## Acerca de Personal vDisk 7.6

Novedades en la versión 7.6:

- Gestión y notificación de errores de Personal vDisk mejoradas. En Studio, al mostrar máquinas con Personal vDisk (PvD) habilitado de un catálogo de máquinas, la ficha “PvD” muestra el estado de la supervisión y el progreso y la hora de finalización estimados de las actualizaciones de imagen. También se ha mejorado la información relacionada con los estados.
- Se ofrece una herramienta de supervisión de actualizaciones de imágenes de Personal vDisk, Personal vDisk Image Update Monitoring Tool, en los medios de soporte ISO (ISO\Support\Tools\Scripts\PvdTool). Las capacidades de supervisión se admiten en versiones anteriores, pero las capacidades de creación de informes no serán tan sólidas comparadas con las de la versión actual.
- El modo de prueba de Provisioning Services permite iniciar máquinas con una imagen actualizada de un catálogo de pruebas. Después de comprobar la estabilidad, puede transferir la versión de prueba de Personal vDisk a producción.
- Una nueva función permite calcular el diferencial entre dos inventarios durante un proceso de inventariado, en lugar de calcularlo para cada escritorio de PvD. Se ofrecen nuevos comandos para exportar e importar un inventario anterior para los catálogos de MCS. (Los discos maestros de vDisk de Provisioning Services ya disponen del inventario anterior.)

Problemas conocidos de 7.1.3 resueltos en la versión 7.6:

- Si se interrumpe una actualización de instalación de Personal vDisk, se puede dañar una instalación actual de Personal vDisk. [#424878]
- Un escritorio virtual puede dejar de responder si Personal vDisk se ejecuta durante un periodo de tiempo largo y se produce una pérdida de memoria no paginada. [#473170]

Nuevos problemas conocidos en la versión 7.6:

- La presencia de productos antivirus puede afectar el tiempo necesario para ejecutar el inventario o realizar una actualización. El rendimiento se puede mejorar si agrega CtxPvD.exe y CtxPvDSvc.exe a la lista de exclusión PROCESS del producto antivirus. Estos archivos se encuentran en C:\Archivos de programa\Citrix\Personal vDisk\bin. [#326735]
- Los vínculos físicos que hay entre los archivos heredados de la imagen maestra no se conservan en los catálogos de Personal vDisk. [#368678]
- Después de actualizar de Office 2010 a 2013 en la imagen maestra del disco Personal vDisk, es posible que Office no se inicie en máquinas virtuales porque la clave de producto de la licencia de KMS de Office se quita durante el proceso de actualización. Como solución temporal, desinstale Office 2010 y vuelva a instalar Office 2013 en la imagen maestra. [#391225]
- Los catálogos de Personal vDisk no admiten Controllers (PVSCSI) SCSI Paravirtual de VMware. Para evitar este problema, use el controlador predeterminado. [#394039]
- Si se trata de escritorios virtuales creados con la versión 5.6.0 de Personal vDisk y se actualizan a 7, es posible que los usuarios que iniciaron sesión en la máquina virtual (VM) maestra no encuentren todos sus archivos en su VM agrupada. Este problema se produce porque se crea un nuevo perfil de usuario cuando los usuarios inician sesión en sus VM agrupadas. No existe ninguna solución para este problema. [#392459]
- La función Copia de seguridad y restauración no se puede usar en los discos Personal vDisk que ejecutan Windows 7 cuando la función Protección del sistema de Windows está habilitada. Si la protección del sistema está inhabilitada, se hacen copias de seguridad del perfil de usuario, pero no del archivo userdata.v2.vhd. Citrix recomienda inhabilitar la protección del sistema y utilizar la función Copia de seguridad y restauración para hacer copias de seguridad del perfil de usuario. [#360582]
- Cuando se crea un archivo VHD en la VM base mediante la herramienta de administración de disco, es posible que no pueda montar el disco VHD. Como solución temporal, copie el archivo VHD al volumen de PvD. [#355576]
- Los accesos directos de Office 2010 permanecen en los escritorios virtuales después de eliminar este software. Como solución temporal, elimine los accesos directos. [#402889]
- Cuando se usa Microsoft Hyper-V, no se puede crear un catálogo de máquinas con discos Personal vDisk cuando las máquinas están almacenadas localmente y los discos virtuales están almacenados en volúmenes compartidos en clúster (CSV); la creación de catálogos falla y genera un error. Como solución temporal, use un almacenamiento alternativo para los discos vDisk. [#423969]
- Al iniciar sesión por primera vez en un escritorio virtual creado a partir de un catálogo de Provisioning Services, el escritorio solicita un reinicio si el disco Personal vDisk ha sido restablecido (mediante el comando ctxpvd.exe -s reset). Como solución temporal, reinicie el escritorio cuando se le solicite. Solo hay que hacer esto una vez, no es necesario hacerlo cuando se vuelve a iniciar la sesión. [#340186]
- Si se instala .NET 4.5 en un disco Personal vDisk y una actualización de imagen posterior instala

o modifica .NET 4.0, las aplicaciones que dependen de .NET 4.5 fallarán. Como solución alternativa, distribuya .NET 4.5 a partir de la imagen base como una actualización de imagen.

- Consulte también la documentación de problemas conocidos referentes a la versión 7.6 de XenApp y XenDesktop.

### **Acerca de Personal vDisk 7.1.3**

Problemas conocidos de 7.1.1 resueltos en la versión 7.1.3:

- Las actualizaciones directas desde Personal vDisk 5.6.0 a Personal vDisk 7.x pueden hacer que falle el disco Personal vDisk. [#432992]
- Es posible que los usuarios solo puedan conectarse de forma intermitente a escritorios virtuales que tienen discos Personal vDisk. [#437203]
- Si una operación de actualización de imagen de Personal vDisk se interrumpe mientras Personal vDisk 5.6.5 o una versión posterior se actualiza a Personal vDisk 7.0 o una versión posterior, las operaciones de actualización posteriores pueden fallar. [#436145]

### **Acerca de Personal vDisk 7.1.1**

Problemas conocidos de 7.1 resueltos en la versión 7.1.1:

- Cuando se actualiza a Symantec Endpoint Protection 12.1.3 a través de una actualización de imagen, symhelp.exe notifica definiciones de antivirus dañadas. [#423429]
- Personal vDisk puede causar que los escritorios agrupados se reinicien si falla Service Control Manager (services.exe). [#0365351]

Nuevos problemas conocidos en la versión 7.1.1: ninguno

### **Acerca de Personal vDisk 7.1**

Novedades en la versión 7.1:

- Ahora se puede usar Personal vDisk con escritorios que ejecutan Windows 8.1 y se ha mejorado el registro de eventos.
- Ya no se admite Copy-on-Write (CoW). Cuando se actualiza desde la versión 7.0 a la versión 7.1 de Personal vDisk, todos los cambios hechos en los datos administrados por CoW se pierden. Se trataba de una funcionalidad que se probó en XenDesktop 7 y estaba inhabilitada de manera predeterminada, de modo que, si no la habilitó, este problema no le afectará.

Problemas conocidos de 7.0.1 resueltos en la versión 7.1:

- Si el valor de la clave del Registro de Personal vDisk EnableProfileRedirection está establecido en 1 o en ON y, después, al actualizar la imagen, este valor se cambia a 0 o a NO, es posible que todo el espacio de Personal vDisk se asigne a aplicaciones instaladas por el usuario, sin dejar espacio para los perfiles de usuario, que permanecen en el disco vDisk. Si esta redirección de perfiles está inhabilitada en un catálogo y se la habilita durante una actualización de imagen, es posible que los usuarios no puedan iniciar sesiones en su escritorio virtual. [#381921]
- El servicio Desktop Service no registra el error correcto en el visor de sucesos cuando falla la actualización de inventario de Personal vDisk. [#383331]
- Cuando se actualiza a Personal vDisk 7.x, las reglas modificadas no se conservan. Este problema se ha resuelto para las actualizaciones desde la versión 7.0 a la versión 7.1. Cuando se actualiza desde la versión 5.6.5 a la versión 7.1, primero debe guardar el archivo de reglas y luego aplicarlas de nuevo después de realizar la actualización. [#388664]
- Los discos Personal vDisk que ejecutan Windows 8 no pueden instalar aplicaciones desde la Tienda Windows. Aparece un error con el siguiente mensaje: “Su compra no se pudo completar”. Este problema no se soluciona habilitando el servicio Windows Update, pero ya se ha resuelto. No obstante, las aplicaciones instaladas por el usuario deben reinstalarse después de reiniciarse el sistema. [#361513]
- Faltan algunos vínculos simbólicos en escritorios agrupados de Windows 7 con discos Personal vDisk. Como resultado de ello, las aplicaciones que guardan iconos en C:\Usuarios\Todos los usuarios no muestran estos iconos en el menú Inicio. [#418710]
- Un disco Personal vDisk no se inicia si se produce un desbordamiento del diario de USN (números de secuencia de actualización) debido a una gran cantidad de cambios hechos en el sistema después de una actualización de inventario. [#369846]
- Un disco Personal vDisk no se inicia, con el código de estado 0x20 y el código de error 0x20000028. [#393627]
- Symantec Endpoint Protection 12.1.3 muestra el mensaje “Proactive Threat Protection is malfunctioning” y el estado LUA (Live Update Status) de este componente no está disponible. [#390204]

Nuevos problemas conocidos en la versión 7.1: Consulte la documentación “Problemas conocidos” para XenDesktop 7.1.

### **Acerca de Personal vDisk 7.0.1**

Novedades en la versión 7.0.1: Ahora, Personal vDisk es más resistente a los cambios del entorno. Los escritorios virtuales con discos Personal vDisk ahora se registran con Delivery Controller incluso aunque fallen las actualizaciones de la imagen, y los apagados no seguros del sistema ya no dejan los discos virtuales en un estado inhabilitado permanente. Además, mediante el uso de reglas se pueden excluir archivos y carpetas de los discos virtuales durante una implementación.

Problemas conocidos de 5.6.13 resueltos en la versión 7.0.1:

- Los cambios hechos por los usuarios en la pertenencia a un grupo en un escritorio virtual agrupado se pueden perder cuando se actualiza la imagen. [#286227]
- Las actualizaciones de la imagen pueden fallar con un error de poco espacio en disco, incluso aunque el disco Personal vDisk tenga espacio suficiente. [#325125]
- La instalación de algunas aplicaciones en escritorios virtuales con disco Personal vDisk falla, y aparece un mensaje indicando que hay que reiniciar. Esto se debe a una operación pendiente de cambio de nombre. [#351520]
- Los vínculos simbólicos creados dentro de una imagen maestra no funcionan en escritorios virtuales con discos Personal vDisk. [#352585]
- En entornos que usan Citrix Profile Management y Personal vDisk, las aplicaciones que exploran perfiles de usuario en un volumen de sistema pueden no funcionar correctamente si está habilitada la redirección de perfiles. [#353661]
- El proceso de actualización del inventario falla en las imágenes maestras si el tamaño del inventario es superior a 2 GB. [#359768]
- Las actualizaciones de imagen fallan con un código de error 112 y los discos Personal vDisk quedan dañados, incluso aunque estos discos tengan espacio suficiente para la actualización. [#363003]
- El script de cambio de tamaño falla para los catálogos que contienen más de 250 escritorios. [#363365]
- Los cambios hechos por los usuarios en una variable de entorno se pierden cuando se realiza una actualización de la imagen. [#372295]
- Los usuarios locales creados en un escritorio virtual con un disco Personal vDisk se pierden cuando se realiza una actualización de la imagen. [#377964]
- Es posible que un disco Personal vDisk no pueda iniciarse si se produjo un desbordamiento del diario de USN (números de secuencia de actualización) debido a una gran cantidad de cambios hechos en el sistema después de una actualización de inventario. Para evitar este problema, aumente el tamaño del diario USN a un mínimo de 32 MB en la imagen maestra y actualice la imagen. [#369846]
- Se ha identificado un problema en Personal vDisk que evita el funcionamiento correcto del Registro de AppSense Environment Manager y oculta acciones cuando AppSense se usa en modo de reemplazo. Citrix y AppSense están trabajando en forma conjunta para resolver el problema, que está relacionado con el comportamiento de la API de RegRestoreKey cuando Personal vDisk está instalado. [#0353936]

### **Problemas conocidos no relacionados con la versión**

- Si Windows Store y las aplicaciones Metro se actualizan en la imagen maestra, pueden surgir conflictos para los dispositivos de destino habilitados con PvD después de que el disco vDisk se actualice al entorno de prueba o producción. Además, es posible que las aplicaciones Metro

no se inicien mientras se desencadenan errores de registro de eventos de la aplicación. Citrix recomienda que desactive Windows Store y las aplicaciones Metro para dispositivos de destino habilitados con PvD.

- Cuando una aplicación instalada en un disco Personal vDisk (PvD) está relacionada con otra aplicación de la misma versión que está instalada en la imagen maestra, la aplicación del disco PvD puede dejar de funcionar después de una actualización de imagen. Esto ocurre si se desinstala la aplicación de la imagen maestra o si la aplicación se actualiza a una versión posterior, ya que esa acción quita de la imagen maestra los archivos que necesita la aplicación ubicada en el disco PvD. Para evitar esto, mantenga en la imagen maestra la aplicación que contiene los archivos necesarios para la aplicación del disco PvD.

Por ejemplo, la imagen maestra contiene Office 2007, y un usuario instala Visio 2007 en el disco PvD; las aplicaciones de Office y Visio funcionan correctamente. Posteriormente, el administrador reemplaza Office 2007 por Office 2010 en la imagen maestra y, a continuación, actualiza todas las máquinas pertinentes con la imagen actualizada. En consecuencia, Visio 2007 deja de funcionar. Para evitarlo, conserve Office 2007 en la imagen maestra. [#320915]

- Al implementar McAfee Virus Scan Enterprise (VSE), use el parche 4 de la versión 8.8 o posterior en una imagen maestra si utiliza Personal vDisk. [#303472]
- Si un acceso directo creado para un archivo ubicado en la imagen maestra deja de funcionar (porque el destino de ese acceso ha cambiado de nombre en el disco PvD), vuelva a crear ese acceso directo. [#367602]
- No use enlaces absolutos o físicos en una imagen maestra. [#368678]
- Personal vDisk no admite la función Copias de seguridad y restauración de Windows 7. [#360582]
- Después de la aplicación de una imagen maestra actualizada, la consola del usuario local y del grupo deja de ser accesible y muestra datos incoherentes. Para resolver este problema, restablezca las cuentas de usuario en la VM, lo que requiere restablecer también el subárbol de Registro de seguridad. Este problema se ha resuelto en la versión 7.1.2 (y funciona en las máquinas virtuales creadas con versiones posteriores), pero la corrección no funciona en el caso de máquinas virtuales que se crearon con una versión anterior y se actualizaron posteriormente. [#488044]
- Cuando se usa una VM agrupada en un entorno de hipervisor ESX, los usuarios ven una solicitud de reinicio si el tipo de controlador SCSI seleccionado es “VMware Paravirtual”. Para solucionar el problema, use un tipo de controlador SCSI LSI. [#394039]
- Después de restablecer un disco PvD en un escritorio creado mediante Provisioning Services, es posible que se solicite a los usuarios que reinicien después de iniciar sesión en la máquina virtual. Para solucionarlo, reinicie el escritorio. [#340186]

- Es posible que los usuarios del escritorio Windows 8.1 no puedan iniciar sesión en su PvD. Es posible que el administrador vea un mensaje similar a “PvD se ha inhabilitado debido a un apagado no seguro”. También es posible que el registro PvDActivation contenga un mensaje similar a “No se ha podido cargar el subárbol del Registro [\\Device\\IvmVhdDisk00000001\CitrixPvD\Settings\RingCube.dat]”. Esto ocurre cuando la máquina virtual de un usuario se apaga de forma no segura. Como solución temporal, restablezca Personal vDisk. [#474071]

## Instalación y actualización

March 10, 2022

Personal vDisk 7.x es compatible con la versión actual de Citrix Virtual Apps and Desktops (y versiones anteriores, a partir de XenDesktop 5.6). La documentación referente a los requisitos del sistema para cada versión ofrece una lista de los sistemas operativos compatibles con los agentes Virtual Delivery Agent (VDA), las versiones compatibles de hosts (recursos de virtualización) y Citrix Provisioning (antes Provisioning Services). Para obtener información más detallada sobre las tareas de Citrix Provisioning, consulte la documentación de Citrix Provisioning.

### Instalar y habilitar Personal vDisk

Puede instalar y habilitar los componentes de PvD al instalar o actualizar un VDA para SO de escritorio en una máquina. Estas acciones se seleccionan en las páginas **Componentes adicionales** y **Funciones** del asistente de instalación, respectivamente. Para obtener más información, consulte [Instalar agentes VDA](#).

Si actualiza el software de Personal vDisk después de instalar el VDA, utilice el archivo MSI de PvD proporcionado en los medios de instalación de Citrix Virtual Apps and Desktops.

Habilitar Personal vDisk:

- Si utiliza Machine Creation Services (MCS), Personal vDisk se habilita automáticamente cuando se crea un catálogo de máquinas con SO de escritorio que usarán un disco Personal vDisk.
- Si utiliza Citrix Provisioning, Personal vDisk se habilita automáticamente, ya sea cuando ejecuta el inventario durante el proceso de creación de imagen maestra (base) o cuando la actualización automática ejecuta el inventario por usted.

Por lo tanto, si instala los componentes de PvD, pero no los habilita durante la instalación del VDA, puede utilizar la misma imagen para crear escritorios con o sin PvD, debido a que PvD se habilita durante el proceso de creación del catálogo.

## Agregar discos Personal vDisk

Los discos Personal vDisk se agregan a hosts cuando configura un sitio. Puede utilizar el mismo almacenamiento en el host tanto para las VM como para los discos Personal vDisk, o bien puede usar otro almacenamiento para los discos Personal vDisk.

Más adelante, también podrá agregar discos Personal vDisk y su almacenamiento a los hosts existentes (conexiones), pero no a catálogos de máquinas.

1. Seleccione Configuración > Alojamiento en el panel de navegación de Studio.
2. Seleccione Agregar almacenamiento de Personal vDisk en el panel Acciones y especifique la ubicación de la unidad de almacenamiento.

## Actualizar PVD

La forma más sencilla de actualizar Personal vDisk desde una versión anterior 7.x consiste simplemente en actualizar los agentes VDA de los SO de escritorio a la versión proporcionada con la versión más reciente de Citrix Virtual Desktops. A continuación, se puede ejecutar el inventario de PVD.

## Desinstalar PVD

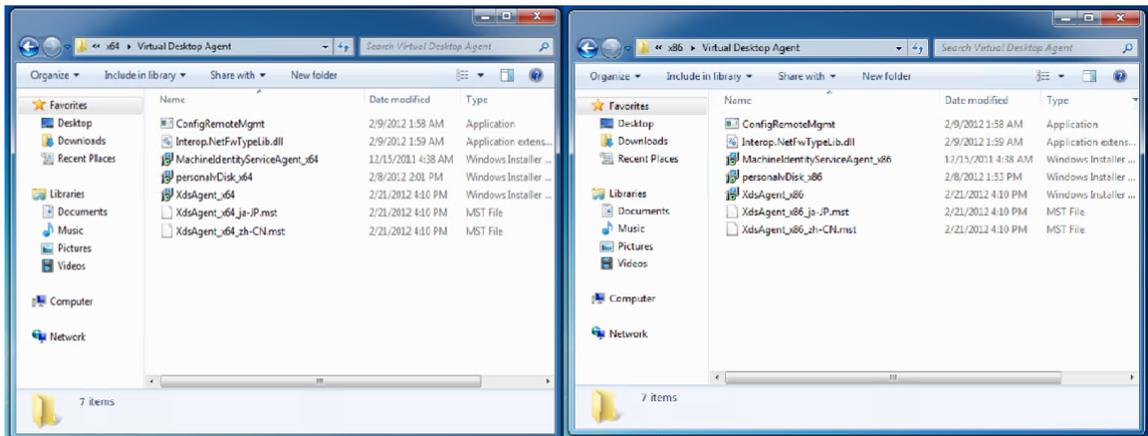
Dispone de las siguientes dos maneras para quitar el software de Personal vDisk:

- Desinstalar el agente VDA. Esta acción quita también el software de Personal vDisk.
- Si ha actualizado Personal vDisk mediante el archivo MSI de PVD, puede desinstalarlo desde la lista de programas.

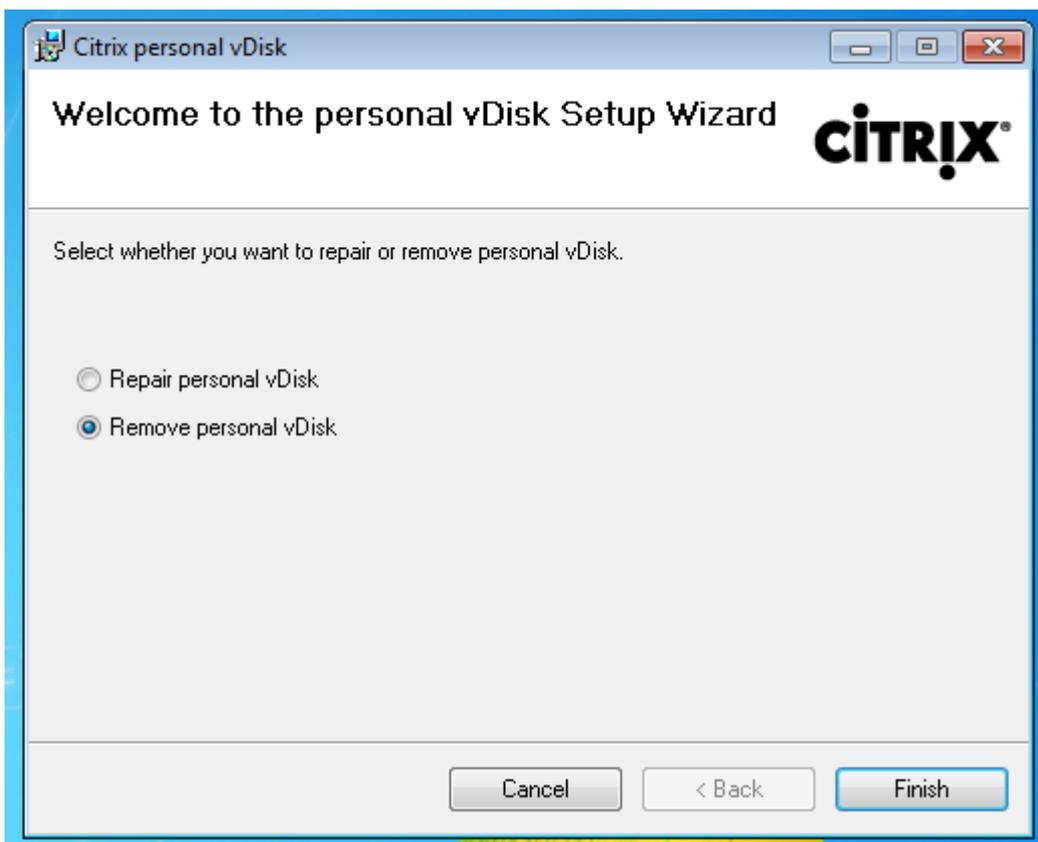
Si desinstala PVD y quiere volver a instalar la misma versión o una versión más reciente, primero haga una copia de seguridad de la clave de Registro HKLM\Software\Citrix\personal vDisk\config, que contiene los parámetros de configuración del entorno que pueden haber cambiado. Después de instalar PVD, restablezca los valores del Registro que puedan haber cambiado. Para ello, compárelos con la versión de la copia de seguridad.

La desinstalación puede fallar si se ha instalado un disco Personal vDisk con Windows 7 (64 bits) en la imagen base. Para evitar este problema, Citrix recomienda que quite el disco Personal vDisk antes de actualizar.

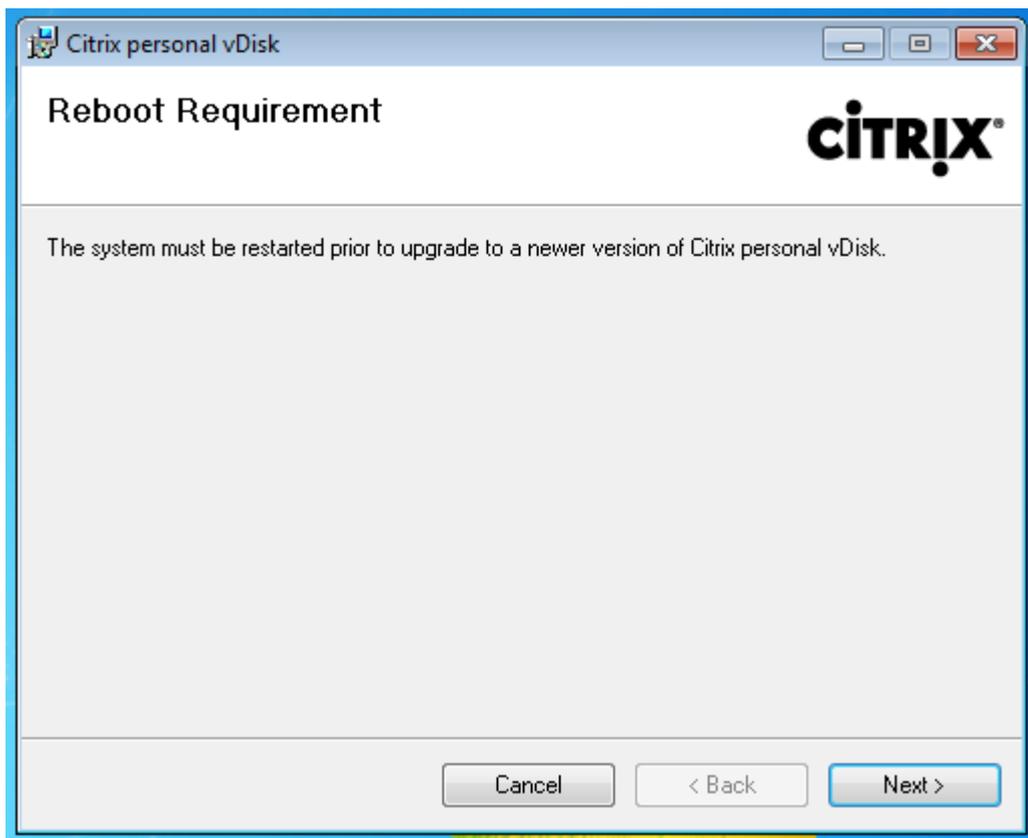
1. Seleccione la copia correspondiente del instalador vDisk en los medios de Citrix Virtual Apps and Desktops. Busque el instalador MSI más reciente de Personal vDisk en uno de los siguientes directorios (según si la máquina virtual actualizada es de 32 o 64 bits):
  - 32 bits: XA and XD\x86\Virtual Desktop Components\personalvDisk\_x86.msi
  - 64 bits: XA and XD\x64\Virtual Desktop Components\personalvDisk\_x64.msi



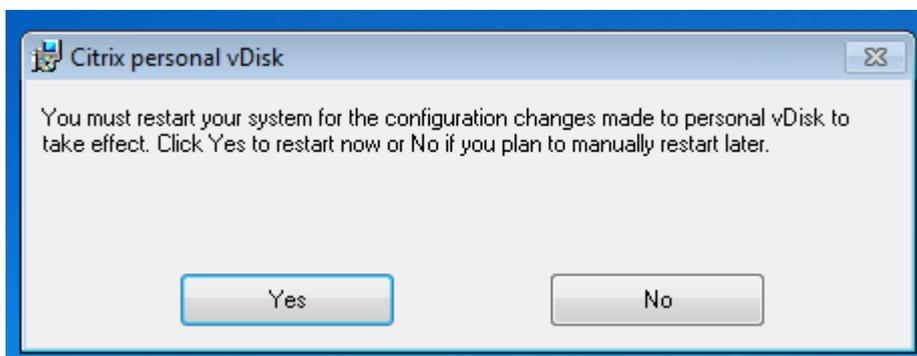
2. Quite la instalación de Personal vDisk. Seleccione el paquete de instalador MSI de Personal vDisk que ha localizado en el paso 1. Aparecerá la pantalla de configuración de Personal vDisk.
3. Seleccione **Quitar Personal vDisk**.
4. Haga clic en **Finish**.



5. Aparecerá una página con el requisito de reiniciar la máquina. Haga clic en **Siguiente**:



6. Haga clic en **Sí** para reiniciar el sistema y aplicar los cambios de configuración:



## Configurar y administrar

September 22, 2021

En este apartado se describen los elementos que se deben tener en cuenta a la hora de configurar y administrar un entorno de Personal vDisk (PvD). También se incluyen las prácticas recomendadas y las descripciones de las tareas pertinentes.

En el caso de tareas que implican trabajar con el Registro de Windows:

Precaución: Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

### **Consideraciones: tamaño del disco Personal vDisk**

Los siguientes factores repercuten en el tamaño del volumen principal del disco Personal vDisk:

- **El tamaño de las aplicaciones que los usuarios instalarán en sus discos PvD**

Durante los reinicios, PvD determina el espacio libre restante en el área de aplicaciones (User-Data.v2.vhd). Si el espacio cae por debajo del 10%, el área de aplicaciones se expande hacia el espacio no utilizado del área de perfiles (de manera predeterminada, el espacio disponible en la unidad P:). El espacio que se agrega al área de aplicaciones es aproximadamente el 50% del espacio libre combinado que queda en el área de aplicaciones y el área de perfiles.

Por ejemplo, si el área de aplicaciones de un disco PvD de 10 GB (que de manera predeterminada tiene un tamaño de 5 GB) alcanza los 4,7 GB y el área de perfiles tiene 3 GB libres, el espacio que se agrega al área de aplicaciones se calcula de la siguiente manera:

$$\text{Espacio agregado} = (5,0 - 4,7) / 2 + 3,0 / 2 = 1,65 \text{ GB}$$

El espacio agregado al área de aplicaciones es solo aproximado porque se reserva un pequeño espacio para guardar registros y otros usos auxiliares. El cálculo y posible cambio de tamaño tienen lugar en cada reinicio.

- **El tamaño de los perfiles de los usuarios (si no se va a usar una solución de administración de perfiles aparte)**

Además del espacio requerido para las aplicaciones, también debe comprobar que haya suficiente espacio disponible en los discos PvD para almacenar los perfiles de los usuarios. Incluya las carpetas especiales no redirigidas (por ejemplo, Mis documentos y Mi música) al calcular los requisitos de espacio. Los tamaños de los perfiles existentes se pueden consultar en el Panel de control (sysdm.cpl).

Algunas soluciones de redirección de perfiles almacenan archivos stub (archivos de centinela) en lugar de los datos de perfil reales. Inicialmente, puede parecer que estas soluciones de perfiles no almacenan ningún dato, pero, en realidad, consumen una entrada de directorio de archivos en el sistema por cada archivo stub (generalmente, son 4 KB por archivo). Si usa una solución de este tipo, debe calcular el tamaño según los datos de perfil reales y no según los archivos stub.

Las aplicaciones empresariales de uso compartido de archivos (como ShareFile y Dropbox) pueden sincronizar o descargar datos en las áreas de perfiles de los usuarios de los discos Personal vDisk. Para utilizar esas aplicaciones, incluya suficiente espacio en los cálculos de tamaño para esos datos.

- **Los recursos consumidos por el disco VHD de plantilla que contiene el inventario de PvD**

El disco VHD de plantilla contiene datos de inventario de PvD (archivos de centinela correspondientes al contenido de la imagen maestra). El área de aplicaciones del PvD se crea a partir de este VHD. Cada carpeta o archivo de centinela comprende una entrada de directorio de archivos en el sistema de archivos, por lo que el contenido de VHD de plantilla consume espacio de aplicaciones del PvD incluso aunque el usuario final todavía no haya instalado ninguna aplicación. Puede determinar el tamaño del disco VHD de plantilla si examina la imagen maestra después seleccionar un inventario. También puede usar la siguiente ecuación para un cálculo aproximado:

tamaño del disco VHD de plantilla = (número de archivos en la imagen base) x 4 KB

Puede determinar la cantidad de archivos y carpetas si hace clic con el botón secundario en la unidad C: (ubicada en la imagen de la máquina virtual base) y selecciona Propiedades. Por ejemplo, una imagen con 250 000 archivos da como resultado un disco VHD de plantilla de 1 024 000 000 bytes aproximadamente (casi 1 GB). Este espacio no estará disponible para la instalación de aplicaciones en el área de aplicaciones de PvD.

- **Recursos consumidos por operaciones de actualización de imágenes de PvD**

Durante las operaciones de actualización de imagen de PvD, debe haber suficiente espacio disponible en la raíz del disco PvD (de manera predeterminada, P:) para fusionar los cambios de las dos versiones de la imagen y los cambios que el usuario efectuó en su disco PvD. Por lo general, PvD reserva unas centenas de megabytes con este fin, pero los datos adicionales que se escribieron en la unidad P: pueden llegar a consumir este espacio reservado, lo que no deja espacio suficiente para completar correctamente la actualización de la imagen. El script de estadísticas de agrupación de PvD (ubicado en la carpeta Support/Tools/Scripts de los medios de instalación de Citrix Virtual Apps and Desktops) o la herramienta Personal vDisk Image Update Monitoring Tool (en la carpeta Support/Tools/Scripts\PvdTool) pueden identificar los discos PvD de un catálogo que se estén actualizando y que están casi llenos.

La presencia de productos antivirus puede afectar el tiempo necesario para ejecutar el inventario o realizar una actualización. El rendimiento se puede mejorar si agrega CtxPvD.exe y CtxPvDSvc.exe a la lista de exclusión del producto antivirus. Estos archivos se encuentran en C:\Archivos de programa\Citrix\Personal vDisk\bin. La exclusión de esos ejecutables para que no sean analizados por el antivirus puede mejorar el rendimiento del inventario y de las actualizaciones de imagen y mejorar su velocidad hasta diez veces.

- **Los recursos por crecimiento inesperado (instalación inesperada de aplicaciones, entre**

**otros)**

Tenga en cuenta la conveniencia de agregar una cantidad de espacio extra (ya sea una cantidad fija o un porcentaje del total del disco PvD) al tamaño total para que, de ese modo, quepan instalaciones no previstas de aplicaciones que el usuario realice durante la implementación.

## **Cómo configurar el tamaño y la asignación del disco Personal vDisk**

Es posible ajustar de forma manual el algoritmo de cambio automático de tamaño que determina el tamaño del disco VHD en relación a la unidad P:. Para ello, establezca el tamaño inicial del disco VHD. Esto puede resultar útil si, por ejemplo, se sabe que los usuarios instalarán varias aplicaciones que son demasiado grandes para la capacidad del VHD, aún después de cambiar el tamaño mediante el algoritmo. En este caso, puede aumentar el tamaño inicial del espacio destinado a las aplicaciones para que quepan las aplicaciones instaladas por los usuarios.

Es preferible que ajuste el tamaño inicial del disco VHD en una imagen maestra. También puede ajustar el tamaño del disco VHD de un escritorio virtual cuando un usuario no tiene espacio suficiente para instalar una aplicación. Sin embargo, debe repetir esta operación en cada escritorio virtual afectado; no es posible ajustar el tamaño inicial del disco VHD en un catálogo ya creado.

Asegúrese de que el VHD tenga un tamaño lo suficientemente grande como para almacenar archivos de definiciones de antivirus, que suelen ser grandes.

Busque y configure las siguientes claves de Registro en HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\personal vDisk\Config. (No modifique ningún otro parámetro de esta clave del Registro). Todos los parámetros deben especificarse en la imagen maestra (excepto MinimumVHDSIZEMB, que se puede cambiar en una máquina individual); los parámetros especificados en la imagen maestra se aplicarán durante la próxima actualización de imagen.

- **MinimumVHDSIZEMB**

Especifica el tamaño mínimo (en megabytes) de la parte de las aplicaciones (C:) del disco Personal vDisk. El nuevo tamaño debe ser mayor que el tamaño existente, pero menor que el tamaño del disco menos PvDReservedSpaceMB.

Cuando se aumenta este valor se asigna espacio libre desde el área del disco virtual a la unidad C:. Este parámetro se ignora si se usa un valor más bajo que el tamaño actual de la unidad C:, o si EnableDynamicResizeOfAppContainer tiene el valor 0.

Valor predeterminado = 2048

- **EnableDynamicResizeOfAppContainer**

Habilita o inhabilita el algoritmo de cambio dinámico de tamaño.

- Cuando el valor se establece en 1, cambia el tamaño del área de las aplicaciones (C:) automáticamente cuando el espacio disponible en C: baja del 10%. Los valores permitidos son 1 y 0. Para que el cambio de tamaño tenga efecto, es necesario un reinicio.
- Cuando se establece en 0, el tamaño del disco VHD se determina según el método usado en las versiones anteriores a XenDesktop 7.x.

Valor predeterminado = 1

• **EnableUserProfileRedirection**

Habilita o inhabilita la redirección del perfil del usuario al disco Personal vDisk.

- Cuando se establece en 1, PvD redirige los perfiles de los usuarios a la unidad del disco Personal vDisk (de manera predeterminada, P:). Los perfiles se redirigen normalmente a P:\Users, lo que corresponde a un perfil de Windows estándar. Esta redirección permite conservar los perfiles en caso de que el escritorio de PvD deba restablecerse.
- Cuando se le da el valor 0, todo el espacio del disco virtual (vDisk) menos PvDReservedSpaceMB se asigna a C:, la parte de aplicaciones del disco virtual, y la unidad P: del disco virtual se oculta en el Explorador de Windows. Citrix recomienda inhabilitar la redirección (para ello, establezca el valor en 0) al usar Citrix Profile Management o alguna otra solución de administración de perfiles móviles.

Este parámetro conserva los perfiles en C:\Usuarios en lugar de redirigirlos al disco Personal vDisk, y deja que la solución de administración de perfiles móviles se ocupe de gestionarlos.

Este valor garantiza que todo el espacio en P: esté asignado a las aplicaciones.

Se asume que si este valor está establecido en 0, hay una solución de administración de perfiles implementada. No se recomienda inhabilitar la redirección de perfiles sin tener una solución de administración de perfiles implementada, porque los restablecimientos de PvD subsiguientes provocan la eliminación de perfiles.

Este parámetro no debe cambiarse cuando la imagen se actualiza porque no cambia la ubicación de los perfiles existentes, pero asigna todo el espacio en el disco PvD a C: y oculta el disco.

Configure este valor antes de implementar un catálogo. No se puede cambiar después de que el catálogo se haya implementado.

Importante: A partir de XenDesktop 7.1, no se respetan los cambios efectuados en este valor al actualizar una imagen. Establezca el valor de la clave la primera vez que cree los catálogos a partir de los que se originarán los perfiles. Más adelante, no podrá modificar el comportamiento de redirección.

Valor predeterminado = 1

- **PercentOfPvDForApps**

Define la división entre la parte de las aplicaciones (C:) y la parte de los perfiles del disco Personal vDisk. Este valor se usa al crear nuevas máquinas virtuales y durante las actualizaciones de imagen cuando EnableDynamicResizeOfAppContainer tiene el valor 0.

Cambiar PercentOfPvDForApps solo es efectivo cuando EnableDynamicResizeOfAppContainer tiene el valor 0. De forma predeterminada, EnableDynamicResizeOfAppContainer está establecido en 1 (habilitado), lo que significa que AppContainer (que aparece como la unidad C:) es dinámico, por lo que solo se expande cuando queda menos del 10% del espacio disponible.

Cuando se aumenta PercentOfPvDForApps solo se aumenta el espacio máximo para el que se permite expandir la parte de Aplicaciones. El espacio no se aprovisiona inmediatamente. También debe configurar la división de espacio en la imagen maestra donde se aplicará durante la próxima actualización de imagen.

Si ya ha generado un catálogo de máquinas con el parámetro EnableDynamicResizeOfAppContainer establecido en 1, cambie ese parámetro a 0 en la imagen maestra para la siguiente actualización y configure una división de espacio apropiada. El tamaño de división solicitado se aplicará siempre que sea mayor que el tamaño actualmente asignado para la unidad C:.

Si quiere conservar el control total sobre la división de espacio, este valor debe establecerse en 0. Esto permite el control total sobre el tamaño de la unidad C:, en lugar de depender de que un usuario consuma espacio por debajo del umbral para expandir la unidad.

Valor predeterminado = 50 % (se asigna un espacio de igual tamaño a ambas partes)

- **PvDReservedSpaceMB**

Define el tamaño del espacio reservado (en MB) en el disco Personal vDisk para almacenar los registros y otros datos de Personal vDisk.

Si la implementación incluye XenApp 6.5 (o una versión anterior) y usa la distribución de aplicaciones por streaming, aumente este valor según el tamaño utilizado para Rade Cache.

Valor predeterminado = 512

- **PvDResetUserGroup**

Válido solamente para XenDesktop 5.6: Permite que un grupo especificado de usuarios restablezca un disco Personal vDisk. En las versiones posteriores se usa la Administración delegada para ello.

Otros parámetros:

- **Windows Update Service:** Defina las actualizaciones de Windows con el valor “No buscar actualizaciones” y Windows Update Service con el valor “Inhabilitado” en la imagen maestra. Además, Citrix recomienda que inhabilite las funciones y actualizaciones de Windows Store y las aplicaciones Metro.

- **Actualizaciones de Windows:** Incluidas las actualizaciones de Internet Explorer, que se deben aplicar a la imagen maestra.
- **Actualizaciones que requieren reinicios:** Las actualizaciones de Windows aplicadas a la imagen maestra pueden requerir varios reinicios para instalarse completamente, según el tipo de revisión que se entregue con ellas. Compruebe que reinicia la imagen maestra correctamente para completar totalmente la instalación de las actualizaciones de Windows aplicadas a ella, antes de seleccionar el inventario de PvD.
- **Actualizaciones de aplicaciones:** Actualice las aplicaciones instaladas en la imagen maestra para conservar espacio en los discos Personal vDisk de los usuarios. Esto también evita que se dupliquen esfuerzos actualizando las aplicaciones en todos y cada uno de los discos virtuales de los usuarios.

### **Consideraciones: aplicaciones en la imagen maestra**

Algunos programas de software pueden entrar en conflicto con el modo en que Personal vDisk crea el entorno del usuario, por lo que hay que instalarlos en la imagen maestra (y no en la máquina en sí) para evitar dichos conflictos. Además, aunque otro software no entre en conflicto con el funcionamiento de Personal vDisk, Citrix recomienda instalarlo en la imagen maestra.

Aplicaciones que deben instalarse en la imagen maestra:

- Agentes y clientes (por ejemplo, el agente de System Center Configuration Manager, el cliente de App-V, la aplicación Citrix Workspace)
- Aplicaciones que instalan o modifican controladores de la primera fase de arranque
- Aplicaciones que instalan controladores o software de impresoras o escáneres
- Aplicaciones que modifican la pila de red de Windows
- Herramientas de la VM como VMware Tools y XenServer Tools

Aplicaciones que se recomienda instalar en la imagen maestra:

- Aplicaciones que se distribuyen a un gran número de usuarios. En cada caso, desactive las actualizaciones de la aplicación antes de implementarla:
  - Aplicaciones de empresa que usan licencias de volumen como, por ejemplo, Microsoft Office y Microsoft SQL Server
  - Aplicaciones de uso frecuente, como Adobe Reader, Firefox y Chrome
- Aplicaciones de gran tamaño como, por ejemplo, SQL Server, Visual Studio y marcos de trabajo de aplicaciones como .NET Framework.

Las siguientes recomendaciones y restricciones se aplican a las aplicaciones instaladas por los usuarios en las máquinas que tienen discos Personal vDisk. Algunas de ellas no pueden imponerse si los usuarios tienen privilegios de administrador:

- Los usuarios no deben desinstalar ninguna aplicación que esté presente en la imagen maestra para volver a instalar esa misma aplicación en su disco Personal vDisk.
- Ponga cuidado a la hora de actualizar o desinstalar aplicaciones en la imagen maestra. Después de instalar una versión de una aplicación en la imagen, un usuario podría instalar una aplicación complementaria (por ejemplo, un plug-in) que requiriera esa versión. Si existe tal dependencia, la actualización o desinstalación de la aplicación en la imagen puede hacer que el complemento no funcione correctamente. Por ejemplo, con Microsoft Office 2010 instalado en la imagen maestra, un usuario instala Visio 2010 en su disco Personal vDisk. Una posterior actualización de Office en la imagen maestra podría hacer que la versión local instalada de Visio pasara a ser inutilizable.
- No se admite el software que usa licencias dependientes del hardware (ya sea mediante llaves o hardware basado en firma).

### **Consideraciones: Citrix Provisioning**

Al usar Citrix Provisioning con Personal vDisk:

- La cuenta de Soap Service debe agregarse al nodo Administradores de Studio, y debe tener un rol de Administrador de máquinas o superior. Eso garantiza que los escritorios PvD se colocan en el estado de preparación (Preparing) cuando el vDisk de Citrix Provisioning pasa a la fase de producción.
- Debe usarse la función de control de versiones de Citrix Provisioning para actualizar el disco Personal vDisk. Cuando la versión se eleva a la fase de producción, Soap Service pone los escritorios con PvD en el estado de preparación (Preparing).
- El tamaño del disco Personal vDisk siempre debe ser mayor que el disco de memoria caché de escritura de Citrix Provisioning (de lo contrario, Citrix Provisioning podría elegir erróneamente el disco Personal vDisk para usarlo como memoria caché de escritura).
- Después de crear un grupo de entrega, puede supervisar el disco Personal vDisk mediante los scripts `Resize` y `Poolstats` (`personal-vdisk-poolstats.ps1`).

Asigne el tamaño adecuado al disco de memoria caché de escritura. Durante una operación normal, PvD captura la mayoría de las escrituras de usuario (cambios) y las redirige al disco PvD. Eso implica que se puede reducir el tamaño del disco de memoria caché de escritura de Citrix Provisioning. No obstante, cuando PvD no está activo (por ejemplo, durante las operaciones de actualización de la imagen), un disco pequeño de caché de escritura de Citrix Provisioning podría llegar a llenarse, lo que provocaría un bloqueo de la máquina.

Citrix recomienda asignar a los discos de caché de escritura de Citrix Provisioning el tamaño adecuado siguiendo las prácticas recomendadas de Citrix Provisioning. Asimismo, se recomienda agregar un espacio que doble el tamaño del disco VHD de plantilla en la imagen maestra (para que se cumplan los

requisitos de fusión). Es muy poco probable que una operación de fusión requiera todo este espacio, pero podría darse el caso.

Al usar Citrix Provisioning para implementar un catálogo de máquinas con Personal vDisk habilitado:

- Siga las instrucciones indicadas en la documentación de [Citrix Provisioning](#).
- Puede cambiar los parámetros de limitación de acciones de energía si modifica la conexión en Studio. Para obtener más información, consulte los apartados siguientes.
- Si actualiza el disco Personal vDisk de Citrix Provisioning después de instalar o actualizar aplicaciones y otro software y de reiniciar el disco, ejecute el inventario de PvD y apague la VM. A continuación, transfiera la nueva versión al modo de producción. Los escritorios con PvD del catálogo deben entrar automáticamente en el estado de preparación (Preparing). Si no lo hacen, compruebe que la cuenta de Soap Service tiene privilegios de administrador de máquinas o superior en el Controller.

La función del modo de prueba de Citrix Provisioning permite crear un catálogo de prueba que contenga máquinas que utilicen una imagen maestra actualizada. Si las pruebas confirman la viabilidad del catálogo de prueba, el catálogo se puede transferir al modo de producción.

### **Consideraciones: Machine Creation Services**

Al usar Machine Creation Services (MCS) para implementar un catálogo de máquinas con Personal vDisk habilitado:

- Siga las instrucciones indicadas en la documentación del producto.
- Ejecute un inventario de PvD después de crear la imagen maestra y, luego, apague la VM (PvD no funcionará correctamente si no se apaga la VM). A continuación, tome una instantánea de la imagen maestra.
- En el asistente Crear catálogo de máquinas, especifique el tamaño del disco Personal vDisk y su letra de unidad.
- Después de crear un grupo de entrega, puede supervisar el disco Personal vDisk mediante los scripts Resize y Poolstats (`personal-vdisk-poolstats.ps1`).
- Puede cambiar los parámetros de limitación de acciones de energía si modifica la conexión en Studio. Para obtener más información, consulte los apartados siguientes.
- Si actualiza la imagen maestra, ejecute el inventario de PvD después de actualizar las aplicaciones y otros programas de software en la imagen y, a continuación, apague la VM. A continuación, tome una instantánea de la imagen maestra.
- Use el script `personal-vdisk-poolstats.ps1` o la herramienta Personal vDisk Image Update Monitoring Tool para comprobar que haya suficiente espacio en cada máquina virtual con PvD habilitado que usará la imagen maestra actualizada.

- Después de actualizar el catálogo de máquinas, los escritorios con PvD entran en el estado de preparación (Preparing) a medida que procesan individualmente los cambios hechos a la nueva imagen maestra. Los escritorios se actualizan de acuerdo con la estrategia de distribución especificada durante la actualización de la máquina.
- Use la herramienta Personal vDisk Image Update Monitoring Tool o el script personal-vdisk-poolstats.ps1 para supervisar el disco Personal vDisk en el estado de preparación (Preparing).
- La selección del almacenamiento en caché de E/S de PVD y MCS se excluyen mutuamente. Si instala PVD, no podrá crear un catálogo con el almacenamiento en caché de E/S de MCS habilitado.

### **Cómo excluir archivos y carpetas de los discos Personal vDisk**

Use los archivos de reglas para excluir archivos y carpetas de los discos virtuales. Puede hacer esto cuando los discos Personal vDisk están en fase de implementación. Los archivos de reglas tienen el nombre custom\_\*\_rules.template.txt y se encuentran en la carpeta \config. Los comentarios de cada archivo ofrecen documentación adicional.

### **Cómo ejecutar el inventario al actualizar una imagen maestra**

Con Personal vDisk habilitado, después de realizar actualizaciones en la imagen maestra posteriores a la instalación, es importante actualizar el inventario del disco (“ejecutar el inventario”) y tomar una nueva instantánea.

Puesto que son los administradores y no los usuarios quienes administran las imágenes maestras, si instala una aplicación que coloca archivos binarios en el perfil de usuario del administrador, dicha aplicación no está disponible para los usuarios de los escritorios virtuales compartidos (incluidos aquellos basados en catálogos agrupados de máquinas y catálogos agrupados de máquinas con Personal vDisk). Son los propios usuarios quienes tienen que instalar las aplicaciones.

Se recomienda tomar una instantánea de la imagen después de realizar cada paso de este procedimiento.

1. Actualice la imagen maestra instalando aplicaciones y actualizaciones del sistema operativo y configurando el sistema en la máquina como desee.

Para las imágenes maestras basadas en Windows XP que desee implementar con discos Personal vDisk, compruebe que no haya ningún cuadro de diálogo abierto (por ejemplo, mensajes que confirman la instalación de un programa o mensajes que piden autorización para usar controladores sin firma). Cuando quedan cuadros de diálogo abiertos en imágenes maestras en este entorno, se impide que VDA pueda registrarse con el Delivery Controller. Para impedir la aparición de mensajes que piden autorización para usar controladores sin firma, use el Panel

de control. Por ejemplo, vaya a Sistema > Hardware > Firma de controladores, y seleccione la opción pertinente para omitir advertencias.

2. Apague la máquina. Para máquinas con Windows 7, haga clic en Cancelar cuando el disco Personal vDisk de Citrix bloquee el apagado de la máquina.
3. En el cuadro de diálogo del disco Citrix Personal vDisk, haga clic en Actualizar inventario. Este paso puede tardar varios minutos en completarse.

Importante: Si interrumpe el siguiente apagado (aunque sea para realizar una pequeña actualización en la imagen), el inventario del disco Personal vDisk ya no coincidirá con la imagen maestra. Esto hace que la función Personal vDisk deje de funcionar. Si interrumpe el apagado del sistema, debe reiniciar la máquina, apagarla y, cuando lo pida el sistema, hacer clic de nuevo en Actualizar inventario.

4. Cuando la operación de inventario haya apagado la máquina, tome una instantánea de la imagen maestra.

Puede exportar un inventario a un punto compartido de red y, a continuación, importar ese inventario en una imagen maestra. Para obtener más información, consulte [Exportar e importar un inventario de PvD](#).

## Cómo configurar los parámetros de la limitación de conexiones

Citrix Broker Service controla el estado de energía de las máquinas que proporcionan los escritorios y las aplicaciones. El servicio Broker Service puede controlar varios hipervisores a través de un Delivery Controller. Mediante las acciones de energía del servicio Broker Service, se controla la interacción entre un Controller y el hipervisor. Para evitar sobrecargar el hipervisor, las acciones que cambian el estado de energía de una máquina reciben una prioridad y se envían al hipervisor mediante un mecanismo de limitación de peticiones. Los siguientes parámetros afectan a la limitación de peticiones. Para especificar esos valores, modifique la conexión (página Avanzada) en Studio.

Para configurar los valores de limitación de conexiones:

1. Seleccione Configuración > Alojamiento en el panel de navegación de Studio.
2. Seleccione la conexión y, a continuación, seleccione Modificar conexión en el panel Acciones.
3. Puede cambiar los siguientes valores:
  - **Acciones simultáneas (de cualquier tipo):** La cantidad máxima de acciones de energía en curso y simultáneas permitidas. Este parámetro se especifica tanto como valor absoluto como un porcentaje de la conexión al hipervisor. Se utiliza el menor de los dos valores. Valor predeterminado = 100 absoluto, 20%

- **Actualizaciones de inventario de Personal vDisk simultáneas:** La cantidad máxima de acciones de energía simultáneas permitidas de Personal vDisk. Este parámetro se especifica tanto como valor absoluto como un porcentaje de la conexión. Se utiliza el menor de los dos valores.

Valor predeterminado = 50 absoluto, 25 %

Para calcular el valor absoluto: determine el total de IOPS (TIOPS) que admite el almacenamiento del usuario final (se debe calcular o debe ser especificado por el fabricante). Con 350 IOPS por VM (IOPS/VM), determine el número de máquinas virtuales que deben estar activas en un momento dado en el almacenamiento. Calcule este valor dividiendo el total de IOPS entre IOPS/VM.

Por ejemplo, si el almacenamiento del usuario final es de 14000 IPS, el número de máquinas virtuales es:  $14000 \text{ IOPS} / 350 \text{ IOPS/VM} = 40$ .

- **Máximo de acciones nuevas por minuto:** La cantidad máxima de acciones de energía nuevas que se pueden enviar al hipervisor por minuto. Especificadas con valor absoluto.  
Valor predeterminado= 10

Para identificar más fácilmente el valor óptimo de estos parámetros en la implementación:

1. Con la ayuda de los valores predeterminados, mida el tiempo total de respuesta de la actualización de una imagen de un catálogo de prueba. Esta es la diferencia entre el inicio de una actualización de imagen (T1) y el momento en que el agente VDA de la última máquina del catálogo se registra con el Controller (T2). Tiempo total de respuesta = T2 - T1.
2. Mida las operaciones de entrada y salida por segundo (IOPS) del almacenamiento del hipervisor durante la actualización de la imagen. Esta información puede servir como referencia para la optimización. (Los valores predeterminados pueden ser la mejor opción; de lo contrario, es posible que el sistema alcance la cantidad máxima de IOPS, lo que requerirá reducir los valores del parámetro.)
3. Cambie el valor “Actualizaciones de inventario simultáneas de Personal vDisk” tal y como se describe a continuación (sin cambiar ninguno de los demás parámetros).
  - a) Aumente el valor en 10 y mida el tiempo total de respuesta después de cada cambio. Siga aumentando el valor de 10 en 10 y realice pruebas con el resultado hasta el deterioro o hasta que el tiempo total de respuesta no cambie en absoluto.
  - b) Si el paso anterior, consistente en aumentar el valor, no produjo ninguna mejora, disminuya el valor de 10 en 10 y mida el tiempo total de respuesta después de cada disminución. Repita este proceso hasta que el tiempo total de respuesta no cambie o hasta que no mejore más. Seguramente, este será el valor óptimo para las acciones de energía de Personal vDisk.
4. Después de obtener el valor del parámetro de acciones de energía de Personal vDisk, modifique uno a uno los valores de las acciones simultáneas (todos los tipos) y la cantidad máxima

de acciones nuevas por minuto. Siga el procedimiento descrito anteriormente (aumentar o disminuir) para probar distintos valores.

## **Cómo configurar Personal vDisk con Microsoft System Center Configuration Manager 2007**

System Center Configuration Manager (Configuration Manager) 2012 no requiere ninguna configuración especial y se puede instalar igual que otra aplicación de imagen maestra. La siguiente información se aplica solo a System Center Configuration Manager 2007. No se admiten las versiones de Configuration Manager anteriores a Configuration Manager 2007.

Complete los siguientes pasos para utilizar el software de agente Configuration Manager 2007 en un entorno de Personal vDisk.

1. Instale el agente cliente en la imagen maestra.
  - a) Instale el cliente de Configuration Manager en la imagen maestra.
  - b) Detenga el servicio ccmexec (SMS Agent) e inhabílitelo.
  - c) Elimine certificados del cliente o SMS del almacén de certificados del equipo local de este modo:
    - Modo mixto: Certificados (equipo local)\SMS\Certificados
    - Modo nativo
      - Certificados (equipo local)\Personal\Certificados
      - Elimine el certificado del cliente emitido por su entidad de certificación (por regla general, una infraestructura de clave pública PKI interna)
  - d) Elimine o cambie de nombre el archivo C:\Windows\smscfg.ini.
2. Quite la información que identifique de manera exclusiva al cliente.
  - a) (Optativo) Elimine o mueva archivos de registros de C:\Windows\System32\CCM\Logs.
  - b) Instale Virtual Delivery Agent (si no estaba ya instalado) y seleccione el inventario de PvD.
  - c) Apague la imagen maestra, tome una instantánea y cree un catálogo de máquinas a partir de esa instantánea.
3. Valide Personal vDisk e inicie los servicios. Lleve a cabo estos pasos una vez en cada escritorio con PvD después de iniciarlos por primera vez. Esto puede hacerse mediante un objeto de directiva de grupo (GPO) de dominio, por ejemplo.
  - Confirme que PvD está activo comprobando la presencia de la clave de Registro HKLM\Software\Citrix\personal vDisk\config\virtual.
  - Configure el servicio ccmexec (agente SMS) en Automático e inicie el servicio. El cliente de Configuration Manager contacta con el servidor de Configuration Manager y obtiene certificados y GUID nuevos y exclusivos.

## Herramientas

November 30, 2020

Puede utilizar las siguientes herramientas y utilidades para adaptar, acelerar y supervisar operaciones de PvD.

### Archivos de reglas personalizadas

Los archivos de reglas personalizadas que se proporcionan con PvD permiten modificar el comportamiento predeterminado de las actualizaciones de imagen de PvD de las siguientes maneras:

- La visibilidad de los archivos en el disco PvD
- Cómo se fusionan los cambios hechos en los archivos
- Si los archivos permiten escritura

Para obtener instrucciones detalladas sobre los archivos de reglas personalizadas y la función CoW, consulte los comentarios en los propios archivos, que se encuentran en C:\ProgramData\Citrix\personalvDisk\Config, en la VM donde está instalado PvD. Los archivos llamados “custom\_\*” describen las reglas y cómo habilitarlas.

### Scripts de cambio de tamaño y poolstats

Se ofrecen dos scripts para supervisar y administrar el tamaño de los discos PvD; se encuentran en la carpeta Support\Tools\Scripts, en los medios de instalación de Citrix Virtual Apps and Desktops.

Use `resize-personalvdisk-pool.ps1` para aumentar el tamaño de los discos PvD en todos los escritorios de un catálogo. Los siguientes complementos y módulos del hipervisor deben estar instalados en la máquina donde se ejecuta Studio:

- XenServer requiere XenServerPSSnapin
- vCenter requiere vSphere PowerCLI
- System Center Virtual Machine Manager requiere la consola VMM

Use `personal-vdisk-poolstats.ps1` para verificar el estado de las actualizaciones de imágenes y comprobar el espacio dedicado a aplicaciones y perfiles de usuarios en un grupo de escritorios con PvD. Ejecute este script antes de actualizar una imagen para comprobar si hay algún escritorio que esté quedándose sin espacio. Esto ayuda a prevenir errores durante el proceso de actualización. El script requiere que el firewall de Windows Management Instrumentation (WMI-In) esté habilitado en los escritorios con PvD. Puede habilitarlo en la imagen maestra o a través de un objeto de directiva de grupo (GPO).

Si una actualización de imagen falla, la entrada en la columna Update da información sobre el motivo del fallo.

## Restablecer el área de aplicaciones

Si un escritorio queda dañado (después de instalar una aplicación defectuosa o por algún otro motivo), puede revertir el área de aplicaciones del disco PvD a su estado predeterminado de fábrica (vacío). La operación de restablecimiento deja intacta el área de datos de perfil de usuario.

Para restablecer el área de aplicaciones del disco PvD, use alguno de estos métodos:

- Inicie una sesión como Administrador en el escritorio del usuario. Inicie un símbolo del sistema y ejecute el comando `C:\Archivos de programa\Citrix\Personal vDisk\bin\CtxPvD.exe -s Reset`.
- Busque el escritorio del usuario en Citrix Director. Haga clic en **Restablecer Personal vDisk** y, a continuación, en **Aceptar**.

## Exportar e importar un inventario de PvD

El proceso de actualización de imagen forma parte de la implementación de imágenes nuevas en escritorios con PvD; este proceso incluye ajustar el disco Personal vDisk existente para que funcione con la nueva imagen base. En caso de implementaciones que usan Machine Creation Services (MCS), puede exportar el inventario de una VM activa a un punto compartido de red y, a continuación, importarlo en una imagen maestra. Se calcula un diferencial con este inventario en la imagen maestra. Aunque no sea obligatorio usar la función de exportación o importación de inventario, puede mejorar el rendimiento de todo el proceso de actualización de imágenes.

Para usar la función de importación o exportación de inventario, debe ser un administrador. Si es necesario, autenticárese con “net use” en el recurso compartido de archivos que se va a utilizar para la exportación o importación. El contexto de usuario debe ser capaz de acceder a los recursos compartidos de archivos utilizados para la importación o exportación.

- Para exportar un inventario, ejecute el comando de exportación como administrador en una máquina que contenga un VDA con PvD habilitado (versión mínima 7.6):

```
Ctxpvdsvc.exe exportinventory “”
```

El software detecta la ubicación del inventario actual y lo exporta a una carpeta denominada “ExportedPvdInventory” en la ubicación especificada. A continuación dispone de un fragmento del resultado del comando:

```
1 C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe  
  exportinventory  
2 \share location\ExportedInventory
```

```

3 Current inventory source location C:\CitrixPvD\Settings\Inventory
  \VER-LAS
4 ...
5 Exporting current inventory to location \ ... .
6 ...
7 Deleting any pre-existing inventory folder at \ ... .
8 .Successfully exported current inventory to location \ ... . Error
  code = OPS
9 <!--NeedCopy-->

```

- Para importar un inventario ya exportado, ejecute el comando de importación como administrador en la imagen maestra:

Para importar:

Ejecute el comando de importación como administrador en la imagen maestra.

`Ctxpvdsvc.exe importinventory` “<path-to-exported-inventory>”

La <path to exported inventory> debe ser la ruta completa a los archivos del inventario; suele ser <ubicación de red\ExportedPvdInventory>.

El inventario se obtiene a partir de la ubicación de importación (donde se exportó previamente mediante la opción `exportinventory`) y se importa al almacén de inventario de la imagen maestra. A continuación dispone de un fragmento del resultado del comando:

```

1 C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe
  importinventory
2 \share location\ExportedInventory\ExportedPvdInventory
3 Importing inventory \share location\ExportedInventory\
  ExportedPvdInventory
4 ...
5 Successfully added inventory \share location\ExportedInventory\
  ExportedPvdInventory to the
6 store at c:\ProgramData\Citrix\personal vDisk\InventoryStore
7 <!--NeedCopy-->

```

Después de la exportación, el punto compartido de red debería contener los siguientes nombres de archivo. Después de la importación, el almacén de inventario ubicado en la imagen maestra debe contener los mismos nombres de archivo.

- Components.DAT
- files\_rules
- folders\_rules
- regkey\_rules
- RINGTHREE.DAT
- S-1-5-18.DAT
- SAM.DAT
- SECURITY.DAT

- SNAPSHOT.DAT
- SOFTWARE.DAT
- SYSTEM.CurrentControlSet.DAT
- VDCATALOG.DAT
- vDiskJournalData

## Pantallas, mensajes y solución de problemas

January 4, 2021

### Supervisar PvD a través de informes

Puede usar una herramienta de diagnóstico para supervisar los cambios hechos por los usuarios en ambas partes de los discos Personal vDisk (la parte dedicada a los datos de usuario y la parte dedicada a aplicaciones). Estos cambios incluyen las aplicaciones que los usuarios han instalado y los archivos que han modificado. Los cambios se almacenan en un conjunto de informes.

1. En la máquina que quiere supervisar, ejecute `C:\Program Files\Citrix\personal vDisk\bin\CtxPvdDiag.exe`.
2. Vaya a la ubicación donde almacenar los registros e informes, seleccione los informes a generar y haga clic en **Aceptar**. A continuación, se ofrece una lista de los informes disponibles.

**Informe del subárbol Software:** Este informe genera dos archivos: `Software.Dat.Report.txt` y `Software.Dat.delta.txt`.

El archivo `Software.Dat.Report.txt` registra los cambios que haya realizado el usuario en el subárbol `HKEY_LOCAL_MACHINE\Software`. Contiene las siguientes secciones:

- Lista de aplicaciones instaladas en la base: Aplicaciones instaladas en la capa 0.
- Lista de software instalado por el usuario: Aplicaciones que el usuario ha instalado en la parte de aplicaciones del disco Personal vDisk.
- Lista de software desinstalado por el usuario: Aplicaciones originalmente presentes en la capa 0 que el usuario ha quitado.

Consulte el informe delta de subárbol para obtener información acerca de `Software.Dat.delta.txt`.

**Informe del subárbol System:** El archivo generado `SYSTEM.CurrentControlSet.DAT.Report.txt` registra los cambios que haya realizado el usuario en el subárbol `HKEY_LOCAL_MACHINE\System`. Contiene las siguientes secciones:

- Lista de servicios instalados por el usuario: Servicios y controladores que haya instalado el usuario.
- Se han cambiado los inicios de los siguientes servicios: Servicios y controladores cuyo tipo de inicio haya modificado el usuario.

**Informe del subárbol Security:** El archivo generado SECURITY.DAT.Report.txt supervisa todos los cambios que el usuario realiza en el subárbol HKEY\_LOCAL\_MACHINE\Security.

**Informe del subárbol Security Account Manager (SAM):** El archivo generado SAM.DAT.Report.txt supervisa todos los cambios que el usuario realiza en el subárbol HKEY\_LOCAL\_MACHINE\SAM.

**Informe delta de subárbol:** El archivo generado Software.Dat.delta.txt registra todos los valores y claves de Registro que se hayan agregado o quitado, así como todos los valores que haya modificado el usuario en el subárbol HKEY\_LOCAL\_MACHINE\Software.

**Registros de Personal vDisk:** De forma predeterminada, los archivos de registro Pud-lvmSupervisor.log, PvDActivation.log, PvDSvc.log, PvDWMI.log, SysVol-lvmSupervisor.log y vDeskService-<#>.log se generan en P:\Usuarios\\AppData\Local\Temp\PVDLOGS, aunque se transfieren a la ubicación seleccionada.

#### **Registros del sistema operativo Windows:**

- EvtLog\_App.xml y EvtLog\_System.xml son los registros de eventos del sistema y de la aplicación en formato XML del volumen del disco Personal vDisk.
- Setupapi.app.log y setuperr.log contienen mensajes registrados en la ejecución de msixec.exe durante la instalación del disco Personal vDisk.
- Setupapi.dev.log contiene los mensajes del registro de la instalación de dispositivo.
- Msinfo.txt contiene la salida de msinfo32.exe. Para obtener información, consulte la documentación de Microsoft.

**Informe del sistema de archivos:** El archivo generado FileSystemReport.txt registra los cambios que haya realizado el usuario en el sistema de archivos. Se divide en las siguientes secciones:

- Archivos reubicados: Archivos de la capa 0 que el usuario ha transferido al disco Personal vDisk. Los archivos de la capa 0 son aquellos que la máquina a la que está vinculado el disco Personal vDisk hereda de la imagen maestra.
- Archivos eliminados: Archivos de la capa 0 que se han ocultado por una acción del usuario (por ejemplo, al eliminar una aplicación).
- Archivos agregados (MOF, INF, SYS): Archivos con las extensiones .mof, .inf o .sys que el usuario ha agregado al disco Personal vDisk (por ejemplo, al instalar una aplicación, como Visual Studio 2010, que registra un archivo .mof para la autorrecuperación).
- Otros archivos agregados: Otros archivos que el usuario ha agregado al disco Personal vDisk (por ejemplo, al instalar una aplicación).

- Archivos base modificados pero no reubicados: Archivos de la capa 0 que el usuario ha modificado, pero que los controladores modo kernel del disco Personal vDisk no han capturado en el disco Personal vDisk.

## Actualizaciones de imagen

En Studio, al elegir una máquina con Personal vDisk (PvD) habilitado de un catálogo de máquinas, la ficha “PvD” muestra el estado de la supervisión y el progreso y la hora de finalización estimados de las actualizaciones de imagen. Los estados que pueden aparecer durante una actualización de imagen son: Ready, Preparing, Waiting, Failed y Requested.

El proceso de actualización de una imagen puede fallar por diversos motivos, incluidos la falta de espacio o que el escritorio no encuentre el disco PvD a tiempo. Cuando Studio indica que un proceso de actualización de imagen no se ha podido realizar, aparece un código de error con texto descriptivo para ayudar a solucionar el problema. Use la herramienta Personal vDisk Image Update Monitoring Tool (herramienta de supervisión de actualizaciones de imagen de Personal vDisk) o el script personal-vdisk-poolstats.ps1 para supervisar el progreso de actualización de imagen y obtener los códigos de error asociados al fallo pertinente.

Si una actualización de imagen no llega a completarse, los siguientes archivos de registro pueden proporcionar más información para la solución de problemas:

- Registro del servicio de PvD: C:\ProgramData\Citrix\personal vDisk\Logs\PvDSvc.log.txt
- Registro de activación de PvD: P:\PVDLOGS\PvDActivation.log.txt

El contenido más reciente se encuentra al final del archivo de registro.

## Mensajes de error: 7.6 y versiones posteriores

Los siguientes errores son válidos para PvD 7.6 y versiones posteriores:

- **Error interno. Revise los registros de Personal vDisk para obtener más información. Código de error %d (%s)**

Este es un comodín para todos los errores sin clasificar, por lo que no tiene ningún valor numérico. Todo error inesperado que haya ocurrido durante la creación de inventario o una actualización de Personal vDisk se indica con este código de error.

- Recopile los registros y póngase en contacto con la asistencia técnica de Citrix.
- Si este error se produce durante una actualización de catálogo, revierta el catálogo a la versión anterior de la imagen maestra.

- **Los archivos de reglas contienen errores de sintaxis. Revise los registros para obtener más información.**

Código de error 2. El archivo de reglas contiene errores de sintaxis. El archivo de registro de Personal vDisk contiene el nombre del archivo de reglas y el número de línea referentes al error de sintaxis encontrado. Corrija el error de sintaxis en el archivo de reglas y vuelva a intentar la operación.

- **El inventario almacenado en el disco Personal vDisk correspondiente a la versión anterior de la imagen maestra está dañado o no se puede leer.**

Código de error 3. El inventario más reciente se guarda en “UserData.V2.vhd” en “\ProgramData\CitrixPvD\SeLAST”. Restaure el inventario que corresponde a la última versión de la imagen maestra. Puede hacerlo si importa la carpeta ‘VER-LAST’ desde una máquina con PvD conocida que funcione y que esté asociada a la versión anterior de la imagen maestra.

- **El inventario almacenado en el disco Personal vDisk correspondiente a la versión anterior de la imagen maestra es de una versión posterior.**

Código de error 4. Este conflicto se debe a incompatibilidades de versión de Personal vDisk entre la última imagen maestra y la imagen maestra actual. Intente actualizar el catálogo después de instalar la última versión de Personal vDisk en la imagen maestra.

- **Se ha detectado un desbordamiento del diario de cambios.**

Código de error 5. Se ha producido un desbordamiento del diario USN porque se ha efectuado un gran número de cambios a la imagen maestra cuando se creaba el inventario. Si este problema sigue produciéndose después de varios intentos, use procmon para determinar si el software de terceros está creando o eliminando un gran número de archivos durante la creación del inventario.

- **Personal vDisk no ha podido encontrar ningún disco conectado al sistema para el almacenamiento de los datos de usuario.**

Código de error 6. En primer lugar, compruebe que el disco PvD está conectado a la máquina virtual a través de la consola del hipervisor. Este error suele ocurrir debido al software de “prevención de pérdida de datos”, el cual impide el acceso al disco PvD. Si el disco PvD está conectado a la VM, intente agregar una excepción para el “disco conectado” a la configuración del software de “prevención de pérdida de datos”.

- **El sistema no se ha reiniciado después de la instalación. Reinicie para implementar los cambios.**

Código de error 7. Reinicie el escritorio y vuelva a intentar la operación.

- **Instalación dañada. Intente volver a instalar Personal vDisk.**

Código de error 8. Instale Personal vDisk e inténtelo de nuevo.

- **El inventario de Personal vDisk no está actualizado. Actualice el inventario en la imagen maestra y, a continuación, inténtelo de nuevo.**

Código de error 9. El inventario de Personal vDisk no se ha actualizado en la imagen maestra antes de apagar el escritorio. Reinicie la imagen maestra y apague el escritorio por medio de la opción “Actualizar Personal vDisk”, a continuación, cree una nueva instantánea; utilice esa instantánea para actualizar el catálogo.

- **Se ha producido un error interno durante el inicio de Personal vDisk. Revise los registros de Personal vDisk para obtener más información.**

Código de error 10. Esto puede deberse a que el controlador de PvD no haya podido iniciar una sesión de virtualización a raíz de un error interno o a que Personal vDisk está dañado. Intente reiniciar el escritorio a través del Controller. Si el problema persiste, recopile los registros y póngase en contacto con la asistencia técnica de Citrix.

- **Se ha agotado el tiempo de espera de Personal vDisk cuando intentaba encontrar un disco para almacenar los parámetros de personalización de los usuarios.**

Código de error 11. Este error se produce cuando el controlador de PvD no puede encontrar el disco PvD en 30 segundos después del reinicio. Esto suele deberse a un tipo de controlador SCSI incompatible o a una latencia de almacenamiento. Si esto ocurre con todos los escritorios del catálogo, cambie el tipo de controlador SCSI asociado a la “VM de plantilla” o a la “VM maestra” por un tipo compatible con la tecnología de Personal vDisk. Si esto ocurre con solo algunos escritorios del catálogo, es posible que se deba a picos de latencia de almacenamiento causados por una gran cantidad de escritorios que se inician al mismo tiempo. Intente limitar el parámetro de número máximo de acciones de energía activo asociado a la conexión de host.

- **Personal vDisk se ha desactivado porque se ha detectado un apagado no seguro del sistema. Reinicie la máquina.**

Código de error 12. Esto puede deberse a un escritorio que no haya podido completar el proceso de arranque con PvD habilitado. Intente reiniciar el escritorio. Si el problema persiste, vea el inicio del escritorio por medio de la consola del hipervisor y, allí, compruebe si el escritorio se bloquea. Si el escritorio se bloquea durante el inicio, restaure PvD a partir de la copia de seguridad (si dispone de una copia) o bien restablezca PvD.

- **La letra de unidad especificada para montar Personal vDisk no está disponible.**

Código de error 13. Esto puede deberse a que Personal vDisk no puede montar el disco PvD en el punto de montaje especificado por el administrador. El disco PvD no se podrá montar si otro hardware ya utiliza la letra de unidad. Seleccione otra letra como punto de montaje para Personal vDisk.

- **Los controladores de modo kernel de Personal vDisk no se han podido instalar.**

Código de error 14. Personal vDisk instala controladores durante la primera actualización de inventario que se realiza después de la instalación. Algunos productos antivirus impiden la instalación del controlador cuando esta instalación tiene lugar fuera del contexto de un instalador. Inhabilite temporalmente el análisis en tiempo real del antivirus o bien agregue excepciones al antivirus para los controladores de PvD durante la creación del primer inventario.

- **No se puede crear una instantánea del volumen del sistema. Compruebe que el Servicio de instantáneas de volumen esté habilitado.**

Código de error 15. Esto puede suceder porque el Servicio de instantáneas de volumen está inhabilitado. Habilite el Servicio de instantáneas de volumen e intente seleccionar un inventario de nuevo.

- **El diario de cambios no se ha podido activar. Inténtelo de nuevo después de esperar unos minutos.**

Código de error 16. Personal vDisk utiliza el diario de cambios para realizar un rastreo de los cambios efectuados en la imagen maestra. Durante una actualización de inventario, si PvD detecta que el diario de cambios está inhabilitado, intenta habilitarlo; este error se produce cuando ese intento falla. Espere unos minutos y vuelva a intentarlo.

- **No hay suficiente espacio disponible en el volumen del sistema.**

Código de error 17. No hay suficiente espacio disponible en la unidad C: del escritorio para la actualización de imagen. Amplíe el volumen del sistema o quite archivos no utilizados para liberar espacio en él. La actualización de la imagen deberá volver a comenzar tras el próximo reinicio.

- **No hay suficiente espacio disponible en el almacenamiento de Personal vDisk. Expanda el almacenamiento de Personal vDisk para proporcionar más espacio.**

Código de error 18. No hay suficiente espacio disponible en la unidad de Personal vDisk cuando se realiza una actualización de imagen. Expanda el almacenamiento de Personal vDisk o elimine archivos no utilizados para liberar espacio en el disco de almacenamiento de Personal vDisk. La actualización de imagen debería volver a iniciarse tras el próximo reinicio.

- **La unidad de almacenamiento de Personal vDisk tiene demasiadas confirmaciones. Expanda el almacenamiento de Personal vDisk para proporcionar más espacio.**

Código de error 19. No hay suficiente espacio disponible en la unidad de Personal vDisk para que quepa el disco de aprovisionamiento pesado “UserData.V2.vhd”. Expanda el almacenamiento de Personal vDisk o elimine archivos no utilizados para liberar espacio en el disco de almacenamiento de Personal vDisk.

- **Registro del sistema dañado.**

Código de error 20. El Registro del sistema está dañado, es ilegible o no se puede encontrar. Restablezca Personal vDisk o restáurelo a partir de una copia de seguridad anterior.

- **Se ha producido un error interno durante el restablecimiento de Personal vDisk. Revise los registros de Personal vDisk para obtener más información.**

Código de error 21. Este es un comodín para todos los errores detectados durante un restablecimiento de Personal vDisk. Recopile los registros y póngase en contacto con la asistencia técnica de Citrix.

- **No se ha podido restablecer Personal vDisk porque no hay suficiente espacio libre en el disco de almacenamiento de Personal vDisk.**

Código de error 22. No hay suficiente espacio disponible en la unidad de Personal vDisk al realizar una operación de restablecimiento. Expanda el almacenamiento de Personal vDisk o elimine archivos no utilizados para liberar espacio en el disco de almacenamiento de Personal vDisk.

## Mensajes de error: versiones anteriores a 7.6

Los siguientes errores son válidos para versiones de PvD 7.x anteriores a 7.6:

- **No se pudo iniciar. Personal vDisk no ha podido encontrar el disco para almacenar los parámetros de personalización de usuario.**

El software de PvD no pudo encontrar el disco Personal vDisk (de manera predeterminada, la unidad P:) o no pudo montarlo como el punto de montaje seleccionado por el administrador cuando se creó el catálogo.

- Compruebe los registros del servicio de PvD para ver si contienen la entrada: “PvD 1 status → 18:183”.
- Si está utilizando una versión de PvD anterior a la versión 5.6.12, resolverá el problema actualizando a la versión más reciente.
- Si está utilizando la versión 5.6.12 o posterior, use la herramienta de administración de discos (diskmgmt.msc) para determinar si la unidad P: está presente como volumen sin montar. Si está presente, ejecute chkdsk en el volumen para determinar si está dañado e intente recuperarlo mediante chkdsk.

- **No se pudo iniciar. Citrix Personal vDisk no se ha podido iniciar. Para obtener ayuda... Código de estado: 7, código de error: 0x70.**

El código de estado 7 implica que se encontró un error al intentar actualizar el disco PvD. El error puede ser uno de los siguientes:

---

Código de error	Descripción
0x20000001	No se pudo guardar el paquete de diferenciación (diff), seguramente debido a que no hay suficiente espacio en disco libre en el VHD.
0x20000004	No se pudo obtener los privilegios requeridos para actualizar el PvD.
0x20000006	No se pudo cargar una sección de la imagen del PvD o del inventario de PvD, seguramente debido a que la imagen o el inventario están dañados.
0x20000007	No se pudo cargar el inventario de sistema de archivos, seguramente debido a que la imagen o el inventario de PvD están dañados.
0x20000009	No se pudo abrir el archivo que contiene el inventario de sistema de archivos, seguramente debido a que la imagen o el inventario de PvD están dañados.
0x2000000B	No se pudo guardar el paquete de diferenciación (diff), seguramente debido a que no hay suficiente espacio en disco libre en el VHD.
0x20000010	No se pudo cargar el paquete de diferenciación.
0x20000011	Faltan archivos de reglas.
0x20000021	Inventario de PvD dañado.
0x20000027	El catálogo “MojoControl.dat” está dañado.
0x2000002B	Falta el inventario de PvD, o está dañado.
0x2000002F	No se pudo registrar un archivo MOF instalado por el usuario en la actualización de la imagen. Actualice el software a la versión 5.6.12 para solucionar el problema.
0x20000032	Consulte PvDactivation.log.txt para ver la entrada de registro más reciente que contenga un código de error Win32.
0x20	No se pudo montar el contenedor de aplicaciones para la actualización de la imagen. Actualice el software a la versión 5.6.12 para solucionar el problema.
0x70	No hay espacio suficiente en el disco.

## Código de error

## Descripción

- **No se pudo iniciar. Citrix Personal vDisk no se ha podido iniciar [o se ha producido un error interno en Personal vDisk]. Para obtener ayuda...Código de estado: 20, código de error: 0x20000028.**

Se ha encontrado Personal vDisk, pero no se ha podido crear una sesión de PvD.

Recopile los registros y compruebe SysVol-IvmSupervisor.log para ver la creación de sesiones no realizadas:

1. Compruebe si existe la entrada “IvmpNativeSessionCreate: failed to create native session, status XXXXX”.
2. Si el estado es 0xc00002cf, solucione el problema agregando una nueva versión de la imagen maestra al catálogo. Este código de estado implica que el diario USN se saturó debido a una gran cantidad de cambios realizados después de una actualización de inventario.
3. Reinicie el escritorio virtual afectado. Si el problema continúa, póngase en contacto con la asistencia técnica de Citrix.

- **No se pudo iniciar. Citrix Personal vDisk se ha desactivado porque se ha detectado un apagado no seguro del sistema. Para volver a intentarlo, seleccione Reintentar. Si el problema continúa, póngase en contacto con el administrador del sistema.**

La VM agrupada no puede iniciarse completamente con PvD habilitado. Primero determine por qué no se puede completar el proceso de inicio. Los motivos posibles por los que aparece una pantalla azul son los siguientes:

- La imagen maestra contiene un producto antivirus incompatible. Por ejemplo: versiones antiguas de Trend Micro.
- El usuario ha instalado software que es incompatible con PvD. Es poco probable, pero puede comprobarlo si agrega una nueva máquina al catálogo y verifica si la VM se reinicia correctamente.
- La imagen de PvD está dañada. Esto se ha observado en la versión 5.6.5.

Para comprobar si la VM agrupada está mostrando una pantalla azul o se está reiniciando prematuramente:

- Inicie sesión en la máquina por medio de la consola del hipervisor.
- Haga clic en Reintentar y espere a que la máquina se apague.
- Inicie la máquina mediante Studio.
- Use la consola del hipervisor para observar el inicio de la consola de la máquina.

Otras soluciones:

- Obtenga un volcado de memoria de la máquina que muestra una pantalla azul y envíelo al servicio de asistencia técnica Citrix Technical Support para su análisis.
- Compruebe si hay errores en los registros de eventos asociados a PvD:
  1. Monte UserData.V2.vhd desde el directorio raíz de la unidad P:, haciendo clic en Acción > Exponer VHD en DiskMgmt.msc.
  2. Inicie Eventvwr.msc.
  3. Abra el registro de eventos de sistema (Windows\System32\winevt\logs\system.evtx) desde UserData.V2.vhd haciendo clic en Acción > Abrir registro guardado.
  4. Abra el registro de eventos de aplicación (Windows\System32\winevt\logs\application.evtx) desde UserData.V2.vhd haciendo clic en Acción > Abrir registro guardado.

- **Personal vDisk no se puede iniciar. Personal vDisk no se ha podido iniciar porque el inventario no se ha actualizado. Actualice el inventario en la imagen maestra e inténtelo de nuevo. Código de estado: 15, código de error: 0x0.**

El administrador seleccionó una instantánea incorrecta al crear o al actualizar el catálogo de PvD (es decir, la imagen maestra no se apagó mediante Actualizar Personal vDisk cuando se creó la instantánea).

## Eventos registrados por Personal vDisk

Si Personal vDisk no está habilitado, puede ver los siguientes eventos en el Visor de eventos de Windows. Seleccione el nodo Aplicaciones en el panel de la izquierda; el Origen de los sucesos en el panel derecho es Citrix Personal vDisk. Si Personal vDisk está habilitado, no se muestra ninguno de estos eventos.

El ID de evento 1 indica un mensaje informativo, un ID de evento 2 indica un error. Es posible que no se usen todos los eventos en cada versión de Personal vDisk.

ID de suceso	Descripción
1	Estado de Personal vDisk: Se ha iniciado la actualización del inventario.
1	Estado de Personal vDisk: Se ha completado la actualización del inventario. GUID: %s.
1	Estado de Personal vDisk: Se ha iniciado la actualización de la imagen.
1	Estado de Personal vDisk: Se ha completado la actualización de la imagen.
1	Restablecimiento en curso.
1	Aceptar.

---

ID de suceso	Descripción
2	Estado de Personal vDisk: Ha fallado la actualización del inventario con el error: %s.
2	Estado de Personal vDisk: Ha fallado la actualización de la imagen con el error: %s.
2	Estado de Personal vDisk: Ha fallado la actualización de la imagen con un error interno.
2	Estado de Personal vDisk: Ha fallado la actualización del inventario con un error interno.
2	Personal vDisk se ha inhabilitado debido a un apagado inapropiado.
2	La actualización de la imagen falló. Código de error %d.
2	Personal vDisk encontró un error interno. Código de estado[%d], código de error[0x%X].
2	El restablecimiento de Personal vDisk falló.
2	No se encuentra el disco para almacenar los parámetros de personalización de usuario.
2	No hay suficiente espacio disponible en el disco de almacenamiento para crear un contenedor de Personal vDisk.

---

## Migrar Personal vDisk a App Layering

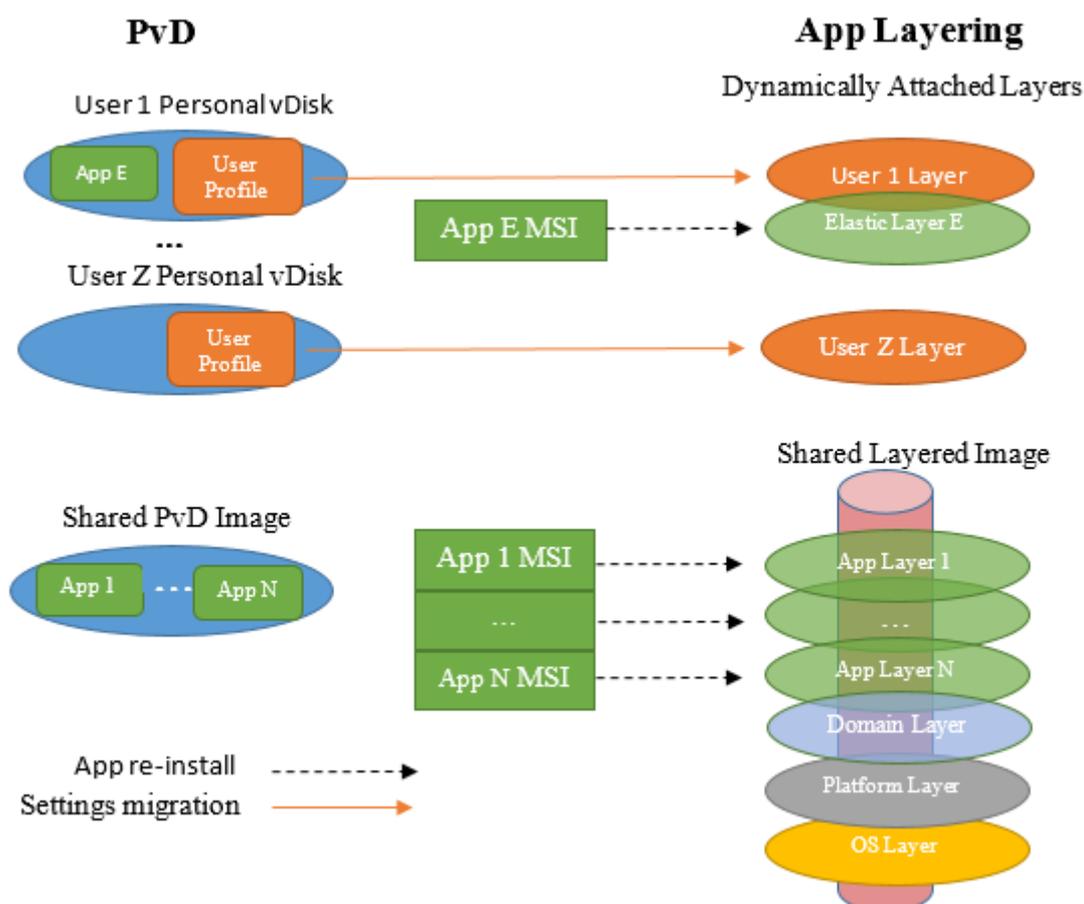
September 22, 2021

Citrix está reemplazando la funcionalidad Personal vDisk (PvD) por la tecnología Citrix App Layering. Utilice la información de este artículo para crear una máquina virtual (VM) de App Layering que sea equivalente en funciones a una VM basada en PvD.

Para obtener información acerca de las capas y el proceso de creación y publicación de plantillas de imagen, consulte la documentación de [Citrix App Layering](#).

Las máquinas virtuales típicas de PvD constan de una imagen compartida y un disco Personal vDisk. La imagen compartida se distribuye a varios usuarios, cada uno de ellos con su propio disco Personal vDisk. Una máquina virtual típica de App Layering consta de varias capas: una capa de sistema operativo, una capa de plataforma y, por lo general, una o varias capas de aplicaciones. Esta VM se comparte entre varios usuarios, cada uno con su propia capa de usuario (User Layer).

Al migrar un conjunto de usuarios que comparten una VM con imagen PvD, se crea una VM de imagen compartida de App Layering con funciones equivalentes. Cada usuario dispone de su perfil y sus parámetros personales migrados desde su disco Personal vDisk a su nueva capa de usuario en App Layering, como se ilustra en la siguiente imagen:



En este artículo se adopta un enfoque para migrar los datos personales de un usuario y otro enfoque para migrar las aplicaciones. Para los datos personales, en este artículo se recomienda utilizar herramientas para copiarlos desde un disco Personal vDisk a una capa de usuario. En cambio, para las aplicaciones, no se recomienda copiarlas. En vez de ello, se recomienda que las aplicaciones se reinstalen en una capa de aplicaciones (App Layer). Además, en este artículo se asume:

- Que la VM de PvD ejecuta Windows 7. La migración desde otras versiones de sistema operativo debería ser similar si App Layering las admite. Por ejemplo, App Layering no admite Windows XP.
- Citrix Hypervisor se utiliza como hipervisor, por lo que se asume que está familiarizado con la administración de éste mediante XenCenter.
- Se utiliza Machine Creation Services (MCS) o Citrix Provisioning (antes Provisioning Services) para el aprovisionamiento. Para MCS o Citrix Provisioning, necesitará la imagen ISO de Citrix

Virtual Apps and Desktops. Para Citrix Provisioning, necesitará “ProvisioningServicesxxx.iso”.

- Se usa Citrix Virtual Desktops para administrar las máquinas virtuales generadas de App Layering.

Si utiliza otro hipervisor o servicio de aprovisionamiento, los procedimientos de migración indicados en este artículo son similares.

En los ejemplos de este artículo se presupone que el usuario es miembro de un dominio de Active Directory (AD).

## Personal vDisk y App Layering

App Layering facilita una separación clara entre las aplicaciones y la información específica del usuario. Las aplicaciones se encuentran en las capas de aplicaciones (App Layer), a menudo con una aplicación por capa, mientras que la información específica del usuario se encuentra en una capa de usuario (User Layer). Se recomienda que un usuario no instale una aplicación en su capa de usuario si cree que la aplicación puede ser de utilidad general. En vez de ello, el usuario puede instalarla en una capa elástica de aplicaciones (Elastic App Layer), que se uniría dinámicamente a sus máquinas virtuales (y a otras) cuando ese usuario iniciara sesión.

PvD no admite esta separación clara porque solo tiene dos capas: la imagen compartida (compartida entre varios usuarios) y un disco virtual específico del usuario. Los usuarios a menudo instalan una aplicación en su disco Personal vDisk si no está disponible en la imagen compartida.

Al migrar una imagen PvD compartida a App Layering, debe determinar todas las aplicaciones que contiene. Para cada aplicación (o un conjunto relacionado de aplicaciones) debe crear una capa de aplicaciones. Se deben tener en cuenta las siguientes cuestiones:

- Si la aplicación es de utilidad general, debe adjuntar la capa de aplicaciones a una plantilla de imagen desde la que esa aplicación se publicará en una imagen en capas (Layered Image).
- Si la aplicación es útil solo para un grupo de usuarios, debe asignarla a ese grupo. Así, cuando los miembros de ese grupo inicien sesión en la máquina virtual, esa aplicación se adjuntará dinámicamente en una capa elástica de aplicaciones.
- Si la aplicación resulta útil solamente para un usuario, debe instalarla en la capa de ese usuario.

## Otros elementos de App Layering

En el proceso de creación de una VM de App Layering, se crean algunos elementos (máquinas virtuales de empaquetado, conectores, agentes y plantillas de máquinas virtuales). Estos elementos son exclusivos de App Layering y se describen brevemente en las siguientes secciones. Para obtener una descripción completa, consulte la [documentación de App Layering](#).

## Máquinas virtuales de empaquetado

El método de App Layering para personalizar el contenido de las capas de plataformas y las capas de aplicaciones consiste en crear una *VM de empaquetado* (Packaging VM), a veces denominada *máquina de instalación* (Install Machine). Crear una capa es un proceso de seis pasos:

1. Desde Enterprise Layer Manager (ELM), cree la capa, y especifique su nombre, entre otros datos.
2. ELM genera una máquina virtual de empaquetado y la copia (normalmente) al hipervisor.
3. Desde el hipervisor, inicie la VM de empaquetado y personalícela.
4. Cuando haya terminado la personalización, haga clic en el icono **Shutdown to Finalize** (Cerrar para finalizar), que está en el escritorio de la VM de empaquetado. Esta acción realiza una comprobación de integridad de la capa, lo que garantiza que no haya reinicios pendientes y que ngen no se está ejecutando. No termina hasta que todas estas tareas estén completas.
5. Desde ELM, haga clic en la acción **Finalize**.
6. ELM termina la generación de la capa en función de la VM de empaquetado personalizada y elimina esa VM de empaquetado.

App Layering no usa una VM de empaquetado para crear la capa de sistema operativo. En vez de ello, usted crea una VM, la personaliza según sea necesario y ELM la importa.

## Conectores y agentes

El ELM se comunica con varias entidades, como hipervisores, recursos compartidos de archivos y herramientas de aprovisionamiento. Realiza diversas tareas en esas entidades, como la creación de máquinas virtuales, lo que implica copiar diversos tipos de datos, como VHD y archivos, hacia o desde esas entidades.

Un conector es un objeto que ELM utiliza cuando se comunica con otra entidad para realizar un conjunto de tareas. Está configurado con el nombre o la dirección IP de la otra entidad, las credenciales necesarias para acceder a esa entidad y cualquier otra información requerida para realizar las tareas. Por ejemplo, una ruta de archivo en la entidad donde se leen o escriben los datos.

Los siguientes elementos son conectores:

- Conector de Citrix Hypervisor: ELM utiliza este conector para crear o eliminar máquinas virtuales, como las máquinas virtuales de empaquetado, que haya en XenServer.
- Conector de archivos compartidos de red (Network File Share Connector): Este conector se configura desde la ficha “System”, la subficha “Settings and Configurations”, en la sección “Network File Share”. ELM y las VM utilizan este proceso para crear archivos en un recurso compartido de archivos de red.
- Citrix MCS para el conector de Citrix Hypervisor: Si utiliza MCS como servicio de aprovisionamiento, se crea este conector. ELM lo usa para copiar las imágenes en capas a Citrix Hypervisor después de eliminar los controladores que MCS no necesita.

- **Citrix Provisioning Connector:** Si utiliza Citrix Provisioning como servicio de aprovisionamiento, se crea este conector. ELM lo usa para copiar el VHD de imagen en capas al servidor de Citrix Provisioning. Crea un disco virtual allí después de eliminar los controladores no requeridos por Citrix Provisioning.

## **Plantilla de VM**

Si utiliza Citrix Hypervisor como hipervisor, se crea una plantilla de VM basada en la capa de SO que tenga la VM. Esta plantilla contiene información sobre el sistema operativo, como las interfaces de red y la cantidad de procesadores. La plantilla es creada después de que su capa de sistema operativo se haya creado. Se utiliza cuando se crea un conector de Citrix Hypervisor.

## **Instalar Unidesk Agent en el servidor Citrix Provisioning**

Si implementa con Citrix Provisioning, debe instalar Unidesk Agent en el servidor Citrix Provisioning. Eso permite que ELM ejecute comandos en el servidor Citrix Provisioning.

Consulte “Install the App Layering Agent (required for Citrix Provisioning and Connector Scripts)” (Instalar el agente de App Layering, requerido para Citrix Provisioning y Connector Scripts) en la documentación de [App Layering](#).

## **Migrar imágenes compartidas**

Para migrar una imagen PvD compartida a App Layering, debe crear una imagen compartida en capas (Shared Layered Image) que tenga funciones equivalentes a la imagen PvD compartida. La imagen compartida en capas se construye publicando una plantilla de imagen. La plantilla de imagen combina una capa de sistema operativo, una capa de plataforma y una o varias capas de aplicaciones. Deberá crear cada una de esas capas. Estos procedimientos se describen en las siguientes secciones.

## **Capa de SO**

Lleve a cabo estos pasos para crear una capa de sistema operativo.

### **Desde XenCenter:**

Cree una VM en Citrix Hypervisor. Esta es la base para su capa de SO y su plantilla de VM.

La versión de SO de la máquina virtual debe coincidir con la de la imagen PvD compartida que está migrando. En estas instrucciones, se presupone que ejecuta Windows 7.

### **Desde la VM de la capa de SO:**

Inicie sesión con la cuenta de administrador local.

Instale todas las actualizaciones importantes de Windows.

Realice las tareas de preparación descritas en “Preparar una imagen de Windows 7”, en la [documentación de App Layering](#).

**Desde XenCenter:**

Haga una copia de la VM de la capa de SO. Elimine todo el almacenamiento local. Convierta la VM a una plantilla. Debe utilizar esta plantilla de VM al crear un conector de Citrix Hypervisor.

**Desde ELM:**

En la ficha **Layers**, haga clic en **Create OS Layer**.

Si utiliza Citrix Hypervisor y aún no ha creado un conector de Citrix Hypervisor, hágalo ahora. Cuando se le solicite la plantilla de máquina virtual (Virtual Machine Template), especifique la plantilla de VM que creó en la sección anterior.

Cuando se le solicite seleccionar la máquina virtual (Select Virtual Machine), elija su VM de capa de sistema operativo.

Después de asignar un icono y especificar cualquier otra información detallada, haga clic en “Create Layer”. Esto copia su VM de capa de sistema operativo al almacén de ELM y generará su capa de sistema operativo.

Con ello, se completa la creación de la capa de SO y esa capa se puede implementar.

## **Capa de plataforma**

Una vez generada la capa de SO, puede continuar con la creación de una capa de plataforma para la imagen compartida.

Un paso en el proceso de personalización de la capa de plataforma es unirse al dominio de Active Directory de los usuarios. Si los usuarios son miembros de varios dominios, debe crear una capa de plataforma por separado para cada dominio. En este artículo se asume que todos los usuarios pertenecen a un solo dominio.

**Desde ELM:**

1. En la ficha **Layers**, haga clic en **Create Platform Layer**.
2. En el panel “OS Layers”, seleccione la capa de SO que creó en la sección anterior.
3. En el panel “Connector”, seleccione el conector de Citrix Hypervisor que creó en la sección anterior. ELM utiliza esta información cuando escribe la VM de empaquetado de la capa de plataforma en Citrix Hypervisor.
4. En el panel “Platform Types”, marque “This platform will be used for publishing Layered Images”(Esta plataforma se utilizará para publicar imágenes en capas).

5. Elija el hipervisor apropiado. En este artículo, se presupone que utiliza “Citrix Hypervisor”.
6. Elija el servicio de aprovisionamiento apropiado. Se asume que utiliza “Citrix MCS” o “Citrix PVS” (si usa Citrix Provisioning).
7. Para el broker de conexión, seleccione “Citrix XenDesktop”.

Después de asignar un icono y especificar cualquier otra información detallada, haga clic en **Create Layer**. Esta acción genera una VM de empaquetado de capa de plataforma. Una vez completado, el estado de la tarea de creación indica “Action Required” (Acción requerida).

#### Desde XenCenter:

Una vez generada su VM de empaquetado de capa de plataforma, aparece en XenCenter. Lleve a cabo lo siguiente:

1. Arránquela.
2. Desde su VM de empaquetado de capa de plataforma, inicie sesión con la cuenta de administrador local.
3. Si se le solicita, reinicie e inicie sesión de nuevo.
4. Únase al dominio de Active Directory de los usuarios de la forma habitual. Es decir, **Panel de control > sistema > cambiar parámetros \ > cambiar**. Reinicie y vuelva a iniciar sesión con la cuenta de administrador local.

Instale el agente Citrix Virtual Delivery Agent (VDA):

1. Monte la ISO de Citrix Virtual Apps and Desktops.
2. Ejecute “AutoSelect.exe” si no se inicia automáticamente.
3. Haga clic en **Iniciar** junto a Citrix Virtual Desktops.
4. Haga clic en **Virtual Delivery Agent para SO de escritorio Windows**.

En general, elija los valores predeterminados en los siguientes paneles de opciones. Sin embargo:

- Puede especificar su Delivery Controller cuando se le solicite, o indique “Do It Later (Advanced)”.
- Compruebe que “Personal vDisk” no esté seleccionado.

Después de instalarse el VDA, se reinicia la VM de empaquetado de capa de plataforma.

Vuelva a iniciar sesión.

Si utiliza Citrix Provisioning como servicio de aprovisionamiento, también debe instalar el software del dispositivo de destino. Para hacerlo:

1. Monte “ProvisionServicesxxx.iso”.
2. Ejecute “AutoSelect.exe” si no se inicia automáticamente.

3. Haga clic en “Target Device Installation”.
4. Haga clic nuevamente en “Target Device Installation” para iniciar el asistente de instalación. El instalador instala Citrix Diagnostics Facility (CDF) y el código del dispositivo de destino de Citrix Provisioning Service.
5. En general, elija los valores predeterminados en los siguientes paneles de opciones.
6. Cuando el asistente de instalación finalice, desmarque “Launch Imaging Wizard” y haga clic en “Finish”.
7. Permita que la máquina virtual se reinicie e inicie sesión.
8. Ejecute la utilidad Citrix Provisioning Optimizer.

Después de instalar todo el software relacionado con la plataforma y realizar todas las personalizaciones, haga clic en el icono del escritorio “Shutdown to Finalize”.

#### **Desde ELM:**

Seleccione el icono de su capa de plataforma, cuyo estado debería ser “Editing”, y haga clic en **Finalize**.

#### **Capas de aplicaciones**

Una vez generada la capa de plataforma, puede continuar con la creación de capas de aplicaciones para la imagen PvD compartida. Determine las aplicaciones instaladas en la imagen PvD compartida. Hay varias formas de hacerlo, por ejemplo:

- Si tiene una versión de arranque de la imagen PvD compartida, arránquela y, desde el Panel de control, seleccione “Programas y características”.
- De lo contrario, desde Citrix Virtual Desktops, use la imagen PvD compartida para crear una VM de PvD para un usuario ficticio. Como el disco Personal vDisk del usuario ficticio está vacío, todas las aplicaciones que se muestran en “Programas y características” se han instalado en la imagen PvD compartida.

Use el panel **Programas y características** para verificar todas las aplicaciones necesarias.

Como alternativa, puede utilizar el programa PCmover, que se describe en la sección “Herramientas de migración”. Identifica muy bien las aplicaciones presentes en un equipo. Detecta programas que se hayan instalado de una forma inhabitual (por lo que no aparecen en “Programas y características”). Si se usa para este propósito, permita que realice su análisis sin realizar ninguna migración en sí. Una vez que la herramienta haya realizado su análisis y usted haya anotado todas las aplicaciones de la imagen compartida, cancele PCmover. Para obtener información más detallada, consulte la sección **Usar PCmover para determinar las aplicaciones necesarias** más adelante en este artículo.

**Sugerencia:**

Si está migrando varias máquinas virtuales PvD, esta sería una buena oportunidad para arrancar cada una de ellas y compilar una lista de las aplicaciones instaladas por el usuario. Todas las aplicaciones que vea situadas encima de las que encontró en la imagen compartida son aplicaciones instaladas por el usuario.

Una vez disponga de la lista completa de las aplicaciones necesarias, cree una o varias capas de aplicaciones. A continuación, instale una o varias aplicaciones necesarias en cada capa de aplicaciones. Por ejemplo, todas las aplicaciones relacionadas pueden instalarse en una sola capa de aplicaciones. Las aplicaciones que utilicen varios usuarios pueden instalarse en una capa elástica de aplicaciones. Una aplicación que utilice un solo usuario se puede instalar en la capa propia de ese usuario. Aunque para muchas aplicaciones es sencillo crear una capa de aplicaciones, otras requieren una preparación especial.

Para muchas aplicaciones, es sencillo crear una capa, mientras que otras requieren una preparación especial. Consulte las diferentes recetas de configuración desarrolladas por Citrix Solution Architects y por la comunidad de App Layering. Verá, por ejemplo, que hay algunas aplicaciones que solo se pueden instalar en una capa de usuario, no en una capa de aplicaciones.

**Para cada capa de aplicaciones, desde ELM:**

1. En la ficha **Layers**, haga clic en **Create App Layer**.
2. En la sección **Layer Details**, especifique el nombre de la capa y su versión.
3. En la capa de sistema operativo, seleccione la capa de SO que creó en la sección anterior.
4. Si esta aplicación depende de aplicaciones que se encuentran en otra capa de aplicaciones, especifíquelas en las capas de requisitos previos. Esto determina el orden en que se crean las capas de aplicaciones.
5. En el panel “Connector”, seleccione el conector de Citrix Hypervisor que creó en la sección anterior. ELM utiliza este conector para escribir la VM de empaquetado de la capa de aplicaciones en Citrix Hypervisor, donde, mediante XenCenter, puede arrancarla y personalizarla.
6. Cuando haya especificado todas las opciones, haga clic en **Create Layer**. Esta acción genera una VM de empaquetado de capa de aplicaciones. Una vez completado, el estado de la tarea de creación indica “Action Required”(Acción requerida). En este ejemplo, no se necesita ninguna capa de plataforma porque se presupone que esta capa de aplicaciones se implementa en el mismo hipervisor que se eligió cuando creó la capa de sistema operativo.

**Desde XenCenter:**

Una vez generada su VM de empaquetado de capa de aplicaciones, aparece en XenCenter. Realice las siguientes tareas:

1. Arránquela.

2. Desde su VM de empaquetado de capa de aplicaciones, inicie sesión con la cuenta de administrador local.
3. Si se requiere un reinicio de inmediato, reinicie y vuelva a iniciar sesión.
4. Instale la aplicación o las aplicaciones que quiere que haya en la capa de aplicaciones y realice las personalizaciones necesarias. Debido a que esta capa es compartida por varios usuarios, no deben realizarse personalizaciones ni configuraciones específicas del usuario. Se realizan cuando se migra el disco personal vDisk de un usuario, como se describe más adelante en este artículo.
5. Después de instalar las aplicaciones en esta capa y realizar todas las personalizaciones, haga clic en el icono de escritorio **Shutdown to Finalize**.

#### Desde ELM:

1. Seleccione el icono de la capa de aplicaciones, cuyo estado debería ser *Editing*.
2. Haga clic en **Finalize**. Con ello, se completa la creación de la capa de aplicaciones y esa capa se puede implementar.
3. Repita este procedimiento para cada capa de aplicaciones requerida.

#### Plantilla de imagen

Después de haber generado la capa de SO, la capa de plataforma y una o varias capas de aplicaciones, ahora puede continuar con el proceso y crear una plantilla de imagen. Decida cuáles serán las capas de aplicaciones que se vincularán a la imagen en capas y cuáles se deben asignar dinámicamente a los usuarios en capas elásticas de aplicaciones. Tenga en cuenta lo siguiente:

- Todas las capas de aplicaciones que incluya en la plantilla de imagen están disponibles para todos los usuarios de la imagen compartida en capas.
- Las capas de aplicaciones que asigne a usuarios específicos (o grupos de AD) están disponibles solo para esos usuarios (o grupos de AD). Puede cambiar dichas asignaciones más adelante, para que las capas de aplicaciones estén disponibles para otros usuarios o grupos.

#### Importante:

Estas dos alternativas son mutuamente excluyentes; es decir, no debe incluir nunca una capa de aplicaciones en una plantilla de imagen y, además, asignarla a un usuario. Hacerlo es innecesario y no se admite.

Como regla general, las aplicaciones que se instalaron en la imagen PvD compartida deben incluirse en la plantilla de imagen. Las aplicaciones que se instalaron en la imagen PvD compartida deberían incluirse en la plantilla de imagen; las aplicaciones que se instalaron en el disco Personal vDisk del usuario deberían asignarse como capas elásticas de aplicaciones; las aplicaciones que utilice un solo usuario y es poco probable que se compartan se instalan en la capa propia de ese usuario.

**Desde ELM:**

1. En la ficha **Imágenes**, haga clic en **Crear plantilla**.
2. Proporcione un nombre y una versión.
3. Seleccione la capa de SO que creó en la sección anterior.
4. Seleccione las capas de aplicaciones que quiera incluir en la plantilla de imagen. No seleccione las capas de aplicaciones que tiene la intención de asignar a usuarios y grupos de AD como capas elásticas de aplicaciones.
5. Seleccione una configuración de conector. Esto determina dónde se implementa la imagen compartida cuando se publica. Cree una configuración de conector la primera vez que use un nuevo destino de implementación.

Suponiendo que utiliza Citrix Hypervisor, dispone de tres tipos de implementación:

- Citrix Hypervisor: Al utilizar el conector de Citrix Hypervisor, ELM implementa la imagen compartida publicada como una VM en Citrix Hypervisor, donde, desde XenCenter, puede arrancarla. Lo habitual, sin embargo, es elegir una de las siguientes dos opciones: Citrix Provisioning o Machine Creation Services.
- Citrix Provisioning: La imagen compartida publicada se implementa como un disco vDisk en un servidor Citrix Provisioning. Al crear una configuración de conector de este tipo, debe especificar el nombre del servidor Citrix Provisioning. Credenciales de inicio de sesión para un usuario con permiso para administrar Citrix Provisioning. Para obtener información más detallada, consulte “Connector Configuration & Optional Script (Citrix Provisioning)” (Configurar conector y script opcional (Citrix Provisioning)) en la documentación en línea de App Layering.
- Citrix MCS para Citrix Hypervisor: La imagen compartida publicada se implementa como una VM en Citrix Hypervisor donde, mediante Citrix Virtual Desktops, puede usarla para crear un catálogo de máquinas.

Al crear este tipo de configuración de conector, debe especificar la dirección y las credenciales de Citrix Hypervisor (para que ELM pueda escribir en él) y el repositorio de almacenamiento de destino. Asimismo, especifique la plantilla de máquina virtual que creó en la sección anterior.

Además:

- Seleccione una capa de plataforma: la capa de plataforma MCS o Citrix Provisioning que creó en la sección anterior o, si está implementando en Citrix Hypervisor, omita esta opción.
- En el panel **Layered Image Disk**: Si aparece la opción “SysPrep”, seleccione “Not Generalized”.
- Para “Elastic Layering” (capa elástica), seleccione “Application and User Layers”. Esta configuración tiene dos efectos.
  - Permite asignar capas adicionales de aplicaciones adicionales a usuarios y grupos de AD, capas que se conectan dinámicamente cuando un usuario inicia sesión.

- Provoca la creación de una nueva capa del usuario la primera vez que inicia sesión. (En App Layering 4.1, esta opción solo está disponible si está habilitada explícitamente. Para habilitarla, vaya a ELM. A continuación, en System > Settings and Configuration > Labs, marque la casilla “User Layers”.)

Una capa de usuario captura el perfil del usuario, sus configuraciones, sus documentos, etc. Como se describe en la siguiente sección, este es el destino donde las herramientas de migración transfieren toda la información específica del usuario proveniente del disco Personal vDisk.

En el panel **Confirm and Complete**, haga clic en **Create Template**. Esto debería completarse casi de inmediato.

### **Publicar imagen compartida en capas**

El último paso para generar la imagen compartida en capas es seleccionar la **plantilla de imagen creada anteriormente** y hacer clic en **Publish Layered Image**.

Cuando esto finalice, la imagen en capas resultante se implementa como 1) para MCS, una VM en Citrix Hypervisor o 2) para Citrix Provisioning, un disco vDisk en el servidor Citrix Provisioning.

Ahora puede usar las herramientas de administración habituales de MCS o Citrix Provisioning para crear un grupo de entrega y un catálogo de máquinas de Citrix Virtual Desktops:

- Para MCS, utilice Studio para crear un catálogo de máquinas e importe la VM de la imagen compartida en capas.
- Para Citrix Provisioning, use el asistente Citrix Virtual Desktops Setup Wizard para crear un catálogo de máquinas en Studio.

En la siguiente sección, se describe el último paso para migrar la VM de Personal vDisk de un usuario a App Layering. Como vista previa del proceso: se ejecuta al mismo tiempo la máquina virtual original de PvD y la nueva máquina virtual de App Layering, se inicia sesión como usuario en la máquina virtual de App Layering y se ejecuta una herramienta de migración para transferir el perfil y la configuración del usuario desde PvD a la capa de usuario de App Layering.

### **Herramientas de migración**

Citrix recomienda que use una de las dos herramientas, PCmover o USMT, para migrar la información personal desde el disco Personal vDisk de un usuario a la capa de usuario de App Layering.

- PCmover es un programa que ofrece LapLink.com a la venta. Puede ejecutar la VM de PvD y la VM de App Layering de un usuario, y usar PCmover para transferir la configuración del usuario de la primera VM a la segunda. Ambas máquinas virtuales pueden ejecutarse al mismo tiempo

que la información que se transfiera a través de una red, o pueden ejecutarse consecutivamente, con la información transferida por archivo.

PCmover presenta una interfaz gráfica de usuario fácil de usar, con la que puede adaptar con precisión la información que se transfiere. Si tiene varias máquinas virtuales de PvD a migrar, puede usar PCmover Policy Manager para crear un Policy File (archivo de directiva). Al usar un archivo de directiva, puede realizar migraciones con interacciones mínimas.

Para obtener más información, consulte la [guía de usuario de PCmover](#).

- USMT es un conjunto de programas disponibles de Microsoft como parte del kit de instalación de automatización de Windows (AIK). Se ejecuta un programa Scanstate en la VM del disco Personal vDisk para escribir un archivo de transferencia. Se ejecuta LoadState en la VM de App Layering para leer y aplicar el archivo de transferencia. Varios archivos XML determinan los datos que se transfieren. Esos archivos se pueden modificar si los valores predeterminados no se ajustan a sus necesidades.

En este artículo, se presupone que ejecutará PCmover.

## Migrar la información del usuario

En este punto, ya debe haber utilizado su imagen PvD compartida original para crear una imagen compartida en capas de App Layering funcionalmente equivalente. Tiene una o varias máquinas virtuales PvD de usuarios, cada una con un disco Personal vDisk que contiene el perfil de usuario y otra información que quiere migrar a una capa de usuario de App Layering.

Debe iniciar la máquina virtual PvD de cada usuario, iniciar la imagen compartida en capas y, en ambas máquinas virtuales, iniciar sesión con las credenciales de dominio de cada usuario y ejecutar PCmover.

Para migrar la información del usuario:

1. Instale PCmover en un recurso compartido al que se pueda acceder desde la VM de PvD y la imagen compartida en capas.
2. Desde Studio, inicie la máquina virtual PvD del usuario. Inicie sesión como el usuario. Inhabilite los firewalls.
3. Desde ELM, asigne al usuario las capas elásticas de aplicaciones que requiera.
4. Compruebe que el usuario tiene acceso de escritura en el directorio donde se encuentra su capa de usuario. Consulte “Configure Security on User Layer Folders”(Configurar la seguridad de las carpetas en la capa de usuario) en la documentación en línea.
5. Desde Studio, inicie la VM de la imagen compartida en capas. Inicie sesión como el usuario. La primera vez que el usuario inicia sesión, la VM crea una capa de usuario en el recurso compartido de archivos de red. Inhabilite los firewalls, los antivirus y el antispyware.

6. Ejecute PCmover en la VM de PvD.
  - a) Seleccione “PC to PC Transfer”y “Next”.
  - b) Seleccione “Old”y “Next”.
  - c) Seleccione “Wifi or Wired Network”y “Next”.
  - d) PCmover tarda unos minutos en examinar la máquina virtual de PvD. Después de eso, seleccione “Next”.
  - e) Suponiendo que no quiere recibir ninguna notificación por correo electrónico cuando se complete la transferencia, simplemente seleccione “Next”.
  - f) Puede introducir una contraseña o no hacerlo. Una contraseña garantiza que la información del usuario se enviará desde la máquina virtual de PvD a la máquina virtual de la imagen compartida en capas, a ninguna otra máquina virtual. Luego, seleccione “Next”.
  
7. Ejecute PCmover en la VM de App Layering.
  - a) Seleccione “PC to PC Transfer”y “Next”.
  - b) Seleccione “New”y “Next”.
  - c) Introduzca los valores requeridos de validación del número de serie.
  - d) En “Network Name”, especifique el nombre de la VM de PvD y haga clic en “Next”.
  - e) Consulte el panel “Application Selections”. Se recomienda desmarcar todas las aplicaciones. Deben haberse creado capas de aplicaciones para todas las aplicaciones necesarias.
  - f) Consulte el panel “User Account Selections”. Se recomienda marcar con “Do not transfer this user”a todos los usuarios que no sean el propietario del disco Personal vDisk.
  - g) Consulte el panel “Custom Settings”. Se recomienda seleccionar “Files and Settings Only”.
  - h) Consulte el panel “Drive Selections”. Se recomienda marcar con “Do not transfer this drive”a todas las unidades que no sean “C:”.
  - i) Después de consultar todos los paneles, haga clic en “Next”.
  - j) Suponiendo que no quiere recibir ninguna notificación por correo electrónico cuando se complete la transferencia, simplemente seleccione “Next”.

En este punto, PCmover comienza a transferir archivos y configuraciones desde la máquina virtual de PvD a la capa del usuario de App Layering.

### **Usar PCmover para determinar las aplicaciones necesarias**

Puede usar PCmover para analizar una VM de PvD y determinar las aplicaciones instaladas. Esto proporciona una alternativa a “Programas y características”del **Panel de control**.

1. Ejecute PCmover en la VM de PvD.
2. Seleccione “PC to PC Transfer”y “Next”.

3. Seleccione “Old”y “Next”.
4. Seleccione “File Storage Device”y “Next”.
5. Consulte el panel “Application Selections”y tome nota de las aplicaciones instaladas.
6. Cancele PCmover.

## Eliminar componentes

September 22, 2021

Para quitar componentes, Citrix recomienda usar la función de Windows para quitar o cambiar programas. También puede quitar componentes mediante la línea de comandos, o un script incluido en los medios de instalación.

Cuando se quitan componentes, no se eliminan sus requisitos previos ni se cambian los parámetros del firewall. Por ejemplo, al quitar un Delivery Controller, el software y las bases de datos de SQL Server no se eliminan.

Si ha actualizado un Controller a partir de una implementación anterior que incluía la Interfaz Web, debe quitar el componente de la Interfaz Web por separado. No puede usar el instalador para eliminar la Interfaz Web.

Para obtener información sobre cómo eliminar funciones que no se mencionan a continuación, consulte la documentación de la función en sí.

### Preparar

Antes de eliminar un Controller, quítelo del sitio. Para obtener más detalles, consulte [Quitar un Controller](#).

Cierre Studio y Director antes de eliminarlo.

### Eliminar componentes con la función de Windows para quitar o cambiar programas

Con la función de Windows para quitar o cambiar programas:

- Para quitar un Controller, Studio, Director, un servidor de licencias o StoreFront, haga clic con el botón secundario en **Citrix Virtual Apps versión** o **Citrix Virtual Desktops versión**. A continuación, seleccione **Desinstalar**. Se inicia el instalador. Seleccione los componentes que se eliminarán.

También puede quitar StoreFront si hace clic con el botón secundario en **Citrix StoreFront** y selecciona **Desinstalar**.

- Para quitar un VDA, haga clic con el botón secundario en **Citrix Virtual Delivery Agent versión** y seleccione **Desinstalar**. Se inicia el instalador y puede seleccionar los componentes que quiere quitar. De forma predeterminada, la máquina se reinicia automáticamente después de la eliminación.
- Para quitar Universal Print Server, haga clic con el botón secundario en **Citrix Universal Print Server** y seleccione **Desinstalar**.

## Eliminar componentes principales mediante la línea de comandos

Desde el directorio `\x64\XenDesktop Setup` en los medios de instalación, ejecute el comando `XenDesktopServerSetup.exe`.

- Para quitar uno o varios componentes, use las opciones `/remove` y `/components`.
- Para quitar todos los componentes, use la opción `/removeall`.

Para obtener información detallada acerca de parámetros y comandos, consulte [Instalación desde la línea de comandos](#).

Por ejemplo, el siguiente comando elimina Studio.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components studio
```

## Eliminar VDA mediante la línea de comandos

Desde el directorio `\x64\XenDesktop Setup` en los medios de instalación, ejecute el comando `XenDesktopVdaSetup.exe`.

- Para quitar uno o más componentes, use las opciones `/remove` y `/components`.
- Para quitar todos los componentes, use la opción `/removeall`.

Para obtener información detallada acerca de parámetros y comandos, consulte [Instalar usando la línea de comandos](#).

De forma predeterminada, la máquina se reinicia automáticamente después de la eliminación.

Por ejemplo, el siguiente comando quita el VDA y la aplicación Citrix Workspace.

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /removeall
```

Para quitar agentes VDA mediante un script en Active Directory, consulte [Instalar o quitar agentes VDA mediante scripts](#).

## Actualización y migración

April 19, 2024

### Acerca de las actualizaciones

Las actualizaciones cambian la implementación de la versión [Long Term Service Release \(LTSR\)](#) de Citrix Virtual Apps and Desktops 7 1912, sin necesidad de instalar nuevas máquinas o nuevos sitios. Este proceso se conoce como “actualización en contexto”.

Actualizar le permite acceder a funciones y tecnologías más recientes que están a su disposición. Las actualizaciones pueden contener correcciones, aclaraciones y mejoras de versiones anteriores.

### Versiones que puede actualizar

Puede actualizar a LTSR desde:

- XenApp y XenDesktop 7.6 LTSR, con o sin actualizaciones acumulativas, hasta la CU9 incluida (solo para las plataformas mencionadas en [Requisitos del sistema](#))
- XenApp y XenDesktop 7.15 LTSR con o sin CU, hasta CU7 incluida
- XenApp y XenDesktop 7.16
- XenApp y XenDesktop 7.17
- XenApp y XenDesktop 7.18
- Citrix Virtual Apps and Desktops 7 1808
- Citrix Virtual Apps and Desktops 7 1811
- Citrix Virtual Apps and Desktops 7 1903
- Citrix Virtual Apps and Desktops 7 1906
- Citrix Virtual Apps and Desktops 7 1909

### Aviso importante sobre la actualización de los agentes VDA

Si el componente Personal vDisk (PvD) se ha instalado alguna vez en un VDA, dicho VDA no se puede actualizar a la versión 1912 LTSR ni a ninguna posterior. Para utilizar el nuevo VDA, debe desinstalar el VDA actual y, a continuación, instalar el nuevo

Este paso debe seguirse aunque nunca haya usado PvD.

## Averigüe si le afecta

Cómo podría haberse instalado PvD en versiones anteriores:

- En la interfaz gráfica del instalador de VDA, PvD era una opción en la página **Componentes adicionales**. La versión 7.15 LTSR y las 7.x anteriores habilitaban esta opción de forma predeterminada. Por lo tanto, si aceptó los valores predeterminados (o habilitó explícitamente la opción en cualquier versión), PvD se ha instalado.
- En la línea de comandos, la opción `/baseimage` instaló PvD. Si especificó esta opción o utilizó un script que contenía esta opción, PvD se ha instalado.

Si no sabe si el VDA tiene PvD instalado, ejecute el instalador del nuevo VDA (1912 LTSR o una versión posterior) en la máquina o en la imagen.

- Si PvD está instalado, aparece un mensaje que indica que hay un componente incompatible.
  - Para la interfaz gráfica, haga clic en **Cancelar** en la página que contiene el mensaje y, a continuación, confirme que quiere cerrar el instalador.
  - Desde la CLI, el comando simplemente falla con el mensaje indicado.
- Si PvD no está instalado, la actualización continúa.

## Qué se debe hacer

Si el VDA no tiene PvD instalado, siga el procedimiento de actualización habitual.

Si el VDA tiene PvD instalado:

1. Desinstale el VDA actual. Para obtener más información, consulte [Eliminación de componentes](#).
2. Instale el nuevo VDA.

Si quiere seguir utilizando PvD, solo puede hacerlo en VDA 7.15 LTSR a través de las versiones para Win 7 y Win 10 (1607 o una anterior).

## Cómo actualizar

Revise la documentación antes de comenzar la actualización.

Para actualizar los componentes principales y los agentes VDA:

1. Ejecute el instalador en las máquinas donde están instalados los componentes. El software determina si hay una actualización disponible e instala la versión más reciente.
2. Use el recién actualizado Studio para actualizar la base de datos y el sitio.

**Preparación y orientación para actualizaciones:** el artículo [Actualizar una implementación](#) es la fuente de información principal para los componentes principales y los agentes VDA. En ese artículo se describe la secuencia y el orden de actualización, las limitaciones, los pasos de preparación y otras consideraciones. También proporciona el procedimiento de actualización paso a paso e instrucciones para actualizar las bases de datos y el sitio después de actualizar los componentes principales.

**Detalles de la instalación:** Después de completar cualquier trabajo de preparación y estar listo para iniciar el instalador, el artículo de instalación muestra lo que verá (si está utilizando la interfaz gráfica) o lo que tendrá que escribir (si está utilizando la interfaz de línea de comandos) para actualizar los componentes. Cuando finalice el programa de instalación, vuelva a la guía de [Actualizar una implementación](#) para actualizaciones de bases de datos y sitios.

- [Instalar/actualizar componentes principales mediante la interfaz gráfica](#)
- [Instalar/actualizar componentes principales mediante la línea de comandos](#)
- [Instalar/actualizar los agentes VDA mediante la interfaz gráfica](#)
- [Instalar/actualizar los agentes VDA mediante la línea de comandos](#)

Para obtener información acerca de la instalación de revisiones hotfix de Controller, consulte [CTX201988](#).

## Actualizar licencias

Para obtener una visión completa de la administración de Citrix Licensing, consulte [Activar, actualizar y administrar licencias de Citrix](#).

Para una implementación local, puede usar el instalador de producto completo para actualizar el servidor de licencias. O bien, puede descargar y actualizar los componentes de la licencia por separado. Consulte [Actualizar](#).

## Actualizar otros componentes

Además de los componentes principales y los agentes VDA, las implementaciones locales de Citrix Virtual Apps and Desktops incluyen los siguientes componentes que puede actualizar cuando se publican nuevas versiones.

- [StoreFront](#)
- [AppDNA](#)
- [Citrix App Layering](#)
- [HDX RealTime Optimization Pack](#)
- [Profile Management](#)
- [Citrix Provisioning](#)
- [Grabación de sesiones](#)

- [Workspace Environment Management](#)

## Preguntas frecuentes

Esta sección responde a algunas preguntas frecuentes sobre la actualización de versión de Citrix Virtual Apps and Desktops.

- **¿Cuál es el orden correcto para actualizar la versión de mi entorno de Virtual Apps and Desktops?**

VDA se puede actualizar en cualquier momento y en cualquier orden. Actualice la mitad de los Controllers antes de actualizar su sitio. A continuación, actualice los Controllers restantes después de la actualización del sitio. Para obtener más información, consulte [Secuencia de actualización](#) y [Procedimiento de actualización](#).

- **Mi sitio tiene varios Delivery Controllers (en diferentes zonas). ¿Qué sucede si actualizo solo algunos de ellos? ¿Debo actualizar todos los Controllers del sitio durante el mismo período de mantenimiento?**

Se recomienda actualizar todos los Delivery Controllers durante el mismo período de mantenimiento, ya que varios servicios de cada Controller se comunican entre sí. Mantener versiones diferentes puede causar problemas. Durante un período de mantenimiento, se recomienda actualizar la mitad de los Controllers, actualizar el sitio y, a continuación, actualizar los Controllers restantes. (Para obtener más información, consulte el [procedimiento de actualización](#).)

- **¿Puedo ir directamente a la versión más reciente o tengo que hacer actualizaciones incrementales?**

Casi siempre puede actualizar la versión a la más reciente y omitir las versiones intermedias, a menos que se indique explícitamente en el artículo **Novedades** de la versión a la que se va a actualizar. Consulte la [Guía sobre la actualización de versiones](#).

- **¿Un cliente puede actualizar la versión de un entorno Long Term Service Release (LTSR) a Current Release?**

Sí. Los clientes no están obligados a permanecer en una versión Long Term Service Release durante un período prolongado. Pueden mover un entorno LTSR a una versión Current Release en función de los requisitos y las funciones del negocio.

- **¿Se permiten versiones mixtas de componentes?**

En cada sitio, Citrix recomienda actualizar todos los componentes a la misma versión. Aunque se pueden usar las versiones anteriores de algunos componentes, es posible que no estén disponibles todas las funciones de la versión más reciente. Para obtener más información, consulte [Consideraciones sobre entornos mixtos](#).

- **¿Con qué frecuencia se debe actualizar una versión Current Release?**

Las versiones Current Release llegan al fin de mantenimiento (EOM) 6 meses después de su publicación. Citrix recomienda a los clientes que adopten la versión Current Release más reciente. Las versiones Current Release llegan al fin de su vida (EOL) 18 meses después de publicarse. Para obtener más información, consulte [Ciclo de vida de las versiones Current Release](#).

- **¿Qué se recomienda: actualizar versiones a LTSR o a CR?**

Las versiones Current Release (CR) ofrecen las funciones más recientes e innovadoras sobre virtualización de aplicaciones, escritorios y servidores. Esto le permite seguir mediante la tecnología de vanguardia y mantenerse por delante de la competencia.

Las versiones Long Term Service Releases (LTSR) son ideales para entornos de producción de grandes empresas que prefieren conservar la misma versión base durante un período prolongado.

Para obtener información más detallada, consulte [Opciones de servicio](#).

- **¿Necesito actualizar mis licencias?**

Debe asegurarse de que la fecha de su licencia actual no haya caducado y que dicha licencia sea válida para la versión a la que va a actualizarse. Véase [CTX111618](#). Para obtener información sobre la renovación, consulte [Licencias de renovación de Customer Success Services](#).

- **¿Cuánto tiempo tarda una actualización?**

El tiempo necesario para actualizar la versión de una implementación varía según la infraestructura y la red. Por lo tanto, no podemos garantizar un tiempo exacto.

- **¿Cuáles son las prácticas recomendadas?**

Asegúrese de que entiende y sigue la [guía de preparación](#).

- **¿Qué sistemas operativos son compatibles?**

Consulte [Requisitos del sistema](#).

Si tiene un sistema operativo anterior que no es válido para la versión a la que está actualizando, consulte [Lo que puede hacer](#).

- **¿Qué versiones de VMware vSphere (vCenter + ESXi) son compatibles?**

[Recursos de hosts/virtualización](#) indica las versiones admitidas para todos los hosts compatibles, incluido VMware.

- **¿Cuándo se termina la vida de mi versión?**

Compruebe la [Tabla de productos](#).

- **¿Cuáles son los problemas conocidos de la última versión?**

- [Citrix Virtual Apps and Desktops](#)
- [StoreFront](#)
- [Citrix Provisioning](#)
- [Citrix License Server](#)
- [Aplicación Citrix Workspace](#)

## Migrar

La migración mueve los datos de una implementación a una versión más reciente. La migración incluye la instalación de nuevos componentes y la creación de un sitio, la exportación de datos desde la comunidad de servidores original y la importación de esos datos en el sitio nuevo.

- Para obtener información sobre los cambios de arquitectura, componentes y características que se han introducido en las versiones 7.x, consulte [Cambios en 7.x](#).
- Para obtener información sobre la migración desde XenApp 6.x, consulte [Migrar XenApp 6.x](#).

## Más información

Las actualizaciones de implementación de [Long Term Service Release \(LTSR\)](#) utilizan actualizaciones acumulativas (CUs). Una CU actualiza los componentes base de la LTSR, y cada CU incluye su propio metainstalador.

Cada actualización acumulativa (CU) tiene su propia documentación dedicada. Por ejemplo, para la versión 7.15 LTSR, consulte el enlace en la página [Novedades](#) de esa LTSR para la última CU. Cada página de CU incluye información de versión admitida, instrucciones y un enlace al paquete de descarga de CU.

## Cambios en 7.x

September 22, 2021

La arquitectura, la terminología y las funciones de Citrix Virtual Apps and Desktops han cambiado a partir de las versiones de XenApp y XenDesktop 7.x. Si solo conoce las versiones anteriores (a 7.x), en este artículo se le explicarán los cambios.

Una vez haya cambiado a la versión 7.x, los cambios en las versiones posteriores se indican en [Novedades](#).

A menos que se indique específicamente, 7.x y “versiones posteriores” hacen referencia a XenApp 7.5 o posterior y XenDesktop 7 o posterior, incluidas todas las versiones de Citrix Virtual Apps and Desktops.

En este artículo, se ofrece una descripción general. Para obtener información detallada sobre cómo cambiar desde versiones anteriores a 7.x a la versión más reciente, consulte [Actualizar a XenApp 7](#).

## Diferencias de elementos entre XenApp 6 y versiones posteriores

Aunque no son equivalentes exactos, la siguiente tabla ayuda a establecer una correspondencia entre los elementos funcionales de XenApp 6.5 y sus versiones anteriores con versiones posteriores. A continuación, dispone de descripciones de las diferencias que existen entre cada arquitectura.

### En lugar de esto en XenApp 6.x y versiones anteriores

### Piense en esto en versiones más recientes

Arquitectura IMA (Independent Management Architecture)	Arquitectura FMA (FlexCast Management Architecture)
Comunidad	Sitio
Grupo de trabajo	Catálogo de máquinas, grupo de entrega
Worker	Virtual Delivery Agent (VDA), máquina con SO multisesión, VDA con SO multisesión, máquina con SO de sesión única, VDA con SO de sesión única
Máquina de Servicios de Escritorio remoto (RDS) o Terminal Services	Máquina con SO multisesión, VDA con SO multisesión
Recopilador de datos y zonas	Delivery Controller
Delivery Services Console	Citrix Studio y Citrix Director
Publicación de aplicaciones	Entrega de aplicaciones
Almacén de datos	Base de datos
Patrón de carga	Directiva de administración de carga
Administrador	Administrador delegado, rol, ámbito

## Diferencias de arquitecturas

A partir de las versiones 7.x, Citrix Virtual Apps and Desktops (antes XenApp y XenDesktop) se basan en la arquitectura FMA (FlexCast Management Architecture). FMA es una arquitectura orientada a servicios que permite la interoperabilidad y administración modular de las diversas tecnologías de Citrix. FMA ofrece una plataforma para la entrega de aplicaciones, movilidad, servicios, aprovisionamiento flexible y administración en la nube.

FMA sustituye a la arquitectura IMA (Independent Management Architecture) de XenApp 6.5 y versiones anteriores.

Estos son los elementos clave de FMA en términos de cómo se relacionan con los elementos de XenApp 6.5 y versiones anteriores:

- **Sitios de entrega:** Las comunidades eran los objetos de nivel superior en XenApp 6.5 y versiones anteriores. En versiones posteriores, el sitio es el elemento de nivel más alto. Los sitios ofrecen aplicaciones y escritorios a grupos de usuarios. FMA requiere que usted se encuentre en un dominio para implementar un sitio. Por ejemplo, para instalar los servidores, su cuenta debe tener privilegios de administrador local y ser un usuario de dominio de Active Directory.
- **Catálogos de máquinas y grupos de entrega:** Las máquinas que alojaban aplicaciones en XenApp 6.5 y versiones anteriores pertenecían a grupos de trabajo para una administración eficaz de las aplicaciones y del software de servidor. Los administradores podían administrar todas las máquinas de un grupo de trabajo como una sola unidad con el objetivo de mejorar la administración de la aplicación y el equilibrio de carga. Las carpetas se utilizaban para organizar aplicaciones y máquinas. En las versiones posteriores, se utiliza una combinación de catálogos de máquinas, grupos de entrega y grupos de aplicaciones para administrar las máquinas, el equilibrio de carga, así como las aplicaciones y los escritorios alojados. También se pueden usar carpetas de aplicaciones.
- **VDA:** En XenApp 6.5 y versiones anteriores, las máquinas de trabajo (trabajadores) de los grupos de trabajo ejecutaban aplicaciones para el usuario y se comunicaban con los recopiladores de datos. En las versiones posteriores, el VDA se comunica con los Delivery Controllers que administran las conexiones de usuario.
- **Delivery Controllers.** En XenApp 6.5 y versiones anteriores, había un maestro de zona que se encargaba de las solicitudes de conexión de los usuarios y de la comunicación con los hipervisores. En las versiones posteriores, los Controllers del sitio se encargan de distribuir y gestionar las solicitudes de conexión. En XenApp 6.5 y las versiones anteriores, las zonas ofrecían una manera de agregar servidores y replicar datos a través de conexiones WAN. Aunque las zonas no tienen equivalente exacto en las versiones posteriores, la función de zonas y preferencia de zonas permiten a los usuarios de regiones remotas a conectarse a recursos sin que las conexiones recorran necesariamente grandes segmentos de red WAN.
- **Studio y Director.** Use la consola de Studio para configurar los entornos y ofrecer a los usuarios acceso a aplicaciones y escritorios. Studio reemplaza Delivery Services Console en XenApp 6.5 y versiones anteriores. Los administradores usan Director para supervisar el entorno, remedar dispositivos de usuario y solucionar problemas de TI. Para remedar usuarios, la Asistencia remota de Windows debe estar habilitada; se habilita de forma predeterminada cuando se instala el VDA.
- **Entrega de aplicaciones.** En XenApp 6.5 y versiones anteriores, se utilizaba el asistente Publicar aplicación para preparar aplicaciones y entregarlas a los usuarios. En las versiones posteriores, se utiliza Studio para crear aplicaciones, agregarlas y ponerlas a disposición de los

usuarios que formen parte de grupos de entrega y, opcionalmente, de grupos de aplicaciones. Mediante Studio, primero debe configurar un sitio, crear y especificar los catálogos de máquinas y, a continuación, crear grupos de entrega en dichos catálogos. Los grupos de entrega determinan qué usuarios tienen acceso a las aplicaciones que usted entrega. Si quiere, puede optar por crear grupos de aplicaciones como alternativa a varios grupos de entrega.

- **Base de datos:** En las versiones posteriores no se usa el almacén de datos IMA para la información de configuración. En su lugar, utilizan una base de datos de Microsoft SQL Server para almacenar información de configuración y de sesión.
- **Directiva de administración de carga:** En XenApp 6.5 y versiones anteriores, los patrones de carga utilizaban métricas predeterminadas para determinar la carga de una máquina. Las conexiones de usuarios se podían asociar a máquinas con menos carga. En las versiones posteriores, se utilizan directivas de administración de carga para equilibrar la carga entre las máquinas.
- **Administración delegada.** En XenApp 6.5 y versiones anteriores, se creaban administradores personalizados y se les asignaban permisos basados en carpetas y objetos. En las versiones posteriores, los administradores personalizados se crean en función de pares de ámbito y rol. Un rol representa una función de trabajo y tiene asociados permisos definidos para él con el objetivo de permitir la delegación. Un ámbito representa un conjunto de objetos. Los roles predefinidos de administrador disponen de conjuntos específicos de permisos, como el servicio de asistencia técnica, las aplicaciones, el alojamiento y el catálogo. Por ejemplo, los administradores del servicio de asistencia pueden trabajar únicamente con usuarios individuales en sitios especificados, mientras que los administradores totales pueden supervisar toda la implementación y resolver problemas de TI de todo el sistema.

## Comparación de funciones

La transición a FMA también implica que algunas funciones que estaban disponibles en XenApp 6.5 y versiones anteriores ahora se implementan de otra forma, o que haya que usar funciones, componentes o herramientas distintas para conseguir los mismos objetivos.

En lugar de esto en XenApp 6.5 y versiones anteriores	Use esto en versiones posteriores
Preinicio de sesiones y persistencia de sesiones configurados por directivas	Preinicio de sesiones y persistencia de sesiones configurados mediante los parámetros del grupo de entrega. Al igual que en XenApp 6.5, estas funciones ayudan a que los usuarios se conecten rápidamente con las aplicaciones, iniciando sesiones antes de que se soliciten (preinicio de sesiones) y manteniendo las sesiones activas después de que el usuario cierra todas las aplicaciones (persistencia de sesiones). En las versiones posteriores, estas funciones se habilitan para usuarios especificados configurando estos parámetros en los grupos de entrega existentes. Consulte <a href="#">Configurar el preinicio y la persistencia de sesiones</a> .
Funcionalidad para usuarios no autenticados (anónimos) mediante la concesión de derechos a usuarios anónimos al configurar las propiedades de las aplicaciones publicadas	La funcionalidad para usuarios no autenticados (anónimos) se ofrece al configurar esta opción cuando establezca las propiedades de los usuarios de un grupo de entrega. Consulte <a href="#">Usuarios</a> .
El caché de host local permite que los servidores de trabajo funcionen incluso aunque pierdan la conexión con el almacén de datos	La Caché de host local permite que la intermediación de operaciones continúe cuando se interrumpa la conexión entre un Controller y la base de datos del sitio. Esta implementación es más sólida y requiere menos mantenimiento. Consulte <a href="#">Caché de host local</a> .
Distribución de aplicaciones por streaming	App-V de Citrix ofrece aplicaciones distribuidas por streaming que se administran mediante Studio. Consulte <a href="#">App-V</a> .
Interfaz Web	Citrix recomienda realizar la transición a StoreFront.
SmartAuditor para grabar la actividad en pantalla de la sesión de un usuario	A partir de 7.6 Feature Pack 1, esta función se ofrece con la grabación de sesiones. También puede usar el Registro de configuración para registrar todas las actividades de sesión desde una perspectiva administrativa.

En lugar de esto en XenApp 6.5 y versiones anteriores	Use esto en versiones posteriores
La función “Administración de energía y capacidad” ayuda a reducir el consumo de energía y administrar la capacidad del servidor	Use el Administrador de configuración de Microsoft.

## Cambios y funciones admitidas

Las siguientes funciones no se ofrecen, ya no se admiten o han cambiado significativamente en Citrix Virtual Apps and Desktops, a partir de XenApp o XenDesktop 7.x.

**Cifrado Secure ICA por debajo de 128 bits:** En versiones anteriores a 7.x, Secure ICA podía cifrar conexiones de cliente para el cifrado básico de 40, 56 y 128 bits. Con las versiones 7.x, el cifrado Secure ICA solo está disponible para el cifrado de 128 bits.

**Impresión antigua:** Las funciones de impresión siguientes ya no se admiten en las versiones 7.x:

- Compatibilidad con versiones anteriores de los clientes de DOS e impresoras de 16 bits.
- Compatibilidad para impresoras conectadas a los sistemas operativos de Windows 95 y Windows NT, incluidas las propiedades de impresora extendidas y mejoradas y Win32FavorRetainedSetting.
- Capacidad para habilitar o inhabilitar impresoras conservadas y restauradas automáticamente.
- DefaultPrnFlag, un parámetro de Registro para servidores que se utiliza para habilitar o inhabilitar impresoras conservadas y restauradas automáticamente, almacenadas en perfiles de usuario del servidor.

Se admiten los nombres de las impresoras del cliente heredadas.

**Secure Gateway:** En versiones anteriores a 7.x, Secure Gateway era una opción para ofrecer conexiones seguras entre el servidor y los dispositivos de usuario. Citrix Gateway es la nueva opción para proteger las conexiones externas.

**Remedo de usuarios:** En versiones anteriores a 7.x, los administradores establecían directivas para controlar el remedo de usuario a usuario. En las versiones 7.x, el remedo de usuarios finales es una función integrada en el componente Director, que utiliza la Asistencia remota de Microsoft para permitir a los administradores remedar y solucionar problemas en la entrega de aplicaciones y escritorios virtuales.

**Redirección de Flash 1:** Los clientes que no admiten la redirección de Flash de segunda generación (incluido Citrix Receiver para Windows anterior a la versión 3.0, Citrix Receiver para Linux anterior a la versión 11.100 y Citrix Online Plug-in 12.1) utilizarán la generación en el lado del servidor para las funciones de redirección de Flash antiguas. Los VDA que se incluyen en las versiones 7.x admiten las funciones de redirección de Flash de segunda generación.

**Repetición local del texto.** Esta funcionalidad se usaba con tecnologías de aplicaciones Windows anteriores para acelerar la presentación del texto introducido en los dispositivos de usuario en conexiones de alta latencia. Ya no se incluye en las versiones 7.x porque se han hecho mejoras en el subsistema de gráficos y el HDX SuperCodec.

**Single Sign-On.** Esta funcionalidad, que ofrece la seguridad de contraseñas, no se admiten en Windows 8, Windows Server 2012 ni en las nuevas versiones de los sistemas operativos Windows compatibles. Sigue siendo compatible en entornos de Windows 2008 R2 y Windows 7, pero no está incluida en las versiones 7.x. Se encuentra en el sitio web de descargas de Citrix: <https://citrix.com/downloads>.

**Compatibilidad con bases de datos de Oracle.** Las versiones 7.x requieren bases de datos SQL Server.

**Supervisión del estado y recuperación (HMR).** En versiones anteriores a 7.x, la supervisión del estado y la recuperación podía ejecutar pruebas en los servidores de una comunidad de servidores para supervisar su estado y detectar cualquier riesgo de funcionamiento. En las versiones 7.x, Director ofrece una vista centralizada del estado del sistema al presentar la supervisión y las alertas para toda la infraestructura en la misma consola de Director.

**Archivos ICA personalizados:** Los archivos ICA personalizados se utilizaban para permitir la conexión directa desde dispositivos de usuario (con el archivo ICA) a una máquina concreta. En las versiones 7.x, esta función está inhabilitada de forma predeterminada, pero puede habilitarse para su uso normal mediante un grupo local, o se puede usar en el modo de alta disponibilidad si el Controller deja de estar disponible.

**Módulo de administración para System Center Operations Manager (SCOM) 2007.** El módulo de administración, que supervisaba la actividad de comunidades de XenApp mediante SCOM, no se admite en versiones 7.x. Consulte el artículo actualizado [Módulo de administración SCOM de Citrix para XenApp y XenDesktop](#).

**Función CNAME.** La función CNAME estaba habilitada de forma predeterminada en las versiones anteriores a 7.x. Las implementaciones en función de los registros CNAME para el reenrutamiento de FQDN y el uso de nombres NetBIOS podrían fallar. En las versiones 7.x, la actualización automática del Delivery Controller actualiza dinámicamente la lista de Controllers y notifica a los VDA automáticamente cuando se agregan y se quitan Controllers en el sitio. La funcionalidad de actualización automática de Controllers está habilitada de forma predeterminada en las directivas de Citrix, pero puede inhabilitarse. De forma alternativa, puede volver a habilitar la función CNAME en el Registro para continuar con la implementación existente y permitir el reenrutamiento de FQDN y el uso de nombres NetBIOS. Para obtener más información, consulte [CTX137960](#).

**Asistente de Implementación rápida.** En versiones de XenDesktop anteriores a 7.x, esta opción de Studio permitía una instalación rápida de una implementación completa de XenDesktop. La nueva y simplificada secuencia de instalación y configuración de las versiones posteriores elimina la necesidad de utilizar el asistente de Implementación rápida.

**Archivo de configuración de servicio de Remote PC y script de PowerShell para la administración automática:** Ahora, el acceso con Remote PC está integrado en Studio y en el Controller.

**Workflow Studio:** En versiones anteriores a 7.x, Workflow Studio era la interfaz gráfica de la composición de flujos de trabajo para XenDesktop. Esta función no se ofrece en las versiones posteriores.

**Inicio de programas no publicados durante la conexión del cliente:** En versiones anteriores a 7.x, esta configuración de directiva de Citrix especificaba si ejecutar aplicaciones de inicio o aplicaciones publicadas mediante ICA o RDP en el servidor. En versiones 7.x, esta configuración solo especifica si ejecutar las aplicaciones de inicio o las aplicaciones publicadas mediante RDP en el servidor.

**Inicios de escritorio:** En versiones anteriores a 7.x, esta configuración de directiva de Citrix especificaba si los usuarios no administrativos podían conectarse a sesiones de escritorio. En las versiones 7.x, los usuarios no administrativos deben formar parte del grupo de usuarios con acceso directo en una máquina de VDA para poder conectarse a las sesiones en ese VDA. El parámetro Inicios de escritorio permite a usuarios no administrativos que formen parte del grupo de usuarios con acceso directo en un VDA conectarse al VDA mediante una conexión ICA. El parámetro Inicios de escritorio no afecta a las conexiones RDP, por lo que los usuarios que estén en el grupo de usuarios con acceso directo en un VDA se pueden conectar al VDA mediante una conexión RDP tanto si esta configuración está habilitada o no.

**Profundidad de color:** En versiones de Studio anteriores a 7.6, se especificaba la profundidad de color en la configuración de usuarios de un grupo de entrega. A partir de la versión 7.6, la profundidad de color para el grupo de entrega se puede configurar mediante los cmdlets de PowerShell Set-BrokerDesktopGroup o New-BrokerDesktopGroup.

**Iniciar escritorio con optimización táctil:** Este parámetro se ha inhabilitado y no está disponible para máquinas Windows 10 y Windows Server 2016. Para obtener más información, consulte [Configuración de directiva de Experiencia móvil](#).

## **Funciones no incluidas en la aplicación Citrix Workspace o que tienen diferentes valores predeterminados**

Se han dado los siguientes cambios en la aplicación Citrix Workspace (anteriormente Citrix Receiver):

- **Asignación de puertos COM:** La asignación de puertos COM permitía o impedía el acceso a los puertos COM en el dispositivo del usuario. La asignación de puertos COM estaba habilitada de forma predeterminada. En las versiones 7.x, la asignación de puertos COM está inhabilitada de forma predeterminada. Para obtener más información, consulte [Configuración de la redirección de puertos COM y puertos LPT mediante el Registro](#).
- **Asignación de puertos LPT:** La asignación de puertos LPT controla el acceso de aplicaciones antiguas a los puertos LPT. La asignación de puertos LPT estaba habilitada de forma predeter-

minada. En las versiones 7.x, la asignación de puertos LPT está inhabilitada de forma predeterminada.

- **Códec de audio PCM:** En las versiones 7.x, solo los clientes HTML5 admiten el códec de audio PCM.
- **Compatibilidad con Microsoft ActiveSync.**
- **Compatibilidad con proxy para versiones anteriores:** Incluye:
  - Microsoft Internet Security and Acceleration (ISA) 2006 (Windows Server 2003)
  - Servidor proxy Oracle iPlanet 4.0.14 (Windows Server 2003)
  - Servidor proxy Squid 3.1.14 (Ubuntu Linux Server 11.10)

Para obtener más información, consulte la documentación de la aplicación Citrix Workspace correspondiente a su versión.

## Actualizar la versión de una implementación

June 27, 2024

### Introducción

Puede actualizar algunas implementaciones a versiones más recientes sin tener que configurar antes nuevas máquinas o sitios. Esto se conoce como “actualización en contexto”. Para saber qué versiones de Citrix Virtual Apps and Desktops puede actualizar, consulte [Citrix Upgrade Guide](#).

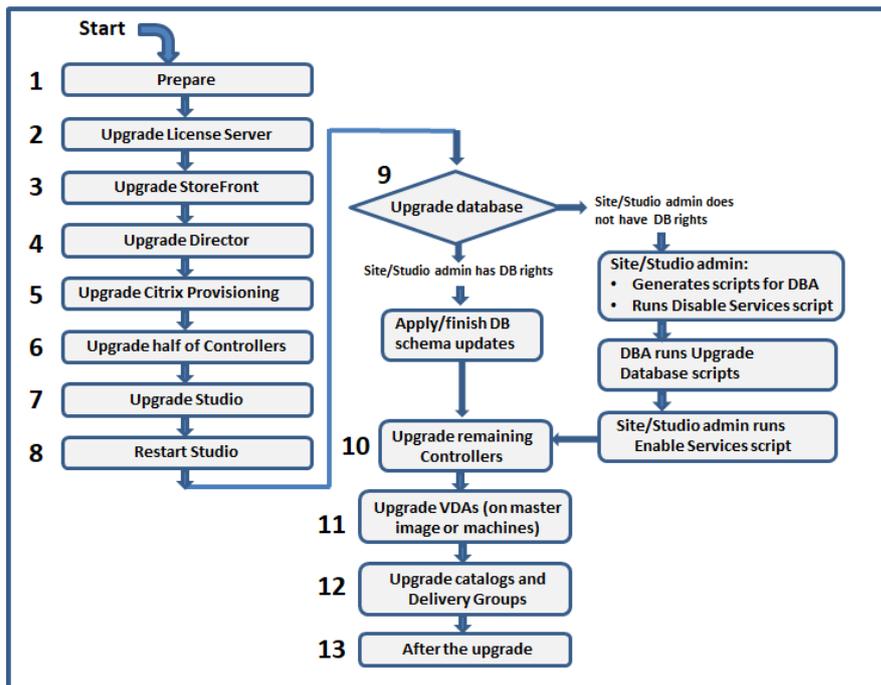
Para iniciar una actualización, ejecute el instalador desde la nueva versión para actualizar los componentes principales, los VDA y otros componentes previamente instalados. A continuación, actualice las bases de datos y el sitio.

Con el instalador de producto completo (y los instaladores independientes de VDA), puede actualizar cualquier componente que se pueda instalar, si hay disponible una versión más reciente de este. Para conocer los componentes que no se instalan con el instalador de producto completo (como Citrix Provisioning y Profile Management), consulte la documentación de esos componentes para obtener información. Para actualizaciones de host, consulte la documentación apropiada.

Consulte toda la información contenida en este artículo antes de comenzar una actualización.

### Secuencia de actualización

El diagrama siguiente muestra los pasos de la secuencia de actualización. El procedimiento de actualización contiene información detallada de cada paso del diagrama.



**Nota:**

Para evitar errores, debe actualizar todos los Delivery Controllers y la base de datos antes de realizar cualquier tarea relacionada con el aprovisionamiento y los grupos de entrega, como crear un nuevo catálogo de máquinas, eliminar un catálogo de máquinas, actualizar una máquina de un grupo de entrega, etc.

**Procedimiento de actualización**

La mayoría de los componentes principales del producto se pueden actualizar ejecutando el instalador del producto en la máquina que contiene el componente.

Si una máquina contiene varios componentes (por ejemplo, Studio y License Server) y el medio de instalación contiene versiones más recientes de su software, se actualizarán todos los componentes de esa máquina.

Para utilizar los instaladores:

- Para ejecutar la interfaz gráfica del instalador de producto completo, inicie sesión en la máquina y, a continuación, inserte el medio de instalación o monte la unidad con la imagen ISO de la nueva versión. Haga doble clic en **AutoSelect**.
- Para usar la interfaz de línea de comandos, emita el comando apropiado. Consulte [Instalación desde la línea de comandos](#).

### **Paso 1: Prepare todo**

Antes de comenzar una actualización, asegúrese de que está preparado. Lea y complete las tareas necesarias:

- Actualizar los VDA a la versión 1912 o una posterior
- Limitaciones
- Consideraciones sobre entornos mixtos
- Sistemas operativos anteriores
- Preparar
- Pruebas preliminares en el sitio
- Comprobación de versión de SQL Server

### **Paso 2: Actualice la versión del servidor de licencias**

Si la instalación tiene una nueva versión del software Citrix License Server, actualice este componente antes que cualquier otro.

Si aún no ha determinado si su servidor de licencias es compatible con la nueva versión, es vital que ejecute el instalador en el servidor de licencias antes de actualizar cualquier otro componente principal.

### **Paso 3: Actualice la versión de StoreFront**

Si el medio de instalación contiene una nueva versión del software StoreFront, ejecute el instalador en la máquina que contiene el servidor StoreFront.

- En la interfaz gráfica, elija **Citrix StoreFront** en la sección **Ampliar implementación**.
- Desde la línea de comandos, ejecute `CitrixStoreFront-x64.exe`, que está disponible en la carpeta `x64` de los medios de instalación de Citrix Virtual Apps and Desktops.

### **Paso 4: Actualice la versión de Director**

Si el medio de instalación contiene una nueva versión del software Director, ejecute el instalador en la máquina que contiene Director.

### **Paso 5: Actualice la versión de Citrix Provisioning**

Los medios de instalación de Citrix Provisioning están disponibles por separado de los medios de instalación de Citrix Virtual Apps and Desktops. Para obtener información sobre cómo instalar

y actualizar el software de servidor y dispositivo de destino de Citrix Provisioning, consulte la [documentación del producto Citrix Provisioning](#).

### **Paso 6: Actualice la versión de la mitad de los Delivery Controllers**

Por ejemplo: si su sitio tiene cuatro Controllers, ejecute el instalador en dos de ellos.

Dejar la mitad de los Controllers activos permite a los usuarios acceder al sitio. Los VDA se pueden registrar en el resto de los Controllers. Es posible que, en ocasiones, la capacidad del sitio se vea reducida porque hay menos Controllers disponibles. La actualización solo provoca una breve interrupción al establecer nuevas conexiones de cliente durante los últimos pasos de la actualización de la base de datos. Los Controllers actualizados no podrán procesar solicitudes hasta que todo el sitio esté actualizado.

Si el sitio tiene un solo Controller, este sitio no funcionará durante la actualización.

Se ejecutan pruebas preliminares del sitio en el primer Controller, antes de que comience la actualización en sí. Para ver información más detallada, consulte Pruebas preliminares en el sitio.

### **Paso 7: Actualice la versión de Studio**

Si aún no ha actualizado Studio (porque estaba en la misma máquina que otro componente), ejecute el instalador en la máquina que contiene Studio.

### **Paso 8: Reinicie Studio**

Reinicie la versión de Studio actualizada. El proceso de actualización de versión se reanuda automáticamente.

### **Paso 9: Actualice la versión de la base de datos y del sitio**

#### **Nota:**

Para evitar errores, debe actualizar todos los Delivery Controllers y la base de datos antes de realizar cualquier tarea relacionada con el aprovisionamiento y los grupos de entrega, como crear un nuevo catálogo de máquinas, eliminar un catálogo de máquinas, actualizar una máquina de un grupo de entrega, etc.

Compruebe los permisos necesarios para actualizar el esquema de las bases de datos de SQL Server en Preparación.

- Si tiene permisos suficientes para actualizar el esquema de base de datos de SQL Server, puede iniciar una actualización automática de la base de datos. Prosiga con Actualizar automáticamente la base de datos y el sitio.
- Si no dispone de suficientes permisos para la base de datos, puede iniciar una actualización manual mediante scripts y continuar con la ayuda del administrador de la base de datos (alguien que tenga los permisos necesarios). Para una actualización manual, el usuario de Studio genera los scripts y, a continuación, ejecuta los scripts que habilitan e inhabilitan los servicios. El administrador de base de datos ejecuta otros scripts que actualizan el esquema, ya sea desde la herramienta SQLCMD o SQL Server Management Studio en modo SQLCMD. Prosiga con Actualizar manualmente la base de datos y el sitio.
- Si tiene una implementación multizona y quiere actualizar la base de datos y el sitio automáticamente, Citrix recomienda que la actualización de dbschema se realice en la misma zona que aloja las bases de datos del servidor SQL del sitio. De lo contrario, la actualización automática de la base de datos y el sitio podría fallar.

Citrix recomienda encarecidamente que realice una copia de seguridad de la base de datos antes de actualizarla. Consulte CTX135207. Durante la actualización de una base de datos, los servicios del producto están inhabilitados. Tenga en cuenta que, durante ese proceso, los Controllers no pueden actuar como intermediarios o brokers en las nuevas conexiones al sitio. Por eso, planifique con cuidado esta actualización.

### **Actualizar automáticamente la base de datos y el sitio**

1. Inicie el recién actualizado Studio.
2. Indique que desea iniciar automáticamente la actualización del sitio y confirme que está listo.

La actualización de la base de datos y el sitio continúa.

### **Actualizar manualmente la base de datos y el sitio**

1. Inicie el recién actualizado Studio.
2. Indique que desea actualizar el sitio manualmente. El asistente comprueba la compatibilidad de License Server y solicita confirmación.
3. Confirme que ha realizado una copia de seguridad de la base de datos.

El asistente genera y muestra los scripts y una lista de verificación de los pasos de la actualización. Si el esquema de una base de datos no ha cambiado desde que se actualizó la versión del producto, ese script no se genera. Por ejemplo: si el esquema de la base de datos de registros no cambia, el script `UpgradeLoggingDatabase.sql` no se genera.

4. Ejecute los siguientes scripts en el orden indicado.

- `DisableServices.ps1`: El usuario de Studio ejecuta este script de PowerShell en un Controller para inhabilitar los servicios del producto.
- `UpgradeSiteDatabase.sql`: El administrador de la base de datos ejecuta este script SQL en el servidor que contiene la base de datos del sitio.
- `UpgradeMonitorDatabase.sql`: El administrador de la base de datos ejecuta este script SQL en el servidor que contiene la base de datos de supervisión.
- `UpgradeLoggingDatabase.sql`: El administrador de la base de datos ejecuta este script SQL en el servidor que contiene la base de datos de registros de configuración. Ejecute este script solo si esta base de datos cambia (por ejemplo, después de aplicar un parche rápido).
- `EnableServices.ps1`: El usuario de Studio ejecuta este script de PowerShell en un Controller para habilitar los servicios del producto.

Una vez actualizada la base de datos y habilitados los servicios de los productos, Studio prueba automáticamente el entorno y la configuración. A continuación, genera un informe HTML. En caso de problemas, se puede restaurar la base de datos con la ayuda de la copia de seguridad. Después de resolver los problemas, puede volver a actualizar la base de datos.

5. Después de completar las tareas de la lista de verificación, haga clic en **Finalizar actualización**.

## Paso 10: Actualice la versión de los Delivery Controllers restantes

Desde el recién actualizado Studio, seleccione **Citrix Studio** *nombre-de-sitio* en el panel de navegación. En la ficha **Tareas comunes**, seleccione **Actualizar los Delivery Controllers restantes**.

Una vez completada la actualización y la confirmación, cierre y vuelva a abrir Studio. Es posible que Studio solicite una actualización adicional de la versión del sitio para registrar los servicios del Controller en el sitio o para crear un ID de zona si aún no existe.

## Paso 11: Actualice la versión de los agentes VDA

### Importante:

Si va a actualizar un VDA a la versión 1912 o posterior, consulte [Actualizar los VDA a la versión 1912 o una posterior](#).

Ejecute el instalador en las máquinas con agentes VDA

Si utilizó Machine Creation Services (MCS) y una imagen maestra para crear máquinas, vaya al host y actualice el VDA en la imagen maestra. Puede utilizar cualquiera de los instaladores de VDA disponibles.

- Para obtener instrucciones acerca de la interfaz gráfica, consulte [Instalar VDA](#).

- Para obtener instrucciones acerca de la línea de comandos, consulte [Instalación desde la línea de comandos](#).

Si utilizó Citrix Provisioning para crear máquinas, consulte la [documentación del producto Citrix Provisioning](#) para obtener instrucciones sobre la actualización.

**Vea este vídeo para obtener [más información](#):**



### **Paso 12: Actualice la versión de catálogos de máquinas y grupos de entrega**

- [Actualizar catálogos que utilizan máquinas con agentes VDA actualizados.](#)
- [Actualizar catálogos que utilizan máquinas con agentes VDA actualizados.](#)
- [Actualizar grupos de entrega que utilizan máquinas con agentes VDA actualizados.](#)

### **Paso 13: Después de la actualización de versión**

Tras completar una actualización, puede probar el sitio recién actualizado. Desde Studio, seleccione **Citrix Studio nombre-de-sitio** en el panel de navegación. En la ficha **Tareas comunes**, seleccione **Probar sitio**. Estas pruebas se ejecutan automáticamente después de actualizar la base de datos, pero se pueden ejecutar de nuevo en cualquier momento.

La prueba puede fallar si hay un Controller instalado en Windows Server 2016, cuando se utiliza una base de datos local Microsoft SQL Server Express como la base de datos del sitio, si no se inicia el servicio SQL Server Browser. Para evitar esto:

- Habilite el servicio SQL Server Browser (si fuera necesario) e inícielo.
- Reinicie el servicio SQL Server (SQLEXPRESS).

Actualice otros componentes de la implementación. Para obtener instrucciones, consulte la siguiente documentación de producto:

- [StoreFront](#)
- [AppDNA](#)
- [Citrix App Layering](#)
- [HDX RealTime Optimization Pack](#)
- [Profile Management](#)
- [Citrix Provisioning](#)
- [Grabación de sesiones](#)
- [Workspace Environment Management.](#)

Si necesita reemplazar el software SQL Server Express LocalDB de Microsoft por una versión posterior, consulte Reemplazar SQL Server Express LocalDB.

### Actualización de DbSchema

Cuando actualiza la implementación a una nueva CU, puede que se actualicen varios de los esquemas de base de datos. En la tabla siguiente se indican los esquemas de base de datos que se actualizan en el proceso:

From\To	1912 CU1	1912 CU2	1912 CU3	1912 CU4	1912 CU5	1912 CU6	1912 CU7	1912 CU8
7.15 RTM/CU	Site; Monitor; Config	Site; Monitor; Config; logging	Site; Monitor; Config; logging					
1912 RTM	Config	Site; Config	Site; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config
1912 CU1		Site; Config	Site; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config
1912 CU2			Site; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config
1912 CU3				Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config
1912 CU4					Site; Config	Site; Config	Site; Config	Site; Monitor; Config
1912 CU5						Site; Config	Site; Config	Site; Monitor; Config
1912 CU6							Config	Monitor; Config
1912 CU7								Monitor; Config

Definición de términos:

- Sitio: Almacén de datos del sitio. La actualización de DbSchema se realiza en el almacén de datos del sitio.
- Supervisor: Almacén de datos de supervisión. La actualización de DbSchema se realiza en el almacén de datos de supervisión.
- Config: Tabla Configuración. La versión de Desktop Studio, la información de licencias o las dos se actualizan en la tabla Configuración.
- Registros: Almacén de datos de registros. La actualización de DbSchema se realiza en el almacén de datos de registros.

## Actualizar los VDA a la versión 1912 o una posterior

Si el componente Personal vDisk (PvD) se ha instalado alguna vez en un VDA, dicho VDA no se puede actualizar a la versión 1912 LTSR ni a ninguna posterior. Para utilizar el nuevo VDA, debe desinstalar el VDA actual y, a continuación, instalar el nuevo

Este paso debe seguirse aunque nunca haya usado PvD.

Así es como el componente PvD podría haberse instalado en versiones anteriores:

- En la interfaz gráfica del instalador de VDA, PvD era una opción en la página **Componentes adicionales**. La versión 7.15 LTSR y las 7.x anteriores habilitaban esta opción de forma predeterminada. Por lo tanto, si aceptó los valores predeterminados (o habilitó explícitamente la opción en cualquier versión), PvD se ha instalado.
- En la línea de comandos, la opción `/baseimage` instaló PvD. Si especificó esta opción o utilizó un script que contenía esta opción, PvD se ha instalado.

Si no sabe si el VDA tiene PvD instalado, ejecute el instalador del nuevo VDA (1912 LTSR o una versión posterior) en la máquina o en la imagen.

- Si PvD está instalado, aparece un mensaje que indica que hay un componente incompatible.
  - Desde la interfaz gráfica, haga clic en **Cancelar** en la página que contiene el mensaje y, a continuación, confirme que quiere cerrar el instalador.
  - Desde la CLI, el comando simplemente falla con el mensaje indicado.
- Si PvD no está instalado, la actualización continúa.

## Qué se debe hacer

Si el VDA no tiene PvD instalado, siga el procedimiento de actualización habitual.

Si el VDA tiene PvD instalado:

1. Desinstale el VDA actual. Para obtener más información, consulte [Eliminación de componentes](#).
2. Instale el nuevo VDA.

Si quiere continuar mediante PvD en sus máquinas con Windows 7 o Windows 10 (1607 y versiones anteriores, sin actualizaciones), VDA 7.15 LTSR es la última versión compatible.

## Limitaciones

Se aplican los siguientes límites a las actualizaciones:

- **Instalación selectiva de componentes:** Si instala o actualiza unos componentes a la nueva versión, pero opta por no actualizar otros componentes (en máquinas diferentes) que requieren la actualización, Studio se lo recuerda. Por ejemplo: supongamos que una actualización incluye versiones nuevas del Controller y de Studio. Actualiza el Controller, pero no ejecuta el instalador en la máquina donde está instalado Studio. No podrá seguir usando Studio para administrar el sitio hasta que actualice Studio.

No es necesario actualizar los agentes VDA, pero Citrix recomienda actualizarlos todos para que pueda utilizar todas las funcionalidades disponibles.

- **Versiones Technology Preview o Early Release:** No puede actualizar desde una versión Technology Preview, Early Release o cualquier versión de vista previa.
- **Componentes en sistemas operativos anteriores:** No puede instalar los VDA actuales en sistemas operativos que Microsoft o Citrix han dejado de admitir. Para obtener más información, consulte Sistemas operativos anteriores.
- **Entornos o sitios mixtos:** Si debe seguir ejecutando sitios con una versión anterior y sitios con la versión actual, consulte Consideraciones sobre entornos mixtos.
- **Selección de producto:** Cuando actualice desde una versión anterior, no seleccione ni especifique el producto (Citrix Virtual Apps o Citrix Virtual Apps and Desktops), porque ya lo ha establecido durante la instalación.

## Consideraciones sobre entornos mixtos

Cuando actualice el producto, Citrix recomienda actualizar todos los componentes y los VDA para aprovechar todas las funciones nuevas y mejoradas de la nueva edición.

Por ejemplo: aunque puede usar agentes VDA actuales en implementaciones que contienen versiones anteriores de Controller, es posible que las nuevas funcionalidades de la versión actual no estén disponibles. También se pueden dar problemas de registro de VDA cuando se usan versiones no actuales.

En algunos entornos, es posible que no se puedan actualizar todos los VDA a la versión más reciente. En este caso, cuando cree un catálogo de máquinas, puede especificar la versión de VDA instalada en las máquinas. (Esto se denomina nivel funcional). De forma predeterminada, esta configuración especifica la versión mínima recomendada del VDA. El valor predeterminado es suficiente para la mayoría de las implementaciones. Considere cambiar la configuración a una versión anterior solo si el catálogo contiene agentes VDA anteriores a la predeterminada. No se recomienda mezclar versiones de VDA en un catálogo de máquinas.

Si se crea un catálogo de máquinas con el parámetro predeterminado de la versión de VDA mínima, y alguna de las máquinas del catálogo tiene una versión de VDA anterior a la predeterminada, esas máquinas no podrán registrarse en el Controller y no funcionarán.

Para obtener más información, consulte [Niveles funcionales y versiones de VDA](#).

### **Varios sitios con diferentes versiones**

Si el entorno contiene sitios con diferentes versiones de producto (por ejemplo, un sitio de XenDesktop 7.18 y un sitio de Citrix Virtual Apps and Desktops 1909), Citrix recomienda usar StoreFront para combinar escritorios y aplicaciones con diferentes versiones de producto. Para obtener más información, consulte la documentación de [StoreFront](#).

En un entorno mixto, puede continuar mediante versiones de Studio y Director para cada versión, pero compruebe que las distintas versiones están instaladas en máquinas independientes.

### **Sistemas operativos anteriores**

Supongamos que ha instalado una versión anterior de un componente en una máquina que ejecutaba una versión compatible de sistema operativo (SO). Ahora, quiere utilizar una versión más reciente del componente, pero ese SO ya no es compatible con la versión actual del componente.

Por ejemplo: suponga que instaló un VDA de servidor en una máquina con Windows Server 2008 R2. Ahora desea actualizar ese VDA a la versión actual, pero Windows Server 2008 R2 no es compatible con la versión actual a la que está actualizando.

Si intenta instalar o actualizar un componente en un sistema operativo que ya no está permitido, aparece un mensaje de error (“No se puede instalar en este sistema operativo”).

Estas consideraciones son aplicables a la actualización de las versiones Current Release y Long Term Service Release. (No afecta a la aplicación de actualizaciones acumulativas a una versión LTSR).

Siga los enlaces para saber qué sistemas operativos son compatibles:

- Para LTSR, seleccione la versión correspondiente en la página principal de la documentación del producto [Citrix Virtual Apps and Desktops](#).
  - [Requisitos del sistema](#).
  - Listas de componentes en artículos de la categoría [Novedades](#).
- Para CR (versiones actuales):
  - [Delivery Controller, Studio, Director, VDA, Universal Print Server](#)
  - [Servicio de autenticación federada](#)
  - Para [StoreFront](#), el [Autoservicio de restablecimiento de contraseñas](#) y la [Grabación de sesiones](#), consulte el artículo de requisitos del sistema para la versión actual.

## Sistemas operativos no válidos

En la siguiente tabla se ofrece una lista de los sistemas operativos anteriores que no son válidos para instalar o actualizar componentes de la versión actual. Se indica la última versión válida del componente admitida para cada SO y la versión del componente cuando la instalación y la actualización dejan de ser válidas.

Los sistemas operativos de la tabla incluyen Service Packs y actualizaciones.

<b>Sistema operativo</b>	<b>Componente o función</b>	<b>Última versión válida</b>	<b>Instalar o actualizar no es posible a partir de la versión</b>
Windows 7 y Windows 8	VDA	7.15 LTSR	7.16
Windows 7 y Windows 8	Otros componentes del instalador	7.17	7.18
Versiones de Windows 10 anteriores a 1607	VDA	7.15 LTSR	7.16
Versión x86 de Windows 10	VDA	1906.2.0	1909
Windows Server 2008 R2	VDA	7.15 LTSR	7.16
Windows Server 2008 R2	Otros componentes del instalador	7.17	7.18
Windows Server 2012	VDA	7.15 LTSR	7.16
Windows Server 2012	Otros componentes del instalador	7.17	7.18
Windows Server 2012 R2	Otros componentes del instalador*	1912 LTSR	2003
Windows Server 2012 R2	VDI de servidor	7.15 LTSR	7.16

Windows XP y Windows Vista no son válidos para ningún componente o tecnología de 7.x.

\* Se aplica a Delivery Controller, Studio, Director y VDA.

## Lo que puede hacer

Tiene opciones. Puede hacer lo siguiente:

- Continuar con el sistema operativo actual

- Restablecer la imagen inicial o actualizar la máquina
- Agregar máquinas nuevas y, a continuación, eliminar máquinas antiguas

**Continuar con el sistema operativo actual** Estos métodos son factibles para VDA. Si quiere seguir usando máquinas con el sistema operativo anterior, puede elegir una de las siguientes opciones:

- Seguir usando la versión instalada del componente.
- Descargar la última versión válida del componente y actualizarlo a esa versión. (Eso supone que la última versión válida del componente aún no está instalada.)

Por ejemplo: tiene un VDA 7.14 en una máquina Windows 7 SP1. La última versión válida de VDA en máquinas con sistema operativo Windows 7 es XenApp y XenDesktop 7.15 LTSR. Puede seguir usando 7.14 o descargar un VDA 7.15 LTSR y actualizar su VDA a esa versión. Esas versiones anteriores de VDA funcionan en implementaciones que contienen Delivery Controllers de versiones más recientes. Por ejemplo: un VDA 7.15 LTSR puede conectarse a un Controller de Citrix Virtual Apps and Desktops 7 1808.

**Restablecer la imagen inicial o actualizar la máquina** Estos métodos son factibles para VDA y otras máquinas que no tienen componentes principales (como Delivery Controllers) instalados. Elija una de las siguientes opciones:

- Tras colocar la máquina en el modo de mantenimiento y permitir que se cierren todas las sesiones, puede restablecer su imagen a una versión compatible de SO Windows, y luego instalar la versión más reciente del componente.
- Para actualizar el sistema operativo sin restablecer imágenes, desinstale el software de Citrix antes de actualizar el sistema operativo. De lo contrario, el software Citrix entrará en un estado no admitido. Luego, instale el nuevo componente.

**Agregar máquinas nuevas y, a continuación, eliminar máquinas antiguas** Este método es factible si debe actualizar el sistema operativo en máquinas que contienen un Delivery Controller u otro componente principal.

Citrix recomienda que todos los Controllers de un sitio tengan el mismo sistema operativo. En la siguiente secuencia de actualización se minimiza el intervalo en que los Controllers tienen diferentes sistemas operativos.

1. Tome una instantánea de todos los Delivery Controllers en el sitio y haga una copia de seguridad de la base de datos del sitio.
2. Instale los nuevos Delivery Controllers en servidores limpios con sistemas operativos admitidos. Por ejemplo: instale un Controller en dos máquinas Windows Server 2016.
3. Agregue los nuevos Controllers al sitio.

4. Elimine los Controllers que se ejecutan en sistemas operativos no válidos para la versión actual. Por ejemplo: elimine dos Controllers en dos máquinas Windows Server 2008 R2. Siga las recomendaciones para eliminar Controllers en [Delivery Controllers](#).

## Preparar

Antes de comenzar una actualización, revise la siguiente información y complete las tareas necesarias.

### Elegir un instalador y una interfaz

Puede usar el instalador de producto completo que se proporciona en el archivo ISO del producto para actualizar los componentes. Puede actualizar los VDA con la ayuda del instalador de producto completo o con uno de los instaladores independientes de VDA. Todos los instaladores ofrecen interfaces gráficas y de línea de comandos.

Para obtener más información, consulte [Instaladores](#).

**Detalles de la instalación:** Después de completar cualquier trabajo de preparación y estar listo para iniciar el instalador, el artículo de instalación muestra lo que verá (si está utilizando la interfaz gráfica) o lo que tendrá que escribir (si utiliza la interfaz de línea de comandos).

- [Instalar/actualizar componentes principales mediante la interfaz gráfica](#)
- [Instalar/actualizar componentes principales mediante la línea de comandos](#)
- [Instalar/actualizar los agentes VDA mediante la interfaz gráfica](#)
- [Instalar/actualizar los agentes VDA mediante la línea de comandos](#)

Si al principio instaló un VDA de sesión única con el instalador `VDAWorkstationCoreSetup.exe`, Citrix recomienda usar el mismo instalador para actualizar su versión. Si utiliza el instalador de VDA de producto completo o el instalador `VDAWorkstationSetup.exe` para actualizar el VDA, los componentes que se hayan excluido en su momento pueden instalarse esta vez, a menos que los omita o excluya expresamente de la actualización.

La máquina se reinicia durante el proceso de actualización de un VDA a esta versión. (Este requisito comenzó con la versión 7.17.) Esto no se puede evitar. La actualización se reanuda automáticamente después del reinicio (a menos que especifique `/noresume` en la línea de comandos).

### Acciones de base de datos

Realice una copia de seguridad de las tres bases de datos: del sitio, de supervisión y de registros de configuración. Siga las instrucciones indicadas en [CTX135207](#). Si se detecta algún problema después de la actualización, se puede restaurar la copia de seguridad.

Para obtener información sobre la actualización de versiones de SQL Server que ya no son compatibles, consulte [Comprobación de versión de SQL Server](#). (Esto se refiere al sistema SQL Server que se utiliza para las bases de datos del sitio, de supervisión y de registros de configuración).

Microsoft SQL Server Express LocalDB se instala automáticamente para su uso con la Caché de host local. Si necesita reemplazar una versión anterior, la nueva versión debe ser SQL Server Express 2017 LocalDB CU16 o una posterior. Para obtener información detallada sobre cómo reemplazar SQL Server Express LocalDB con una nueva versión después de actualizar los componentes y el sitio, consulte [Reemplazar SQL Server Express LocalDB](#).

### **Compruebe que las licencias de Citrix están actualizadas**

Para obtener una visión completa de la administración de Citrix Licensing, consulte [Activar, actualizar y administrar licencias de Citrix](#).

Puede usar el instalador de producto completo para actualizar el servidor de licencias. O bien, puede descargar y actualizar los componentes de la licencia por separado. Consulte [Actualizar](#).

Antes de actualizar, compruebe que la fecha de Customer Success Services, Software Maintenance o Subscription Advantage es válida para la nueva versión del producto. Si va a actualizar desde una versión de producto anterior a 7.x, la fecha debe ser al menos 2019.1115.

### **Compruebe que su Citrix License Server sea compatible**

Debe comprobar si su Citrix License Server es compatible con la nueva versión. Hay dos formas de hacerlo:

- Antes de actualizar cualquier otro componente de Citrix, ejecute el instalador [XenDesktopServerSetup.exe](#) desde la distribución ISO de la máquina que contiene el Delivery Controller. Si hay algún problema de incompatibilidad, el instalador lo notifica con los pasos recomendados para resolverlo.
- En el directorio de [XenDesktop Setup](#) del medio de instalación, ejecute el comando `.\LicServVerify.exe -h <license-server-fqdn> -p 27000 -v`. La pantalla resultante indica si el servidor de licencias es compatible. Si el servidor de licencias no es compatible, actualice el servidor de licencias.

### **Realizar copias de seguridad de las modificaciones de StoreFront**

Antes de iniciar una actualización de versión, si ha hecho modificaciones en los archivos de `C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data`, como `default.ica` y `usernamepass-`

*word.tfrm*, realice una copia de seguridad de ellos para cada almacén. Después de la actualización de la versión, puede restaurarlos para restablecer las modificaciones.

### **Cierre aplicaciones y consolas**

Antes de iniciar una actualización, cierre todos los programas que podrían bloquear los archivos, como las consolas de administración y las sesiones de PowerShell.

Reiniciar la máquina garantiza que no haya archivos bloqueados y que no haya actualizaciones de Windows pendientes.

Antes de comenzar una actualización, detenga e inhabilite los servicios de agentes de supervisión externos que haya.

### **Compruebe que dispone de los permisos correctos**

Además de ser un usuario del dominio, usted debe ser un administrador local en las máquinas donde quiere actualizar los componentes de producto.

La base de datos del sitio y el sitio pueden actualizarse de manera automática o manual. Para realizar una actualización automática de la base de datos, los permisos de usuario de Studio deben incluir la capacidad de actualizar el esquema de la base de datos de SQL Server (por ejemplo, el rol de base de datos `db_securityadmin` o `db_owner`). Para obtener más información, consulte [Bases de datos](#).

Si el usuario de Studio no tiene los permisos necesarios, se generan scripts al iniciar una actualización manual de la base de datos. El usuario de Studio ejecuta algunos de los scripts desde Studio. El administrador de la base de datos ejecuta otros scripts mediante una herramienta como SQL Server Management Studio.

### **Otras tareas de preparación**

- También puede hacer una copia de seguridad de las plantillas y actualizar los hipervisores, si es necesario.
- Complete las demás tareas de preparación estipuladas en el plan de continuidad empresarial.

### **Pruebas preliminares en el sitio**

Cuando actualiza los Delivery Controllers y un sitio, se ejecutan pruebas preliminares en el sitio antes de que comience la actualización en sí. En estas pruebas se comprueba si:

- Se puede establecer conexión con la base de datos del sitio y esta tiene copia de seguridad

- Las conexiones a los servicios esenciales de Citrix funcionan correctamente
- La dirección del servidor de licencias de Citrix está disponible
- Se puede establecer conexión con la base de datos de registros de configuración

Tras ejecutarse las pruebas, podrá ver un informe de los resultados. A continuación, podrá solucionar los problemas que se detectaran y ejecutar las pruebas nuevamente. El funcionamiento del sitio puede verse afectado negativamente si no ejecuta las pruebas preliminares del sitio y no resuelve los problemas que surjan.

El informe que contiene los resultados de las pruebas es un archivo HTML ([PreliminarySiteTestResult.html](#)) ubicado en el mismo directorio que los registros de instalación. Si aún no existe, el archivo se creará. Si el archivo ya existe, su contenido se sobrescribirá.

### **Ejecutar las pruebas**

- Cuando usa la interfaz gráfica del instalador para actualizar, el asistente incluye una página donde puede iniciar las pruebas y luego ver el informe. Después de que se ejecuten las pruebas, haya visto el informe y haya resuelto los problemas que se encontraran, puede volver a ejecutar las pruebas. Cuando las pruebas se ejecuten sin detectar errores, haga clic en “Siguiente” para continuar con el asistente.
- Cuando usa la interfaz de línea de comandos para actualizar, las pruebas se ejecutan automáticamente. De forma predeterminada, si una prueba falla, la actualización no se realiza. Después de ver el informe y resolver los problemas, vuelva a ejecutar el comando.

Citrix recomienda ejecutar siempre las pruebas preliminares del sitio y resolver todos los problemas que surjan antes de continuar con la actualización del sitio y del Controller. Los beneficios potenciales que aportan las pruebas valen la pena frente al poco tiempo que se necesita para ejecutar las pruebas. Sin embargo, puede anular esta acción recomendada.

- Al actualizar desde la interfaz gráfica, puede optar por omitir las pruebas y continuar con la actualización.
- Al actualizar desde la línea de comandos, no puede omitir las pruebas. De forma predeterminada, una prueba de sitio que haya fallado detiene el instalador, sin realizar la actualización. En la mayoría de los casos, si incluye la opción `/ignore_site_test_failure`, los fallos en las pruebas se ignoran y la actualización de la versión continúa (Consulte Comprobación de versión de SQL Server para ver si hay excepciones).

### **Al actualizar varios Controllers**

Cuando inicia una actualización en un Controller y luego inicia una actualización de otro Controller ubicado en el mismo sitio (antes de que se complete la primera actualización):

- Si las pruebas preliminares del sitio se han completado en el primer Controller, la página de pruebas preliminares del sitio no aparece en el asistente del segundo Controller.
- Si las pruebas en el primer Controller aún están en curso cuando se inicia la actualización del segundo Controller, la página de pruebas del sitio aparece en el asistente del segundo Controller. Sin embargo, si finalizan las pruebas en el primer Controller, solo se conservan los resultados de las pruebas del primer Controller.

### Fallos de pruebas no relacionados con el estado del sitio

- Si las pruebas preliminares del sitio fallan debido a una memoria insuficiente, aumente la cantidad de memoria disponible y vuelva a ejecutar las pruebas.
- Si tiene permisos para actualizar, pero no para ejecutar pruebas en el sitio, las pruebas preliminares del sitio fallan. Para solucionar este problema, vuelva a ejecutar el instalador con una cuenta de usuario que tenga permiso para ejecutar las pruebas.

### Comprobación de versión de SQL Server

Una implementación correcta de Citrix Virtual Apps and Desktops requiere una versión compatible de Microsoft SQL Server para las bases de datos del sitio, de supervisión y de registros de configuración. Al actualizar la versión de una implementación de Citrix con una versión de SQL Server que ya no es compatible, puede provocar problemas de funcionalidad, por lo que el sitio no estará disponible.

Para saber qué versiones de SQL Server son compatibles con la versión de Citrix a la que va a actualizarse, consulte el artículo [Requisitos del sistema](#) correspondiente a dicha versión.

Al actualizar la versión de un Controller, el instalador de Citrix comprueba la versión actual instalada de SQL Server que se utiliza para las bases de datos del sitio, de supervisión y de registros de configuración.

- Si la comprobación determina que la versión de SQL Server instalada actualmente no es compatible con la versión de Citrix a la que va a actualizarse:
  - Interfaz gráfica: La actualización de versión se detiene y muestra un mensaje. Haga clic en **Aceptar** y, a continuación, haga clic en **Cancelar** para cerrar el instalador de Citrix (no puede continuar con la actualización).
  - Interfaz de línea de comandos: El comando falla (aunque haya incluido la opción `/ignore_db_check_failure` con el comando).

Actualice la versión de SQL Server y vuelva a iniciar la actualización de la versión de Citrix.

- Si la comprobación no puede determinar qué versión de SQL Server hay instalada actualmente, averigüe si la versión instalada actualmente es compatible con la versión a la que va a actualizarse ([Requisitos del sistema](#)).

- Interfaz gráfica: La actualización de versión se detiene y muestra un mensaje.
  - \* Si la versión de SQL Server instalada actualmente es compatible, haga clic en **Aceptar** para cerrar el mensaje y, a continuación, haga clic en **Siguiente** para continuar con la actualización de la versión de Citrix.
  - \* Si la versión de SQL Server instalada actualmente no es compatible, haga clic en **Aceptar** para cerrar el mensaje y, a continuación, haga clic en **Cancelar** para finalizar la actualización de la versión de Citrix. Actualice la versión de SQL Server a una compatible y vuelva a iniciar la actualización de la versión de Citrix.
- Interfaz de línea de comandos: El comando falla y muestra un mensaje. Después de cerrar el mensaje:
  - \* Si la versión de SQL Server instalada actualmente es compatible, ejecute el comando de nuevo con la opción `/ignore_db_check_failure`.
  - \* Si la versión de SQL Server instalada actualmente no es compatible, actualice la versión de SQL Server a una compatible. Vuelva a ejecutar el comando para iniciar la actualización de la versión de Citrix.

### Actualizar la versión de SQL Server

Si trae nuevos servidores de SQL Server y migra la base de datos del sitio, las cadenas de conexión deben actualizarse.

Si el sitio utiliza actualmente SQL Server Express (que Citrix instaló automáticamente durante la creación del sitio):

1. Instale la versión más reciente de SQL Server Express.
2. Desconecte la base de datos.
3. Conecte la base de datos al nuevo SQL Server Express.
4. Migre las cadenas de conexión.

Para obtener más información, consulte [Configurar cadenas de conexión](#) y la documentación de Microsoft SQL Server.

### Reemplazar SQL Server Express LocalDB

Microsoft SQL Server Express LocalDB es una función de SQL Server Express que la Caché de host local utiliza de forma independiente. La Caché de host local no requiere ningún componente de SQL Server Express aparte de SQL Server Express LocalDB.

Si instaló una versión de Delivery Controller anterior a 1912 y, a continuación, actualiza la implementación a la versión 1912 o una posterior, Citrix no actualiza automáticamente la versión de Lo-

calDB de SQL Server Express. ¿Por qué no? Porque es posible que tenga componentes que no dependen de Citrix y usen SQL Server Express LocalDB. Si tiene componentes que no son Citrix que utilizan SQL Server Express LocalDB, compruebe que la actualización de SQL Server Express LocalDB no interrumpa el servicio de dichos componentes. Para actualizar (reemplazar) la versión LocalDB de SQL Server Express, siga las instrucciones de esta sección.

- **Al actualizar Delivery Controllers a Citrix Virtual Apps and Desktops 1912, 1912 LTSR o 2003:** La actualización de SQL Server Express LocalDB es opcional. La función Caché de host local funciona correctamente, sin pérdida de funcionalidad, independientemente de si actualiza SQL Server Express LocalDB. Agregamos la opción de pasar a una versión más reciente de SQL Server Express LocalDB por si le preocupa que Microsoft deje de desarrollar SQL Server Express LocalDB 2014.
- **Al actualizar Delivery Controllers a versiones de Citrix Virtual Apps and Desktops posteriores a 2003:** La versión mínima admitida es SQL Server Express 2017 LocalDB Cumulative Update (CU) 16. Si instaló originalmente un Delivery Controller anterior a la versión 1912 y no ha reemplazado SQL Server Express LocalDB con una versión más reciente desde entonces, deberá reemplazar ese software de base de datos ahora. De lo contrario, la Caché de host local no funcionará.

Se necesitan:

- Los medios de instalación de Citrix Virtual Apps and Desktops (para la versión a la que ha actualizado). Los medios contienen una copia de Microsoft SQL Server Express LocalDB 2017 CU 16.
- Una herramienta de Windows Sysinternals que puede descargar desde Microsoft.

Procedimiento:

1. Complete la actualización de los componentes, las bases de datos y el sitio de Citrix Virtual Apps and Desktops (estas actualizaciones de bases de datos afectan a las bases de datos del sitio, supervisión y registros de configuración; no afectan a la base de datos de la Caché de host local que utiliza SQL Server Express LocalDB).
2. En el Delivery Controller, descargue [PsExec](#) desde Microsoft. Consulte el documento [PsExec v2.2](#) de Microsoft.
3. Detenga Citrix High Availability Service (Servicio de alta disponibilidad de Citrix).
4. Desde el símbolo del sistema, ejecute [PsExec](#) y cambie a la cuenta Servicio de red.

```
psexec -i -u "NT AUTHORITY\NETWORK SERVICE"cmd
```

Opcionalmente, puede utilizar [whoami](#) para confirmar que el símbolo del sistema se está ejecutando como la cuenta Servicio de red.

```
whoami
```

```
nt authority\network service
```

5. Vaya a la carpeta que contiene SqlLocalDB.

```
cd "C:\Program Files\Microsoft SQL Server\120\Tools\Binn"
```

6. Detenga y elimine CitrixHA (LocalDB).

```
SqlLocalDB stop CitrixHA
```

```
SqlLocalDB delete CitrixHA
```

7. Elimine los archivos relacionados que se encuentran en `C:\Windows\ServiceProfiles\NetworkService`.

```
1 HADatabaseName.*
2 HADatabaseName_log.*
3 HAImportDatabaseName.*
4 HAImportDatabaseName_log.*
5 <!--NeedCopy-->
```

Consejo: Es posible que su implementación no tenga `HAImportDatabaseName.*` ni `HAImportDatabaseName_log.*`.

8. Desinstale SQL Server Express LocalDB 2014 que haya en el servidor. Utilice para ello la función de Windows para quitar los programas.
9. Instale SQL Server Express LocalDB 2017. En la carpeta `Support > SQLLocalDB` de los medios de instalación de Citrix Virtual Apps and Desktops, haga doble clic en `sqllocaldb.msi`. Es posible que se solicite un reinicio para completar la instalación. (El nuevo SQLLocalDB reside en `C:\Program Files\Microsoft SQL Server\140\Tools\Binn`.)
10. Inicie el servicio Citrix High Availability Service.
11. Compruebe que se creó la base de datos de la Caché de host local en cada Delivery Controller. Eso confirma que el servicio de alta disponibilidad (broker secundario) puede tomar el control, si fuera necesario.
  - En el servidor del Controller, vaya a `C:\Windows\ServiceProfiles\NetworkService`.
  - Compruebe que se hayan creado `HaDatabaseName.mdf` y `HaDatabaseName_log.ldf`.

## Actualizar un servidor de trabajo XenApp 6.5 a un nuevo VDA

September 11, 2023

Después de migrar una comunidad XenApp 6.5, puede utilizar los servidores XenApp 6.5 que se habían configurado en el modo solo host de sesión (también conocido como servidores de trabajo o solo sesión). Para ello, elimine el software anterior, actualice el SO y, a continuación, instale un nuevo VDA para SO de servidor.

Aunque puede actualizar un servidor de trabajo XenApp 6.5, instalar el software actual de VDA en una máquina limpia ofrece una mayor seguridad.

Para actualizar un servidor de trabajo XenApp 6.5 a un nuevo VDA:

1. Quite Hotfix Rollup Pack 7 para XenApp 6.5 siguiendo las instrucciones descritas en el archivo Léame del hotfix. Consulte [CTX202095](#).
2. Desinstale XenApp 6.5. Este proceso requiere varios reinicios. Si se produce un error durante el proceso de desinstalación, compruebe el registro de errores de desinstalación al que hace referencia el mensaje de error. El archivo de registro se encuentra en la carpeta “%TEMP%\Citrix\XenDesktop Installation\XenApp 6.5 Uninstall Log Files\”.
3. Actualice el sistema operativo del servidor a una versión admitida. Para ver una lista de las plataformas compatibles, consulte la sección de VDA para SO de servidor en [Requisitos del sistema](#).
4. Instale un VDA para SO de servidor mediante un instalador suministrado con esta versión. Consulte [Instalar agentes VDA](#) o [Instalación desde la línea de comandos](#).

Después de instalar el nuevo VDA, desde Studio en el nuevo sitio de XenApp, cree catálogos de máquinas (o modifique los existentes) para los servidores de trabajo actualizados.

## Solución de problemas

**Falla la eliminación del software de XenApp 6.5.** Los registros de desinstalación contienen el mensaje: “Error 25703. An error occurred while plugging XML into Internet Information Server. Setup cannot copy files to your IIS Scripts directory. Please make sure that your IIS installation is correct.”

Causa: El problema ocurre en sistemas donde (1) durante el proceso inicial de instalación de XenApp 6.5, usted indicó que Citrix XML Service (CtxHttp.exe) no debe compartir el puerto con IIS, y (2) .NET Framework 3.5.1 está instalado.

Solución:

1. Quite el rol de Servidor web (IIS) mediante el asistente para quitar roles del servidor. (Puede volver a instalar el rol de Servidor web (IIS) más tarde.)
2. Reinicie el servidor.
3. Mediante Agregar o quitar programas, desinstale Citrix XenApp 6.5 y Microsoft Visual C++ 2005 Redistributable (x64), versión 8.0.56336.
4. Reinicie el servidor.
5. Instale el VDA para SO de servidor.

## Migrar XenApp 6.x

September 22, 2021

### Importante:

La migración mueve los datos de una implementación a una versión más reciente. El proceso incluye la instalación de nuevos componentes y la creación de un sitio, la exportación de datos desde la comunidad de servidores original y la importación de esos datos en el sitio nuevo.

Los scripts de migración en código abierto están disponibles en <https://github.com/citrix/xa65migrationtool>. Sin embargo, Citrix no admite estos scripts.

El resto de este artículo contiene información que se puede utilizar como referencia con los scripts de migración en código abierto.

## Introducción

Puede usar la herramienta de migración descrita en este artículo para migrar de XenApp 6.x a XenApp 7.6. Luego, puede actualizar XenApp 7.6 a una versión LTSR compatible o la versión actual de Citrix Virtual Apps and Desktops; consulte [Actualizar una implementación](#).

Para obtener información sobre los cambios de arquitectura, componentes y características que se han introducido en las versiones 7.x, consulte [Cambios en 7.x](#).

## XenApp 6.x Migration Tool

La herramienta de migración de XenApp 6.x (Migration Tool) es una colección de scripts de PowerShell que contienen cmdlets para migrar los datos de las comunidades y las directivas de XenApp 6.x (6.0 o 6.5). En el servidor del Controller de XenApp 6.x, ejecute los cmdlets de exportación que recopilan dichos datos en archivos XML. A continuación, desde el Controller de XenApp 7.6, ejecute los cmdlets de importación, que crean objetos mediante los datos recopilados durante la exportación.

La siguiente secuencia resume el proceso de migración, los detalles se proporcionan más adelante.

1. En un Controller de XenApp 6.0 o 6.5:
  - a) Importe los módulos de exportación de PowerShell.
  - b) Ejecute los cmdlets de exportación para exportar datos de la comunidad y/o de directivas en archivos XML.
2. Copie los archivos XML (y la carpeta de iconos si eligió no incrustarlos en los archivos XML durante la exportación) en el Controller de XenApp 7.6.

3. En el Controller de XenApp 7.6:
  - a) Importe los módulos de importación de PowerShell.
  - b) Ejecute los cmdlets de importación para importar los datos de la comunidad (aplicaciones) y/o de directivas, mediante los archivos XML como entrada.
4. Complete los pasos posteriores a la migración.

Antes de iniciar una migración real, puede exportar la configuración de XenApp 6.x y, a continuación, realizar una vista previa de la importación en el sitio de XenApp 7.6. La vista previa puede identificar posibles puntos de fallo para que usted pueda resolver los problemas antes de ejecutar la importación en sí. Por ejemplo, una vista previa puede detectar que ya existe una aplicación con el mismo nombre en el nuevo sitio de XenApp 7.6. También puede usar los archivos de registros generados a partir de la vista previa como guía para la migración.

A menos que se indique lo contrario, el término 6.x hace referencia a XenApp 6.0 o 6.5.

## Paquete de herramienta de migración

La herramienta de migración contiene dos paquetes separados:

- **ReadIMA:** Contiene los archivos utilizados para exportar datos desde las comunidades de XenApp 6.x, además de módulos compartidos.

---

Módulo o archivo	Descripción
ExportPolicy.psm1	Módulo de script de PowerShell para exportar las directivas de XenApp 6.x a un archivo XML.
ExportXAFarm.psm1	Módulo de scripts de PowerShell para exportar la configuración de la comunidad de XenApp 6.x a un archivo XML.
ExportPolicy.psd1	Archivo de manifiesto de PowerShell para el módulo de script ExportPolicy.psm1.
ExportXAFarm.psd1	Archivo de manifiesto de PowerShell para el módulo de script ExportXAFarm.psm1.
LogUtilities.psm1	Módulo de script compartido de PowerShell que contiene las funciones de registro.
XmlUtilities.psd1	Archivo de manifiesto de PowerShell para el módulo de script XmlUtilities.psm1.
XmlUtilities.psm1	Módulo de script compartido de PowerShell que contiene las funciones de XML.

---

- **ImportFMA:** Contiene los archivos utilizados para importar datos en las comunidades de XenApp 7.6, además de módulos compartidos.

Módulo o archivo	Descripción
ImportPolicy.psm1	Módulo de scripts de PowerShell para importar las directivas en XenApp 7.6.
ImportXAFarm.psm1	Módulo de scripts de PowerShell para importar las aplicaciones en XenApp 7.6.
ImportPolicy.psd1	Archivo de manifiesto de PowerShell para el módulo de script ImportPolicy.psm1.
ImportXAFarm.psd1	Archivo de manifiesto de PowerShell para el módulo de script ImportXAFarm.psm1.
PolicyData.xsd	Esquema XML para datos de directivas.
XAFarmData.xsd	Esquema XML para datos de la comunidad XenApp.
LogUtilities.psm1	Módulo de script compartido de PowerShell que contiene las funciones de registro.
XmlUtilities.psd1	Archivo de manifiesto de PowerShell para el módulo de script XmlUtilities.psm1.
XmlUtilities.psm1	Módulo de script compartido de PowerShell que contiene las funciones de XML.

## Limitaciones

- No se importan todas las configuraciones de directivas; consulte Configuraciones de directivas que no se importan. Las configuraciones que no son compatibles se ignoran y esto se indica en el archivo de registros.
- Aunque se recopilan detalles de todas las aplicaciones en el archivo XML de salida durante la operación de exportación, solo se importan en el sitio de XenApp 7.6 las aplicaciones instaladas en el servidor. Los escritorios publicados, el contenido y la mayoría de las aplicaciones distribuidas por streaming no están disponibles (consulte los parámetros del cmdlet Import-XAFarm en Importar datos: paso a paso para ver las excepciones).
- Los servidores de aplicaciones no se importan.
- Muchas de las propiedades de aplicación no se importan debido a diferencias entre la arquitectura IMA (Independent Management Architecture) de XenApp 6.x y las tecnologías FlexCast Management Architecture (FMA) de XenApp 7.6; consulte Asignación de propiedades de aplicaciones.

- Se crea un grupo de entrega durante la importación. Consulte Uso avanzado para obtener más información sobre cómo usar los parámetros para filtrar lo que se importa.
- Solo se importan las configuraciones de directiva de Citrix creadas con la consola de administración de AppCenter; las configuraciones de directiva de Citrix creadas con objetos de directiva de grupo (GPO) de Windows no se importan.
- Los scripts de migración están diseñados para las migraciones desde XenApp 6.x a XenApp 7.6 únicamente.
- Studio no admite el uso de carpetas anidadas a más de cinco niveles de profundidad, por lo que no se importarán. Si la estructura de carpetas de aplicaciones incluye carpetas a más de cinco niveles de profundidad, considere la posibilidad de reducir la cantidad de niveles de anidación de carpetas antes de realizar la importación.

## Consideraciones sobre seguridad

Los archivos XML creados por los scripts de exportación pueden contener información confidencial acerca de su entorno y organización, como nombres de usuario, nombres de servidor, y otros datos de configuración de directivas, comunidades y aplicaciones de XenApp. Almacene y gestione estos archivos en entornos seguros.

Repase cuidadosamente los archivos XML antes de usarlos como material para la importación de directivas y aplicaciones, y compruebe que no contienen modificaciones no autorizadas.

Las asignaciones de objeto de directiva (antes conocidas como filtros de directivas) son las que gestionan la forma en que se aplican las directivas. Después de importar las directivas, revise meticulosamente las asignaciones de objeto de cada directiva para comprobar que no haya vulnerabilidades de seguridad a raíz de la importación. Tras la importación, se pueden aplicar a la directiva diferentes conjuntos de usuarios, direcciones IP o nombres de cliente. Después de la importación, es posible que los parámetros “Permitir” o “Denegar” tengan implicaciones diferentes.

## Capturar registros y controlar errores

Los scripts ofrecen gran cantidad de registros que hacen un rastreo de todas las ejecuciones de cmdlets, mensajes informativos, resultados de la ejecución de cmdlets, advertencias y errores.

- Queda registrada la mayor parte del uso de cmdlets de PowerShell de Citrix. Se registran todos los cmdlets de PowerShell en los scripts de importación que crean nuevos objetos del sitio.
- Se registra el progreso de la ejecución de scripts, incluidos los objetos procesados.
- Se registran las principales acciones que afectan al flujo de trabajo, incluidos flujos dirigidos desde la línea de comandos.
- Se registran todos los mensajes que se imprimen en la consola, incluidas las advertencias y los errores.

- Cada línea recibe una marca de hora, con precisión de milésima de segundo.

Citrix recomienda especificar un archivo de registros cuando se ejecute cada uno de los cmdlets de importación y exportación.

Si no se especifica un nombre de archivo de registros, el archivo de registros se almacena en la carpeta principal del usuario (especificada por la variable \$HOME de PowerShell) si dicha carpeta existe; de lo contrario, se coloca en la carpeta de ejecución del script actual. El nombre predeterminado de los registros es “XFarmAAAAMDDHmSS-xxxxxx” donde los últimos seis dígitos son un número aleatorio.

De forma predeterminada, se muestra toda la información de progreso. Para evitar que se muestre, especifique el parámetro NoDetails en los scripts de exportación e importación.

Por lo general, la ejecución de un script se detiene cuando se encuentra un error, y se puede ejecutar el cmdlet de nuevo después de eliminar las condiciones de error.

Las condiciones que no se consideran errores se registran; muchas se notifican como advertencias, y la ejecución del script continúa. Por ejemplo, los tipos de aplicación no compatibles se notifican como advertencias y no se importan. Las aplicaciones que ya existen en el sitio de XenApp 7.6 no se importan. Las configuraciones de directiva retiradas de XenApp 7.6 no se importan.

Los scripts de migración usan muchos cmdlets de PowerShell y puede ser que no se registren todos los errores posibles. Para ver información adicional sobre la cobertura de registros, use la funcionalidad de registros de PowerShell. Por ejemplo, las transcripciones de PowerShell registran todo lo que se imprime en pantalla. Para obtener más información, consulte la ayuda de los cmdlets Start-Transcript y Stop-Transcript.

## Requisitos, preparación y procedimientos recomendados

Para migrar, debe usar el SDK de Citrix XenApp 6.5. Descargue ese SDK desde <https://www.citrix.com/downloads/xenapp/sdks/powershell-sdk.html>.

Consulte este artículo antes de iniciar una migración.

Es necesario comprender los conceptos básicos de PowerShell sobre directiva de ejecución, módulos, cmdlets y scripts. Aunque no es necesario tener una amplia experiencia en creación de scripts, es conveniente entender los cmdlets que hay que ejecutar. Use el cmdlet Get-Help para consultar la ayuda de cada cmdlet de migración antes de ejecutarlo. Por ejemplo: `Get-Help -full Import -XFarm`.

Especifique un archivo de registros en la línea de comandos y consulte siempre el archivo de registros después de ejecutar el cmdlet. Si un script falla, compruebe y corrija el error identificado en el archivo de registros y, a continuación, ejecute el cmdlet de nuevo.

## Información útil

- Para facilitar la entrega de aplicaciones mientras hay dos implementaciones ejecutándose (la comunidad de XenApp 6.x y el nuevo sitio de XenApp 7.6), puede realizar un agregado de ambas implementaciones en StoreFront o la Interfaz Web. Consulte la documentación de la versión de StoreFront o la Interfaz Web que esté utilizando.
- Los datos de iconos de las aplicaciones se pueden gestionar de dos formas:
  - Si especifica el parámetro `EmbedIconData` en el cmdlet `Export-XAFarm`, los datos de iconos de aplicaciones se incrustan en el archivo XML.
  - Si no especifica el parámetro `EmbedIconData` en el cmdlet `Export-XAFarm`, los datos de iconos de aplicaciones exportados se almacenan en una carpeta cuyo nombre se forma al agregar la cadena “-icons” al nombre básico del archivo XML de salida. Por ejemplo, si el parámetro `XmlOutputFile` es “FarmData.xml”, se creará la carpeta “FarmData-icons” para almacenar los iconos de aplicaciones.

Los archivos de datos de iconos de esta carpeta son archivos .txt nombrados mediante el nombre de explorador de la aplicación publicada (aunque los archivos son .txt, los datos guardados son datos de icono binarios codificados que el script de importación puede leer para volver a crear el icono de la aplicación). Durante la operación de importación, si la carpeta de iconos no se encuentra en la misma ubicación que el archivo XML de importación, se usan iconos genéricos para cada aplicación importada.

- Los nombres de los módulos de script, archivos de manifiesto, módulo compartido y cmdlets son similares. Ponga cuidado al utilizar el procedimiento de completar con tabulador, para evitar errores. Por ejemplo, `Export-XAFarm` es un cmdlet. `ExportXAFarm.psd1` y `ExportXAFarm.psm1` son archivos que no se pueden ejecutar.
- En las secciones paso a paso siguientes, la mayoría de los valores de parámetro de <cadena> van entre comillas. Estas son optativas si la cadena solo es de una palabra.

## Para exportar desde el servidor XenApp 6.x

- La exportación debe ejecutarse en un servidor XenApp 6.x configurado con el modo de servidor Controller y host de sesión (comúnmente llamado Controller).
- Para ejecutar los cmdlets de exportación, hay que ser un administrador XenApp con permisos para leer objetos. También hay que tener suficientes permisos de Windows para ejecutar scripts de PowerShell; los procedimientos paso a paso siguientes contienen instrucciones.
- Asegúrese de que el estado de integridad de la comunidad XenApp 6.x es correcto antes de comenzar una exportación. Haga una copia de seguridad de la base de datos de la comunidad. Verifique la integridad de la comunidad con la utilidad Citrix IMA Helper ([CTX133983](#)). En la

ficha IMA Datastore, ejecute Master Check. A continuación, use la opción DSCheck para resolver las entradas no válidas. Repare cualquier problema que haya en la comunidad, antes de realizar la migración, para evitar fallos de exportación. Por ejemplo, si un servidor no se quitó correctamente de la comunidad, es posible que sus datos sigan existiendo en la base de datos; esto puede hacer que fallen los cmdlets del script de exportación (por ejemplo, Get-XAServer -ZoneName). Si los cmdlets fallan, el script falla.

- Puede ejecutar los cmdlets de exportación en una comunidad de servidores en ejecución, con conexiones de usuario activas, ya que los scripts de exportación solo leen los datos estáticos de directivas y configuración de la comunidad.

### **Para importar en el servidor XenApp 7.6**

- Puede importar datos a las implementaciones de XenApp 7.6 (y versiones posteriores admitidas). Debe instalar un Controller de XenApp 7.6 y Studio, y crear un sitio, antes de importar los datos exportados desde la comunidad XenApp 6.x. Aunque los VDA no son necesarios para importar configuraciones, permiten que los tipos de archivo de las aplicaciones estén disponibles.
- Para ejecutar los cmdlets de importación de XenApp, debe ser un administrador XenApp con permisos para leer y crear objetos. Un administrador total tiene estos permisos. También hay que tener suficientes permisos de Windows para ejecutar scripts de PowerShell; los procedimientos paso a paso siguientes contienen instrucciones.
- No debe haber otras conexiones de usuario activas durante una importación. Los scripts de importación crean muchos objetos nuevos y pueden producirse interrupciones si hay otros usuarios cambiando la configuración al mismo tiempo.

Recuerde que puede exportar datos y, a continuación, usar el parámetro -Preview con los cmdlets de importación para tener una vista previa de lo que sucedería durante una importación real, sin importar nada todavía. Los registros indicarán exactamente lo que sucedería durante la importación; si se producen errores, resuélvalos antes de iniciar la importación real.

### **Exportar datos: paso a paso**

Complete los siguientes pasos para exportar datos desde un Controller de XenApp 6.x a archivos XML.

1. Descargue el paquete de la herramienta de migración XAMigration.zip desde el sitio de descargas de Citrix. Para mayor comodidad, colóquelo en un recurso compartido de archivos en la red, al que tengan acceso tanto la comunidad XenApp 6.x como el sitio XenApp 7.6. Descomprima XAMigration.zip en el recurso compartido de archivos en la red. Se descomprimirá en otros dos archivos zip: ReadIMA.zip e ImportFMA.zip.

2. Inicie la sesión en el Controller de XenApp 6.x como un administrador de XenApp con, al menos, permiso de solo lectura y permisos de Windows para ejecutar scripts de PowerShell.
3. Copie ReadIMA.zip desde el recurso compartido de archivos de la red al Controller de XenApp 6.x. Descomprima y extraiga el contenido de ReadIMA.zip en el Controller en una carpeta (por ejemplo: C:\XAMigration).
4. Abra una consola de PowerShell y establezca como directorio actual el directorio donde se encuentran los scripts. Por ejemplo: `cd C:\XAMigration`.
5. Ejecute `Get-ExecutionPolicy` para consultar la directiva de ejecución de scripts.
6. Establezca la directiva de ejecución de scripts como, al menos, `RemoteSigned` para permitir que los scripts se ejecuten. Por ejemplo: `Set-ExecutionPolicy RemoteSigned`.
7. Importe los archivos de definición de módulos `ExportPolicy.psd1` y `ExportXAFarm.psd1`:  
`Import-Module .\ExportPolicy.psd1` y `Import-Module .\ExportXAFarm.psd1`.

### Información útil

- Si va a exportar solo datos de directivas, importe solo el archivo de definición de módulos `ExportPolicy.psd1`. Del mismo modo, si va a importar solo los datos de la comunidad, importe solo `ExportXAFarm.psd1`.
  - Al importar los archivos de definición de módulos también se agregan los complementos de PowerShell requeridos.
  - No importe los archivos de script `.psm1`.
8. Para exportar datos de directiva y datos de comunidad, ejecute los siguientes cmdlets.

Datos de directiva: ejecute `Export-Policy`.

Parámetro	Descripción
<code>-XmlOutputFile "cadena.xml"</code>	Nombre del archivo XML resultante; este archivo contendrá los datos exportados. Debe tener la extensión <code>.xml</code> . El archivo no debe existir previamente, pero si se especifica una ruta, la ruta sí debe existir. Valor predeterminado: Ninguno; este parámetro es obligatorio.

Parámetro	Descripción
-LogFile <i>cadena</i>	El nombre del archivo de registros. La extensión es optativa. Si aún no existe, el archivo se creará. Si el archivo existe y se especifica también el parámetro NoClobber, se genera un error; de lo contrario, el contenido del archivo se sobrescribe. Valor predeterminado: Consulte Capturar registros y controlar errores.
-NoLog	No se generan registros. Este parámetro anula el parámetro LogFile si ambos están especificados. Valor predeterminado: False; se generan registros
-NoClobber	No sobrescribir el archivo de registros existente especificado en el parámetro LogFile. Si el archivo de registros no existe, este parámetro no tiene ningún efecto. Valor predeterminado: False; si el archivo de registros ya existe, se sobrescribe
-NoDetails	No enviar a la consola informes detallados acerca de la ejecución de los scripts. Valor predeterminado: False; se envían informes detallados a la consola
-SuppressLogo	No imprimir el mensaje “XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #aaaaMMdd-hhmm#” en la consola. Este mensaje identifica la versión del script y puede resultar útil durante la solución de problemas. Citrix recomienda omitir este parámetro. Valor predeterminado: False; el mensaje se imprime en la consola

Ejemplo: El cmdlet siguiente exporta la información sobre directivas al archivo XML denominado MyPolicies.xml. La operación genera registros que se guardan en el archivo MyPolicies.log.

```
Export-Policy -XmlOutputFile ".\MyPolicies.XML"-LogFile ".\MyPolicies
.Log"
```

Datos de comunidad: ejecute `Export-XAFarm`.

---

Parámetro	Descripción
XmlOutputFile “cadena.xml”	Nombre del archivo XML resultante; este archivo contendrá los datos exportados. Debe tener la extensión .xml. El archivo no debe existir previamente, pero si se especifica una ruta, la ruta sí debe existir. Valor predeterminado: Ninguno; este parámetro es obligatorio.
-LogFile “cadena”	El nombre del archivo de registros. La extensión es optativa. Si aún no existe, el archivo se creará. Si el archivo existe y se especifica también el parámetro NoClobber, se genera un error; de lo contrario, el contenido del archivo se sobrescribe. Valor predeterminado: Consulte Capturar registros y controlar errores.
-NoLog	No se generan registros. Este parámetro anula el parámetro LogFile si ambos están especificados. Valor predeterminado: False; se generan registros
-NoClobber	No sobrescribir el archivo de registros existente especificado en el parámetro LogFile. Si el archivo de registros no existe, este parámetro no tiene ningún efecto. Valor predeterminado: False; si el archivo de registros ya existe, se sobrescribe
-NoDetails	No enviar a la consola informes detallados acerca de la ejecución de los scripts. Valor predeterminado: False; se envían informes detallados a la consola
-SuppressLogo	No imprimir el mensaje “XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #aaaaMMdd-hhmm#” en la consola. Este mensaje identifica la versión del script y puede resultar útil durante la solución de problemas. Citrix recomienda omitir este parámetro. Valor predeterminado: False; el mensaje se imprime en la consola

Parámetro	Descripción
-IgnoreAdmins	No exportar la información de administradores. Consulte Uso avanzado. Valor predeterminado: False; se exporta la información sobre administradores
-IgnoreApps	No exportar información de aplicaciones. Consulte Uso avanzado. Valor predeterminado: False; se exporta la información sobre aplicaciones
-IgnoreServers	No exportar información de servidores. Valor predeterminado: False; se exporta la información sobre servidores
-IgnoreZones	No exportar información de zonas. Valor predeterminado: False; se exporta la información sobre zonas
-IgnoreOthers	No exportar otros tipos de información como el registro de configuración, los patrones de carga, las directivas de equilibrio de carga, los controladores de impresora y los grupos de trabajo. Valor predeterminado: False; se exportan otros tipos de información. La finalidad de este modificador de línea de comandos es permitir continuar una exportación aunque haya un error, siempre que el error no afecte a los datos en sí utilizados en el proceso de importación o exportación.
-AppLimit <i>número entero</i>	Cantidad de aplicaciones a exportar. Consulte Requisitos, preparación y procedimientos recomendados. Valor predeterminado: se exportan todas las aplicaciones
-EmbedIconData	Incrustar los datos de iconos de aplicaciones en el mismo archivo XML donde están los otros objetos. Valor predeterminado: los iconos se guardan por separado. Consulte Requisitos, preparación y procedimientos recomendados.
-SkipApps <i>número entero</i>	Cantidad de aplicaciones a omitir. Consulte Uso avanzado. Valor predeterminado: no se omite ninguna aplicación

Ejemplo: El cmdlet siguiente exporta la información sobre la comunidad al archivo XML denominado MyFarm.xml. La operación genera registros que se guardan en el archivo MyFarm.log. Se crea una carpeta denominada “MyFarm-icons” para almacenar los archivos de datos de iconos de las aplicaciones; esta carpeta está en la misma ubicación que MyFarm.XML.

```
Export-XAFarm -XmlOutputFile ".\MyFarm.XML"-LogFile ".\MyFarm.Log"
```

Una vez ejecutados los scripts de exportación, los archivos XML especificados en las líneas de comandos contienen los datos de la comunidad XenApp y las directivas. Los archivos de iconos de aplicaciones contienen archivos de datos de icono, y el archivo de registros indica qué ocurrió durante la exportación.

### Importar datos: paso a paso

Recuerde que puede ejecutar una vista previa de la importación (mediante los comandos `Import-Policy` o `Import-XAFarm` con el parámetro `Preview`) y consultar los archivos de registros antes de realizar la importación propiamente dicha.

Complete los siguientes pasos para importar datos a un sitio de XenApp 7.6, mediante los archivos XML generados en la exportación.

1. Inicie una sesión en el Controller de XenApp 7.6 como administrador con permisos de lectura/escritura y con permisos Windows para ejecutar scripts de PowerShell.
2. Si aún no ha descomprimido el paquete de la herramienta de migración XAMigration en el recurso compartido de archivos de la red, descomprímalo ahora. Copie ImportFMA.zip desde el recurso compartido de archivos de la red al Controller de XenApp 7.6. Descomprima y extraiga el contenido de ImportFMA.zip en el Controller en una carpeta (por ejemplo: C:\XAMigration).
3. Copie los archivos XML (los archivos de salida generados durante la exportación) desde el Controller de XenApp 6.x a la misma ubicación del Controller de XenApp 7.6 donde extrajo los archivos de ImportFMA.zip.

Si eligió no incrustar los datos de iconos de aplicaciones en el archivo XML de salida al ejecutar el cmdlet `Export-XAFarm`, asegúrese de que copia la carpeta y los archivos de los datos de iconos en la misma ubicación del Controller de XenApp 7.6 donde ya se encuentra el archivo XML de salida que contiene los datos de aplicaciones y los archivos extraídos de ImportFMA.zip.

4. Abra una consola de PowerShell y establezca como directorio actual el directorio donde se encuentran los scripts: `cd C:\XAMigration`.
5. Ejecute `Get-ExecutionPolicy` para consultar la directiva de ejecución de scripts.
6. Establezca la directiva de ejecución de scripts como, al menos, `RemoteSigned` para permitir que los scripts se ejecuten. Por ejemplo: `Set-ExecutionPolicy RemoteSigned`.

7. Importe los archivos de definición de módulos `ImportPolicy.psd1` y `ImportXAFarm.psd1` de PowerShell: `Import-Module .\ImportPolicy.psd1` y `Import-Module .\ImportXAFarm.psd1`.

**Información útil:**

- Si va a importar solo datos de directivas, importe solo el archivo de definición de módulos `ImportPolicy.psd1`. Del mismo modo, si va a importar solo los datos de la comunidad, importe solo `ImportXAFarm.psd1`.
- Al importar los archivos de definición de módulos también se agregan los complementos de PowerShell requeridos.
- No importe los archivos de script `.psm1`.

8. Para importar datos de directiva y datos de comunidad, ejecute los siguientes cmdlets.

Datos de directiva: Ejecute `Import-Policy`. Deberá especificar el archivo XML que contiene los datos exportados de las directivas.

Parámetro	Descripción
<code>-XmlInputFile "cadena.xml"</code>	Nombre del archivo XML de entrada; este archivo contiene los datos recopilados tras ejecutar el cmdlet <code>Export-Policy</code> . Debe tener la extensión <code>.xml</code> . Valor predeterminado: Ninguno; este parámetro es obligatorio.
<code>-XsdFile "cadena"</code>	Nombre del archivo XSD. Los scripts de importación usan este archivo para validar la sintaxis del archivo XML de entrada. Consulte <a href="#">Uso avanzado</a> . Valor predeterminado: <code>PolicyData.XSD</code>
<code>-LogFile "cadena"</code>	El nombre del archivo de registros. Si copió los archivos de registros de exportación en este servidor, use un nombre de archivo distinto para los registros del cmdlet de importación. Valor predeterminado: Consulte <a href="#">Capturar registros y controlar errores</a> .
<code>-NoLog</code>	No se generan registros. Este parámetro anula el parámetro <code>LogFile</code> si ambos están especificados. Valor predeterminado: <code>False</code> ; se generan registros

Parámetro	Descripción
-NoClobber	No sobrescribir el archivo de registros existente especificado en el parámetro LogFile. Si el archivo de registros no existe, este parámetro no tiene ningún efecto. Valor predeterminado: False; si el archivo de registros ya existe, se sobrescribe
-NoDetails	No enviar a la consola informes detallados acerca de la ejecución de los scripts. Valor predeterminado: False; se envían informes detallados a la consola
-SuppressLogo	No imprimir el mensaje “XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #aaaaMMdd-hhmm#” en la consola. Este mensaje identifica la versión del script y puede resultar útil durante la solución de problemas. Citrix recomienda omitir este parámetro. Valor predeterminado: False; el mensaje se imprime en la consola
-Preview	Realizar una vista previa de la importación: leer los datos del archivo XML de entrada, pero sin importar los objetos en el sitio. El archivo de registros y la consola indican qué ocurre durante la vista previa de la importación. La vista previa muestra a los administradores lo que sucedería durante una importación real. Valor predeterminado: False; se produce una importación real

Ejemplo: El cmdlet siguiente importa la información sobre directivas desde el archivo XML denominado MyPolicies.xml. La operación genera registros que se guardan en el archivo MyPolicies.log.

```
Import-Policy -XmlInputFile ".\MyPolicies.XML"-LogFile ".\MyPolicies.Log"
```

Aplicaciones: Ejecute `Import-XAFarm`. Deberá especificar un archivo de registros y el archivo XML que contiene los datos exportados de la comunidad de servidores.

---

Parámetro	Descripción
-XmlInputFile “cadena.xml”	Nombre del archivo XML de entrada; este archivo contiene los datos recopilados tras ejecutar el cmdlet Export-XAFarm. Debe tener la extensión .xml. Valor predeterminado: Ninguno; este parámetro es obligatorio.
-XsdFile “cadena”	Nombre del archivo XSD. Los scripts de importación usan este archivo para validar la sintaxis del archivo XML de entrada. Consulte Uso avanzado. Valor predeterminado: XAFarmData.XSD
-LogFile “cadena”	El nombre del archivo de registros. Si copió los archivos de registros de exportación en este servidor, use un nombre de archivo distinto para los registros del cmdlet de importación. Valor predeterminado: Consulte Capturar registros y controlar errores.
-NoLog	No se generan registros. Este parámetro anula el parámetro LogFile si ambos están especificados. Valor predeterminado: False; se generan registros
-NoClobber	No sobrescribir el archivo de registros existente especificado en el parámetro LogFile. Si el archivo de registros no existe, este parámetro no tiene ningún efecto. Valor predeterminado: False; si el archivo de registros ya existe, se sobrescribe
-NoDetails	No enviar a la consola informes detallados acerca de la ejecución de los scripts. Valor predeterminado: False; se envían informes detallados a la consola
-SuppressLogo	No imprimir el mensaje “XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #aaaaMMdd-hhmm#” en la consola. Este mensaje identifica la versión del script y puede resultar útil durante la solución de problemas. Citrix recomienda omitir este parámetro. Valor predeterminado: False; el mensaje se imprime en la consola

---

Parámetro	Descripción
-Preview	Realizar una vista previa de la importación: leer los datos del archivo XML de entrada, pero sin importar los objetos en el sitio. El archivo de registros y la consola indican qué ocurre durante la vista previa de la importación. La vista previa muestra a los administradores lo que sucedería durante una importación real. Valor predeterminado: False; se produce una importación real
-DeliveryGroupName “cadena”	Nombre del grupo de entrega para todas las aplicaciones importadas. Consulte Uso avanzado. Valor predeterminado: “nombre de la comunidad XenApp - Delivery Group”
-MatchFolder “cadena”	Importar solo las aplicaciones que se encuentran en carpetas cuyos nombres coinciden con la cadena suministrada. Consulte Uso avanzado. Valor predeterminado: no se realiza ninguna búsqueda de coincidencias.
-NotMatchFolder “cadena”	Importar solo las aplicaciones que se encuentran en carpetas cuyos nombres no coinciden con la cadena suministrada. Consulte Uso avanzado. Valor predeterminado: no se realiza ninguna búsqueda de coincidencias.
-MatchServer “cadena”	Importar solo las aplicaciones que se encuentran en servidores cuyos nombres coinciden con la cadena suministrada. Consulte Uso avanzado.
-NotMatchServer “cadena”	Importar solo las aplicaciones que se encuentran en servidores cuyos nombres no coinciden con la cadena suministrada. Consulte Uso avanzado. Valor predeterminado: no se realiza ninguna búsqueda de coincidencias.
-MatchWorkerGroup “cadena”	Importar solo las aplicaciones publicadas para grupos de trabajo cuyos nombres coinciden con la cadena suministrada. Consulte Uso avanzado. Valor predeterminado: no se realiza ninguna búsqueda de coincidencias.

Parámetro	Descripción
-NotMatchWorkerGroup “cadena”	Importar solo las aplicaciones publicadas para grupos de trabajo cuyos nombres no coinciden con la cadena suministrada. Consulte Uso avanzado. Valor predeterminado: no se realiza ninguna búsqueda de coincidencias.
-MatchAccount “cadena”	Importar solo las aplicaciones publicadas para cuentas de usuarios cuyos nombres coinciden con la cadena suministrada. Consulte Uso avanzado. Valor predeterminado: no se realiza ninguna búsqueda de coincidencias.
-NotMatchAccount “cadena”	Importar solo las aplicaciones publicadas para cuentas de usuarios cuyos nombres no coinciden con la cadena suministrada. Consulte Uso avanzado. Valor predeterminado: no se realiza ninguna búsqueda de coincidencias.
-IncludeStreamedApps	Importar aplicaciones del tipo: “StreamedToClientOrServerInstalled”(No se importan otras aplicaciones de streaming.) Valor predeterminado: las aplicaciones de streaming no se importan.
-IncludeDisabledApps	Importar aplicaciones que se han marcado como inhabilitadas. Valor predeterminado: las aplicaciones inhabilitadas no se importan

Ejemplo: El cmdlet siguiente importa aplicaciones desde el archivo XML denominado MyFarm.xml. La operación genera registros que se guardan en el archivo MyFarm.log.

```
Import-xAFarm -XmlInputFile ".\MyFarm.XML"-LogFile ".\MyFarm.Log"
```

Una vez completada correctamente la migración, hay que realizar las tareas posteriores a la migración.

### Tareas posteriores a la migración

Una vez importadas las directivas y la configuración de la comunidad de XenApp 6.x en un sitio de XenApp 7.6, siga las siguientes instrucciones para asegurarse de que los datos se han importado correctamente.

## Directivas y configuraciones de directivas

La importación de directivas es fundamentalmente una operación de copia, con la excepción de las directivas y configuraciones que se han retirado y, por tanto, no se importan. La comprobación posterior a la migración consiste en comparar ambas partes.

1. El archivo de registros enumera todas las directivas y las configuraciones de directiva que se han importado y que se han omitido. Primero, revise el archivo de registros e identifique qué configuraciones y directivas no se importaron.
2. Compare las directivas de XenApp 6.x con las directivas importadas en XenApp 7.6. Los valores de las configuraciones deben quedar igual (excepto en el caso de las configuraciones retiradas, como se indica en el paso siguiente).
  - Si la cantidad de directivas es pequeña, puede realizar una comparación visual entre las directivas que aparecen en AppCenter en XenApp 6.x y las directivas que aparecen en Studio en XenApp 7.6.
  - Si cuenta con una gran cantidad de directivas, puede que no sea posible hacer una comparación visual. En estos casos, use el cmdlet de exportación de directivas (Export-Policy) para exportar las directivas de XenApp 7.6 a un archivo XML diferente y, a continuación, use una herramienta de comparación de texto (como windiff) para comparar los datos de ese archivo con los datos que aparecen en el archivo XML usado durante la exportación de directivas desde XenApp 6.x.
3. Use la información de la sección Configuraciones de directivas que no se importan para determinar qué puede haber cambiado durante la importación. Si una directiva de XenApp 6.x solo contiene configuraciones retiradas, la directiva no se importará. Por ejemplo, si una directiva de XenApp 6.x solo contiene configuraciones de pruebas de HMR, dicha directiva se omitirá por completo porque no hay ninguna configuración equivalente admitida en XenApp 7.6.

Algunas configuraciones de directiva de XenApp 6.x ya no se admiten, pero la funcionalidad equivalente está implementada en XenApp 7.6. Por ejemplo, en XenApp 7.6, puede configurar una programación de reinicios para las máquinas con sistema operativo de servidor mediante la modificación de un grupo de entrega; esta funcionalidad se implementaba antes mediante configuraciones de directiva.

4. Revise y confirme cómo se aplicarán los filtros al sitio de XenApp 7.6 frente a cómo se usaban en XenApp 6.x; las diferencias significativas entre la comunidad XenApp 6.x y el sitio XenApp 7.6 pueden cambiar el efecto de los filtros.

**Filtros**

Examine con cuidado los filtros para cada directiva. Puede que sea necesario hacer cambios para asegurarse de que funcionen en XenApp 7.6 como funcionaban originalmente en XenApp 6.x.

---

Filtrar	Consideraciones
Control de acceso	El control de acceso debe tener los mismos valores que los filtros originales de XenApp 6.x y debe funcionar sin necesidad de hacer cambios.
Citrix CloudBridge	Un valor booleano; debe funcionar sin necesidad de hacer cambios. (Ahora, este producto se denomina NetScaler SD-WAN.)
Dirección IP del cliente	Enumera los intervalos de direcciones IP de cliente; cada intervalo se permite o se deniega. El script de importación conserva los valores, pero puede ser necesario hacer cambios si diferentes clientes se conectan a las máquinas VDA de XenApp 7.6.
Nombre del cliente	Al igual que sucede con el filtro de dirección IP de cliente, el script de importación conserva los valores, pero puede ser necesario hacer cambios si diferentes clientes se conectan a las máquinas VDA de XenApp 7.6.

Filtrar	Consideraciones
Unidad organizativa	<p>Los valores pueden conservarse, dependiendo de si las OU se pueden resolver en el momento de la importación. Revise cuidadosamente este filtro, especialmente si las máquinas de XenApp 6.x y de XenApp 7.6 residen en dominios diferentes. Si no se configuran los valores de filtro correctamente, la directiva podría aplicarse a un conjunto incorrecto de unidades organizativas. Las unidades organizativas están representadas solo por nombres, por lo que existe la posibilidad de que el nombre de una unidad organizativa se resuelva incorrectamente con una unidad organizativa distinta que contenga miembros diferentes de unidades organizativas del dominio de XenApp 6.x. Incluso aunque se conserven algunos valores del filtro de unidad organizativa, es necesario revisar cuidadosamente esos valores.</p>
Usuario o grupo	<p>Los valores pueden conservarse, dependiendo de si las cuentas se pueden resolver en el momento de la importación. Al igual que ocurre con las unidades organizativas, las cuentas se resuelven mediante solo sus nombres. Por lo tanto, si el sitio de XenApp 7.6 tiene un dominio con el mismo nombre y los mismos nombres de usuario, pero en realidad se trata de dos dominios y conjuntos de usuarios distintos, puede suceder que las cuentas se resuelvan incorrectamente con usuarios diferentes de los usuarios de dominio de XenApp 6.x. Si no se revisan y modifican los valores de los filtros según sea necesario, las directivas pueden aplicarse incorrectamente.</p>

Filtrar	Consideraciones
Grupo de trabajo	Los grupos de trabajo no se admiten en XenApp 7.6. Considere la posibilidad de usar filtros de Grupo de entrega, Tipo de grupo de entrega y Etiqueta, que sí se admiten en XenApp 7.6 (no en XenApp 6.x). <b>Grupo de entrega:</b> Permite aplicar directivas basadas en grupos de entrega. Cada entrada de filtro especifica un grupo de entrega y puede permitirse o denegarse. <b>Tipo de grupo de entrega:</b> Permite aplicar directivas basadas en tipos de grupos de entrega. Cada filtro especifica un tipo de grupo de entrega, que puede permitirse o denegarse. <b>Etiqueta:</b> Especifica la aplicación de directivas basándose en etiquetas creadas para las máquinas VDA. Cada etiqueta se puede permitir o denegar.

---

En resumen, los filtros relacionados con cambios de usuarios de dominio necesitan más atención si la comunidad XenApp 6.x y el sitio XenApp 7.6 están en dominios diferentes. Debido a que el script de importación solo utiliza cadenas de nombres de dominio y de nombres de usuario para resolver los usuarios en el nuevo dominio, algunas de las cuentas pueden resolverse correctamente y otras no. Aunque solo exista una pequeña posibilidad de que los distintos dominios y usuarios tengan los mismos nombres, debe revisar cuidadosamente estos filtros para asegurarse de que contienen los valores correctos.

## Aplicaciones

Los scripts de importación de aplicaciones no solo importan aplicaciones, sino que también crean objetos como por ejemplo, grupos de entrega. Si la importación de aplicaciones se realiza en varias iteraciones, la jerarquía de las carpetas de aplicaciones original puede cambiar considerablemente.

1. Primero, lea los archivos de registros de la migración, que contienen detalles sobre qué aplicaciones se importaron y cuáles se omitieron, y los cmdlets que se usaron para crear las aplicaciones.
2. Para cada aplicación:
  - Compruebe visualmente que se conservaron sus propiedades básicas durante la importación. Use la información de Asignación de propiedades de aplicaciones para

determinar qué propiedades se importaron sin cambios, cuáles no se importaron y cuáles se inicializaron con los datos de aplicación de XenApp 6.x.

- Compruebe la lista de usuarios. El script de importación importa automáticamente la lista explícita de usuarios en la lista “Limitar visibilidad” de la aplicación en XenApp 7.6. Compruebe que la lista queda igual.
3. Los servidores de aplicaciones no se importan. Esto significa que no se puede acceder todavía a ninguna de las aplicaciones importadas. Es necesario asignar catálogos de máquinas a los grupos de entrega que contienen estas aplicaciones. Los catálogos contienen las máquinas que tienen las imágenes ejecutables de las aplicaciones publicadas. Para cada aplicación:
- Asegúrese de que el nombre del archivo ejecutable y el directorio de trabajo hacen referencia a un ejecutable que existe en las máquinas asignadas al grupo de entrega (a través de los catálogos de máquinas).
  - Compruebe un parámetro de línea de comandos (que puede ser cualquier cosa como, por ejemplo, un nombre de archivo, una variable de entorno, o el nombre del ejecutable). Verifique que el parámetro es válido para todas las máquinas de los catálogos de máquinas asignadas al grupo de entrega.

## Archivos de registros

Los archivos de registros son el recurso de referencia más importante durante las operaciones de importación y exportación. Esta es la razón por la cual los archivos de registros existentes no se sobrescriben de forma predeterminada y los nombres de los archivos de registros predeterminados son únicos.

Como se indica en [Capturar registros y controlar errores](#), si se quiere usar una captura de registros adicional con los cmdlets de PowerShell `Start-Transcript` y `Stop-Transcript` (que graban todo lo que se escribe y se imprime en la consola), sus resultados, junto con el archivo de registros, ofrecen una referencia completa de toda la actividad de importación y exportación.

Gracias a las marcas de hora incluidas en los archivos de registros se pueden diagnosticar ciertos problemas. Por ejemplo, si una exportación o importación tardó mucho tiempo en ejecutarse, se puede averiguar si la causa fue una conexión de base de datos defectuosa o algún problema al resolver las cuentas de usuario.

Los comandos grabados en los archivos de registros también indican cómo se leen o se crean algunos objetos. Por ejemplo, para crear un grupo de entrega, se ejecutan varios comandos no solo para crear el grupo de entrega propiamente dicho, sino también otros objetos tales como reglas de directivas de acceso que permiten asignar objetos de aplicación al grupo de entrega.

El archivo de registros se puede usar también para diagnosticar un fallo de importación o exportación. Por lo general, las últimas líneas del archivo de registros indican la causa del fallo; el mensaje de error

del fallo también se guarda en el archivo de registros. Junto con el archivo XML, el archivo de registros se puede usar para determinar qué objeto estuvo implicado en el fallo.

Después de revisar y hacer pruebas en la migración:

1. Actualice sus servidores de trabajo XenApp 6.5 con los VDA (Virtual Delivery Agent) actuales ejecutando el instalador de la versión 7.6 en el servidor, lo que quitará el software de XenApp 6.5 e instalará automáticamente el VDA actualizado. Para obtener instrucciones al respecto, consulte [Actualización de un servidor de trabajo de XenApp 6.5 a un nuevo VDA para SO de servidor Windows](#).

En el caso de servidores de trabajo con XenApp 6.0, es necesario desinstalar manualmente el software de XenApp 6.0 del servidor. A continuación, puede usar el instalador de la versión 7.6 para instalar el VDA actual. No se puede usar el instalador de la versión 7.6 para quitar automáticamente el software de XenApp 6.0.

2. En Studio, en el nuevo sitio de XenApp, cree catálogos de máquinas (o modifique los catálogos existentes) para los servidores de trabajo actualizados.
3. Agregue las máquinas actualizadas desde el catálogo de máquinas a los grupos de entrega que contengan las aplicaciones instaladas en los VDA para SO de servidor Windows.

## Uso avanzado

De forma predeterminada, el cmdlet `Export-Policy` exporta todos los datos de directiva a un archivo XML. Del mismo modo, `Export-XAFarm` exporta todos los datos de comunidad a un archivo XML. Se pueden usar parámetros de línea de comandos para controlar con más detalle qué se exporta y se importa.

### Exportar aplicaciones parcialmente

Si tiene una gran cantidad de aplicaciones y quiere controlar cuántas de ellas se exportan al archivo XML, use los parámetros siguientes:

- `AppLimit`: Especifica la cantidad de aplicaciones a exportar.
- `SkipApps`: Especifica la cantidad de aplicaciones a omitir antes de exportar las aplicaciones subsiguientes.

Puede usar ambos parámetros para exportar una gran cantidad de aplicaciones en fragmentos más manejables. Por ejemplo, supongamos que la primera vez que ejecuta `Export-XAFarm`, quiere exportar solo las primeras 200 aplicaciones; para ello, especifique ese valor en el parámetro `AppLimit`.

```
Export-XAFarm -XmlOutputFile "Apps1-200.xml"
```

La siguiente vez que ejecute `Export-XAFarm`, quiere exportar las 100 aplicaciones siguientes; para ello, use el parámetro `SkipApps` para descartar las aplicaciones que ya exportó antes (las primeras 200) y el parámetro `AppLimit` para exportar las 100 aplicaciones siguientes.

```
Export-XAFarm -XmlOutputFile "Apps201-300.xml"-AppLimit "100"-SkipApps "200"
```

### No exportar determinados objetos

Algunos objetos pueden omitirse y no es necesario exportarlos, como es el caso, en particular, de los objetos que no se importan. Consulte Configuraciones de directivas que no se importan y Asignación de propiedades de aplicaciones. Utilice los siguientes parámetros para evitar que se exporten objetos innecesarios:

- `IgnoreAdmins`: No exportar los objetos de administrador
- `IgnoreServers`: No exportar los objetos de servidor
- `IgnoreZones`: No exportar los objetos de zona
- `IgnoreOthers`: No exportar objetos de registro de configuración, patrones de carga, directivas de equilibrio de carga, controladores de impresora y grupos de trabajo
- `IgnoreApps`: No exportar aplicaciones. Permite exportar otros datos a un archivo XML de salida y, a continuación, ejecutar de nuevo la exportación para exportar las aplicaciones a otro archivo XML de salida distinto.

También se puede usar estos parámetros para solucionar los problemas que podrían provocar el fallo de la exportación. Por ejemplo, si tiene un servidor defectuoso en una zona, la exportación de la zona podría fallar; si incluye el parámetro `IgnoreZones`, la exportación continúa con otros objetos.

### Nombres de grupo de entrega

Si no quiere incluir todas las aplicaciones en un mismo grupo de entrega (por ejemplo, porque acceden a ellas diferentes conjuntos de usuarios y están publicadas en diferentes conjuntos de servidores), puede ejecutar `Import-XAFarm` varias veces, especificando distintas aplicaciones y un grupo de entrega diferente cada vez. Aunque se pueden usar cmdlets de PowerShell para mover las aplicaciones desde un grupo de entrega a otro después de la migración, la importación selectiva en grupos de entrega determinados puede reducir o eliminar el esfuerzo de mover las aplicaciones más tarde.

- Use el parámetro `DeliveryGroupName` con el cmdlet `Import-XAFarm`. El script crea el grupo de entrega especificado si éste no existe.
- Utilice los siguientes parámetros con expresiones regulares para filtrar las aplicaciones que se importan en el grupo de entrega, en función de carpetas, grupos de trabajo, cuentas de usuario y/o nombres de servidores. Se recomienda poner la expresión regular entre comillas simples o

dobles. Para obtener información sobre expresiones regulares, consulte <https://docs.microsoft.com/en-us/dotnet/standard/base-types/regular-expressions?redirectedfrom=MSDN>.

- **MatchWorkerGroup** y **NotMatchWorkerGroup**: Por ejemplo, para aplicaciones publicadas en grupos de trabajo, el siguiente cmdlet importa las aplicaciones del grupo de trabajo llamado “Productivity Apps” a un grupo de entrega de XenApp 7.6 con el mismo nombre:

```
Import-XAFarm -XmlInputFile XAFarm.xml -LogFile XAFarmImport.log -MatchWorkerGroup 'Productivity Apps' -DeliveryGroupName 'Productivity Apps'
```

- **MatchFolder** y **NotMatchFolder**: Por ejemplo, para aplicaciones organizadas en carpetas, el siguiente cmdlet importa las aplicaciones de la carpeta “Productivity Apps” a un grupo de entrega de XenApp 7.6 con el mismo nombre.

```
Import-XAFarm -XmlInputFile XAFarm.xml -LogFile XAFarmImport.log -MatchFolder 'Productivity Apps' -DeliveryGroupName 'Productivity Apps'
```

Por ejemplo, el siguiente cmdlet importa en el grupo de entrega predeterminado todas aquellas aplicaciones de cualquier carpeta cuyo nombre contenga “MS Office Apps”.

```
Import-XAFarm -XmlInputFile .\TheFarmApps.XML -MatchFolder ".*\/MS Office Apps\/.*"
```

- **MatchAccount** y **NotMatchAccount**: Por ejemplo, para aplicaciones publicadas para usuarios y grupos de usuarios de Active Directory, el siguiente cmdlet importa las aplicaciones publicadas para el grupo de usuarios “Finance Group” a un grupo de entrega de XenApp 7.6 llamado “Finance”.

```
Import-XAFarm -XmlInputFile XAFarm.xml -LogFile XAFarmImport.log -MatchAccount 'DOMAIN\\Finance Group' -DeliveryGroupName 'Finance'
```

- **MatchServer** y **NotMatchServer**: Por ejemplo, para las aplicaciones organizadas en servidores, el siguiente cmdlet importa las aplicaciones asociadas al servidor no llamado “Current” a un grupo de entrega de XenApp llamado “Legacy”.

```
Import-XAFarm -XmlInputFile XAFarm.xml -LogFile XAFarmImport.log -NotMatchServer 'Current' -DeliveryGroupName 'Legacy'
```

**Personalización** Los programadores de PowerShell pueden crear sus propias herramientas. Por ejemplo, puede usar el script de exportación como una herramienta de inventario para realizar un rastreo de los cambios en una comunidad XenApp 6.x. También puede modificar los archivos XSD (o

crear sus propios archivos XSD) para almacenar datos adicionales o datos en diferentes formatos en los archivos XML. Puede especificar un archivo XSD no predeterminado con cada uno de los cmdlets de importación.

Aunque se pueden modificar los archivos de scripts para ajustarse a requisitos de migración específicos o avanzados, la funcionalidad ofrecida se limita a los scripts no modificados. El servicio de asistencia técnica (Citrix Support) le recomendará utilizar los scripts sin modificaciones, para determinar cuál es el comportamiento esperado y ofrecer asistencia técnica, si es necesario.

## Solución de problemas

- Si usa PowerShell 2.0 y agregó el complemento Citrix Group Policy PowerShell Provider o el complemento Citrix Common Commands mediante el cmdlet `Add-PSSnapIn`, puede que aparezca un mensaje de error como el siguiente: “Referencia a objeto no establecida como instancia de un objeto” cuando ejecute los cmdlets de importación o exportación. Este error no afecta a la ejecución del script y puede ignorarse.
- Evite agregar o quitar el complemento Citrix Group Policy PowerShell Provider en la misma sesión de consola donde se usan los módulos de scripts de exportación e importación, porque esos módulos agregan automáticamente el complemento. Si agrega o quita el complemento por separado, puede que vea uno de los siguientes errores:
  - “Ya existe una unidad llamada ‘LocalGpo’”. Este error aparece cuando el complemento se agrega dos veces; el complemento intenta montar la unidad LocalGpo cuando se ha cargado y luego notifica el error.
  - “Un parámetro que no se puede encontrar coincide con el nombre de parámetro ‘Controller’”. Este error aparece cuando el complemento no ha sido agregado pero el script intenta montar la unidad. El script no tiene constancia de que el complemento se quitó. Cierre la consola e inicie una nueva sesión. En la nueva sesión, importe los módulos de scripts, no agregue ni quite el complemento por separado.
- Al importar los módulos, si hace clic con el botón secundario en un archivo PSD1 y selecciona **Abrir** o **Abrir con PowerShell**, la ventana de la consola de PowerShell se abrirá y se cerrará rápidamente hasta que detenga el proceso. Para evitar este error, introduzca el nombre completo del módulo de scripts de PowerShell directamente en la ventana de la consola de PowerShell (por ejemplo, `Import-Module .\ExportPolicy.psd1`).
- Si recibe un error de permisos al ejecutar una exportación o importación, asegúrese de que usted es un administrador de XenApp con permisos para leer objetos (para poder exportar), o para leer y crear objetos (para poder importar). También debe tener suficientes permisos de Windows para ejecutar scripts de PowerShell.
- Si la exportación falla, compruebe si la comunidad de XenApp 6.x se encuentra en un estado correcto, ejecutando las utilidades DSMaint y DSCheck en el servidor de Controller de XenApp

6.x.

- Si ejecuta una vista previa de la importación y luego ejecuta los cmdlets de importación de nuevo para una migración real, pero descubre que no se ha importado nada, compruebe si quitó el parámetro Preview de los cmdlets de importación.

## **Configuraciones de directivas que no se importan**

Las siguientes configuraciones de directiva de usuario y de equipo no se importan porque ya no se admiten. Las directivas sin filtrar nunca se importan. Las funciones y los componentes que admiten estas configuraciones han sido reemplazadas por otras tecnologías y componentes nuevos, o estas configuraciones ya no se aplican debido a cambios de arquitectura y plataforma.

## **Configuraciones de directiva de equipo que no se importan**

- Control de acceso de las conexiones
- Nivel de administración de CPU de servidor
- Resolución de direcciones DNS
- Farm name
- Almacenamiento completo de iconos en caché
- Supervisión de estado, Pruebas de supervisión de estado
- Nombre de host del servidor de licencias, Puerto del servidor de licencias
- Límite de sesiones de usuario, Límites de sesiones de administrador
- Nombre del patrón de carga
- Registro de sucesos de límites de inicios de sesión
- Porcentaje máximo de servidores con control de inicio de sesión
- Optimización de memoria, Lista de aplicaciones excluidas de la optimización de memoria, Intervalo de optimización de memoria, Programación de la optimización de memoria: día del mes, Programación de la optimización de memoria: día de la semana, Programación de la optimización de memoria: hora
- Confianza en clientes de aplicaciones sin conexión, Registro de sucesos de aplicaciones sin conexión, Periodo de licencias de aplicaciones sin conexión, Usuarios de aplicaciones sin conexión
- Pedir contraseña
- Advertencia personalizada de reinicio, Texto personalizado de advertencia de reinicio, Hora de inhabilitación de inicios de sesión por reinicio, Frecuencia de reinicio programado, Intervalo de selección de hora de reinicio programado, Fecha de comienzo del reinicio programado, Hora del reinicio programado, Intervalo de advertencias de reinicio, Comienzo de advertencias de reinicio, Advertencia de reinicios para los usuarios, Reinicios programados
- Remedo

- Confiar en solicitudes XML (configurada en StoreFront)
- Filtrado de direcciones de adaptador de IP virtual, Lista de programas para compatibilidad con IP virtual, Compatibilidad mejorada de IP virtual, Lista de programas para filtrado de direcciones de adaptador de IP virtual
- Nombre de la carga de trabajo
- Edición del producto XenApp, Modelo del producto XenApp
- Puerto de XML Service

\* Reemplazada por Asistencia remota de Windows

### **Configuraciones de directiva de usuario que no se importan**

- Conectar automáticamente puertos COM del cliente, Conectar automáticamente puertos LPT del cliente
- Redirección de puertos COM del cliente, Redirección de puertos LPT del cliente
- Nombres de impresora del cliente
- Límite de sesiones simultáneas
- Entradas de conexiones de remedo \*
- Intervalo de temporizador de desconexión de sesión persistente, Intervalo de temporizador de fin de sesión persistente
- Registrar intentos de remedo \*
- Notificar al usuario sobre conexiones de remedo pendientes \*
- Intervalo de temporizador de desconexión de sesión de preinicio, Intervalo de temporizador de fin de sesión de preinicio
- Importancia de la sesión
- Single Sign-On, almacén central de Single Sign-On
- Usuarios que pueden remedar a otros usuarios, Usuarios que no pueden remedar a otros usuarios \*

\* Reemplazada por Asistencia remota de Windows

### **Tipos de aplicaciones no importados**

Los siguientes tipos de aplicación no se importan.

- Escritorios de servidor
- Contenido
- Aplicaciones distribuidas por streaming (App-V es el nuevo método utilizado para la distribución de aplicaciones por streaming)

## Asignación de propiedades de aplicaciones

El script para importar datos de comunidad solo importa aplicaciones. Las siguientes propiedades de aplicación se importan sin cambios.

Propiedad de IMA	Propiedad de FMA
AddToClientDesktop	ShortcutAddedToDesktop
AddToClientStartMenu	ShortcutAddedToStartMenu
ClientFolder	ClientFolder
CommandLineExecutable	CommandLineExecutable
CpuPriorityLevel	CpuPriorityLevel
Descripción	Descripción
DisplayName	PublishedName
Habilitado	Habilitado
StartMenuFolder	StartMenuFolder
WaitOnPrinterCreation	WaitForPrinterCreation
WorkingDirectory	WorkingDirectory
FolderPath	AdminFolderName

IMA y FMA tienen restricciones diferentes en cuanto a la longitud de nombre de carpeta. En IMA, el límite para los nombres de carpeta es de 256 caracteres. El límite en FMA es de 64 caracteres. Al realizar la importación, las aplicaciones cuya ruta de acceso contenga un nombre de carpeta de más de 64 caracteres se omitirán. El límite se aplica solamente al nombre de cada carpeta dentro de la ruta de carpetas; la ruta de carpetas entera puede ser más larga que los límites indicados. Para evitar que se omitan aplicaciones durante la importación, Citrix recomienda comprobar la longitud del nombre de las carpetas de las aplicaciones, y acortarlos si es necesario antes de realizar la exportación.

Las siguientes propiedades de aplicación están inicializadas o no inicializadas de forma predeterminada, o están definidas con los valores proporcionados en los datos de XenApp 6.x:

Propiedad de FMA	Valor
Nombre	Inicializada con el nombre completo de la ruta, que contiene las propiedades de IMA FolderPath y DisplayName, pero sin la cadena inicial "Applications\"

Propiedad de FMA	Valor
ApplicationType	HostedOnDesktop
CommandLineArguments	Inicializada mediante argumentos de línea de comandos de XenApp 6.x
IconFromClient	No inicializada; el valor predeterminado es false
IconUid	Inicializada con un objeto de icono creado mediante los datos de iconos de XenApp 6.x
SecureCmdLineArgumentsEnabled	No inicializada; el valor predeterminado es true
UserFilterEnabled	No inicializada; el valor predeterminado es false
UUID	Solo lectura, asignado por el Controller
Visible	No inicializada; el valor predeterminado es true

Las siguientes propiedades de aplicación se migran parcialmente:

Propiedad de IMA	Comentarios
FileTypes	Solo se migran los tipos de archivos que ya existen en el nuevo sitio de XenApp. Aquellos tipos de archivo que no existan en el sitio nuevo se omiten. Los tipos de archivo se importan solo después de que se actualicen los tipos de archivo del sitio nuevo.
IconData	Se crean nuevos objetos de icono si los datos de icono se han proporcionado para las aplicaciones exportadas.
Cuentas	Las cuentas de usuario de una aplicación se dividen entre la lista de usuarios para el grupo de entrega y la aplicación. Los usuarios explícitos se usan para inicializar la lista de usuarios para la aplicación. Además, la cuenta “Usuarios de dominio” del dominio de las cuentas de usuario se agrega a la lista de usuarios para el grupo de entrega.

Las siguientes propiedades de XenApp 6.x no se importan:

---

Propiedad de IMA	Comentarios
ApplicationType	Omitido.
HideWhenDisabled	Omitido.
AccessSessionConditions	Reemplazada por las directivas de acceso de grupos de entrega.
AccessSessionConditionsEnabled	Reemplazada por las directivas de acceso de grupos de entrega.
ConnectionsThroughAccessGatewayAllowed	Reemplazada por las directivas de acceso de grupos de entrega.
OtherConnectionsAllowed	Reemplazada por las directivas de acceso de grupos de entrega.
AlternateProfiles	FMA no admite aplicaciones distribuidas por streaming.
OfflineAccessAllowed	FMA no admite aplicaciones distribuidas por streaming.
ProfileLocation	FMA no admite aplicaciones distribuidas por streaming.
ProfileProgramArguments	FMA no admite aplicaciones distribuidas por streaming.
ProfileProgramName	FMA no admite aplicaciones distribuidas por streaming.
RunAsLeastPrivilegedUser	FMA no admite aplicaciones distribuidas por streaming.
AnonymousConnectionsAllowed	FMA usa una tecnología diferente para admitir conexiones no autenticadas (anónimas).
ApplicationId, SequenceNumber	Datos exclusivos de IMA.
AudioType	FMA no admite opciones avanzadas de conexión de cliente.
EncryptionLevel	SecureICA se habilita o inhabilita en los grupos de entrega.
EncryptionRequired	SecureICA se habilita o inhabilita en los grupos de entrega.
SslConnectionEnabled	FMA usa una implementación de TLS diferente.
ContentAddress	FMA no admite contenido publicado.
ColorDepth	FMA no admite opciones avanzadas de apariencia de ventanas.

---

Propiedad de IMA	Comentarios
MaximizedOnStartup	FMA no admite opciones avanzadas de apariencia de ventanas.
TitleBarHidden	FMA no admite opciones avanzadas de apariencia de ventanas.
WindowsType	FMA no admite opciones avanzadas de apariencia de ventanas.
InstanceLimit	FMA no admite límites de aplicación.
MultipleInstancesPerUserAllowed	FMA no admite límites de aplicación.
LoadBalancingApplicationCheckEnabled	FMA usa una tecnología diferente para admitir el equilibrio de carga.
PreLaunch	FMA usa una tecnología diferente para admitir el preinicio de sesiones.
CachingOption	FMA usa una tecnología diferente para admitir el preinicio de sesiones.
ServerNames	FMA usa una tecnología diferente.
WorkerGroupNames	FMA no admite los grupos de trabajo.

---

## Protección

January 4, 2021

Citrix Virtual Apps and Desktops ofrecen una solución, de diseño seguro, que permite ajustar el entorno a sus necesidades de seguridad.

Un problema de seguridad con el que se enfrentan ahora los departamentos de TI es la pérdida o robo de datos de usuarios móviles. Al alojar escritorios y aplicaciones, Citrix Virtual Apps and Desktops gestiona de manera segura los datos confidenciales y de propiedad intelectual al separarlos de los dispositivos de punto final guardándolos en un centro de datos. Cuando se habilitan las directivas para permitir la transferencia de datos, todos los datos se cifran.

Los centros de datos de Citrix Virtual Apps and Desktops también facilitan la respuesta a los incidentes, gracias a un servicio de administración y supervisión centralizado. Director permite al personal de TI supervisar y analizar los datos a los que los usuarios están accediendo en toda la red, y Studio permite al personal de TI corregir la mayoría de los problemas de vulnerabilidad en el centro de datos en lugar de tener que solucionar los problemas de forma local en cada dispositivo de usuario final.

Citrix Virtual Apps and Desktops también simplifican las auditorías y el cumplimiento de la normativa porque los investigadores pueden usar un registro de auditoría centralizado para determinar quién accedió a las aplicaciones y los datos. Director recopila datos históricos acerca de las actualizaciones del sistema y los datos de uso de los usuarios mediante el acceso a los registros de configuración y el uso de la API de OData.

La administración delegada permite configurar roles de administrador para controlar con detalle el acceso a Citrix Virtual Apps and Desktops. Esto da flexibilidad a la organización para conceder a ciertos administradores un acceso completo a ciertas tareas, operaciones y ámbitos mientras otros administradores tienen acceso limitado.

Con Citrix Virtual Apps and Desktops, los administradores tienen un control minucioso sobre los usuarios mediante la aplicación de directivas en diferentes niveles de la red: desde el nivel local al nivel de unidad organizativa. Este control de directivas determina si un usuario, un dispositivo o un grupo de usuarios y dispositivos pueden conectar, imprimir, copiar/pegar, o asignar las unidades locales, lo que puede ayudar a reducir los riesgos de seguridad cuando se emplea a trabajadores temporales o de terceros. Los administradores también pueden usar la función de Desktop Lock, de modo que los usuarios finales pueden usar solo el escritorio virtual al tiempo que se impide el acceso al sistema operativo local del dispositivo de usuario final.

Los administradores pueden aumentar la seguridad de Citrix Virtual Apps o Citrix Virtual Desktops configurando el sitio para que use el protocolo de seguridad Secure Sockets Layer (TLS) del Controller o entre los usuarios finales y los Virtual Delivery Agents (VDA). El protocolo de seguridad Transport Layer Security (TLS) también se puede habilitar en un sitio para proporcionar autenticación de servidores, cifrado del flujo de datos y comprobación de integridad de los mensajes para una conexión TCP/IP.

Citrix Virtual Apps and Desktops también admiten la autenticación de varios factores para Windows o para una aplicación específica. La autenticación de varios factores también se puede usar para administrar todos los recursos entregados por Citrix Virtual Apps and Desktops. Estos métodos incluyen:

- Tokens
- Tarjetas inteligentes
- RADIUS
- Kerberos
- Biometría

Citrix Virtual Desktops pueden integrarse con muchas soluciones de seguridad de terceros, desde software de gestión de identidades a software antivirus. Puede ver una lista de los productos admitidos en <http://www.citrix.com/ready>.

Determinadas versiones de Citrix Virtual Apps and Desktops están certificadas para el estándar de Common Criteria. Para obtener una lista de esos estándares, vaya a <https://www.commoncriteriaportal.org/cc/>.

## Recomendaciones y consideraciones de seguridad

January 19, 2023

### Nota:

Es posible que la organización deba cumplir con estándares de seguridad específicos para satisfacer requisitos normativos. Este documento no abarca este tema, dado que tales estándares de seguridad cambian con el tiempo. Para obtener información actualizada acerca de los estándares de seguridad y los productos de Citrix, consulte <http://www.citrix.com/security/>.

### Recomendaciones referentes a la seguridad

Mantenga actualizadas todas las máquinas del entorno instalando las revisiones de seguridad que sean necesarias. Una de las ventajas es que se pueden utilizar clientes ligeros como terminales, lo cual simplifica esta tarea.

Proteja todas las máquinas del entorno con software antivirus.

Piense en utilizar software antimalware para plataformas específicas.

Al instalar el software, instálelo en las rutas predeterminadas proporcionadas.

- Si instala software en una ubicación de archivo distinta de la ruta predeterminada proporcionada, considere la posibilidad de agregar medidas de seguridad adicionales, como permisos restringidos, a la ubicación del archivo.

Todas las comunicaciones de red deben contar con la protección adecuada y deben cifrarse correctamente de acuerdo con las directivas de seguridad. Es posible proteger todas las comunicaciones entre los equipos con Microsoft Windows que utilicen IPSec; consulte la documentación de su sistema operativo para obtener información sobre la forma de hacerlo. Además, la comunicación entre los dispositivos de usuario y los escritorios se protege mediante Citrix SecureICA, el cual se configura de manera predeterminada con el cifrado de 128 bit. Es posible configurar SecureICA al crear o actualizar un grupo de entrega.

### Nota:

Citrix SecureICA forma parte del protocolo ICA/HDX, pero no es un protocolo de seguridad de red conforme con los estándares, como Transport Layer Security (TLS). También puede proteger las comunicaciones de red entre dispositivos de usuario y escritorios mediante TLS. Para configurar TLS, consulte [Transport Layer Security \(TLS\)](#).

Aplique los procedimientos recomendados de Windows para la administración de cuentas. No cree cuentas en una plantilla o imagen antes de duplicarlas mediante Machine Creation Services o Pro-

visioning Services. No programe tareas mediante cuentas de dominio almacenadas con privilegios. No cree manualmente cuentas de equipo compartidas de Active Directory. Estos consejos ayudan a evitar ataques a la máquina que se pueden dar por haber obtenido contraseñas persistentes de cuentas locales y usarlas para iniciar sesión en las imágenes de Machine Creation Services o Provisioning Services compartidas que pertenecen a los usuarios.

## Firewalls

Proteja todas las máquinas del entorno con firewalls perimetrales, incluido en los límites de enclave, según corresponda.

Todas las máquinas del entorno deben contar con la protección de un firewall personal. Al instalar componentes principales y agentes VDA puede elegir que los puertos necesarios para la comunicación de funciones y componentes se abran automáticamente si se detecta el servicio Firewall de Windows (incluso aunque el firewall no esté habilitado). También puede configurar manualmente los puertos del firewall. Si usa un firewall diferente, debe configurarlo manualmente.

Si planea migrar un entorno convencional a esta versión, es posible que necesite cambiar la posición de un firewall perimetral existente o agregar firewalls perimetrales nuevos. Por ejemplo, supongamos que existe un firewall perimetral entre un cliente convencional y un servidor de base de datos en el centro de datos. Cuando se usa esta versión, ese firewall perimetral debe colocarse de modo que el escritorio virtual y el dispositivo del usuario queden de un lado, y los servidores de base de datos y Delivery Controllers del centro de datos queden del otro lado. Por lo tanto, considere la posibilidad de crear un enclave dentro del centro de datos que contenga los servidores y los Controllers. Asimismo, debe contar con una protección entre el dispositivo del usuario y el escritorio virtual.

### Nota:

Los puertos TCP 1494 y 2598 se utilizan para ICA y CGP. Por lo tanto, es probable que estén abiertos en los firewalls para que los usuarios que están fuera del centro de datos puedan acceder a ellos. Citrix sugiere no utilizar estos puertos con otros fines para evitar la posibilidad de dejar accidentalmente las interfaces administrativas vulnerables al ataque. Los puertos 1494 y 2598 tienen registro oficial en la Agencia de Asignación de Números de Internet (<http://www.iana.org/>).

## Seguridad de las aplicaciones

Para evitar que los usuarios que no son administradores realicen acciones malintencionadas, se recomienda configurar reglas de Windows AppLocker para instaladores, aplicaciones, ejecutables y scripts en el host VDA y en el cliente Windows local.

## Administrar privilegios de usuario

Solo conceda a los usuarios las capacidades que necesitan. Los privilegios de Microsoft Windows continúan aplicándose a los escritorios de la forma habitual: se configuran los privilegios mediante la Asignación de derechos de usuario y la pertenencia a grupos a través de la directiva de grupo. Una de las ventajas de esta versión es que permite otorgar permisos administrativos a un usuario para un escritorio sin concederle también el control físico del equipo en el cual se almacena el escritorio.

Tenga en cuenta lo siguiente cuando planifique privilegios de escritorio:

- De forma predeterminada, cuando un usuario con privilegios reducidos se conecta a un escritorio, ve la zona horaria del sistema que ejecuta el escritorio en lugar de la zona horaria de su propio dispositivo de usuario. Para obtener información sobre cómo permitir que los usuarios vean su hora local al utilizar escritorios, consulte Administración de grupos de entrega.
- Un usuario que es administrador de un escritorio posee total control sobre ese escritorio. Si un escritorio es un escritorio agrupado en lugar de un escritorio dedicado, el usuario debe ser de confianza para todos los demás usuarios de ese escritorio, incluidos los futuros usuarios. Todos los usuarios de ese escritorio deben ser conscientes del riesgo potencial permanente que esta situación representa para la seguridad de sus datos. Esta consideración no se aplica a los escritorios dedicados, que solo contienen un usuario; ese usuario no debe ser el administrador de ningún otro escritorio.
- Un usuario que es administrador en un escritorio generalmente puede instalar software en ese escritorio, incluido software potencialmente malicioso. El usuario también puede supervisar o controlar el tráfico de cualquier red conectada al escritorio.

## Administrar derechos de inicio de sesión

Se necesitan derechos de inicio de sesión para las cuentas de usuario y las cuentas de equipo. Al igual que los privilegios de Microsoft Windows, los derechos de inicio de sesión continúan aplicándose a los escritorios de la forma habitual: configure los derechos de inicio de sesión a través de la Asignación de derechos de usuario y la pertenencia a grupos a través de Directiva de grupo.

Los derechos de inicio de sesión de Windows son: iniciar sesión localmente, iniciar sesión con Servicios de Escritorio remoto, iniciar sesión en la red (tener acceso a este equipo desde la red), iniciar sesión como trabajo por lotes e iniciar sesión como servicio.

Para las cuentas de equipo, conceda a los equipos únicamente los derechos de inicio de sesión que necesiten. El derecho de inicio de sesión “Tener acceso a este equipo desde la red” es obligatorio:

- En los VDA, para las cuentas de equipo de los Delivery Controllers
- En los Delivery Controllers, para las cuentas de equipo de los VDA. Consulte [Detección de Controladores basada en unidades organizativas de Active Directory](#).

- En los servidores de StoreFront, para las cuentas de equipo de otros servidores que se encuentren en el mismo grupo de servidores de StoreFront

En el caso de cuentas de usuario, conceda a los usuarios únicamente los permisos de inicio de sesión que necesiten.

Según Microsoft, de manera predeterminada el grupo Usuarios de escritorio remoto tienen el derecho de inicio de sesión “Permitir inicio de sesión a través de Servicios de Escritorio remoto”(excepto en controladores de dominio).

Las directivas de seguridad de su organización pueden establecer explícitamente que se quite este derecho de inicio de sesión para este grupo. Considere el enfoque siguiente:

- El Virtual Delivery Agent (VDA) para SO multisesión usa Servicios de Escritorio remoto de Microsoft. Puede configurar el grupo de Usuarios de escritorio remoto como un grupo restringido, y controlar la pertenencia al grupo mediante directivas de grupo de Active Directory. Para obtener más información, consulte la documentación de Microsoft.
- Para los demás componentes de Citrix Virtual Apps and Desktops, incluido el VDA para SO de sesión única, el grupo Usuarios de escritorio remoto no es necesario. Por tanto, para esos componentes, el grupo Usuarios de escritorio remoto no requiere el derecho de inicio de sesión “Permitir inicio de sesión a través de Servicios de Escritorio remoto”y puede quitarlo. Además:
  - Si administra esos equipos a través de Servicios de Escritorio remoto asegúrese de que esos administradores ya son miembros del grupo Administradores.
  - Si no administra esos equipos mediante Servicios de Escritorio remoto, considere la posibilidad de inhabilitar los propios Servicios de Escritorio remoto en esos equipos.

Aunque es posible agregar usuarios y grupos al derecho de inicio de sesión “Denegar inicio de sesión a través de Servicios de Escritorio remoto”, en general no se recomienda el uso de derechos de denegar inicios de sesión. Para obtener más información, consulte la documentación de Microsoft.

## Configurar derechos de usuario

La instalación de Delivery Controller crea los siguientes servicios de Windows:

- Citrix AD Identity Service (NT SERVICE\CitrixADIdentityService): Administra las cuentas de equipo de Microsoft Active Directory para las VM.
- Citrix Analytics (NT SERVICE\CitrixAnalytics): Recopila información de uso de la configuración de sitios para que Citrix pueda utilizarla, si dicha recopilación de datos fue aprobada por el administrador del sitio. A continuación, esta información se envía a Citrix, para ayudar a mejorar el producto.
- Citrix App Library (NT SERVICE\CitrixAppLibrary): Admite la administración y aprovisionamiento de AppDisks, la integración con AppDNA y la administración de App-V.

- Citrix Broker Service (NT SERVICE\servicio CitrixBrokerService): Selecciona los escritorios virtuales o las aplicaciones que están disponibles para los usuarios.
- Citrix Configuration Logging Service (NT SERVICE\CitrixConfigurationLogging): Registra todos los cambios de configuración y otros cambios de estado realizados por los administradores del sitio.
- Citrix Configuration Service (NT SERVICE\CitrixConfigurationService): Repositorio de la configuración compartida para todo el sitio.
- Citrix Delegated Administration Service (NT SERVICE\CitrixDelegatedAdmin): Administra los permisos concedidos a los administradores.
- Citrix Environment Test Service (NT SERVICE\CitrixEnvTest): Administra pruebas automáticas de los demás servicios de Delivery Controller.
- Citrix Host Service (NT SERVICE\CitrixHostService): Almacena información sobre las infraestructuras de hipervisor utilizadas en una implementación de Citrix Virtual Apps o Citrix Virtual Desktops, y también ofrece la funcionalidad utilizada por la consola para enumerar los recursos de una agrupación de hipervisores.
- Citrix Machine Creation Services (NT SERVICE\CitrixMachineCreationService): Organiza la creación de las máquinas virtuales de escritorio.
- Citrix Monitor Service (NT SERVICE\CitrixMonitor): Recopila métricas de Citrix Virtual Apps o Citrix Virtual Desktops, almacena información histórica y proporciona una interfaz de consultas para la solución de problemas y herramientas para la generación de informes.
- Citrix StoreFront Service (NT SERVICE\CitrixStoreFront): Admite la administración de StoreFront (no es parte del componente de StoreFront en sí).
- Citrix StoreFront Privileged Administration Service (NT SERVICE\CitrixPrivilegedService): Admite las operaciones de administración con privilegios de StoreFront (no es parte del componente de StoreFront en sí).
- Citrix Config Synchronizer Service (NT SERVICE\CitrixConfigSyncService): Propaga los datos de configuración desde el sitio principal a la Caché de host local.
- Citrix High Availability Service (NT SERVICE\CitrixHighAvailabilityService): Selecciona los escritorios virtuales o las aplicaciones que están disponibles para los usuarios, si la base de datos principal del sitio no está disponible.

La instalación de Delivery Controller también crea los siguientes servicios de Windows. Estos también se crean al instalarlo con otros componentes de Citrix:

- Citrix Diagnostic Facility COM Server (NT SERVICE\CdfSvc): Admite la recopilación de información de diagnóstico para la asistencia técnica de Citrix.
- Citrix Telemetry Service (NT SERVICE\CitrixTelemetryService): Recopila información de diagnóstico para ser analizada por Citrix, de forma que los administradores pueden ver los resultados del análisis y las recomendaciones, para ayudarles a diagnosticar problemas con el sitio.

La instalación de Delivery Controller también crea el siguiente servicio de Windows. No se usa actual-

mente. Si se ha habilitado, inhabíltelo.

- Citrix Remote Broker Provider (NT SERVICE\XaXdCloudProxy)

La instalación de Delivery Controller también crea los siguientes servicios de Windows. Estos parámetros no se usan actualmente, pero deben estar habilitados. No los inhabilite.

- Citrix Orchestration Service (NT SERVICE\CitrixOrchestration)
- Citrix Trust Service (NT SERVICE\CitrixTrust)

Excepto Citrix StoreFront Privileged Administration Service, estos servicios tienen concedido el derecho de Iniciar sesión como servicio y los privilegios de Ajustar las cuotas de la memoria para un proceso, Generar auditorías de seguridad y Reemplazar un símbolo (token) de nivel de proceso. No es necesario que cambie estos derechos de usuario. Delivery Controller no utiliza estos privilegios y están inhabilitados automáticamente.

## Configurar parámetros de servicios

Excepto Citrix StoreFront Privileged Administration Service y Citrix Telemetry Service, los servicios Windows de Delivery Controller enumerados arriba en la sección Configurar derechos de usuario están configurados para iniciar sesión como la identidad NETWORK SERVICE. No modifique estos parámetros de servicio.

Citrix StoreFront Privileged Administration está configurado para iniciar la sesión de sistema local (NT AUTHORITY\SYSTEM). Esto es necesario para las operaciones de StoreFront con Delivery Controller que no están normalmente disponible para los servicios (incluida la creación de sitios de IIS de Microsoft). No modifique estos parámetros de servicio.

Citrix Telemetry Service está configurado para iniciar sesión como su propia identidad específica de servicio.

Si quiere, puede inhabilitar Citrix Telemetry Service. Aparte de este servicio y de los servicios que ya están inhabilitados, no inhabilite ninguno de los otros servicios de Windows de Delivery Controller.

## Configurar parámetros de Registro

Ya no es necesario habilitar la creación de carpetas y nombres de archivo 8.3 en el sistema de archivos del VDA. La clave de Registro **NtfsDisable8dot3NameCreation** se puede configurar para inhabilitar la creación de carpetas y nombres de archivo 8.3. También puede configurar este comportamiento mediante el comando **fsutil.exe behavior set disable8dot3**.

## **Implicaciones de seguridad en los casos de implementación**

El entorno de usuario puede contener dispositivos de usuario que la empresa no administra y, por tanto, están bajo el control total del usuario, o bien, dispositivos de usuario que administra totalmente la empresa. En general, las consideraciones de seguridad para estos dos entornos son diferentes.

### **Dispositivos del usuario administrados**

Los dispositivos de usuario administrados permanecen bajo un control administrativo; se encuentran bajo el control del usuario o de otra organización de su confianza. Es posible configurar y suministrar dispositivos del usuario directamente a usuarios. También es posible proporcionar terminales en los que se ejecute un solo escritorio en modo solo de pantalla completa. Es necesario respetar las recomendaciones de seguridad descritas anteriormente para todos los dispositivos de usuario administrados. La ventaja de esta versión es que presenta requisitos mínimos de software para un dispositivo del usuario.

Un dispositivo de usuario administrado puede configurarse para su uso solo en el modo de pantalla completa o en el modo de ventana:

- Modo solo de pantalla completa. Los usuarios inician sesión en la pantalla habitual de Iniciar sesión en Windows. A continuación, se utilizan las mismas credenciales de usuario para iniciar sesión automáticamente en esta versión.
- Los usuarios ven su escritorio en una ventana. Primero deben iniciar sesión en el dispositivo del usuario y luego en esta versión a través del sitio web proporcionado con ella.

### **Dispositivos del usuario no administrados**

Los dispositivos de usuario que no se encuentran bajo la administración de una organización fiable no pueden considerarse parte de un control administrativo. Por ejemplo, se puede permitir que los usuarios obtengan y configuren sus propios dispositivos, pero es posible que los usuarios no respeten las prácticas recomendadas de seguridad general descritas anteriormente. Esta versión presenta la ventaja de permitir la entrega de escritorios de forma segura a dispositivos del usuario no administrados. Aun así, estos dispositivos deben contar con una protección antivirus básica que anule los registradores de pulsaciones de teclas y los ataques de entrada similares.

### **Aspectos a tener en cuenta sobre el almacenamiento de datos**

Al utilizar esta versión, es posible evitar que los usuarios almacenen datos en los dispositivos del usuario que se encuentren bajo su control físico. No obstante, es necesario tener en cuenta las implicaciones del almacenamiento de datos en los escritorios por parte de los usuarios. Almacenar datos

en los escritorios no es una práctica recomendada para los usuarios; los datos deben conservarse en servidores de archivos, servidores de base de datos u otros repositorios donde se encuentren debidamente protegidos.

El entorno de escritorio puede estar compuesto por varios tipos de escritorios, como escritorios agrupados y dedicados. Los usuarios no deben almacenar nunca sus datos en escritorios compartidos entre los usuarios, como es el caso de los escritorios agrupados. Cuando los usuarios almacenan datos en escritorios dedicados, esos datos deben eliminarse si el escritorio posteriormente pasa a estar disponible para otros usuarios.

### Entornos de versiones mixtas

En algunas actualizaciones, los entornos que contienen varias versiones son inevitables. Siga las prácticas recomendadas y minimice el tiempo de coexistencia para los componentes de Citrix de versiones distintas. En entornos de varias versiones, es posible que las directivas de seguridad, por ejemplo, no se cumplan uniformemente.

#### Nota:

Esta es una situación habitual en caso de otros productos de software. Una versión anterior de Active Directory solo aplica parcialmente la directiva de grupo cuando se trata de versiones posteriores de Windows.

En el siguiente caso, se describe un problema de seguridad que se puede dar en un entorno Citrix concreto que contenga varias versiones. Cuando se usa Citrix Receiver 1.7 para conectarse a un escritorio virtual con Virtual Delivery Agent en XenApp y XenDesktop 7.6 Feature Pack 2, la configuración de directiva **Permitir transferencia de archivos entre escritorio y cliente** se habilita en el sitio, pero un Delivery Controller que ejecute XenApp y XenDesktop 7.1 no puede inhabilitarla. No reconoce la configuración de directiva, que se publicó en la versión posterior del producto. Esta configuración de directiva permite a los usuarios cargar y descargar archivos en su escritorio virtual; de ahí el problema de seguridad. Para solucionarlo, actualice el Delivery Controller (o una instancia independiente de Studio) a la versión 7.6 Feature Pack 2 y, a continuación, use la directiva de grupo para inhabilitar la directiva. Si lo prefiere, puede usar la directiva local de todos los escritorios virtuales pertinentes.

### Consideraciones de seguridad sobre el acceso con Remote PC

El acceso con Remote PC es una función que implementa las siguientes funciones de seguridad:

- Compatible con la tarjeta inteligente.
- Cuando se inicia una sesión remota, la pantalla del PC de la oficina aparece en blanco.

- La función de acceso con Remote PC redirige todas las entradas del teclado y puntero a la sesión remota, excepto CTRL+ALT+SUPR, las tarjetas inteligentes con USB habilitado y los dispositivos biométricos.
- SmoothRoaming se ofrece solamente para un usuario.
- Cuando un usuario tiene una sesión remota conectada a un PC de la oficina, solo ese usuario puede reanudar el acceso local al PC de la oficina. Para reanudar el acceso local, el usuario debe pulsar CTRL+ALT+SUPR en el equipo local y, a continuación, iniciar sesión con las mismas credenciales que usa la sesión remota. El usuario también puede reanudar el acceso local mediante la inserción de una tarjeta inteligente o aprovechar la biometría, si el sistema tiene integrado un Proveedor de credenciales de terceros apropiado. Este comportamiento predeterminado se puede anular mediante la habilitación de Cambio rápido de usuario a través de objetos de directiva de grupo (GPO) o al modificar el Registro.

**Nota:**

Citrix recomienda no asignar privilegios de administrador de VDA a usuarios generales de sesión.

### Asignaciones automáticas

De forma predeterminada, la función de acceso con Remote PC admite la asignación automática de varios usuarios a un agente VDA. En XenDesktop 5.6 Feature Pack 1, los administradores pueden invalidar este comportamiento mediante el script de PowerShell RemotePCAccess.ps1. Esta versión usa una entrada del Registro para permitir o prohibir varias asignaciones automáticas de Remote PC; este parámetro se aplica a todo el sitio.

**Precaución:**

Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Para restringir la asignación automática a un único usuario:

En cada Controller del sitio, configure la siguiente entrada del Registro:

```
1 HKEY\_LOCAL\_MACHINE\Software\Citrix\DesktopServer
2 Name: AllowMultipleRemotePCAssignments
3 Type: REG_DWORD
4 Data: 0 = Disable multiple user assignment, 1 = (Default) Enable
      multiple user assignment.
```

Si hay asignaciones de usuario, se pueden eliminar mediante comandos de SDK para que más adelante el VDA pueda ser apto para una asignación automática.

- Para quitar todos los usuarios asignados del VDA: `$machine.AssociatedUserNames | % { Remove-BrokerUser-Name $_ -Machine $machine }`
- Para eliminar el VDA del grupo de entrega: `$machine | Remove-BrokerMachine -DesktopGroup $desktopGroup`

Reinicie el PC físico de la oficina.

## Confianza en XML

La configuración de confianza en XML se aplica a las implementaciones que utilizan:

- Un StoreFront local.
- Tecnología de autenticación de suscriptor (usuario) que no requiere contraseñas. Ejemplos de tales tecnologías son las soluciones de PassThrough de dominio, tarjetas inteligentes, SAML y Veridium.

Habilitar la configuración de confianza en XML permite a los usuarios autenticarse correctamente y, a continuación, iniciar las aplicaciones. Delivery Controller confía en las credenciales enviadas desde StoreFront. Habilite esta configuración solo cuando haya protegido las comunicaciones entre Delivery Controllers y StoreFront (mediante firewalls, IPSec u otras recomendaciones de seguridad).

Este parámetro está inhabilitado de forma predeterminada.

Use Citrix Virtual Apps and Desktops PowerShell SDK para comprobar, habilitar o inhabilitar la configuración de confianza en XML.

- Para comprobar el valor actual de la configuración de confianza en XML, ejecute `Get-BrokerSite` e inspeccione el valor de `TrustRequestsSentToTheXMLServicePort`.
- Para habilitar la confianza en XML, ejecute `Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true`.
- Para inhabilitar la confianza en XML, ejecute `Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $false`.

## Integrar Citrix Virtual Apps and Desktops con Citrix Gateway

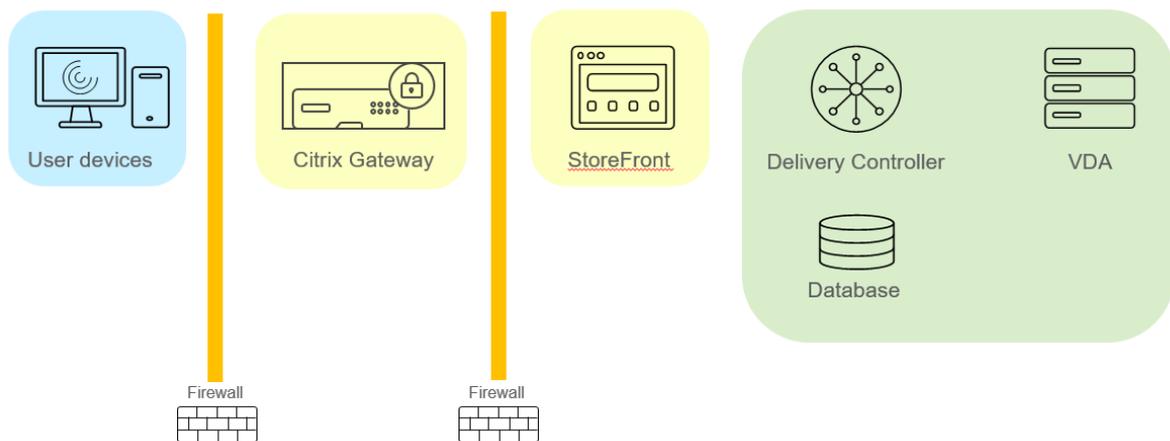
February 7, 2020

Los servidores de StoreFront se implementan y se configuran para administrar el acceso a los datos y los recursos publicados. Para el acceso remoto, se recomienda agregar Citrix Gateway y colocarlo delante de StoreFront.

**Nota:**

Para conocer los pasos detallados de configuración para integrar Citrix Virtual Apps and Desktops con Citrix Gateway, consulte la [documentación de StoreFront](#).

En el siguiente diagrama, se ofrece un ejemplo de una implementación simplificada de Citrix que incluye Citrix Gateway. Citrix Gateway se comunica con StoreFront para proteger las aplicaciones y los datos que entregan Citrix Virtual Apps and Desktops. Los dispositivos de usuario ejecutan la aplicación Citrix Workspace para crear una conexión segura y acceder a las aplicaciones, los escritorios y los archivos.



Los usuarios inician sesiones y se autentican mediante Citrix Gateway. Citrix Gateway se implementa y se protege en la zona DMZ. Se configura la autenticación de dos factores. En función de sus credenciales de usuario, los usuarios reciben los recursos y las aplicaciones que les corresponden. Las aplicaciones y los datos se encuentran en los servidores adecuados (no aparecen en el diagrama). Se utilizan servidores independientes para los datos y las aplicaciones confidenciales de seguridad.

## Administración delegada

September 22, 2021

El modelo de administración delegada ofrece flexibilidad para adaptarse al modo en que la organización desee delegar actividades de administración. Para ello, utiliza el control basado en los roles y los objetos. La administración delegada se adapta a implementaciones de todos los tamaños y permite configurar permisos con mucho más detalle a medida que la implementación adquiere complejidad. La administración delegada utiliza tres conceptos: los administradores, los roles y los ámbitos.

- **Administradores:** Un administrador representa una persona o un grupo de usuarios identificados por su cuenta de Active Directory. Cada administrador está asociado a uno o varios pares de rol y ámbito.
- **Roles:** Un rol representa una función de trabajo para la que se han definido y asociado permisos. Por ejemplo, el rol del administrador de grupos de entrega tiene permisos tales como “Crear grupo de entrega” y “Eliminar escritorio del grupo de entrega”. Un administrador puede tener varios roles en un sitio, de modo que una persona puede ser un administrador de grupos de entrega y un administrador de catálogos de máquinas. Los roles pueden ser integrados o personalizados.

Los roles integrados son:

Rol	Permisos
Administrador total	Puede realizar todas las tareas y operaciones. Un administrador total siempre se combina con Todos los ámbitos.
Administrador de solo lectura	Puede ver todos los objetos en los ámbitos especificados e información global, pero no puede modificar nada. Por ejemplo, un administrador de solo lectura con Ámbito = Londres puede ver todos los objetos globales (como, por ejemplo, el registro de configuración) y todos los objetos del ámbito Londres (por ejemplo, grupos de entrega de Londres). No obstante, ese administrador no puede ver los objetos del ámbito de Nueva York (a menos que los ámbitos de Londres y Nueva York se superpongan).
Administrador de asistencia técnica	Puede ver los grupos de entrega y administrar las sesiones y las máquinas asociadas a dichos grupos. Puede ver el catálogo de máquinas y la información de host de los grupos de entrega que están bajo supervisión. También puede realizar tareas de administración de sesiones y de administración de energía en las máquinas de esos grupos de entrega.

Rol	Permisos
Administrador de catálogos de máquinas	Puede crear y administrar catálogos de máquinas y aprovisionar máquinas en ellos. Puede crear catálogos de máquinas a partir de la infraestructura de virtualización, Provisioning Services y máquinas físicas. Este rol puede administrar las imágenes base e instalar software, pero no puede asignar las aplicaciones o los escritorios a los usuarios.
Administrador de grupos de entrega	Puede entregar aplicaciones, escritorios y máquinas, además de administrar las sesiones asociadas. También puede administrar las configuraciones de aplicaciones y escritorios, tales como las configuraciones de directivas y de administración de energía.
Administrador de host	Puede administrar conexiones de host y sus parámetros de recursos asociados. No puede entregar máquinas, aplicaciones ni escritorios a los usuarios.

En algunas ediciones de producto, se pueden crear roles personalizados (para que coincidan con los requisitos de la empresa) y delegar permisos con mayor flexibilidad. Puede usar los roles personalizados para asignar permisos a la granularidad de una acción o tarea en una consola.

- **Ámbitos:** Un ámbito representa una colección de objetos. Los ámbitos se usan para agrupar objetos de una manera que sea relevante para la organización (por ejemplo, el conjunto de grupos de entrega utilizado por el equipo de ventas). Los objetos pueden estar en más de un ámbito; es como si estuvieran etiquetados con uno o más ámbitos. Hay un ámbito integrado: 'Todo', que contiene todos los objetos. El rol de administrador total siempre va asociado al ámbito Todo.

## Ejemplo

La compañía XYZ ha decidido administrar aplicaciones y escritorios según el departamento (Cuentas, Ventas, y Almacén) y el sistema operativo de escritorio (Windows 7 o Windows 8). El administrador creó cinco ámbitos. Luego, etiquetó cada grupo de entrega con dos ámbitos: una para el departamento en el que se utilizan y otra para el sistema operativo.

Se crearon los siguientes administradores:

Administrador	Roles	Ámbitos
dominio/Fred	Administrador total	Todo (el rol de administrador total siempre tiene el ámbito Todo)
dominio/Rob	Administrador de solo lectura	Todas
dominio/Heidi	Administrador de solo lectura, administrador de asistencia técnica	Todo Ventas
dominio/adminalmacén	Administrador de asistencia técnica	Almacén
dominio/Miguel	Administrador de grupos de entrega, administrador de catálogos de máquinas	Win7

- Fred es un administrador total y puede ver, modificar y eliminar todos los objetos del sistema.
- Rob puede ver todos los objetos del sitio, pero no los puede modificar ni eliminar.
- Heidi puede ver todos los objetos y puede realizar tareas de asistencia técnica en grupos de entrega del ámbito Ventas. De esta manera, ella puede administrar las sesiones y las máquinas asociadas a esos grupos, pero no puede realizar cambios en el grupo de entrega, tales como agregar o eliminar máquinas.
- Todos los miembros del grupo de seguridad de Active Directory Adminalmacén pueden ver y realizar tareas de asistencia técnica en las máquinas del ámbito Almacén.
- Miguel es un especialista de Windows 7, por lo que puede administrar todos los catálogos de máquinas de Windows 7 y puede entregar aplicaciones, escritorios y máquinas de Windows 7, independientemente de si se encuentran dentro del ámbito del departamento o no. El administrador se planteó si convertir a Miguel en administrador completo para el ámbito Win7. Sin embargo, descartó esa opción porque un administrador total también tiene derechos totales sobre todos los objetos no incluidos en ningún ámbito, como “sitio” y “administrador”.

## Uso de la administración delegada

Por lo general, el número de administradores y la granularidad de sus permisos dependen del tamaño y la complejidad de la implementación.

- En implementaciones pequeñas o de prueba de concepto, un administrador o un número reducido de ellos puede hacer cualquier cosa. No hay delegación. En este caso, cree a cada administrador con el rol integrado de administrador total, cuyo ámbito es Todo.
- Las implementaciones grandes con más máquinas, aplicaciones y escritorios implican mayor delegación. Varios administradores pueden tener responsabilidades funcionales más específi-

cas (roles). Por ejemplo, dos son administradores totales y los demás son administradores de asistencia técnica. Además, un administrador puede gestionar solamente grupos determinados de objetos (ámbitos), como los catálogos de máquinas. En este caso, cree nuevos ámbitos y administradores con uno de los roles integrados y los ámbitos correspondientes.

- Incluso las implementaciones de gran envergadura pueden necesitar más ámbitos (o más específicos), además de diferentes administradores con roles poco comunes. En este caso, modifique o cree más ámbitos, cree roles personalizados y asocie a cada administrador con un rol personalizado o integrado, además de los ámbitos existentes y nuevos.

Para ofrecer mayor flexibilidad y facilidad de configuración, puede crear ámbitos al crear un administrador. También puede especificar los ámbitos al crear o modificar catálogos de máquinas o conexiones.

## Crear y gestionar administradores

Cuando un administrador local crea un sitio, la cuenta de usuario de ese administrador se convierte automáticamente en administrador total con permisos completos sobre todos los objetos. Después de crear un sitio, los administradores locales no tienen privilegios especiales.

El rol de administrador total siempre tiene el ámbito Todo y esto no se puede cambiar.

De manera predeterminada, hay un administrador habilitado. Inhabilitar un administrador puede ser necesario si se va a crear un administrador, pero esa persona no comenzará a desempeñar sus tareas de administración hasta más adelante. En el caso de administradores existentes ya habilitados, es posible que quiera inhabilitar algunos de ellos mientras reorganiza sus objetos y ámbitos, para volver a habilitarlos de nuevo cuando la nueva configuración esté lista para aplicarse en el entorno. No se puede inhabilitar un administrador total si se trata del único administrador total habilitado en ese momento. La casilla de verificación para habilitar o inhabilitar está activa al crear, copiar o modificar un administrador.

Cuando se elimina un rol y su ámbito correspondiente al copiar, modificar o eliminar un administrador, se elimina solamente la relación entre el rol y el ámbito de ese administrador. No elimina ni el rol ni el ámbito. Tampoco afecta a ningún otro administrador que esté configurado con ese par de rol y ámbito.

Para administrar a los administradores, haga clic en **Configuración > Administradores** en el panel de navegación de Studio y, a continuación, haga clic en la ficha **Administradores** del panel central superior.

- **Crear un administrador:** Haga clic en **Crear administrador** en el panel Acciones. Escriba o vaya al nombre de la cuenta de usuario, seleccione o cree un ámbito, y seleccione un rol. El nuevo administrador se habilita de forma predeterminada, aunque puede modificar este valor.

- **Copiar un administrador:** Seleccione el administrador en el panel central y, a continuación, haga clic en **Copiar administrador** en el panel Acciones. Escriba o vaya al nombre de la cuenta de usuario. Puede seleccionar y, a continuación, modificar o eliminar los pares de rol y ámbito, así como agregar otros nuevos. El nuevo administrador se habilita de forma predeterminada, aunque puede modificar este valor.
- **Modificar un administrador:** Seleccione el administrador en el panel central y, a continuación, haga clic en **Modificar administrador** en el panel Acciones. Puede modificar o eliminar los pares de rol y ámbito, así como agregar otros nuevos.
- **Eliminar un administrador:** Seleccione el administrador en el panel central y, a continuación, haga clic en **Eliminar administrador** en el panel Acciones. No se puede eliminar un administrador total si se trata del único administrador total habilitado en ese momento.

El panel superior muestra los administradores que ha creado. Seleccione un administrador para ver información detallada sobre él en el panel inferior. La columna **Advertencias** indica si los pares de rol y ámbito asociados al administrador contienen roles o ámbitos que no se pueden utilizar. Este mensaje de advertencia aparece si un par de rol y ámbito asociados contiene roles o ámbitos que no se pueden utilizar:

- Rol o ámbito asociado no utilizable
  - Quite el par de rol y ámbito del administrador.

#### **Importante:**

Un mensaje de advertencia aparece solamente cuando un par de rol y ámbito asociados contiene roles o ámbitos que no se pueden utilizar.

Para quitar el par de rol y ámbito del administrador, siga uno de los pasos siguientes:

- Elimine el par de rol y ámbito.
  1. En el panel **Acciones**, haga clic en **Modificar administrador**.
  2. En la ventana **Modificar administrador**, seleccione el par de rol y ámbito y, a continuación, haga clic en **Eliminar**.
  3. Haga clic en **Aceptar** para salir.
- Elimine al administrador.
  1. En el panel **Acciones**, haga clic en **Eliminar administrador**.
  2. En la ventana **Studio**, haga clic en **Eliminar**.

## **Crear y gestionar roles**

Cuando los administradores crean o modifican un rol, solo pueden habilitar los permisos que ellos mismos tienen. Esto impide que los administradores creen un rol con más permisos de los que tienen

actualmente y luego se lo asignen a sí mismos (o modifiquen un rol que ya tienen asignado).

Los nombres de rol pueden contener un máximo de 64 caracteres Unicode y no pueden incluir los siguientes caracteres: barra diagonal inversa, barra diagonal, punto y coma, dos puntos, almohadilla, coma, asterisco, signo de interrogación, signo igual, flecha izquierda o derecha, barra vertical, corchete izquierdo o derecho, paréntesis izquierdo o derecho, comillas dobles ni apóstrofe. Las descripciones pueden contener un máximo de 256 caracteres Unicode.

Los roles integrados no se pueden modificar ni eliminar. No se puede eliminar un rol personalizado si algún administrador lo está utilizando.

**Nota:**

Solo algunas ediciones de producto admiten los roles personalizados. Solamente las ediciones que admiten roles personalizados contienen entradas relacionadas en el panel Acciones.

Para administrar los roles, haga clic en **Configuración > Administradores** en el panel de navegación de Studio y, a continuación, haga clic en la ficha **Roles** del panel central superior.

- **Ver información detallada de un rol:** selecciónelo en el panel central. La parte inferior del panel central muestra los tipos de objeto y los permisos asociados con el rol. Haga clic en la ficha Administradores en el panel inferior para ver una lista de los administradores que actualmente tienen ese rol.
- **Crear un rol personalizado:** haga clic en **Crear nuevo rol** en el panel Acciones. Escriba un nombre y una descripción. Seleccione los tipos de objeto y los permisos pertinentes.
- **Copiar un rol:** selecciónelo en el panel central y, a continuación, haga clic en **Copiar rol** en el panel Acciones. Cambie el nombre, la descripción, los tipos de objeto y los permisos, según sea necesario.
- **Modificar un rol personalizado:** selecciónelo en el panel central y, a continuación, haga clic en **Modificar rol** en el panel Acciones. Cambie el nombre, la descripción, los tipos de objeto y los permisos, según sea necesario.
- **Eliminar un rol personalizado:** selecciónelo en el panel central y, a continuación, haga clic en **Eliminar rol** en el panel Acciones. Cuando se le solicite, confirme la eliminación.

## Crear y gestionar ámbitos

Cuando se crea un sitio, el único ámbito disponible es el ámbito ‘Todo’, que no se puede eliminar.

Puede crear ámbitos mediante el procedimiento siguiente. También puede crear ámbitos al tiempo que crea un administrador; cada administrador debe estar asociado a al menos un par rol/ámbito. Al crear o modificar escritorios, catálogos de máquinas, aplicaciones o hosts, es posible agregarlos a un ámbito existente. Si no se agregan a un ámbito específico, forman parte del ámbito “Todo”.

En la creación de sitios no se puede aplicar ámbitos. Tampoco se puede aplicar ámbitos a los objetos de la administración delegada, es decir, a los propios ámbitos y roles. Los objetos que no pueden incluirse en ámbitos específicos se integran en el ámbito “Todo”(los administradores totales siempre disponen del ámbito Todo). Las máquinas, las acciones de energía, los escritorios y las sesiones no tienen un ámbito directo. Se pueden asignar permisos a los administradores sobre estos objetos a través de los catálogos de máquinas o grupos de entrega asociados.

Los nombres de los ámbitos pueden contener un máximo de 64 caracteres Unicode. Sin embargo, los nombres de los ámbitos no pueden contener estos caracteres: barra diagonal inversa, barra diagonal, punto y coma, dos puntos, almohadilla, coma, asterisco, signo de interrogación, signo igual, flecha izquierda o derecha, barra vertical, corchete izquierdo o derecho, paréntesis izquierdo o derecho, comillas dobles ni apóstrofe. Las descripciones pueden contener un máximo de 256 caracteres Unicode.

Al copiar o modificar un ámbito, tenga en cuenta que eliminar objetos del ámbito puede tener como consecuencia que el administrador no pueda acceder a ellos. Si el ámbito modificado está emparejado con uno o varios roles, compruebe que los cambios que haga en el ámbito no hagan que el par de rol y ámbito no se pueda utilizar.

Para administrar ámbitos, haga clic en **Configuración > Administradores** en el panel de navegación de Studio y, a continuación, haga clic en la ficha **Ámbitos** del panel central superior.

- **Crear un ámbito:** haga clic en **Crear ámbito** en el panel Acciones. Escriba un nombre y una descripción. Para incluir todos los objetos de un tipo concreto (por ejemplo, grupos de entrega), seleccione el tipo de objeto. Para incluir objetos concretos, expanda el tipo y, a continuación, seleccione objetos individualmente (por ejemplo, grupos de entrega individuales utilizados por el equipo de Ventas).
- **Para copiar un ámbito:** Selecciónelo en el panel central y, a continuación, haga clic en **Copiar ámbito** en el panel Acciones. Escriba un nombre y una descripción. Cambie los objetos y los tipos de objeto, según sea necesario.
- **Para modificar un ámbito:** Selecciónelo en el panel central y, a continuación, haga clic en **Modificar ámbito** en el panel Acciones. Cambie el nombre, la descripción, los tipos de objeto y los objetos, según sea necesario.
- **Para eliminar un ámbito:** Selecciónelo en el panel central y, a continuación, haga clic en **Eliminar ámbito** en el panel Acciones. Cuando se le solicite, confirme la eliminación.

## Crear informes

Puede generar dos tipos de informes de administración delegada:

- Un informe HTML que ofrece una lista de los pares de rol y ámbito asociados a un administrador, además de los permisos individuales de cada tipo de objeto (por ejemplo, grupos de entrega y catálogos de máquinas). Este informe se genera desde Studio.

Para crear este informe, haga clic en **Configuración > Administradores** en el panel de navegación de Studio. Seleccione un administrador en el panel central y, a continuación, haga clic en **Crear informe** en el panel Acciones.

También puede solicitar este informe al crear, copiar o modificar un administrador.

- Un informe HTML o CSV donde figuran todas las asignaciones de roles integrados y personalizados con sus correspondientes permisos. Este informe se genera al ejecutar un script de PowerShell denominado `OutputPermissionMapping.ps1`.

Para ejecutar este script, es necesario ser un administrador total, un administrador de solo lectura, o un administrador personalizado que cuente con permiso para leer roles. El script se encuentra en: Archivos de programa\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Scripts.

Sintaxis:

```
OutputPermissionMapping.ps1 [-Help] [-Csv] [-Path string] [-AdminAddress string] [-Show] [CommonParameters]
```

Parámetro	Descripción
<code>-Help</code>	Muestra la ayuda del script.
<code>-Csv</code>	Especifica el archivo CSV resultante. Valor predeterminado = HTML
<code>-Path string</code>	Destino de escritura de los resultados. Valor predeterminado = stdout
<code>-AdminAddress string</code>	La dirección IP o el nombre de host del Delivery Controller con el que hay que establecer conexión. Predeterminado = localhost
<code>-Show</code>	(Válido solamente cuando el parámetro <code>-Path</code> también se especifica) Cuando se escribe el resultado en un archivo, <code>-Show</code> hace que dicho archivo se abra con el programa adecuado como, por ejemplo, un explorador web.
CommonParameters	<code>Verbose</code> , <code>Debug</code> , <code>ErrorAction</code> , <code>ErrorVariable</code> , <code>WarningAction</code> , <code>WarningVariable</code> , <code>OutBuffer</code> y <code>OutVariable</code> . Para obtener más información, consulte la documentación de Microsoft.

El siguiente ejemplo escribe una tabla HTML en un archivo denominado `Roles.html` y abre la tabla en un explorador web.

```

1 & "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
2 Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
3 -Path Roles.html - Show
4 <!--NeedCopy-->

```

El siguiente ejemplo escribe una tabla CSV en un archivo denominado Roles.csv. La tabla no se muestra.

```

1 & "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
2 Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
3 - CSV -Path Roles.csv
4 <!--NeedCopy-->

```

En una ventana de símbolo de sistema de Windows, el comando para el ejemplo anterior es:

```

1 powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\
2 Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1 '
3 -CSV -Path Roles.csv"
4 <!--NeedCopy-->

```

## Tarjetas inteligentes

September 22, 2021

Las tarjetas inteligentes y otras tecnologías equivalentes se admiten si se ajustan a las directrices descritas en este artículo. Para usar tarjetas inteligentes con Citrix Virtual Apps o Citrix Virtual Desktops:

- Debe conocer las directivas de seguridad de la empresa relacionadas con el uso de tarjetas inteligentes. Estas directivas pueden, por ejemplo, indicar cómo se proporcionan las tarjetas inteligentes a los usuarios y cómo estos deben protegerlas. Es posible que algunos aspectos de estas directivas deban evaluarse de nuevo en un entorno Citrix Virtual Apps o Citrix Virtual Desktops.
- Debe determinar los tipos de dispositivos de usuario, sistemas operativos y aplicaciones publicadas que deben usarse con las tarjetas inteligentes.
- Debe familiarizarse con la tecnología de las tarjetas inteligentes y el proveedor de hardware y software de tarjetas inteligentes que haya elegido.
- Debe saber cómo implementar certificados digitales en un entorno distribuido.

### Nota:

La inscripción con tarjeta inteligente no es compatible con [tarjetas inteligentes rápidas](#). La inscripción con tarjeta inteligente podría funcionar cuando la tarjeta inteligente rápida está inhabilitada.

ilitada, pero depende del tipo de tarjeta inteligente y del middleware. Para obtener información sobre la integración con Citrix Virtual Apps and Desktops y la compatibilidad para la inscripción con tarjetas inteligentes a través de sesiones virtuales, póngase en contacto con su proveedor de tarjetas inteligentes y middleware.

## Tipos de tarjetas inteligentes

Las tarjetas inteligentes de empresa y de consumidor tienen las mismas dimensiones, los mismos conectores eléctricos y se insertan en los mismos lectores de tarjetas inteligentes.

Las tarjetas inteligentes para empresa contienen certificados digitales. Estas tarjetas inteligentes admiten el inicio de sesión Windows, y también se pueden usar con aplicaciones para la firma digital y el cifrado de documentos y correos electrónicos. Citrix Virtual Apps and Desktops admiten estos usos.

En cambio, las tarjetas inteligentes de consumidor no contienen certificados digitales, sino un secreto compartido. Esas tarjetas inteligentes pueden admitir pagos (como una tarjeta de crédito de chip y firma o de chip y código secreto). No admiten inicios de sesión Windows ni aplicaciones típicas Windows. Por lo que se necesitan aplicaciones Windows especiales y una infraestructura de software adecuada (que incluya, por ejemplo, una conexión a una red de tarjetas de pago). Póngase en contacto con su representante de Citrix para obtener información acerca de la compatibilidad con esas aplicaciones especializadas en Citrix Virtual Apps o Citrix Virtual Desktops.

Para tarjetas inteligentes de empresa, existen opciones equivalentes que son compatibles y se pueden utilizar de una forma similar.

- Un token USB equivalente a una tarjeta inteligente se conecta directamente a un puerto USB. Esos tokens USB tienen normalmente el tamaño de una unidad flash USB, pero pueden ser tan pequeños como la tarjeta SIM de un teléfono móvil. Aparecen como la combinación de una tarjeta inteligente y un lector USB de tarjetas inteligentes.
- Una tarjeta inteligente virtual que utiliza el módulo de plataforma segura (Trusted Platform Module) de Windows aparece como una tarjeta inteligente. Esas tarjetas inteligentes virtuales se admiten en Windows 8 y Windows 10 con la aplicación Citrix Workspace (Citrix Receiver 4.3 como versión mínima).
  - Las versiones de Citrix Virtual Apps and Desktops (antes XenApp y XenDesktop) que sean anteriores a XenApp y XenDesktop 7.6 FP3 no admiten las tarjetas inteligentes virtuales.
  - Para obtener más información acerca de las tarjetas inteligentes virtuales, consulte [Virtual Smart Card Overview](#).

**Nota:** El término “tarjeta inteligente virtual” también se utiliza para designar un certificado digital que se almacena en el equipo del usuario. Esos certificados digitales no son estrictamente equivalentes a tarjetas inteligentes.

La funcionalidad de tarjetas inteligentes de Citrix Virtual Apps and Desktops está basada en las especificaciones estándar Personal Computer/Smart Card (PC/SC) de Microsoft. Requisito mínimo: las tarjetas inteligentes y los dispositivos de tarjeta inteligente deben ser compatibles con el sistema operativo Windows subyacente y deben estar aprobados por Microsoft Windows Hardware Quality Labs (WHQL) para utilizarse en equipos con sistemas operativos Windows válidos. Consulte la documentación de Microsoft para obtener más información sobre el cumplimiento normativo de hardware de PC/SC. Existen otros tipos de dispositivos de usuario que pueden cumplir el estándar PS/SC. Para obtener más información, consulte el [programa Citrix Ready](#).

Por lo general, se necesita un controlador de dispositivo independiente para la tarjeta inteligente o equivalente de cada proveedor. Sin embargo, si las tarjetas inteligentes cumplen un estándar como Personal Identity Verification (PIV) de NIST, se puede usar un solo controlador de dispositivo para una gama de tarjetas inteligentes. El controlador del dispositivo debe instalarse tanto en el dispositivo del usuario como en Virtual Delivery Agent (VDA). Ese controlador de dispositivo se incluye a menudo en el paquete de middleware de la tarjeta inteligente, disponible de un socio de Citrix. Ese paquete ofrece funciones avanzadas. El controlador del dispositivo también puede describirse como un mini-controlador, un proveedor de servicios de cifrado (CSP) o un proveedor de almacenamiento de claves (KSP).

Citrix ha probado las siguientes combinaciones de tarjeta inteligente con middleware para sistemas Windows como ejemplos representativos de su tipo. Sin embargo, también se pueden utilizar otras tarjetas inteligentes y otro middleware. Para obtener más información acerca de tarjetas inteligentes y middleware compatibles con Citrix, consulte <http://www.citrix.com/ready>.

---

Middleware	Tarjetas válidas
Minicontrolador Gemalto para tarjeta .NET	Gemalto .NET v2+

---

Para obtener información sobre el uso de tarjetas inteligentes con otros tipos de dispositivo, consulte la documentación de la aplicación Citrix Workspace referente al dispositivo concreto.

### **Acceso con Remote PC**

El uso de tarjetas inteligentes se admite solamente en el acceso remoto a PC físicos de oficina con Windows 10, Windows 8 o Windows 7.

Las siguientes tarjetas inteligentes se han probado con el acceso con Remote PC:

---

Middleware	Tarjetas válidas
Minicontrolador Gemalto .NET	Gemalto .NET v2+

---

## Tarjeta inteligente rápida

La tarjeta inteligente rápida es una mejora con respecto a la redirección HDX existente de tarjetas inteligentes basada en PC/SC. Mejora el rendimiento cuando se usan tarjetas inteligentes en redes WAN con latencia alta.

La tarjeta inteligente rápida está habilitada de forma predeterminada en máquinas host con agentes VDA de Windows compatibles actualmente. Para inhabilitar la tarjeta inteligente rápida en el lado del host (por ejemplo, con fines de diagnóstico), establezca el parámetro de Registro “CryptographicRedirectionDisable” en cualquier valor distinto de cero:

```
1 HKLM\SOFTWARE\Citrix\SmartCard
2 CryptographicRedirectionDisable (DWORD)
3 <!--NeedCopy-->
```

En el lado del cliente, para habilitar la tarjeta inteligente rápida, incluya el parámetro ICA SmartCard-CryptographicRedirection en el archivo *default.ica* del sitio StoreFront asociado:

```
1 [WFClient]
2 SmartCardCryptographicRedirection=0n
```

### Limitaciones:

- Solo Citrix Receiver para Windows admite las tarjetas inteligentes rápidas. Si configura tarjetas inteligentes rápidas en el archivo *default.ica*, los Citrix Receivers que no son para Windows seguirán funcionando con la redirección existente de PC/SC.
- Los únicos casos de doble salto donde se admiten las tarjetas inteligentes rápidas son ICA > ICA con la tarjeta inteligente rápida habilitada en ambos saltos. Como la tarjeta inteligente rápida no admite casos de doble salto ICA > RDP, esas situaciones no funcionan.
- La tarjeta inteligente rápida no es compatible con Cryptography Next Generation. Por lo tanto, la tarjeta inteligente rápida no admite tarjetas inteligentes de criptografía de curva elíptica (Elliptic Curve Cryptography o ECC).
- La tarjeta inteligente rápida solo admite operaciones de contenedor de claves de solo lectura.
- La tarjeta inteligente rápida no admite el cambio del PIN de la tarjeta inteligente.

## Tipos de lectores de tarjetas inteligentes

El lector de tarjetas inteligentes se puede integrar en el dispositivo del usuario, o bien se puede conectar al dispositivo del usuario (normalmente mediante USB o Bluetooth). Se admiten los lectores de

tarjetas con contacto que cumplen con la especificación de los dispositivos de interfaz de tarjetas inteligentes/chips USB (CCID). Contienen una ranura donde el usuario debe introducir o pasar la tarjeta inteligente. El estándar (Deutsche Kreditwirtschaft DK) define cuatro clases de lectores de tarjetas con contacto.

- Los lectores de tarjetas inteligentes de clase 1 son los más comunes, y normalmente solo contienen una ranura. Por norma general, los lectores de tarjetas inteligentes de clase 1 se admiten con un controlador de dispositivo CCID estándar que se suministra con el sistema operativo.
- Los lectores de tarjetas inteligentes de clase 2 constan, además, de un teclado seguro al que no se puede acceder desde el dispositivo de usuario. Los lectores de tarjetas inteligentes de clase 2 pueden estar integrados en un teclado que contenga a su vez un teclado numérico seguro. Para lectores de tarjetas inteligentes de clase 2, póngase en contacto con su representante de Citrix. Puede ser necesario un controlador de dispositivo específico del lector para habilitar la función de teclado numérico seguro.
- Los lectores de tarjetas inteligentes de clase 3 contienen, además, una pantalla segura. Los lectores de tarjetas inteligentes de clase 3 no se admiten.
- Los lectores de tarjetas inteligentes de clase 4 contienen, además, un módulo de transacción segura. Los lectores de tarjetas inteligentes de clase 4 no se admiten.

**Nota:**

La clase que tenga el lector de tarjetas inteligentes no tiene que ver con la clase de dispositivo USB.

Los lectores de tarjetas inteligentes deben instalarse con el controlador de dispositivo correspondiente en el dispositivo de usuario.

Para obtener información sobre los lectores admitidos de tarjetas inteligentes, consulte la documentación de la aplicación Citrix Workspace que utilice. En la documentación de la aplicación Citrix Workspace, las versiones admitidas suelen incluirse en el artículo de tarjetas inteligentes o en el artículo de requisitos del sistema.

## **Experiencia de usuario**

La funcionalidad de tarjetas inteligentes está integrada en Citrix Virtual Apps and Desktops mediante un canal virtual ICA/HDX determinado para tarjetas inteligentes que está habilitado de forma predefinida.

Importante: No utilice la redirección de USB genérico para lectores de tarjetas inteligentes. Esta funcionalidad está inhabilitada de forma predeterminada para lectores de tarjetas inteligentes y no se admite si se habilita.

Es posible utilizar varias tarjetas inteligentes y varios lectores en el mismo dispositivo de usuario, pero si la autenticación PassThrough se encuentra en uso solo debe insertarse una tarjeta inteligente

cuando el usuario inicia un escritorio virtual o una aplicación. Cuando se utiliza una tarjeta inteligente en una aplicación (por ejemplo, para las funciones de cifrado o firma digital), es posible que aparezcan solicitudes adicionales para insertar una tarjeta inteligente o introducir un PIN. Esto puede suceder cuando se inserta más de una tarjeta inteligente al mismo tiempo.

- Si se les solicita a los usuarios que inserten una tarjeta inteligente cuando la tarjeta inteligente ya se encuentra en el lector, deben seleccionar Cancelar.
- Si se solicita el PIN a los usuarios, deben introducirlo de nuevo.

Puede restablecer los PIN con un sistema de administración de tarjetas o alguna herramienta del proveedor.

**Importante:**

En una sesión de Citrix Virtual Apps o Citrix Virtual Desktops, no se admite el uso de una tarjeta inteligente con la aplicación Conexión a Escritorio remoto de Microsoft. Esto a veces se describe como un uso de “doble salto”.

### **Antes de implementar tarjetas inteligentes**

- Obtenga un controlador de dispositivo para el lector de tarjetas inteligentes e instálelo en el dispositivo de usuario. Muchos lectores de tarjetas inteligentes pueden usar el controlador de dispositivo CCID que proporciona Microsoft.
- Obtenga un controlador de dispositivo y el software de proveedor de servicios de cifrado (CSP) del proveedor de la tarjeta inteligente e instálelos en los dispositivos de usuario y escritorios virtuales. El controlador y el software CSP deben ser compatibles con Citrix Virtual Apps and Desktops; consulte la documentación del proveedor para comprobarlo. Para los escritorios virtuales con tarjetas inteligentes que admiten y usan el modelo de minicontroladores, esos minicontroladores de tarjeta inteligente deberían descargarse automáticamente, aunque pueden obtenerse del proveedor o en <http://catalog.update.microsoft.com>. Además, si se necesita middleware de PKCS #11, puede obtenerlo del proveedor de tarjetas.
- Importante: Se recomienda instalar y probar los controladores y el software CSP en un equipo físico antes de instalar el software de Citrix.
- Agregue la URL de Citrix Receiver para Web a la lista de sitios de confianza para los usuarios que trabajan con tarjetas inteligentes en Internet Explorer con Windows 10. En Windows 10, Internet Explorer no se ejecuta en el modo protegido de forma predeterminada para los sitios de confianza.
- Asegúrese de que la infraestructura de clave pública (PKI) está configurada correctamente. Esto incluye comprobar que la asignación de certificados a cuentas está configurada correctamente para el entorno de Active Directory y que la validación de certificados de usuario puede realizarse correctamente.

- Compruebe que su implementación cumple los requisitos del sistema de los demás componentes de Citrix utilizados con tarjetas inteligentes, incluidos la aplicación Citrix Workspace y StoreFront.
- Compruebe que tiene acceso a los siguientes servidores de su sitio:
  - El controlador de dominio de Active Directory para la cuenta de usuario que está asociada a un certificado de inicio de sesión de la tarjeta inteligente
  - Delivery Controller
  - Citrix StoreFront
  - Citrix Gateway/Citrix Access Gateway 10.x
  - VDA
  - (Optativo para acceso con Remote PC) Microsoft Exchange Server

## Habilitar el uso de tarjetas inteligentes

**Paso 1.** Proporcione tarjetas inteligentes a los usuarios de acuerdo con su directiva de emisión de tarjetas.

**Paso 2.** (Opcional) Configure las tarjetas inteligentes para permitir a los usuarios el acceso con Remote PC.

**Paso 3.** Instale y configure el Delivery Controller y StoreFront (si no están ya instalados) para la comunicación remota con tarjetas inteligentes.

**Paso 4.** Habilite StoreFront para el uso de tarjetas inteligentes. Para obtener más información, consulte Configuración de la autenticación con tarjeta inteligente en la documentación de StoreFront.

**Paso 5.** Habilite Citrix Gateway o Access Gateway para el uso de tarjetas inteligentes. Para obtener más información, consulte Configuración de la autenticación y la autorización y Configuración del acceso de tarjetas inteligentes con la Interfaz Web en la documentación de NetScaler.

**Paso 6.** Habilite agentes VDA para el uso de tarjetas inteligentes.

- Compruebe que el VDA tiene las aplicaciones y las actualizaciones necesarias.
- Instale el middleware.
- Configure la comunicación remota con tarjetas inteligentes, habilite la comunicación de datos de la tarjeta inteligente entre la aplicación Citrix Workspace presente en un dispositivo de usuario y una sesión de escritorio virtual.

**Paso 7.** Habilite los dispositivos de usuario (incluidas las máquinas que estén o no estén unidas a un dominio) para el uso de tarjetas inteligentes. Para obtener más información, consulte Configuración de la autenticación con tarjeta inteligente en la documentación de StoreFront.

- Importe el certificado raíz y el certificado de emisión de la entidad de certificación en el almacén de claves del dispositivo.

- Instale el middleware del proveedor de la tarjeta inteligente.
- Instale y configure la aplicación Citrix Workspace para Windows; importe icaclient.adm mediante la Consola de administración de directivas de grupo y habilite la autenticación con tarjeta inteligente.

**Paso 8.** Realice pruebas en la implementación. Compruebe que la implementación está correctamente configurada iniciando un escritorio virtual con la tarjeta inteligente de un usuario de prueba. Pruebe todos los mecanismos de acceso posibles (por ejemplo, el acceso al escritorio a través de Internet Explorer y la aplicación Citrix Workspace).

## Implementaciones de tarjeta inteligente

January 4, 2021

Los siguientes tipos de implementaciones de tarjeta inteligente se admiten en esta versión del producto y en entornos mixtos que contengan esta versión. Hay otras configuraciones que pueden funcionar, pero no se admiten.

---

Tipo	Conectividad con StoreFront
Equipos unidos a un dominio local	Conectados directamente
Acceso remoto desde equipos unidos a un dominio	Conectados a través de Citrix Gateway
Equipos no unidos a dominio	Conectados directamente
Acceso remoto desde equipos no unidos a un dominio	Conectados a través de Citrix Gateway
Clientes ligeros y equipos que no pertenecen a un dominio y acceden a un sitio de Desktop Appliance	Conectados a través de sitios de Desktop Appliance
Clientes ligeros y equipos que pertenecen a un dominio y acceden a StoreFront con una URL de Servicios XenApp	Conectados a través de direcciones URL de Servicios XenApp

---

Los tipos de implementación se definen por las funciones del dispositivo del usuario al que está conectado el lector de tarjetas inteligentes:

- Si el dispositivo está unido a un dominio o no.
- Cómo se conecta el dispositivo con StoreFront.
- Qué software se usa para ver las aplicaciones y los escritorios virtuales.

Además, las aplicaciones habilitadas para tarjeta inteligente, tales como Microsoft Word y Microsoft Excel, también se pueden utilizar en estas implementaciones. Esas aplicaciones permiten a los usuarios firmar o cifrar documentos digitalmente.

## **Autenticación bimodal**

Cuando es posible en cada una de estas implementaciones, Receiver admite la autenticación bimodal, que ofrece al usuario la posibilidad de elegir si quiere autenticarse con tarjeta inteligente o con nombre de usuario y contraseña. Esto resulta útil cuando no se puede usar la tarjeta inteligente por alguna razón (por ejemplo, si el usuario la olvidó en casa o el certificado de inicio de sesión caducó).

Como los usuarios de dispositivos que no pertenecen a un dominio inician sesión en Receiver para Windows directamente, puede permitir que los usuarios recurran a la autenticación explícita. Si configura la autenticación bimodal, a los usuarios se les solicita que inicien sesión con una tarjeta inteligente y su PIN, pero tienen la opción de seleccionar la autenticación explícita si tienen problemas con las tarjetas inteligentes.

Si implementa Citrix Gateway, los usuarios inician sesión en sus dispositivos y Receiver para Windows les pedirá autenticarse en Citrix Gateway. Esto se aplica a dispositivos unidos a un dominio y a dispositivos que no pertenecen a ningún dominio. Los usuarios pueden iniciar sesión en Citrix Gateway con su tarjeta inteligente y su PIN o con credenciales explícitas. Eso permite ofrecer a los usuarios la autenticación bimodal para los inicios de sesión en Citrix Gateway. Configure la autenticación PassThrough desde Citrix Gateway a StoreFront y delegue la validación de las credenciales a Citrix Gateway para los usuarios de tarjeta inteligente, de modo que los usuarios se autentifiquen silenciosamente en StoreFront.

## **Consideraciones cuando hay varios bosques de Active Directory**

En un entorno Citrix, se admite el uso de tarjetas inteligentes dentro de un único bosque. Los inicios de sesión con tarjeta inteligente que abarcan varios bosques requieren una relación de confianza bidireccional de bosques en todas las cuentas de usuario. Las implementaciones más complejas de tarjeta inteligente con varios bosques (es decir, donde las relaciones de confianza son unidireccionales o de diferentes tipos) no se admiten.

Se puede usar tarjetas inteligentes en entornos Citrix que incluyen escritorios remotos. Esta función se puede instalar localmente (en el dispositivo de usuario al que está conectada la tarjeta inteligente) o de forma remota (en el escritorio remoto al que se conecta el dispositivo del usuario).

## Directiva de extracción de tarjetas inteligentes

La directiva de extracción de tarjetas inteligentes definida en el producto determina el comportamiento al extraer la tarjeta inteligente del lector durante una sesión. El sistema operativo Windows configura y controla esta directiva de extracción.

---

Configuración de directiva	Comportamiento del escritorio
Ninguna acción	Ninguna acción.
Bloquear estación de trabajo	La sesión de escritorio se desconecta y el escritorio virtual queda bloqueado.
Forzar cierre de sesión	El usuario se ve forzado a cerrar la sesión. Si se pierde la conexión de red y esta configuración está habilitada, es posible que se cierre la sesión y el usuario pierda ciertos datos.
Desconectar si es una sesión remota de Terminal Services	La sesión se desconecta y el escritorio virtual queda bloqueado.

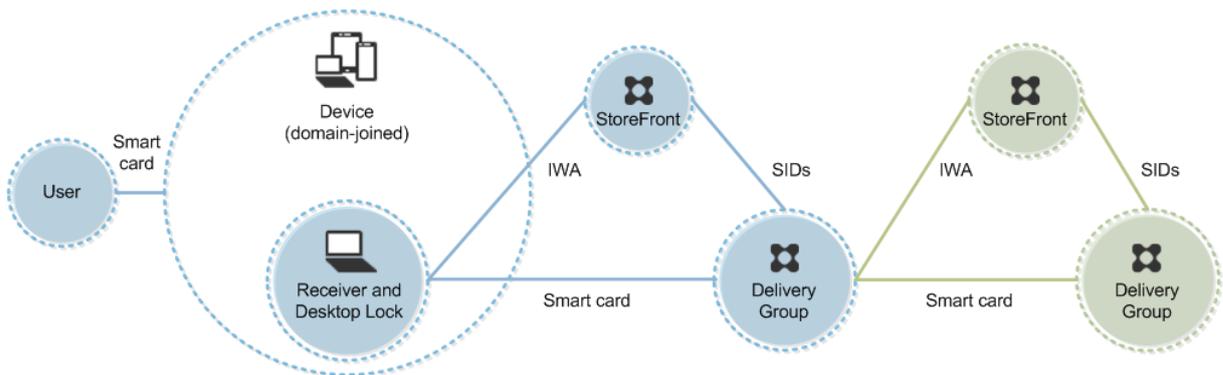
---

## Comprobar la revocación de certificados

Si la comprobación de revocación de certificados está habilitada y un usuario introduce una tarjeta inteligente con un certificado no válido en el lector de tarjetas, el usuario no se puede autenticar ni acceder al escritorio o a la aplicación relacionados con el certificado. Por ejemplo, si el certificado no válido se usa para el proceso de descifrado de correo electrónico, el correo electrónico seguirá cifrado. Si hay otros certificados en la tarjeta, tales como los utilizados para la autenticación, que aún son válidos, sus funciones permanecen activas.

## Ejemplo de implementación: equipos que pertenecen a un dominio

Esta implementación contiene dispositivos de usuario que están unidos a un dominio, y que ejecutan Desktop Viewer y se conectan directamente a StoreFront.

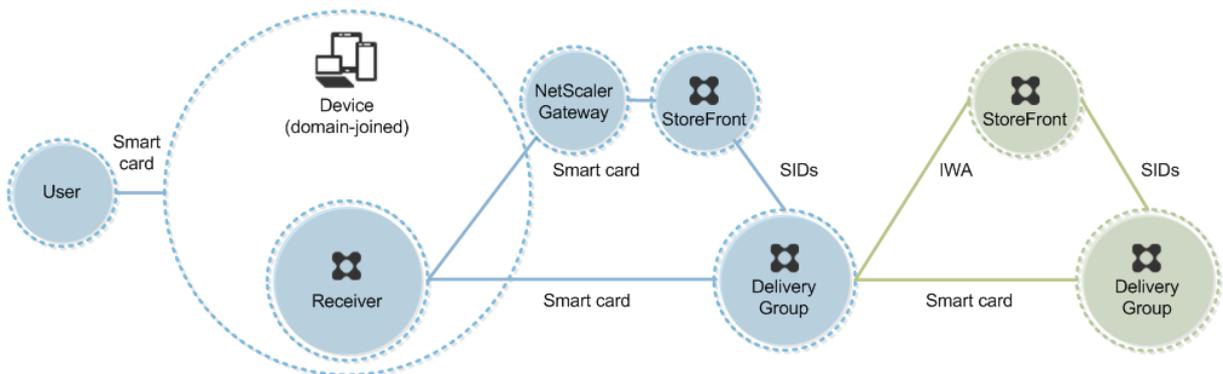


El usuario inicia sesión en un dispositivo mediante una tarjeta inteligente y un PIN. Receiver autentica al usuario en un servidor de StoreFront mediante la autenticación integrada de Windows (IWA). StoreFront pasa los identificadores de seguridad del usuario (SID) a Citrix Virtual Apps o Citrix Virtual Desktops. Cuando el usuario inicia una aplicación o un escritorio virtual, no se vuelve a solicitar el PIN al usuario porque la función de Single Sign-On está configurada en Receiver.

Esta implementación se puede ampliar a una configuración de doble salto con la incorporación de un segundo servidor de StoreFront y un servidor que aloja aplicaciones. Un Receiver desde el escritorio virtual se autentica en el segundo servidor de StoreFront. Con esta segunda conexión se puede usar cualquier método de autenticación. La configuración que se muestra para el primer salto se puede volver a utilizar en el segundo salto o usarse en el segundo salto solamente.

### Ejemplo de implementación: acceso remoto desde equipos unidos a un dominio

Esta implementación contiene dispositivos de usuario que están unidos a un dominio, que ejecutan Desktop Viewer y se conectan a StoreFront a través de Citrix Gateway o Access Gateway.



El usuario inicia sesión en un dispositivo con una tarjeta inteligente y un PIN. A continuación, inicia otra sesión en Citrix Gateway o Access Gateway. Este segundo inicio de sesión puede realizarse con la tarjeta inteligente y el PIN, o con un nombre de usuario y una contraseña, porque Receiver permite la autenticación bimodal en esta implementación.

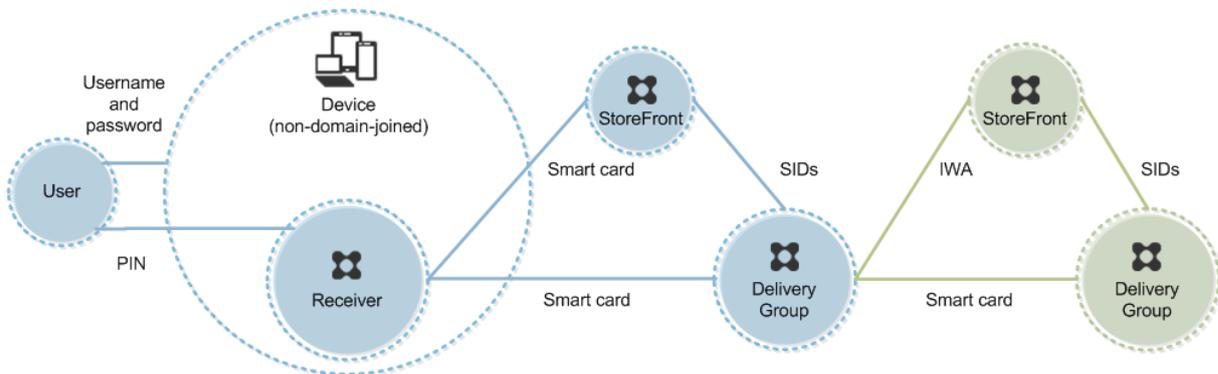
El usuario inicia sesión automáticamente en StoreFront, el cual pasa los identificadores de seguridad

(SID) del usuario a Citrix Virtual Apps o Citrix Virtual Desktops. Cuando el usuario inicia una aplicación o un escritorio virtual, no se vuelve a solicitar el PIN al usuario porque la función de Single Sign-On está configurada en Receiver.

Esta implementación se puede ampliar a una configuración de doble salto con la incorporación de un segundo servidor de StoreFront y un servidor que aloja aplicaciones. Un Receiver desde el escritorio virtual se autentica en el segundo servidor de StoreFront. Con esta segunda conexión se puede usar cualquier método de autenticación. La configuración que se muestra para el primer salto se puede volver a utilizar en el segundo salto o usarse en el segundo salto solamente.

### Ejemplo de implementación: equipos que no pertenecen a un dominio

Esta implementación contiene dispositivos de usuario que no están unidos a un dominio, y que ejecutan Desktop Viewer y se conectan directamente a StoreFront.



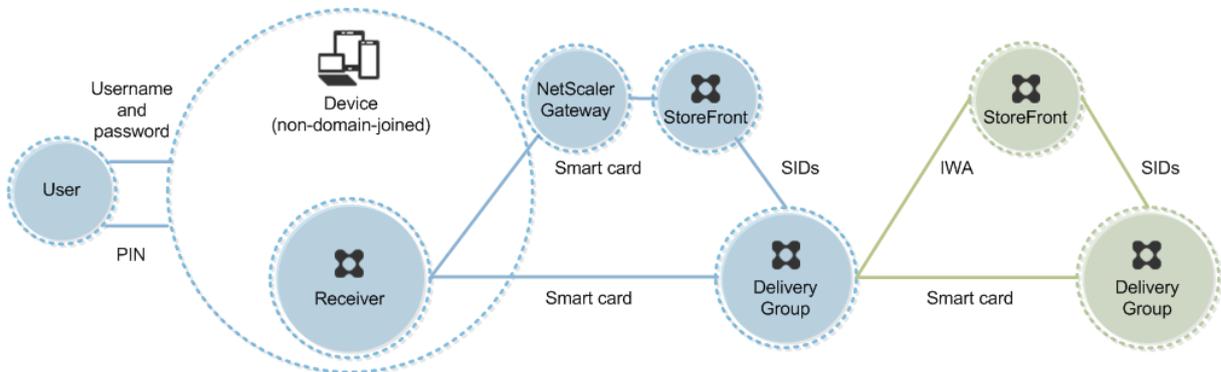
El usuario inicia la sesión en un dispositivo. Por lo general, el usuario introduce un nombre de usuario y una contraseña pero, como el dispositivo no está unido a un dominio, las credenciales de inicio de sesión son optativas. Como la autenticación bimodal es posible en esta implementación, Receiver pide al usuario una tarjeta inteligente y un PIN, o un nombre de usuario y una contraseña. A continuación, Receiver se autentica en StoreFront.

StoreFront pasa los identificadores de seguridad del usuario (SID) a Citrix Virtual Apps o Citrix Virtual Desktops. Cuando el usuario inicia una aplicación o un escritorio virtual, se solicita un PIN al usuario de nuevo porque la función de Single Sign-On no está disponible en esta implementación.

Esta implementación se puede ampliar a una configuración de doble salto con la incorporación de un segundo servidor de StoreFront y un servidor que aloja aplicaciones. Un Receiver desde el escritorio virtual se autentica en el segundo servidor de StoreFront. Con esta segunda conexión se puede usar cualquier método de autenticación. La configuración que se muestra para el primer salto se puede volver a utilizar en el segundo salto o usarse en el segundo salto solamente.

## Ejemplo de implementación: acceso remoto desde equipos que no están unidos a un dominio

Esta implementación contiene dispositivos de usuario que no están unidos a un dominio, y que ejecutan Desktop Viewer y se conectan directamente a StoreFront.



El usuario inicia la sesión en un dispositivo. Por lo general, el usuario introduce un nombre de usuario y una contraseña pero, como el dispositivo no está unido a un dominio, las credenciales de inicio de sesión son optativas. Como la autenticación bimodal es posible en esta implementación, Receiver pide al usuario una tarjeta inteligente y un PIN, o un nombre de usuario y una contraseña. A continuación, Receiver se autentica en StoreFront.

StoreFront pasa los identificadores de seguridad del usuario (SID) a Citrix Virtual Apps o Citrix Virtual Desktops. Cuando el usuario inicia una aplicación o un escritorio virtual, se solicita un PIN al usuario de nuevo porque la función de Single Sign-On no está disponible en esta implementación.

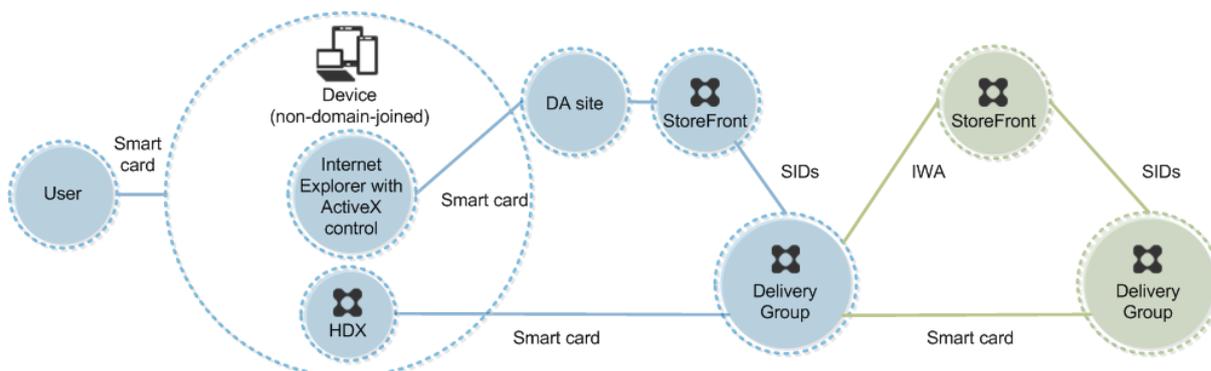
Esta implementación se puede ampliar a una configuración de doble salto con la incorporación de un segundo servidor de StoreFront y un servidor que aloja aplicaciones. Un Receiver desde el escritorio virtual se autentica en el segundo servidor de StoreFront. Con esta segunda conexión se puede usar cualquier método de autenticación. La configuración que se muestra para el primer salto se puede volver a utilizar en el segundo salto o usarse en el segundo salto solamente.

## Ejemplo de implementación: acceso al sitio de Desktop Appliance desde clientes ligeros y equipos que no pertenecen a un dominio

Esta implementación contiene dispositivos de usuario que no están unidos a un dominio que pueden ejecutar Desktop Lock y se conectan a StoreFront a través de sitios de Desktop Appliance.

Desktop Lock es un componente independiente que se suministra con Citrix Virtual Apps, Citrix Virtual Desktops y VDI-in-a-Box. Es una alternativa a Desktop Viewer que se ha diseñado principalmente para equipos Windows reasignados y clientes ligeros Windows. Desktop Lock reemplaza el shell y el Administrador de tareas de Windows en los dispositivos de los usuarios, lo que impide que los usuarios accedan al dispositivo subyacente. Con Desktop Lock, los usuarios pueden acceder a los escritorios

de máquinas de servidor Windows y a escritorios de máquinas de escritorio Windows. La instalación de Desktop Lock es optativa.



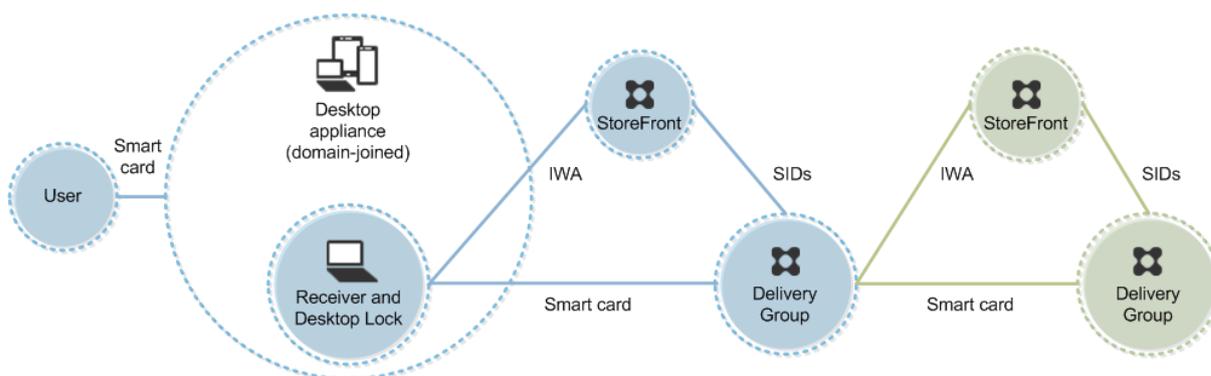
El usuario inicia una sesión en un dispositivo mediante una tarjeta inteligente. Si Desktop Lock se está ejecutando en el dispositivo, el dispositivo está configurado para iniciar el sitio de Desktop Appliance a través de Internet Explorer ejecutado en modo quiosco (pantalla completa). Un control ActiveX en el sitio solicita el PIN al usuario y lo envía a StoreFront. StoreFront pasa los identificadores de seguridad del usuario (SID) a Citrix Virtual Apps o Citrix Virtual Desktops. Se iniciará el primer escritorio que esté disponible en la lista alfabética del grupo de escritorios asignado.

Esta implementación se puede ampliar a una configuración de doble salto con la incorporación de un segundo servidor de StoreFront y un servidor que aloja aplicaciones. Un Receiver desde el escritorio virtual se autentica en el segundo servidor de StoreFront. Con esta segunda conexión se puede usar cualquier método de autenticación. La configuración que se muestra para el primer salto se puede volver a utilizar en el segundo salto o usarse en el segundo salto solamente.

### **Ejemplo de implementación: implementación de clientes ligeros y equipos que pertenecen a un dominio y acceden a StoreFront a través de la URL de servicios XenApp**

Esta implementación contiene dispositivos de usuario que están unidos a un dominio y que ejecutan Desktop Lock y se conectan a StoreFront a través de direcciones URL de Servicios XenApp.

Desktop Lock es un componente independiente que se suministra con Citrix Virtual Apps, Citrix Virtual Desktops y VDI-in-a-Box. Es una alternativa a Desktop Viewer que se ha diseñado principalmente para equipos Windows reasignados y clientes ligeros Windows. Desktop Lock reemplaza el shell y el Administrador de tareas de Windows en los dispositivos de los usuarios, lo que impide que los usuarios accedan al dispositivo subyacente. Con Desktop Lock, los usuarios pueden acceder a los escritorios de máquinas de servidor Windows y a escritorios de máquinas de escritorio Windows. La instalación de Desktop Lock es optativa.



El usuario inicia sesión en un dispositivo mediante una tarjeta inteligente y un PIN. Si Desktop Lock se está ejecutando en el dispositivo, autentica al usuario en un servidor de StoreFront mediante la autenticación integrada de Windows (IWA). StoreFront pasa los identificadores de seguridad del usuario (SID) a Citrix Virtual Apps o Citrix Virtual Desktops. Cuando el usuario inicia un escritorio virtual, no se vuelve a solicitar el PIN al usuario porque la función de Single Sign-On está configurada en Receiver.

Esta implementación se puede ampliar a una configuración de doble salto con la incorporación de un segundo servidor de StoreFront y un servidor que aloja aplicaciones. Un Receiver desde el escritorio virtual se autentica en el segundo servidor de StoreFront. Con esta segunda conexión se puede usar cualquier método de autenticación. La configuración que se muestra para el primer salto se puede volver a utilizar en el segundo salto o usarse en el segundo salto solamente.

## Autenticación PassThrough y Single Sign-On con tarjetas inteligentes

January 4, 2021

### Autenticación mediante paso de credenciales (PassThrough)

La autenticación PassThrough con tarjeta inteligente en los escritorios virtuales se admite en los dispositivos de usuario con Windows 10, Windows 8 y Windows 7 SP1, ediciones Enterprise y Profesional.

La autenticación PassThrough con tarjeta inteligente en aplicaciones alojadas se admite en servidores que ejecutan Windows Server 2016, Windows Server 2012 R2, Windows Server 2012 y Windows Server 2008 R2 SP1.

Para utilizar la autenticación PassThrough con tarjeta inteligente en aplicaciones alojadas, asegúrese de habilitar el uso de Kerberos cuando configure PassThrough con tarjeta inteligente como el método de autenticación para el sitio.

Nota: La disponibilidad de la autenticación PassThrough con tarjeta inteligente depende de varios factores, incluidos, entre otros:

- Las directivas de seguridad de la organización respecto a la autenticación PassThrough.
- El tipo y la configuración del middleware.
- Los tipos de lectores de tarjetas inteligentes.
- Las directivas de caché de PIN en el middleware.

La autenticación PassThrough con tarjeta inteligente se configura en Citrix StoreFront. Consulte la documentación de StoreFront para obtener más información.

## Single Sign-On

Single Sign-On es una función de Citrix que implementa la autenticación PassThrough en el inicio de escritorios virtuales y aplicaciones. Puede utilizar esta función en implementaciones de tarjeta inteligente unidas a dominio, para la autenticación directa en StoreFront y desde NetScaler a StoreFront para reducir la cantidad de veces que los usuarios tienen que introducir su PIN. Para usar Single Sign-On en estos tipos de implementación, modifique los siguientes parámetros en el archivo default.ica, que se encuentra en el servidor de StoreFront:

- Implementaciones de tarjetas inteligentes unidas a dominio, directas a StoreFront: `DisableCtrlAltDel`
- Implementaciones de tarjetas inteligentes unidas a dominio, desde NetScaler a StoreFront: `ActiveUseLocalUserAndPassword`

Para obtener instrucciones sobre cómo configurar estos parámetros, consulte la documentación de StoreFront o Citrix Gateway.

La disponibilidad de la funcionalidad de Single Sign-On depende de varios factores, incluidos, entre otros:

- Las directivas de seguridad de la organización respecto a Single Sign-On.
- El tipo y la configuración del middleware.
- Los tipos de lectores de tarjetas inteligentes.
- Las directivas de caché de PIN en el middleware.

### Nota:

Cuando el usuario inicia sesión en el Virtual Delivery Agent (VDA) presente en una máquina que tiene un lector de tarjetas inteligentes conectado, puede aparecer un icono de Windows que representa el anterior método de autenticación utilizado correctamente (como una tarjeta inteligente o contraseña). Como resultado, cuando se habilita Single Sign-On, puede aparecer el icono de Single Sign-On. Para iniciar una sesión, el usuario debe hacer clic en **Cambiar de**

**usuario** para seleccionar otro icono ya que el de Single Sign-On no funcionará.

## Transport Layer Security (TLS)

June 9, 2022

Citrix Virtual Apps and Desktops admiten el protocolo Transport Layer Security (TLS) para las conexiones por TCP entre los componentes. Citrix Virtual Apps and Desktops también admiten el protocolo Datagram Transport Layer Security (DTLS) para las conexiones ICA o HDX por UDP cuando se utiliza el [transporte adaptable](#).

TLS y DTLS son similares y admiten los mismos certificados digitales. Configurar un sitio Citrix Virtual Apps o Citrix Virtual Desktops para usar TLS también lo configura para usar DTLS. Siga estos procedimientos; son los mismos pasos tanto para TLS como para DTLS (excepto donde se indique):

- Obtener, instalar y registrar un certificado de servidor en todos los Delivery Controllers y configurar un puerto con el certificado TLS. Para obtener más información, consulte [Instalar certificados de servidor TLS en los Controllers](#).

Si lo quiere, puede cambiar los puertos que Controller utiliza para escuchar el tráfico HTTP y HTTPS.

- Habilite las conexiones TLS entre la aplicación Citrix Workspace y los agentes VDA (Virtual Delivery Agent) completando las siguientes tareas:
  - Configure TLS en las máquinas donde los VDA están instalados. (Para simplificar, en adelante se usará “VDA” para hacer referencia a la máquina donde está instalado un VDA.) Para obtener información general, consulte [Parámetros de TLS en los VDA](#). Se recomienda que utilice el script de PowerShell suministrado por Citrix para configurar TLS o DTLS. Para obtener información detallada, consulte [Configurar TLS en un VDA mediante el script de PowerShell](#). Sin embargo, si quiere configurar TLS o DTLS manualmente, consulte [Configurar TLS manualmente en un VDA](#).
  - Configure TLS en los grupos de entrega que contienen los VDA mediante la ejecución de un conjunto de cmdlets de PowerShell en Studio. Para obtener más información, consulte [Configuración de TLS en los grupos de entrega](#).

Requisitos y consideraciones:

- \* El hecho de habilitar conexiones TLS entre los usuarios y los VDA solo es válido para los sitios de XenApp 7.6 y XenDesktop 7.6 y versiones posteriores compatibles.
- \* Configure TLS en los grupos de entrega y en los VDA después de instalar los componentes, crear un sitio, crear catálogos de máquinas y crear grupos de entrega.

- \* Para configurar TLS en los grupos de entrega, debe tener permiso para cambiar las reglas de acceso a los Controllers. Un administrador total tiene este permiso.
- \* Para configurar TLS en los VDA, debe ser un administrador Windows en la máquina donde está instalado el VDA.
- \* En agentes VDA agrupados y aprovisionados por Machine Creation Services o Provisioning Services, la imagen de la máquina del VDA se restablece en el proceso de reinicio, lo que provoca la pérdida de la configuración anterior de TLS. Ejecute el script de PowerShell cada vez que se reinicie el VDA para volver a configurar los parámetros de TLS.

#### **Advertencia:**

Para las tareas que impliquen modificar el Registro de Windows, tenga cuidado: si se modifica de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Para obtener información acerca de la habilitación de TLS para la base de datos del sitio, consulte [CTX137556](#).

## **Instalar certificados de servidor TLS en los Controllers**

Para HTTPS, XML Service admite las funciones de TLS cuando se usan certificados de servidor, no cuando se usan certificados de cliente. En esta sección, se describe la adquisición e instalación de certificados TLS en Delivery Controllers. Los mismos pasos se pueden aplicar a Cloud Connectors para cifrar el tráfico STA y XML.

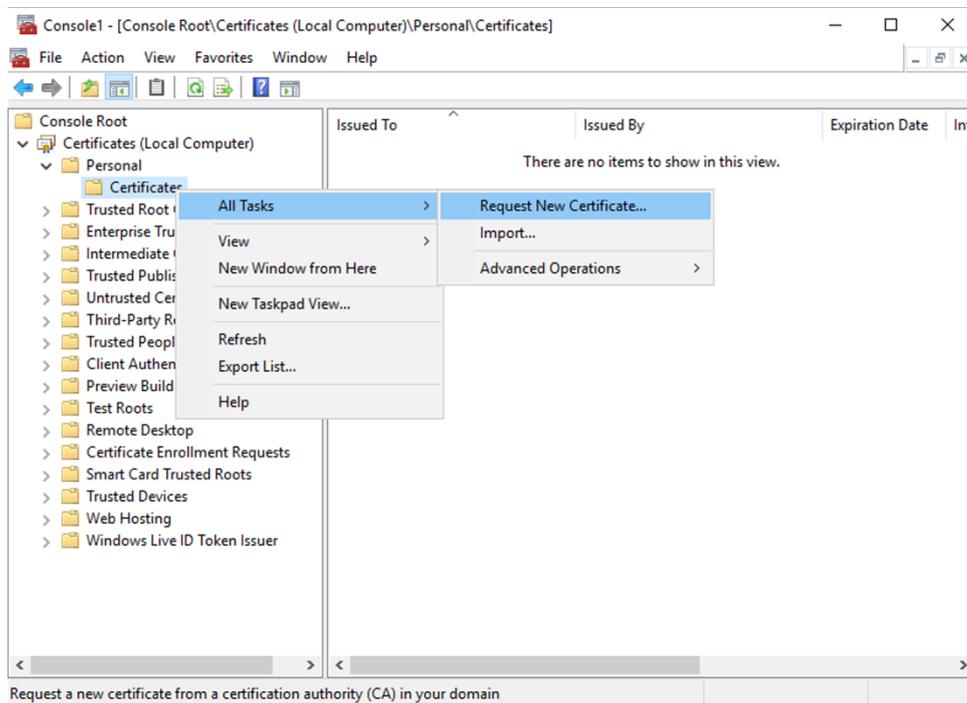
Aunque hay varios tipos diferentes de entidades de certificación y métodos para solicitar certificados de ellas, en este artículo se describe la entidad emisora de certificados de Microsoft. La entidad de certificación de Microsoft debe tener una plantilla de certificado publicada con el propósito Autenticación de servidor.

Si la entidad de certificación de Microsoft está integrada en un dominio de Active Directory o en el bosque de confianza al que están unidos los Delivery Controllers, se puede adquirir un certificado desde el asistente para inscripción de certificados del complemento MMC Certificados.

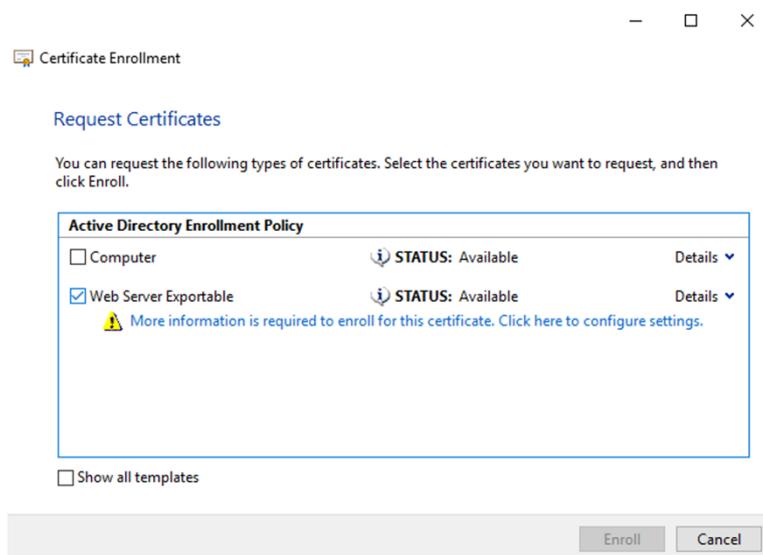
### **Solicitar e instalar un certificado**

1. En el Delivery Controller, abra la consola de MMC y agregue el complemento Certificados. Cuando se le solicite, seleccione Cuenta de equipo.

2. Expanda **Personal > Certificados** y, a continuación, utilice la opción de menú contextual **Todas las tareas > Solicitar un nuevo certificado**.



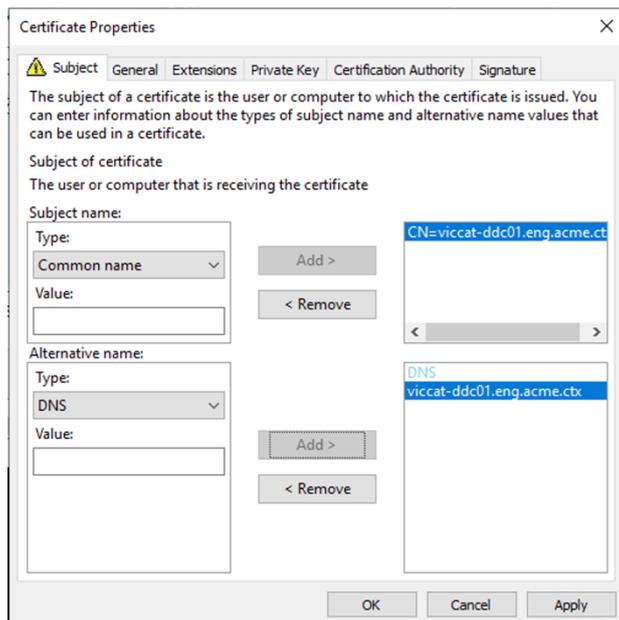
3. Haga clic en **Siguiente** para comenzar y en **Siguiente** para confirmar que va a adquirir el certificado de inscripción en Active Directory.
4. Seleccione la plantilla para Certificado de autenticación de servidor. Si la plantilla se ha configurado para proporcionar automáticamente los valores para Asunto, puede hacer clic en **Inscribir** sin proporcionar más datos.



5. Para proporcionar más detalles para la plantilla de certificado, haga clic en el botón de flecha **Detalles** y configure lo siguiente:

**Nombre del asunto:** Seleccione Nombre común y agregue el FQDN del Delivery Controller.

**Nombre alternativo:** Seleccione DNS y agregue el FQDN del Delivery Controller.



## Configurar el puerto de escucha SSL/TLS

1. Abra una ventana de comandos de PowerShell como administrador de la máquina.
2. Ejecute los siguientes comandos para obtener el GUID de aplicación de Broker Service:

```

1 New-PSDrive -Name HKCR -PSProvider Registry -Root
   HKEY_CLASSES_ROOT
2
3 $Service_Guid = Get-ChildItem HKCR:\Installer\Products -Recurse -
   Ea 0 | Where-Object {
4   $key = $_; $_.GetValueNames() | ForEach-Object {
5   $key.GetValue($_) }
6   | Where-Object {
7   $_ -like 'Citrix Broker Service' }
8   }
9   | Select-Object Name
10
11 $Service_Guid.Name -match "[A-Z0-9]*$"
12
13 $Guid = $Matches[0]
14
15 [GUID]$Formatted_Guid = $Guid
16
17 Remove-PSDrive -Name HKCR
18
19 Write-Host "Broker Service Application GUID: $($Formatted_Guid)" -
   ForegroundColor Yellow

```

```
20 <!--NeedCopy-->
```

3. Ejecute los siguientes comandos en la misma ventana de PowerShell para obtener la huella digital del certificado que instaló anteriormente:

```
1 $HostName = ([System.Net.Dns]::GetHostByName(($env:computerName)))
   .Hostname
2
3 $Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-
   Object {
4   $_.Subject -match ("CN=" + $HostName) }
5   ).Thumbprint -join ';'
6
7 Write-Host -Object "Certificate Thumbprint for $($HostName): $(
   $Thumbprint)" -ForegroundColor Yellow
8 <!--NeedCopy-->
```

4. Ejecute los siguientes comandos en la misma ventana de PowerShell para configurar el puerto SSL/TLS de Broker Service y usar el certificado para el cifrado:

```
1 $IPV4_Address = Test-Connection -ComputerName $HostName -Count 1
   | Select-Object -ExpandProperty IPV4Address
2
3 $IPPort = "$($IPV4_Address):443"
4
5 $SSLxml = "http add sslcert ipport=$IPPort certhash=$Thumbprint
  appid={
6   $Formatted_Guid }
7   "
8
9 $SSLxml | netsh
10
11 . netsh http show sslcert
12 <!--NeedCopy-->
```

Cuando se configura correctamente, el resultado del último comando `.netsh http show sslcert` muestra que el agente de escucha utiliza el `IP:port` correcto y que `Application ID` es el GUID de aplicación de Broker Service.

Si los servidores confían en el certificado instalado en los Delivery Controllers, ahora puede configurar los vínculos de Delivery Controllers de StoreFront y Citrix Gateway STA para que utilicen HTTPS, en lugar de HTTP.

**Nota:**

Si el Controller está instalado en Windows Server 2016 o Windows Server 2019, y StoreFront está instalado en Windows Server 2012 R2, es necesario cambiar la configuración en el Controller o en StoreFront para cambiar el orden de los conjuntos de cifrado TLS. Este cambio de configuración no es necesario para Controller ni StoreFront con otras combinaciones de versiones de Windows

Server.

La lista ordenada de los conjuntos de cifrado debe incluir el conjunto de cifrado `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384` o `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` (o ambos) o conjuntos de cifrado `TLS_ECDHE` similares, y estos conjuntos deben preceder los conjuntos de cifrado `TLS_DHE`.

1. Desde el editor de directivas de grupo de Microsoft, vaya a Configuración del equipo > Plantillas administrativas > Red > Opciones de configuración SSL.
2. Modifique la directiva “Orden de conjuntos de cifrado SSL”. De manera predeterminada, esta directiva está establecida en “No configurada”. Habilite esta directiva.
3. Ordene los conjuntos de cifrado; quite aquellos conjuntos que no quiera usar.

Compruebe que `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384`, `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` o un conjunto de cifrado `TLS_ECDHE` similar preceda los conjuntos de cifrado `TLS_DHE`.

En Microsoft MSDN, también puede consultar [Prioritizing Schannel Cipher Suites](#).

## Cambiar puertos HTTP o HTTPS

De forma predeterminada, el XML Service en el Controller escucha en los puertos 80 para el tráfico HTTP y 443 para el tráfico HTTPS. Aunque se pueden utilizar otros puertos distintos de los predeterminados, tenga en cuenta los riesgos de seguridad que implica la exposición de un Controller a redes que no son de confianza. Antes que cambiar los valores predeterminados, es preferible implementar un servidor de StoreFront independiente.

Para cambiar los puertos HTTP o HTTPS predeterminados que usa el Controller, ejecute el comando siguiente en Studio:

**BrokerService.exe -WIPORT <puerto http> -WISSLPORIT <puerto https>**

<puerto http> es el número de puerto para el tráfico HTTP y <puerto https> es el número de puerto para el tráfico HTTPS.

### Nota:

Después de cambiar de un puerto, Studio puede mostrar un mensaje acerca de la actualización y la compatibilidad de licencias. Para resolver el problema, vuelva a registrar las instancias de servicio mediante esta secuencia de cmdlet de PowerShell:

```
1 Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding
   XML_HTTPS |
2 Unregister-ConfigRegisteredServiceInstance
3 Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |
4 Register-ConfigServiceInstance
5 <!--NeedCopy-->
```

### **Solo aplicar el tráfico HTTPS**

Si quiere que XML Service ignore el tráfico HTTP, cree el siguiente parámetro de Registro en HKLM\Software\Citrix\DesktopServer\ en el Controller y reinicie el Broker Service.

Para ignorar el tráfico HTTP, cree DWORD XmlServicesEnableNonSsl y dele el valor 0.

Se puede crear el valor DWORD de Registro correspondiente para ignorar el tráfico HTTPS: DWORD XmlServicesEnableSsl. Compruebe que no está establecido en 0.

### **Parámetros de TLS en agentes VDA**

Un grupo de entrega no puede incluir una mezcla de VDA con TLS configurado y VDA sin TLS configurado. Antes de configurar TLS para un grupo de entrega, debe haber configurado TLS para todos los VDA en ese grupo de entrega.

Si configura TLS en los VDA, cambian los permisos en el certificado TLS instalado, lo que da al servicio ICA acceso de lectura a la clave privada del certificado e informa al servicio ICA de lo siguiente:

- **Qué certificado del almacén de certificados hay que usar para TLS.**
- **Qué número de puerto TCP hay que usar para las conexiones TLS.**

El Firewall de Windows (si está habilitado) debe estar configurado para permitir conexiones entrantes en este puerto TCP. Esta configuración se lleva a cabo cuando se usa el script de PowerShell.

- **Qué versiones del protocolo TLS se deben permitir.**

**Importante:**

Citrix recomienda revisar el uso de SSL 3 y volver a configurar las implementaciones para retirar la compatibilidad con SSL 3 donde corresponda. Consulte [CTX200238](#).

Las versiones compatibles con el protocolo TLS siguen una jerarquía (de menor a mayor): SSL 3.0, TLS 1.0, TLS 1.1 y TLS 1.2. Debe especificar la versión mínima permitida; se permitirán todas las conexiones que usen esa versión del protocolo o una versión más alta.

Por ejemplo, si especifica TLS 1.1 como la versión mínima, se permitirán conexiones con TLS 1.1 y TLS 1.2. Si elige SSL 3.0 como la versión mínima, se permitirán conexiones con todas las versiones admitidas. Si especifica TLS 1.2 como la versión mínima, solo se permiten conexiones con TLS 1.2.

DTLS 1.0 corresponde a TLS 1.1, mientras que DTLS 1.2 corresponde a TLS 1.2.

- **Qué conjuntos de cifrado TLS se deben permitir.**

El conjunto de cifrado selecciona el cifrado que se usa para una conexión. Los clientes y los agentes VDA pueden admitir varios grupos diferentes de conjuntos de cifrado. Cuando un cliente (la aplicación Citrix Workspace o StoreFront) se conecta y envía una lista de los conjuntos de cifrado TLS compatibles, el VDA asigna uno de los conjuntos de cifrado del cliente a uno de los conjuntos de cifrado en su propia lista de conjuntos de cifrado configurados y acepta la conexión. Si no encaja ningún conjunto de cifrado, el VDA rechazará la conexión.

El VDA admite tres grupos de conjuntos de cifrado (también conocidos como modos de conformidad): GOV (Government o Gobierno), COM (Commercial o Comercial) y ALL (Todos). Los conjuntos de cifrado que se aceptan también dependen del modo FIPS de Windows; consulte <http://support.microsoft.com/kb/811833> para obtener información sobre el modo FIPS de Windows. La tabla siguiente muestra los conjuntos de cifrado en cada grupo:

<b>Conjunto de cifrado</b>	<b>ALL</b>	<b>COM</b>	<b>GOV</b>	<b>ALL</b>	<b>COM</b>	<b>GOV</b>
<b>Modo FIPS</b>	No	No	No	Sí	Sí	Sí
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	X			X		X
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	X			X		X
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA				X	X	

\* No se admite en Windows Server 2012 R2.

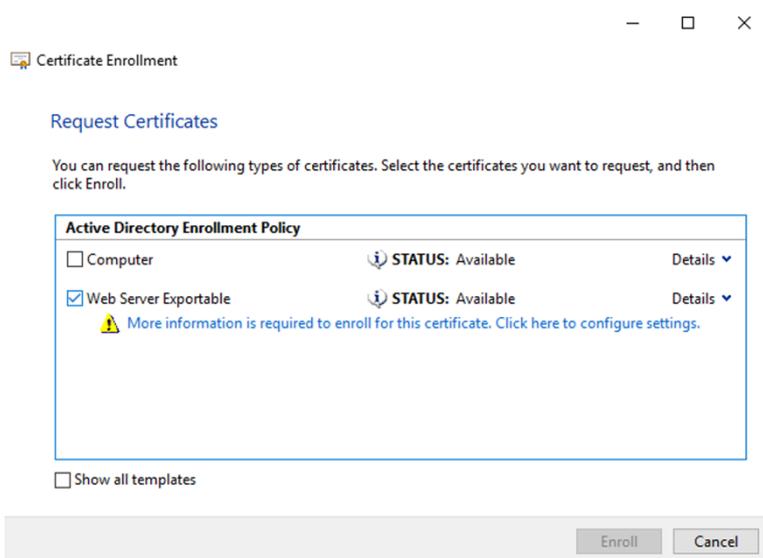
**Nota:**

El VDA no admite conjuntos de cifrado DHE (por ejemplo, TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384, TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA, TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 o TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA). Si Windows lo selecciona, es posible que Receiver no los utilice.

Si utiliza Citrix Gateway, consulte la documentación de Citrix ADC para obtener información sobre la disponibilidad del conjunto de cifrado para la comunicación back-end. Para obtener información sobre la disponibilidad del conjunto de cifrado TLS, consulte [Cifrados disponibles en los dispositivos Citrix ADC](#). Para obtener información sobre la disponibilidad del conjunto de cifrado DTLS, consulte [Compatibilidad con cifrado DTLS](#).

## Solicitar e instalar un certificado

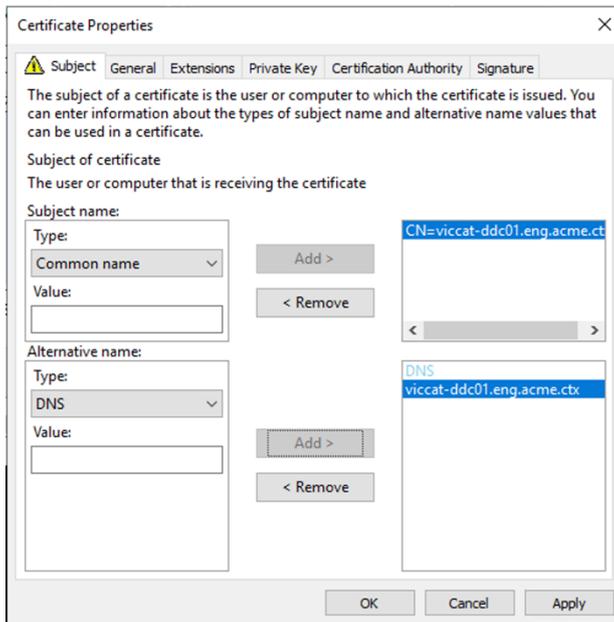
1. En el VDA, abra la consola de MMC y agregue el complemento Certificados. Cuando se le solicite, seleccione Cuenta de equipo.
2. Expanda **Personal > Certificados** y, a continuación, utilice el comando de menú contextual **Todas las tareas > Solicitar un nuevo certificado**.
3. Haga clic en **Siguiente** para comenzar y en **Siguiente** para confirmar que va a adquirir el certificado de inscripción en Active Directory.
4. Seleccione la plantilla para Certificado de autenticación de servidor. Tanto el **equipo** Windows predeterminado como el **servidor web exportable** son aceptables. Si la plantilla se ha configurado para proporcionar automáticamente los valores para Asunto, puede hacer clic en **Inscribir** sin proporcionar más datos.



5. Para proporcionar más detalles para la plantilla de certificado, haga clic en **Detalles** y configure lo siguiente:

**Nombre del sujeto:** Seleccione el tipo **Nombre común** y agregue el nombre de dominio completo (FQDN) del VDA

**Nombre alternativo:** Seleccione el tipo **DNS** y agregue el FQDN del VDA



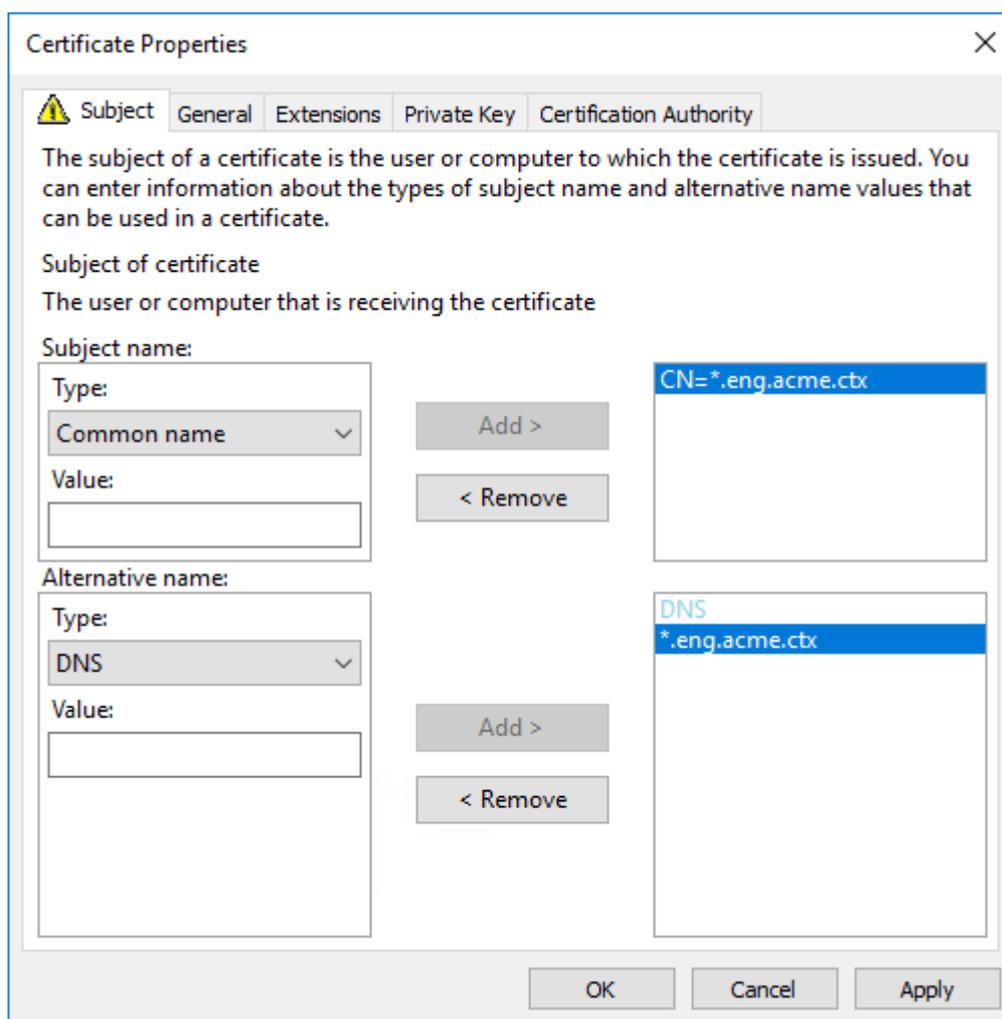
**Nota:**

Use la función de inscripción automática de certificados de Servicios de certificados de Active Directory para automatizar la emisión y la implementación de certificados en los VDA. Esto se describe en <https://support.citrix.com/article/CTX205473>.

Puede usar certificados comodín para permitir que un solo certificado cubra varios VDA:

**Nombre del sujeto:** Seleccione el tipo **Nombre común** e introduzca el dominio \*.primary.domain de los VDA

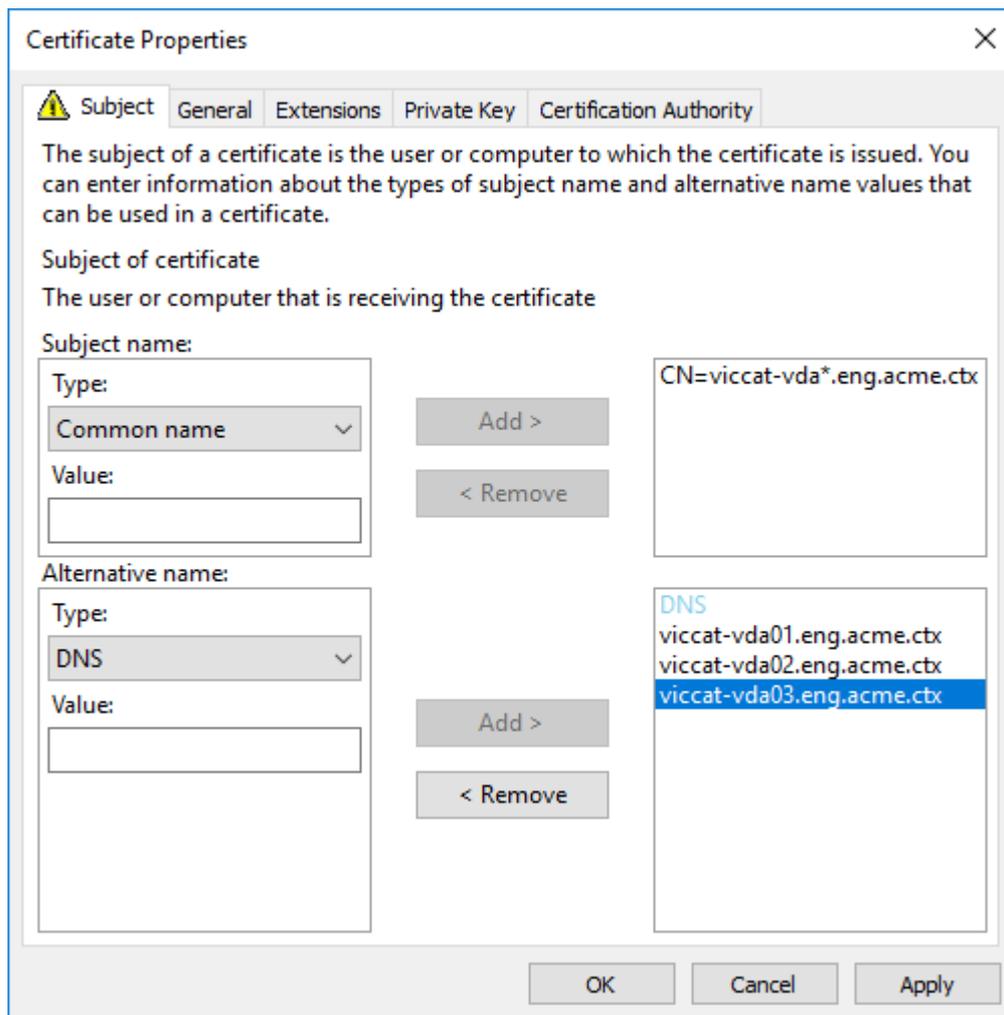
**Nombre alternativo:** Seleccione el tipo **DNS** y agregue el dominio \*.primary.domain de los VDA



Puede usar certificados SAN para permitir que un solo certificado cubra diversos VDA específicos:

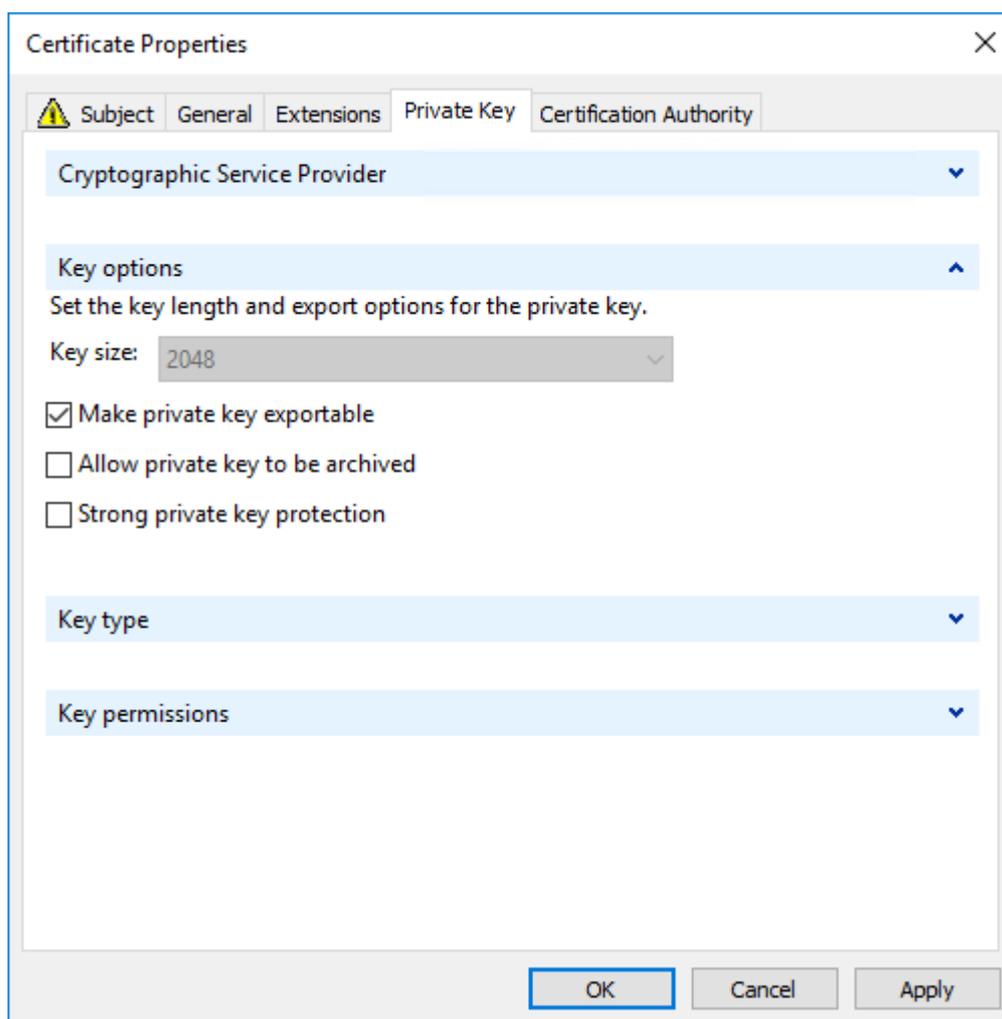
**Nombre del sujeto:** Seleccione el tipo **Nombre común** e introduzca una cadena que ayude a identificar el uso del certificado

**Nombre alternativo:** Seleccione el tipo **DNS** y agregue una entrada para el FQDN de cada VDA. Mantenga el número de nombres alternativos al mínimo para garantizar una negociación de TLS óptima.



**Nota:**

Tanto los certificados comodín como los certificados SAN requieren que se seleccione **Hacer exportable la clave privada** en la ficha Clave privada:



### Configurar TLS en un VDA mediante el script de PowerShell

Instale el certificado TLS en Equipo local > Personal > área Certificados del almacén de certificados. Si hay más de un certificado en esa ubicación, proporcione la huella digital del certificado al script de PowerShell.

**Nota:**

A partir de XenApp y XenDesktop 7.16 LTSR, el script de PowerShell busca el certificado correcto basándose en el nombre de dominio completo del VDA. No es necesario facilitar la huella digital cuando existe solo un certificado para el FQDN del VDA.

El script `Enable-VdaSSL.ps1` habilita o inhabilita la escucha de TLS en un VDA. Este script está disponible en la carpeta `Support > Tools > SslSupport` de los medios de instalación.

Cuando habilita TLS, los conjuntos de cifrado DHE se inhabilitan. Los conjuntos de cifrado ECDHE no se ven afectados.

Al habilitar TLS, el script inhabilita todas las reglas de Firewall de Windows para el puerto TCP especificado. A continuación, agrega una nueva regla que permite al servicio ICA aceptar conexiones entrantes solo en los puertos UDP y TCP de TLS. También inhabilita las reglas de Firewall de Windows para:

- Citrix ICA (predeterminado: 1494)
- Citrix CGP (predeterminado: 2598)
- Citrix WebSocket (predeterminado: 8008)

La consecuencia es que los usuarios solo pueden conectarse con TLS o DTLS. No pueden usar ICA/HDX, ICA/HDX con fiabilidad de la sesión o HDX por WebSocket, sin TLS o DTLS.

**Nota:**

No se admite el protocolo DTLS con audio ICA/HDX por protocolo UDP de transporte en tiempo real ni con ICA/HDX Framhawk.

Consulte [Puertos de red](#).

El script contiene las siguientes descripciones de sintaxis, además de ejemplos adicionales; puede usar una herramienta como Notepad++ para consultar esta información.

**Importante:**

Debe indicar el parámetro Enable o Disable, así como el parámetro CertificateThumbPrint. Los demás parámetros son opcionales.

## Sintaxis

## Transport Layer Security (TLS)

Citrix Virtual Apps and Desktops admiten el protocolo Transport Layer Security (TLS) para las conexiones por TCP entre los componentes. Citrix Virtual Apps and Desktops también admiten el protocolo Datagram Transport Layer Security (DTLS) para las conexiones ICA o HDX por UDP cuando se utiliza el [transporte adaptable](#).

TLS y DTLS son similares y admiten los mismos certificados digitales. Configurar un sitio Citrix Virtual Apps o Citrix Virtual Desktops para usar TLS también lo configura para usar DTLS. Siga estos procedimientos; son los mismos pasos tanto para TLS como para DTLS (excepto donde se indique):

- Obtener, instalar y registrar un certificado de servidor en todos los Delivery Controllers y configurar un puerto con el certificado TLS. Para obtener más información, consulte [Instalar certificados de servidor TLS en los Controllers](#).

Si lo quiere, puede cambiar los puertos que Controller utiliza para escuchar el tráfico HTTP y HTTPS.

- Habilite las conexiones TLS entre la aplicación Citrix Workspace y los agentes VDA (Virtual Delivery Agent) completando las siguientes tareas:
  - Configure TLS en las máquinas donde los VDA están instalados. (Para simplificar, en adelante se usará “VDA” para hacer referencia a la máquina donde está instalado un VDA.) Para obtener información general, consulte [Parámetros de TLS en los VDA](#). Se recomienda que utilice el script de PowerShell suministrado por Citrix para configurar TLS o DTLS. Para obtener información detallada, consulte [Configurar TLS en un VDA mediante el script de PowerShell](#). Sin embargo, si quiere configurar TLS o DTLS manualmente, consulte [Configurar TLS manualmente en un VDA](#).
  - Configure TLS en los grupos de entrega que contienen los VDA mediante la ejecución de un conjunto de cmdlets de PowerShell en Studio. Para obtener más información, consulte [Configuración de TLS en los grupos de entrega](#).

Requisitos y consideraciones:

- \* El hecho de habilitar conexiones TLS entre los usuarios y los VDA solo es válido para los sitios de XenApp 7.6 y XenDesktop 7.6 y versiones posteriores compatibles.
- \* Configure TLS en los grupos de entrega y en los VDA después de instalar los componentes, crear un sitio, crear catálogos de máquinas y crear grupos de entrega.
- \* Para configurar TLS en los grupos de entrega, debe tener permiso para cambiar las reglas de acceso a los Controllers. Un administrador total tiene este permiso.
- \* Para configurar TLS en los VDA, debe ser un administrador Windows en la máquina donde está instalado el VDA.
- \* En agentes VDA agrupados y aprovisionados por Machine Creation Services o Provisioning Services, la imagen de la máquina del VDA se restablece en el proceso de reinicio, lo que provoca la pérdida de la configuración anterior de TLS. Ejecute el script de PowerShell cada vez que se reinicie el VDA para volver a configurar los parámetros de TLS.

#### **Advertencia:**

Para las tareas que impliquen modificar el Registro de Windows, tenga cuidado: si se modifica de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Para obtener información acerca de la habilitación de TLS para la base de datos del sitio, consulte [CTX137556](#).

## Instalar certificados de servidor TLS en los Controllers

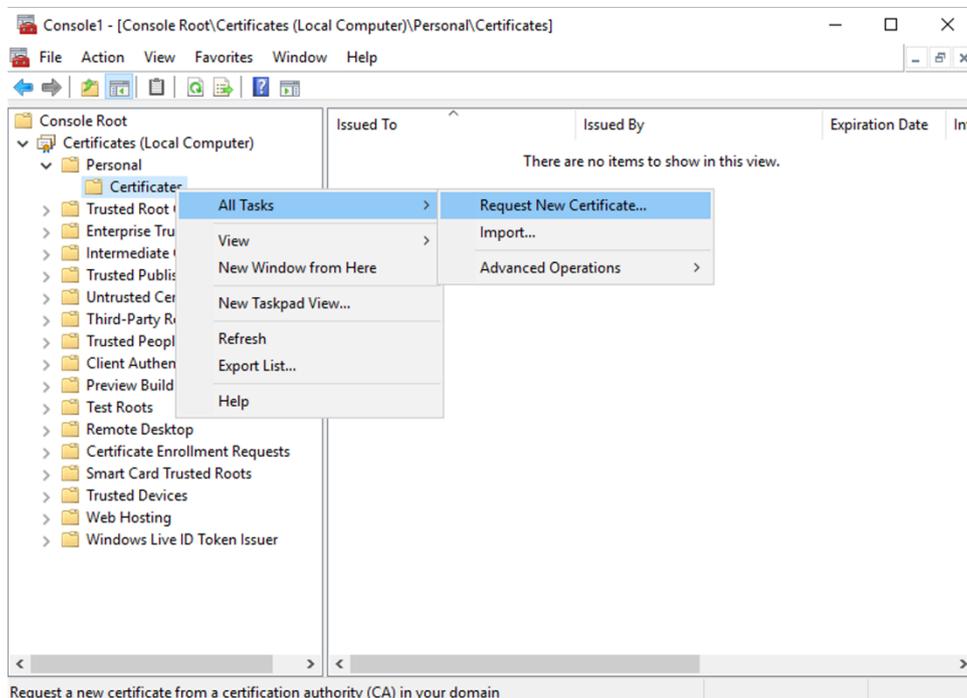
Para HTTPS, XML Service admite las funciones de TLS cuando se usan certificados de servidor, no cuando se usan certificados de cliente. En esta sección, se describe la adquisición e instalación de certificados TLS en Delivery Controllers. Los mismos pasos se pueden aplicar a Cloud Connectors para cifrar el tráfico STA y XML.

Aunque hay varios tipos diferentes de entidades de certificación y métodos para solicitar certificados de ellas, en este artículo se describe la entidad emisora de certificados de Microsoft. La entidad de certificación de Microsoft debe tener una plantilla de certificado publicada con el propósito Autenticación de servidor.

Si la entidad de certificación de Microsoft está integrada en un dominio de Active Directory o en el bosque de confianza al que están unidos los Delivery Controllers, se puede adquirir un certificado desde el asistente para inscripción de certificados del complemento MMC Certificados.

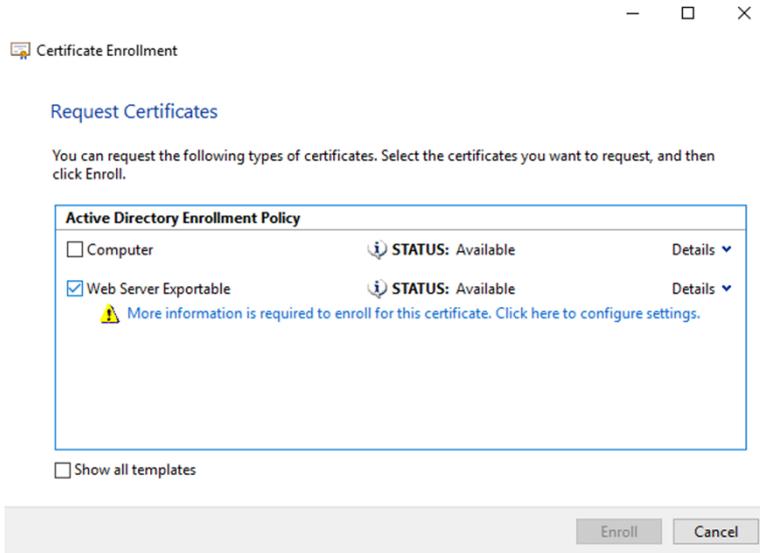
### Solicitar e instalar un certificado

1. En el Delivery Controller, abra la consola de MMC y agregue el complemento Certificados. Cuando se le solicite, seleccione Cuenta de equipo.
2. Expanda **Personal > Certificados** y, a continuación, utilice la opción de menú contextual **Todas las tareas > Solicitar un nuevo certificado**.



3. Haga clic en **Siguiente** para comenzar y en **Siguiente** para confirmar que va a adquirir el certificado de inscripción en Active Directory.

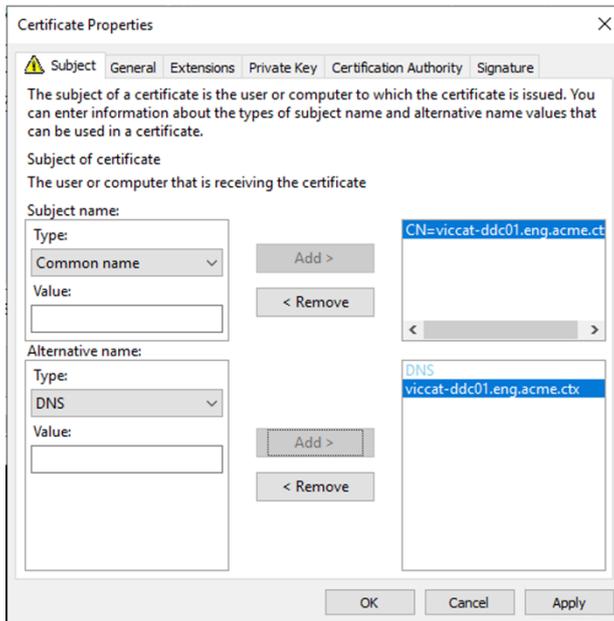
4. Seleccione la plantilla para Certificado de autenticación de servidor. Si la plantilla se ha configurado para proporcionar automáticamente los valores para Asunto, puede hacer clic en **Inscribir** sin proporcionar más datos.



5. Para proporcionar más detalles para la plantilla de certificado, haga clic en el botón de flecha **Detalles** y configure lo siguiente:

**Nombre del asunto:** Seleccione Nombre común y agregue el FQDN del Delivery Controller.

**Nombre alternativo:** Seleccione DNS y agregue el FQDN del Delivery Controller.



## Configurar el puerto de escucha SSL/TLS

1. Abra una ventana de comandos de PowerShell como administrador de la máquina.
2. Ejecute los siguientes comandos para obtener el GUID de aplicación de Broker Service:  
<!JEKYLL@5300@0>
3. Ejecute los siguientes comandos en la misma ventana de PowerShell para obtener la huella digital del certificado que instaló anteriormente:  
<!JEKYLL@5300@1>
4. Ejecute los siguientes comandos en la misma ventana de PowerShell para configurar el puerto SSL/TLS de Broker Service y usar el certificado para el cifrado:  
<!JEKYLL@5300@2>

Cuando se configura correctamente, el resultado del último comando <!JEKYLL@5300@3> muestra que el agente de escucha utiliza el <!JEKYLL@5300@4> correcto y que <!JEKYLL@5300@5> es el GUID de aplicación de Broker Service.

Si los servidores confían en el certificado instalado en los Delivery Controllers, ahora puede configurar los vínculos de Delivery Controllers de StoreFront y Citrix Gateway STA para que utilicen HTTPS, en lugar de HTTP.

### Nota:

Si el Controller está instalado en Windows Server 2016 o Windows Server 2019, y StoreFront está instalado en Windows Server 2012 R2, es necesario cambiar la configuración en el Controller o en StoreFront para cambiar el orden de los conjuntos de cifrado TLS. Este cambio de configuración no es necesario para Controller ni StoreFront con otras combinaciones de versiones de Windows Server.

La lista ordenada de los conjuntos de cifrado debe incluir el conjunto de cifrado <!JEKYLL@5300@6> o <!JEKYLL@5300@7> (o ambos) o conjuntos de cifrado TLS\_ECDHE similares, y estos conjuntos deben preceder los conjuntos de cifrado TLS\_DHE.

1. Desde el editor de directivas de grupo de Microsoft, vaya a Configuración del equipo > Plantillas administrativas > Red > Opciones de configuración SSL.
2. Modifique la directiva “Orden de conjuntos de cifrado SSL”. De manera predeterminada, esta directiva está establecida en “No configurada”. Habilite esta directiva.
3. Ordene los conjuntos de cifrado; quite aquellos conjuntos que no quiera usar.

Compruebe que <!JEKYLL@5300@8>, <!JEKYLL@5300@9> o un conjunto de cifrado TLS\_ECDHE similar preceda los conjuntos de cifrado TLS\_DHE.

En Microsoft MSDN, también puede consultar [Prioritizing Schannel Cipher Suites](#).

## Cambiar puertos HTTP o HTTPS

De forma predeterminada, el XML Service en el Controller escucha en los puertos 80 para el tráfico HTTP y 443 para el tráfico HTTPS. Aunque se pueden utilizar otros puertos distintos de los predeterminados, tenga en cuenta los riesgos de seguridad que implica la exposición de un Controller a redes que no son de confianza. Antes que cambiar los valores predeterminados, es preferible implementar un servidor de StoreFront independiente.

Para cambiar los puertos HTTP o HTTPS predeterminados que usa el Controller, ejecute el comando siguiente en Studio:

**BrokerService.exe -WIPORT <puerto http> -WISSLPOR *T* <puerto https>**

<puerto http> es el número de puerto para el tráfico HTTP y <puerto https> es el número de puerto para el tráfico HTTPS.

### Nota:

Después de cambiar de un puerto, Studio puede mostrar un mensaje acerca de la actualización y la compatibilidad de licencias. Para resolver el problema, vuelva a registrar las instancias de servicio mediante esta secuencia de cmdlet de PowerShell:

```
<!JEKYL@5300@10>
```

## Solo aplicar el tráfico HTTPS

Si quiere que XML Service ignore el tráfico HTTP, cree el siguiente parámetro de Registro en HKLM\Software\Citrix\DesktopServer\ en el Controller y reinicie el Broker Service.

Para ignorar el tráfico HTTP, cree DWORD XmlServicesEnableNonSsl y dele el valor 0.

Se puede crear el valor DWORD de Registro correspondiente para ignorar el tráfico HTTPS: DWORD XmlServicesEnableSsl. Compruebe que no está establecido en 0.

## Parámetros de TLS en agentes VDA

Un grupo de entrega no puede incluir una mezcla de VDA con TLS configurado y VDA sin TLS configurado. Antes de configurar TLS para un grupo de entrega, debe haber configurado TLS para todos los VDA en ese grupo de entrega.

Si configura TLS en los VDA, cambian los permisos en el certificado TLS instalado, lo que da al servicio ICA acceso de lectura a la clave privada del certificado e informa al servicio ICA de lo siguiente:

- **Qué certificado del almacén de certificados hay que usar para TLS.**

- **Qué número de puerto TCP hay que usar para las conexiones TLS.**

El Firewall de Windows (si está habilitado) debe estar configurado para permitir conexiones entrantes en este puerto TCP. Esta configuración se lleva a cabo cuando se usa el script de PowerShell.

- **Qué versiones del protocolo TLS se deben permitir.**

**Importante:**

Citrix recomienda revisar el uso de SSL 3 y volver a configurar las implementaciones para retirar la compatibilidad con SSL 3 donde corresponda. Consulte [CTX200238](#).

Las versiones compatibles con el protocolo TLS siguen una jerarquía (de menor a mayor): SSL 3.0, TLS 1.0, TLS 1.1 y TLS 1.2. Debe especificar la versión mínima permitida; se permitirán todas las conexiones que usen esa versión del protocolo o una versión más alta.

Por ejemplo, si especifica TLS 1.1 como la versión mínima, se permitirán conexiones con TLS 1.1 y TLS 1.2. Si elige SSL 3.0 como la versión mínima, se permitirán conexiones con todas las versiones admitidas. Si especifica TLS 1.2 como la versión mínima, solo se permiten conexiones con TLS 1.2.

DTLS 1.0 corresponde a TLS 1.1, mientras que DTLS 1.2 corresponde a TLS 1.2.

- **Qué conjuntos de cifrado TLS se deben permitir.**

El conjunto de cifrado selecciona el cifrado que se usa para una conexión. Los clientes y los agentes VDA pueden admitir varios grupos diferentes de conjuntos de cifrado. Cuando un cliente (la aplicación Citrix Workspace o StoreFront) se conecta y envía una lista de los conjuntos de cifrado TLS compatibles, el VDA asigna uno de los conjuntos de cifrado del cliente a uno de los conjuntos de cifrado en su propia lista de conjuntos de cifrado configurados y acepta la conexión. Si no encaja ningún conjunto de cifrado, el VDA rechazará la conexión.

El VDA admite tres grupos de conjuntos de cifrado (también conocidos como modos de conformidad): GOV (Government o Gobierno), COM (Commercial o Comercial) y ALL (Todos). Los conjuntos de cifrado que se aceptan también dependen del modo FIPS de Windows; consulte <http://support.microsoft.com/kb/811833> para obtener información sobre el modo FIPS de Windows. La tabla siguiente muestra los conjuntos de cifrado en cada grupo:

Conjunto de cifrado						
TLS/DTLS	ALL	COM	GOV	ALL	COM	GOV
<b>Modo FIPS</b>	No	No	No	Sí	Sí	Sí
<!JEKYL@530@11>*			X	X		X

<b>Conjunto de cifrado</b>						
<b>TLS/DTLS</b>	<b>ALL</b>	<b>COM</b>	<b>GOV</b>	<b>ALL</b>	<b>COM</b>	<b>GOV</b>
<!JEKYLL@5300@12>			X	X		X
<!JEKYLL@5300@13>		X		X	X	

\* No se admite en Windows Server 2012 R2.

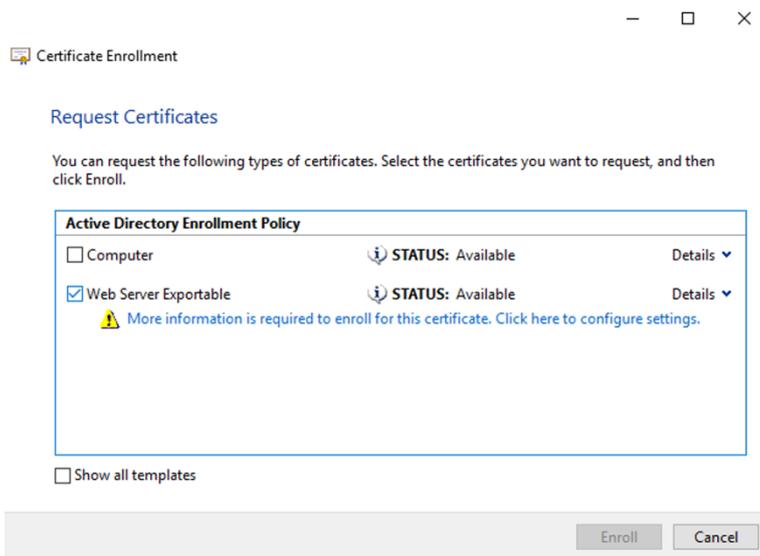
**Nota:**

El VDA no admite conjuntos de cifrado DHE (por ejemplo, <!JEKYLL@5300@14>, <!JEKYLL@5300@15>, <!JEKYLL@5300@16> o <!JEKYLL@5300@17>). Si Windows lo selecciona, es posible que Receiver no los utilice.

Si utiliza Citrix Gateway, consulte la documentación de Citrix ADC para obtener información sobre la disponibilidad del conjunto de cifrado para la comunicación back-end. Para obtener información sobre la disponibilidad del conjunto de cifrado TLS, consulte [Cifrados disponibles en los dispositivos Citrix ADC](#). Para obtener información sobre la disponibilidad del conjunto de cifrado DTLS, consulte [Compatibilidad con cifrado DTLS](#).

### Solicitar e instalar un certificado

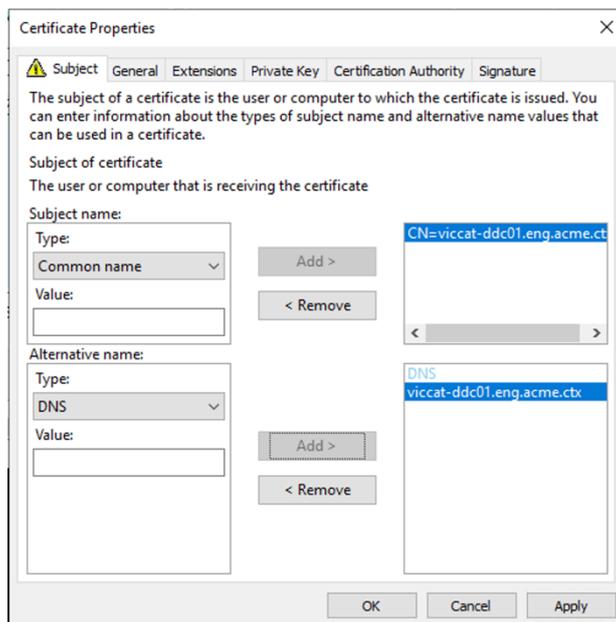
1. En el VDA, abra la consola de MMC y agregue el complemento Certificados. Cuando se le solicite, seleccione Cuenta de equipo.
2. Expanda **Personal > Certificados** y, a continuación, utilice el comando de menú contextual **Todas las tareas > Solicitar un nuevo certificado**.
3. Haga clic en **Siguiente** para comenzar y en **Siguiente** para confirmar que va a adquirir el certificado de inscripción en Active Directory.
4. Seleccione la plantilla para Certificado de autenticación de servidor. Tanto el **equipo** Windows predeterminado como el **servidor web exportable** son aceptables. Si la plantilla se ha configurado para proporcionar automáticamente los valores para Asunto, puede hacer clic en **Inscribir** sin proporcionar más datos.



- Para proporcionar más detalles para la plantilla de certificado, haga clic en **Detalles** y configure lo siguiente:

**Nombre del sujeto:** Seleccione el tipo **Nombre común** y agregue el nombre de dominio completo (FQDN) del VDA

**Nombre alternativo:** Seleccione el tipo **DNS** y agregue el FQDN del VDA



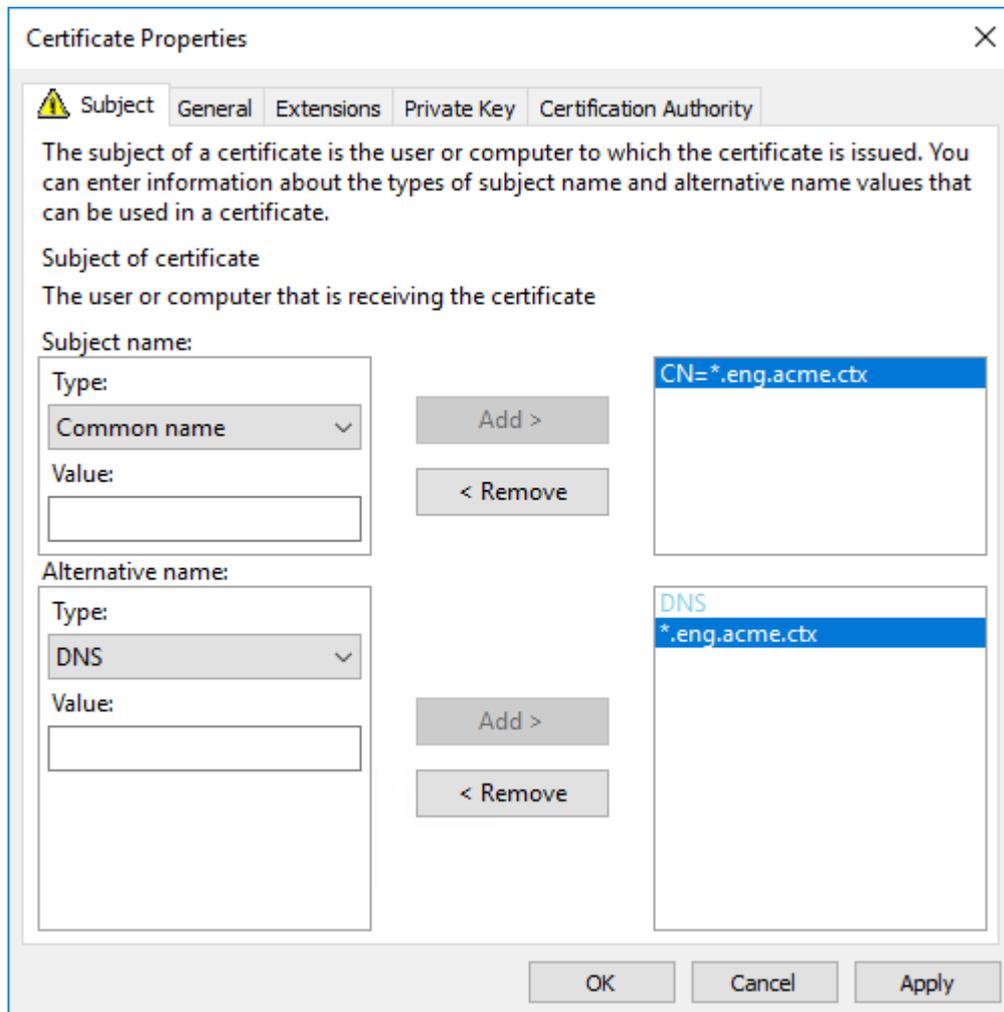
**Nota:**

Use la función de inscripción automática de certificados de Servicios de certificados de Active Directory para automatizar la emisión y la implementación de certificados en los VDA. Esto se describe en <https://support.citrix.com/article/CTX205473>.

Puede usar certificados comodín para permitir que un solo certificado cubra varios VDA:

**Nombre del sujeto:** Seleccione el tipo **Nombre común** e introduzca el dominio \*.primary.domain de los VDA

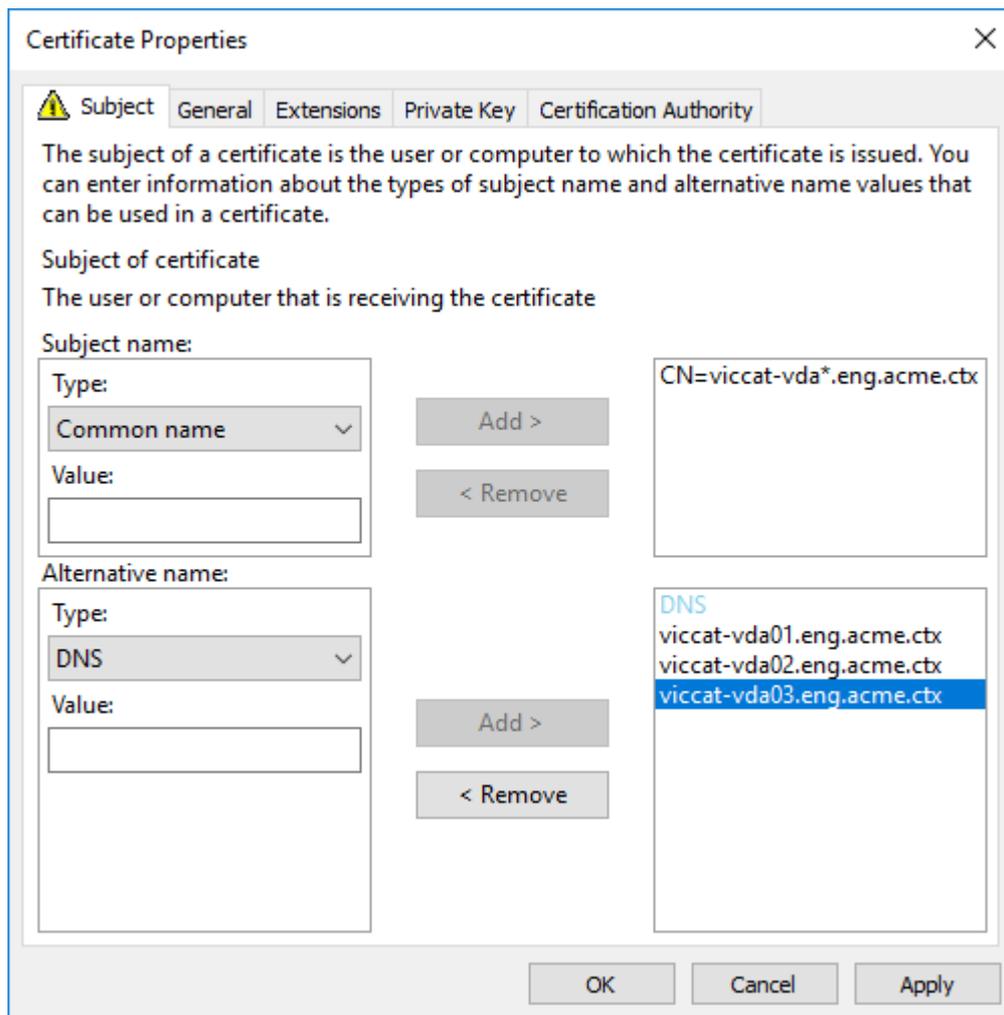
**Nombre alternativo:** Seleccione el tipo **DNS** y agregue el dominio \*.primary.domain de los VDA



Puede usar certificados SAN para permitir que un solo certificado cubra diversos VDA específicos:

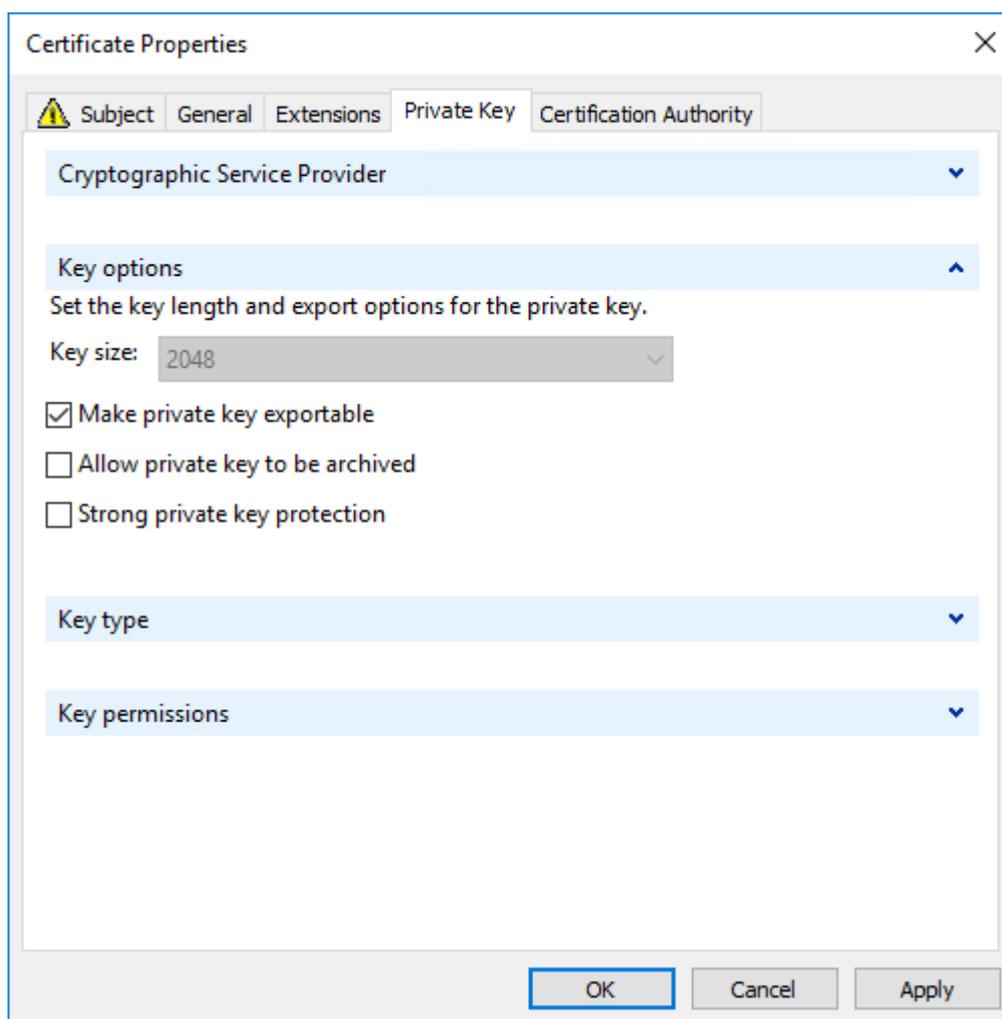
**Nombre del sujeto:** Seleccione el tipo **Nombre común** e introduzca una cadena que ayude a identificar el uso del certificado

**Nombre alternativo:** Seleccione el tipo **DNS** y agregue una entrada para el FQDN de cada VDA. Mantenga el número de nombres alternativos al mínimo para garantizar una negociación de TLS óptima.



**Nota:**

Tanto los certificados comodín como los certificados SAN requieren que se seleccione **Hacer exportable la clave privada** en la ficha Clave privada:



### Configurar TLS en un VDA mediante el script de PowerShell

Instale el certificado TLS en Equipo local > Personal > área Certificados del almacén de certificados. Si hay más de un certificado en esa ubicación, proporcione la huella digital del certificado al script de PowerShell.

**Nota:**

A partir de XenApp y XenDesktop 7.16 LTSR, el script de PowerShell busca el certificado correcto basándose en el nombre de dominio completo del VDA. No es necesario facilitar la huella digital cuando existe solo un certificado para el FQDN del VDA.

El script `Enable-VdaSSL.ps1` habilita o inhabilita la escucha de TLS en un VDA. Este script está disponible en la carpeta `Support > Tools > SslSupport` de los medios de instalación.

Cuando habilita TLS, los conjuntos de cifrado DHE se inhabilitan. Los conjuntos de cifrado ECDHE no se ven afectados.

Al habilitar TLS, el script inhabilita todas las reglas de Firewall de Windows para el puerto TCP especificado. A continuación, agrega una nueva regla que permite al servicio ICA aceptar conexiones entrantes solo en los puertos UDP y TCP de TLS. También inhabilita las reglas de Firewall de Windows para:

- Citrix ICA (predeterminado: 1494)
- Citrix CGP (predeterminado: 2598)
- Citrix WebSocket (predeterminado: 8008)

La consecuencia es que los usuarios solo pueden conectarse con TLS o DTLS. No pueden usar ICA/HDX, ICA/HDX con fiabilidad de la sesión o HDX por WebSocket, sin TLS o DTLS.

**Nota:**

No se admite el protocolo DTLS con audio ICA/HDX por protocolo UDP de transporte en tiempo real ni con ICA/HDX Framhawk.

Consulte [Puertos de red](#).

El script contiene las siguientes descripciones de sintaxis, además de ejemplos adicionales; puede usar una herramienta como Notepad++ para consultar esta información.

**Importante:**

Debe indicar el parámetro Enable o Disable, así como el parámetro CertificateThumbPrint. Los demás parámetros son opcionales.

**Sintaxis** Enable-VdaSSL {-Enable | -Disable} -CertificateThumbPrint "<thumbprint>" [-SSLPort \<port>] [-SSLMinVersion "\<min-ssl-version>"] [-SSLCipherSuite "\<suite>"]

Parámetro	Descripción
Enable	Instala y habilita la escucha de TLS en el VDA. Este parámetro o el parámetro Disable es obligatorio.
Disable	Inhabilita la escucha de TLS en el VDA. Este parámetro o el parámetro Enable es obligatorio. Si se especifica este parámetro, ningún otro parámetro es válido.

Parámetro	Descripción
CertificateThumbPrint ""	Huella digital del certificado TLS en el almacén de certificados, entre comillas. El script utiliza la huella digital especificada para seleccionar el certificado a utilizar. Este parámetro es obligatorio; si no lo indica, se selecciona un certificado incorrecto.
SSLPort	Puerto TLS. Valor predeterminado: 443
SSLMinVersion ""	Versión mínima del protocolo TLS, indicada entre comillas. Valores válidos: "TLS_1.0" (predeterminado), "TLS_1.1" y "TLS_1.2".
SSLCipherSuite ""	Conjunto de cifrado TLS, entre comillas. Valores válidos: "GOV", "COM" y "ALL" (valor predeterminado).

**Ejemplos** El siguiente script instala y habilita el valor de versión del protocolo TLS. La huella digital (representada como "12345678987654321" en este ejemplo) se utiliza para seleccionar el certificado que se utilizará.

```
1 Enable-VdaSSL - Enable -CertificateThumbPrint "12345678987654321"
```

El siguiente script instala y habilita la escucha de TLS, y especifica el puerto TLS 400, el conjunto de cifrado GOV y una versión de protocolo mínima de TLS 1.2. La huella digital (representada como "12345678987654321" en este ejemplo) se utiliza para seleccionar el certificado que se utilizará.

```
1 Enable-VdaSSL - Enable
2 -CertificateThumbPrint "12345678987654321"
3 - SSLPort 400 - SSLMinVersion "TLS_1.2"
4 - SSLCipherSuite "All"
```

El siguiente script inhabilita la escucha de TLS en el VDA.

```
1 Enable-VdaSSL - Disable
```

### Configurar TLS manualmente en un VDA

Al configurar manualmente TLS en un VDA, se concede acceso genérico de lectura a la clave privada del certificado TLS para el servicio apropiado en cada VDA: NT SERVICE\PorticaService para un VDA de SO de sesión única Windows o NT SERVICE\TermService para un VDA de SO multisesión Windows. En la máquina donde está instalado el VDA:

**PASO 1.** Abra la consola Microsoft Management Console (MMC): Inicio > Ejecutar > mmc.exe.

**PASO 2.** Agregue el complemento Certificados en la consola MMC:

1. Seleccione Archivo > Agregar o quitar complemento.
2. Seleccione Certificados y haga clic en Agregar.
3. En “Este complemento administrará siempre certificados de”, elija “Cuenta de equipo” y luego haga clic en “Siguiente”.
4. En “Seleccione el equipo que desea administrar con este complemento”, elija “Equipo local” y, a continuación, haga clic en “Finalizar”.

**PASO 3.** En Certificados (Equipo local) > Personal > Certificados, haga clic con el botón secundario en el certificado y seleccione Todas las tareas > Administrar claves privadas.

**PASO 4.** El editor de la lista de control de acceso muestra “Permisos para claves privadas de (nombre)” , donde (nombre) es el nombre del certificado TLS. Agregue uno de los siguientes servicios y dele acceso de lectura:

- Para un VDA con SO de sesión única de Windows, “PORTICASERVICE”
- Para un VDA con SO multisesión Windows, “TERMSERVICE”

**PASO 5.** Haga doble clic en el certificado TLS instalado. En el cuadro de diálogo del certificado, seleccione la ficha Detalles y vaya a la parte inferior. Haga clic en Huella digital.

**PASO 6.** Ejecute regedit y vaya a HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd.

1. Modifique la clave de huella digital SSL Thumbprint y copie en el valor binario la huella digital que figura en el certificado TLS. Puede ignorar los elementos desconocidos del diálogo Modificar valor binario (por ejemplo, ‘0000’ y los caracteres especiales).
2. Modifique la clave SSLEnabled y cambie el valor DWORD a 1 (para inhabilitar SSL más adelante, cambie el valor DWORD a 0).
3. Si quiere cambiar la configuración predeterminada (optativo), use lo siguiente en la misma ruta de Registro:

SSLPort DWORD –número de puerto SSL. Valor predeterminado: 443.

SSLMinVersion DWORD –1 = SSL 3.0, 2 = TLS 1.0, 3 = TLS 1.1, 4 = TLS 1.2. Valor predeterminado: 2 (TLS 1.0).

SSLCipherSuite DWORD –1 = GOV, 2 = COM, 3 = ALL. Valor predeterminado: 3 (ALL).

**PASO 7.** Compruebe que los puertos UDP y TCP de TLS están abiertos en el Firewall de Windows, si no son el predeterminado 443 (cuando cree la regla de entrada en el Firewall de Windows, compruebe que tenga seleccionadas las entradas “Permitir la conexión” y “Habilitada” en las propiedades).

**PASO 8.** Asegúrese de que no hay otros servicios o aplicaciones (por ejemplo, IIS) que estén utilizando el puerto TCP de TLS.

**PASO 9.** Para los VDA para SO multisesión Windows, reinicie la máquina para que los cambios tengan efecto (no es necesario reiniciar las máquinas que contienen los VDA para SO de sesión única Windows).

**Importante:**

Se necesita un paso adicional si el VDA está en Windows Server 2012 R2, Windows Server 2016, o bien en Windows 10 Anniversary Edition o una versión posterior compatible. Esto afecta a las conexiones procedentes de la aplicación Citrix Workspace para HTML5 y la aplicación Citrix Workspace para Chrome. También se incluyen las conexiones a través de Citrix Gateway.

Este paso también es necesario para todas las conexiones que pasan por Citrix Gateway, para todas las versiones de VDA, si TLS entre Citrix Gateway y el VDA está configurado.

En el VDA (Windows Server 2012 R2, Windows Server 2016 o Windows 10 Anniversary Edition o versiones posteriores), mediante el Editor de directivas de grupo, vaya a Configuración del equipo > Directivas > Plantillas administrativas > Red > Opciones de configuración SSL > Orden de conjuntos de cifrado SSL. Seleccione el orden siguiente:

- 1 TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384\_P384
- 2 TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384\_P256
- 3 TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384\_P384
- 4 TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384\_P256
- 5 TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA\_P384
- 6 TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA\_P256

**Nota:**

Los seis primeros elementos también indican una curva elíptica, P384 o P256. Compruebe que la opción “curve25519” no está seleccionada. El modo FIPS no impide el uso de “curve25519”.

Cuando esta configuración de la directiva de grupo esté configurada, el VDA selecciona un conjunto de cifrado solo si aparece en las dos listas: la lista de la directiva de grupo y la lista del modo de conformidad seleccionado (COM, GOV o ALL). El conjunto de cifrado también debe aparecer en la lista que envíe el cliente (la aplicación Citrix Workspace o StoreFront).

Esta configuración de directiva de grupo también afecta a otras aplicaciones y servicios TLS del VDA. Si sus aplicaciones requieren conjuntos de cifrado determinados, deberá agregarlos a la lista de esta directiva de grupo.

**Importante:**

Aunque los cambios de directiva de grupo se muestran cuando se aplican, los cambios de directiva de grupo para la configuración de TLS solo tienen efecto después de reiniciar el sistema operativo. Por lo tanto, para escritorios agrupados, los cambios de directiva de grupo referentes a la configuración de TLS se deben aplicar a la imagen base.

## Configurar TLS en grupos de entrega

Lleve a cabo este procedimiento para cada grupo de entrega que contenga VDA configurados para conexiones TLS.

1. Desde Studio, abra la consola de PowerShell.
2. Ejecute **asnp Citrix.\*** para cargar los cmdlets de producto Citrix.
3. Ejecute **Get-BrokerAccessPolicyRule -DesktopGroupName '<nombre del grupo de entrega>' | Set-BrokerAccessPolicyRule -HdxSslEnabled \$true.**
4. Ejecute **Set-BrokerSite -DnsResolutionEnabled \$true.**

## Solución de problemas

Si se produce un error de conexión, consulte el registro de eventos del sistema en el VDA.

Cuando usa la aplicación Citrix Workspace para Windows, si recibe un error de conexión que indica un error de TLS, inhabilite Desktop Viewer y, a continuación, intente conectarse de nuevo. Aunque la conexión siga fallando, podrá obtener una explicación del problema de TLS subyacente. Por ejemplo, que especificó una plantilla incorrecta al solicitar un certificado de la entidad de certificación.)

La mayoría de las configuraciones que usan el transporte adaptable HDX funcionan con DTLS, incluidas las que utilizan las versiones más recientes de la aplicación Citrix Workspace, Citrix Gateway y VDA. Algunas configuraciones que usan DTLS entre la aplicación Citrix Workspace y Citrix Gateway, y que usan DTLS entre Citrix Gateway y el VDA, requieren configuración adicional.

Es necesario adoptar medidas adicionales si se producen estos casos:

- La versión de Citrix Gateway admite DTLS al VDA, pero la versión de VDA no admite DTLS (7.15 o anterior)
- La versión de VDA admite DTLS (7.16 o una versión posterior), pero la versión de Citrix Gateway no admite DTLS al VDA

Para evitar errores en las conexiones, lleve a cabo una de estas acciones:

- Actualice Citrix Gateway a una versión que admita DTLS al VDA.
- Actualice el VDA a la versión 7.16 o a una posterior.
- Inhabilite DTLS en el VDA.
- Inhabilite el transporte adaptable HDX.

### Nota:

Para inhabilitar DTLS en el VDA, modifique la configuración del firewall del VDA para inhabilitar el puerto UDP 443. Consulte [Puertos de red](#).

## Comunicación entre Controller y VDA

Con su protección de mensajes, Windows Communication Framework (WCF) protege la comunicación entre el Controller y el VDA. No se necesita protección adicional de transporte mediante el protocolo TLS. La configuración de WCF usa Kerberos para la autenticación mutua entre el Controller y el VDA. Para el cifrado, se usa AES en el modo CBC con una clave de 256 bits. Para la integridad de los mensajes, se usa SHA-1.

Según Microsoft, los [Protocolos de seguridad](#) que utiliza WCF cumplen los estándares de OASIS (Organization for the Advancement of Structured Information Standards), incluidos los WS-SecurityPolicy 1.2. Además, Microsoft afirma que WCF admite todos los conjuntos de algoritmos que constan en [Security Policy 1.2](#).

La comunicación entre el Controller y el VDA usa el conjunto de algoritmos basic256, cuyos algoritmos son como se ha señalado anteriormente.

## TLS, la redirección de vídeo HTML5 y la redirección de contenido del explorador web

Puede usar la redirección de vídeo HTML5 y la redirección de contenido del explorador web para redirigir los sitios web HTTPS. El JavaScript insertado en esos sitios web debe establecer una conexión TLS al servicio Citrix HDX HTML5 Video Redirection Service que se ejecuta en el VDA. Para ello, HTML5 Video Redirection Service genera dos certificados personalizados en el almacén de certificados presente en el VDA. Al detener este servicio, también se quitan los certificados.

La directiva de redirección de vídeo HTML5 está inhabilitada de forma predeterminada.

En cambio, la redirección de contenido del explorador web está habilitada de forma predeterminada.

Para obtener más información sobre la redirección de vídeos HTML5, consulte [Configuraciones de directiva de Multimedia](#).

## Protocolo TLS en Universal Print Server

November 4, 2021

El protocolo Transport Layer Security (TLS) se admite para conexiones TCP entre el Virtual Delivery Agent (VDA) y el Universal Print Server.

### **Advertencia:**

Para las tareas que impliquen modificar el Registro de Windows, tenga cuidado: si se modifica

de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

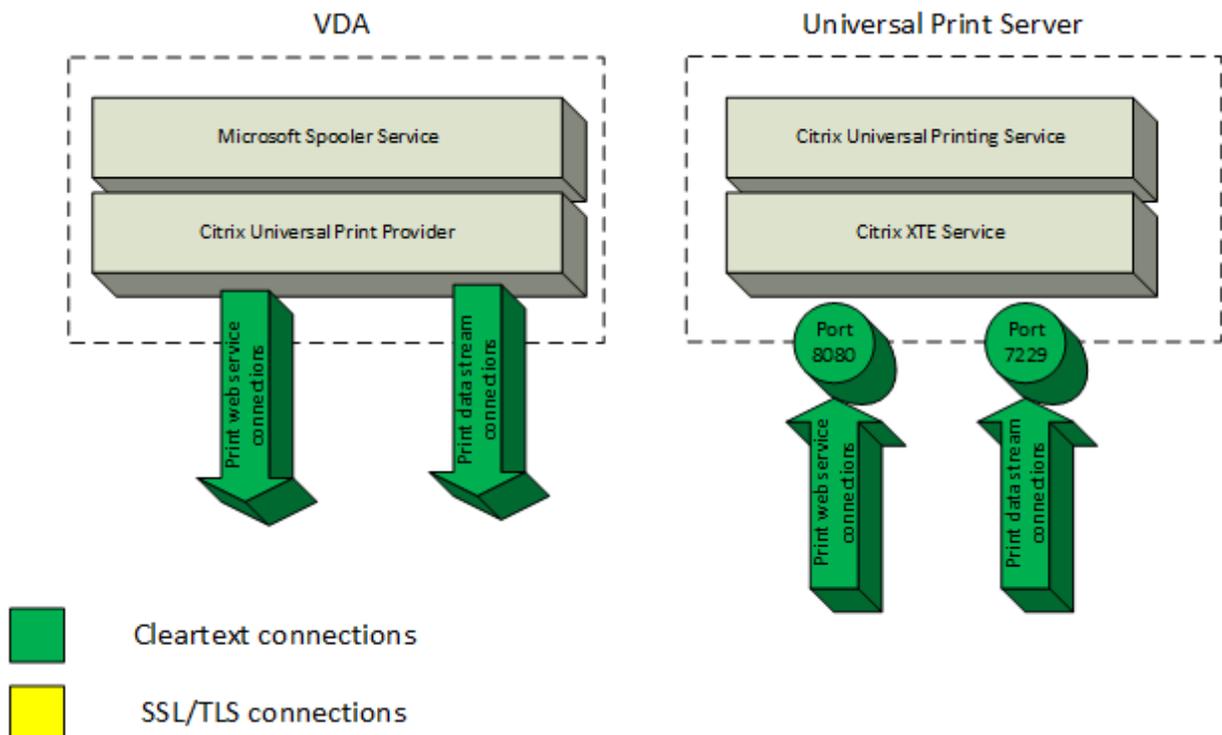
## Tipos de conexiones de impresión entre el VDA y el Universal Print Server

### Conexiones de texto no cifrado

Las siguientes conexiones relacionadas con la impresión se originan en el VDA y se conectan a los puertos del Universal Print Server. Esas conexiones se realizan solo cuando la configuración de directiva **Habilitado para SSL** está **inhabilitada** (el valor predeterminado).

- Conexiones del servicio web de impresión para texto no cifrado (puerto TCP 8080)
- Conexiones del flujo de datos de impresión (CGP) para texto no cifrado (puerto TCP 7229)

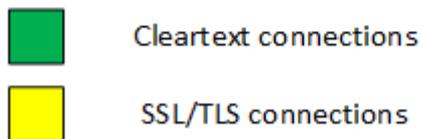
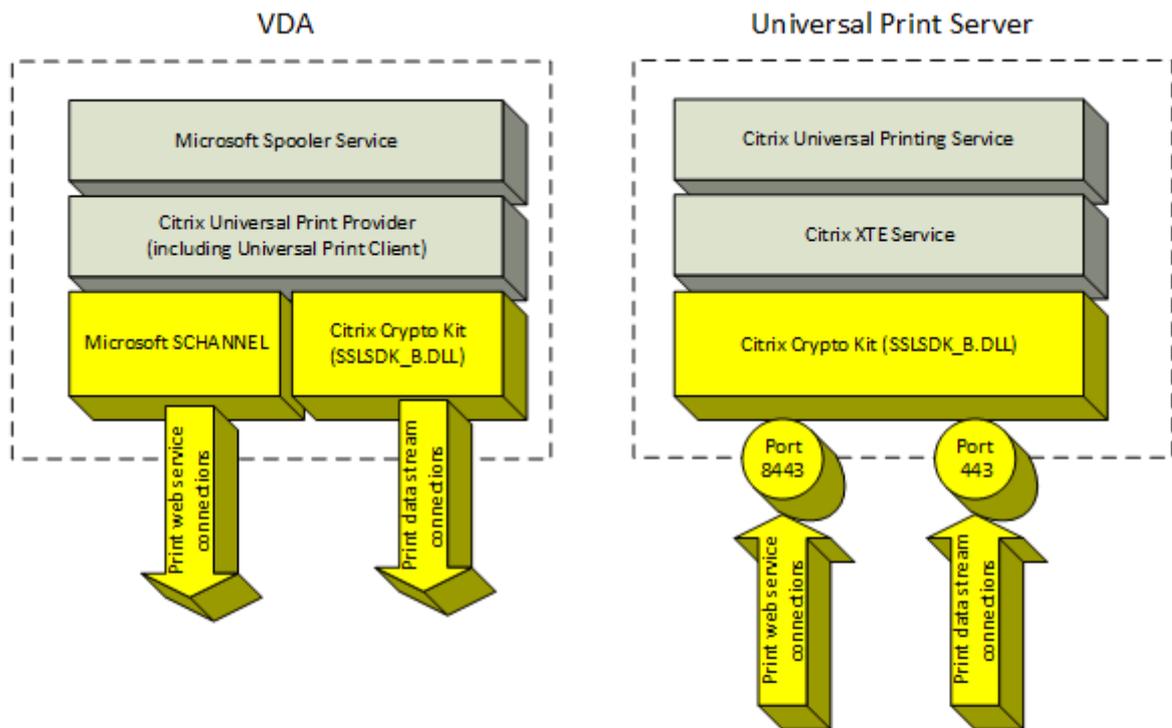
En el artículo [Introducción a los servicios y requisitos de puerto de red para Windows](#) de asistencia de Microsoft, se describen los puertos que utiliza el administrador de trabajos de impresión de Microsoft Windows, el servicio Print Spooler. La configuración de SSL/TLS de este documento no se aplica a las conexiones NetBIOS y RPC realizadas por el servicio Print Spooler de Windows. El VDA utiliza el proveedor de impresión de red de Windows (win32spl.dll) como alternativa si la configuración de directiva **Habilitar Universal Print Server** se ha establecido en **Habilitado, con opción de reserva de la impresión remota nativa de Windows**.



## Conexiones cifradas

Estas conexiones SSL/TLS relacionadas con la impresión se originan en el VDA y se conectan a los puertos del Universal Print Server. Esas conexiones se realizan solo cuando la configuración de directiva **Habilitado para SSL** está **habilitada**.

- Conexiones cifradas del servicio web de impresión (puerto TCP 8443)
- Conexiones cifradas del flujo de datos de impresión o CGP (puerto TCP 443)



## Configuración de SSL/TLS del cliente

El VDA funciona como el cliente de SSL/TLS.

Utilice la directiva de grupo de Microsoft y el Registro para configurar Microsoft SCHANNEL SSP en las conexiones cifradas del servicio web de impresión (puerto TCP 8443). El artículo de asistencia de

Microsoft [TLS Registry Settings](#) (Configuración del Registro para TLS) describe la configuración del Registro para Microsoft SCHANNEL SSP.

En el Editor de directivas de grupo del VDA (Windows Server 2016 o Windows 10), vaya a **Configuración del equipo > Plantillas administrativas > Red > Opciones de configuración SSL > Orden de conjuntos de cifrado SSL**. Seleccione el orden siguiente:

TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384\_P384  
TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384\_P256  
TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384\_P384  
TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384\_P256  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA\_P384  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA\_P256

**Nota:**

Al establecer la configuración de esta directiva de grupo, el VDA selecciona un conjunto de cifrado para las conexiones cifradas del servicio web de impresión (puerto predeterminado: 8443) solo si las conexiones aparecen en las listas de conjuntos de cifrado SSL:

- Lista ordenada de conjuntos de cifrado SSL de directiva de grupo
- Lista correspondiente a la configuración de la directiva Conjunto de cifrado SSL seleccionada (COM, GOV o ALL)

Esta configuración de directiva de grupo también afecta a otras aplicaciones y servicios TLS del VDA. Si sus aplicaciones requieren conjuntos de cifrado determinados, puede que deba agregarlos a la lista ordenada de conjuntos de cifrado de esta directiva de grupo.

**Importante:**

Los cambios de directiva de grupo para la configuración de TLS solo surten efecto después de reiniciar el sistema operativo.

Utilice una directiva de Citrix para establecer la configuración de SSL/TLS en conexiones cifradas del flujo de datos de impresión o CGP (puerto TCP 443).

## Configuración de SSL/TLS del servidor

Universal Print Server funciona como el servidor de SSL/TLS.

Utilice el script de PowerShell `Enable-UpsSsl.ps1` para establecer la configuración de SSL/TLS.

## Instalar el certificado del servidor de TLS en Universal Print Server

Para HTTPS, Universal Print Server admite las funciones de TLS mediante certificados de servidor. Los certificados de cliente no se utilizan. Use los Servicios de certificados de Microsoft Active Directory u otra entidad de certificación con el fin de solicitar un certificado para Universal Print Server.

Tenga en cuenta las siguientes consideraciones al inscribir o solicitar un certificado mediante los Servicios de certificados de Microsoft Active Directory:

1. Coloque el certificado en el almacén de certificados **personal** del equipo local.
2. Asigne al atributo **Common Name** (Nombre común) de Subject Distinguished Name o Subject DN (Nombre distintivo del sujeto) del certificado el nombre de dominio completo (FQDN) de Universal Print Server. Especifique esto en la plantilla de certificado.
3. Establezca el proveedor de servicios de cifrado (CSP) utilizado para generar la solicitud de certificado y la clave privada en **Microsoft Enhanced RSA and AES Cryptographic Provider (Encryption)**. Especifique esto en la plantilla de certificado.
4. Establezca el tamaño de la clave en, al menos, 2048 bits. Especifique esto en la plantilla de certificado.

## Configurar SSL en Universal Print Server

El servicio XTE de Universal Print Server escucha las conexiones entrantes. Funciona como un servidor de SSL cuando SSL está habilitado. Las conexiones entrantes son de dos tipos: conexiones del servicio web de impresión, que contienen comandos de impresión, y conexiones del flujo de datos de impresión, que contienen trabajos de impresión. SSL se puede habilitar en estas conexiones. SSL protege la confidencialidad y la integridad de estas conexiones. De forma predeterminada, SSL está inhabilitado.

El script de PowerShell utilizado para configurar SSL se encuentra en los medios de instalación y su nombre de archivo es: `\Support\Tools\SslSupport\Enable-UpsSsl.ps1`.

## Configurar números de puerto de escucha en Universal Print Server

Estos son los puertos predeterminados del servicio XTE:

- Puerto TCP del servicio web de impresión (HTTP) para texto no cifrado: 8080
- Puerto TCP del flujo de datos de impresión (CGP) para texto no cifrado: 7229
- Puerto TCP del servicio web de impresión cifrado (HTTPS): 8443
- Puerto TCP del flujo de datos de impresión (CGP) cifrado: 443

Para cambiar los puertos utilizados por el servicio XTE en Universal Print Server, ejecute los siguientes comandos en PowerShell como administrador (consulte la siguiente sección para ver comentarios sobre el uso del script de PowerShell Enable-UpsSsl.ps1):

1. `Stop-Service CitrixXTEServer, UpSvc`
2. `Enable-UpsSsl.ps1 -Enable -HTTPSPort <port> -CGPSSLPort <port>` o  
`Enable-UpsSsl.ps1 -Disable -HTTPPort <port> -CGPPort <port>`
3. `Start-Service CitrixXTEServer`

## Configuración de TLS en Universal Print Server

Si tiene varios servidores Universal Print Server en una configuración con equilibrio de carga, asegúrese de que la configuración de TLS sea coherente en todos los servidores Universal Print Server.

Al configurar TLS en Universal Print Server, los permisos del certificado de TLS instalado cambian, lo que da a Universal Printing Service acceso de lectura a la clave privada del certificado y le informa de lo siguiente:

- Qué certificado del almacén de certificados hay que usar para TLS.
- Qué números de puerto TCP hay que usar para las conexiones TLS.

El Firewall de Windows (si está habilitado) debe estar configurado para permitir conexiones entrantes en estos puertos TCP. Esta configuración se lleva a cabo cuando se usa el script de PowerShell Enable-UpsSsl.ps1.

- Qué versiones del protocolo TLS se deben permitir.

Universal Print Server admite las versiones de protocolo TLS 1.2, 1.1 y 1.0. Especifique la versión mínima permitida.

La versión predeterminada del protocolo TLS es 1.2.

- Qué conjuntos de cifrado TLS se deben permitir.

Un conjunto de cifrado selecciona los algoritmos criptográficos que se utilizan para una conexión. Los VDA y Universal Print Server pueden admitir varios grupos diferentes de conjuntos de cifrado. Cuando un VDA se conecta y envía una lista de los conjuntos de cifrado TLS admitidos, Universal Print Server asigna uno de los conjuntos de cifrado del cliente a uno de los conjuntos de cifrado de su propia lista de conjuntos de cifrado configurados y acepta la conexión. Si no encaja ningún conjunto de cifrado, Universal Print Server rechaza la conexión.

El servidor de impresión universal Universal Print Server admite los siguientes conjuntos de cifrado denominados GOV (gubernamental), COM (comercial) y ALL para los modos OPEN, FIPS y los modos

nativos SP800-52 del kit Crypto. Los conjuntos de cifrado aceptables también dependen de la configuración de directiva **Modo FIPS de SSL** y del modo FIPS de Windows. Consulte este [artículo de asistencia de Microsoft](#) para obtener información sobre el modo FIPS de Windows.

Conjunto de cifrado (en orden de prioridad decreciente)	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
TLS_ECDHE_RSA_AES256_GCM_SHA384			X	X		X	X		X
TLS_ECDHE_RSA_AES256_CBC_SHA384			X	X		X	X		X
TLS_ECDHE_RSA_AES256_CBC_SHA	X			X	X		X	X	

### Configurar TLS en un servidor Universal Print Server mediante el script de PowerShell

Instale el certificado TLS en **Equipo local > Personal > área Certificados** del almacén de certificados. Si hay más de un certificado en esa ubicación, proporcione la huella digital del certificado al script `Enable-UpsSsl.ps1` de PowerShell.

**Nota:**

El script de PowerShell busca el certificado correcto basándose en el FQDN de Universal Print Server. No hace falta agregar la huella digital del certificado cuando existe solo un certificado para el FQDN de Universal Print Server.

El script `Enable-UpsSsl.ps1` habilita o inhabilita las conexiones TLS procedentes del VDA y dirigidas a Universal Print Server. Este script está disponible en la carpeta **Support > Tools > SslSupport** de los medios de instalación.

Al habilitar TLS, el script inhabilita todas las reglas de Firewall de Windows para los puertos TCP de Universal Print Server. A continuación, agrega nuevas reglas que permiten al servicio XTE aceptar conexiones entrantes solo en los puertos UDP y TCP de TLS. También inhabilita las reglas de Firewall de Windows para:

- Conexiones del servicio web de impresión para texto no cifrado (puerto predeterminado: 8080)

- Conexiones del flujo de datos de impresión (CGP) para texto no cifrado (puerto predeterminado: 7229)

La consecuencia es que los VDA pueden realizar estas conexiones solamente al utilizar TLS.

**Nota:**

Habilitar TLS no afecta a las conexiones RPC/SMB del servicio Print Spooler de Windows procedentes del VDA y dirigidas a Universal Print Server.

**Importante:**

Especifique **Enable** o **Disable** como primer parámetro. El parámetro CertificateThumbprint es opcional si solamente hay un certificado del almacén de certificados de la carpeta Personal del equipo local con el FQDN de Universal Print Server. Los demás parámetros son opcionales.

**Sintaxis**

```
1 Enable-UpsSSL.ps1 -Enable [-HTTPPort <port>] [-CGPPort <port>] [-
  HTTPSPort <port>] [-CGPSSLPort <port>] [-SSLMinVersion <version>] [-
  SSLCipherSuite <name>] [-CertificateThumbprint <thumbprint>] [-
  FIPSMODE <Boolean>] [-ComplianceMode <mode>]
2 Enable-UpsSSL.ps1 -Disable [-HTTPPort <portnum>] [-CGPPort <portnum>]
```

Parámetro	Descripción
Enable	Habilita SSL/TLS en XTE Server. Este parámetro o el parámetro Disable es obligatorio.
Disable	Inhabilita SSL/TLS en XTE Server. Este parámetro o el parámetro Enable es obligatorio.
CertificateThumbprint "<thumbprint>"	Huella digital del certificado TLS en el almacén de certificados de la carpeta Personal del equipo local, indicada entre comillas. El script utiliza la huella digital especificada para seleccionar el certificado a utilizar.
HTTPPort <port>	Puerto del servicio web de impresión (HTTP/SOAP) para texto no cifrado. Predeterminado: 8080
CGPPort <port>	Puerto del flujo de datos de impresión (CGP) para texto no cifrado. Predeterminado: 7229
HTTPSPort <port>	Puerto del servicio web de impresión (HTTPS/SOAP) cifrado. Predeterminado: 8443

Parámetro	Descripción
CGPSSLPort <port>	Puerto del flujo de datos de impresión (CGP) cifrado. Valor predeterminado: 443
SSLMinVersion "<version>"	Versión mínima del protocolo TLS, indicada entre comillas. Valores válidos: "TLS_1.0", "TLS_1.1"y "TLS_1.2". Predeterminado: TLS_1.2.
SSLCipherSuite " <name> "	Nombre del paquete del conjunto de cifrado TLS, indicado entre comillas. Valores válidos: "GOV", "COM"y "ALL"(valor predeterminado).
FIPSMODE <Boolean>	Habilita o inhabilita el modo FIPS 140 en XTE Server. Valores válidos: \$true para habilitar el modo FIPS 140, \$false para inhabilitar el modo FIPS 140.

---

## Ejemplos

El siguiente script habilita TLS. La huella digital (representada como "12345678987654321"en este ejemplo) se utiliza para seleccionar el certificado que se utilizará.

```
Enable-UpsSsl.ps1 -Enable -CertificateThumbprint "12345678987654321"
```

El siguiente script inhabilita TLS.

```
Enable-UpsSsl.ps1 -Disable
```

## Configurar el modo FIPS

Habilitar los Estándares federal de procesamiento de información (o modo FIPS) de Estados Unidos garantiza el uso exclusivo de criptografía que cumpla los estándares FIPS 140 en las conexiones cifradas de Universal Print Server.

Configure el modo FIPS en el servidor antes de configurarlo en el cliente.

Consulte el sitio web de la documentación de Microsoft para habilitar o inhabilitar el modo FIPS de Windows.

### Habilitar el modo FIPS en el cliente

En Delivery Controller, ejecute Citrix Studio y establezca la configuración de directiva de Citrix **Modo FIPS de SSL** como **Habilitada**. Habilite la directiva de Citrix.

Haga esto en cada VDA:

1. Habilite el modo FIPS de Windows.
2. Reinicie el VDA.

### Habilitar el modo FIPS en el servidor

Haga esto en cada servidor Universal Print Server:

1. Habilite el modo FIPS de Windows.
2. Ejecute este comando de PowerShell como administrador: `stop-service CitrixXTEServer , UpSvc`
3. Ejecute el script `Enable-UpsSsl.ps1` con los parámetros `-Enable -FIPSMode $true`.
4. Reinicie Universal Print Server.

### Inhabilitar el modo FIPS en el cliente

En Delivery Controller, ejecute Citrix Studio y establezca la configuración de directiva de Citrix **Modo FIPS de SSL** como **Inhabilitada**. Habilite la directiva de Citrix. También puede eliminar la configuración de directiva de Citrix **Modo FIPS de SSL**.

Haga esto en cada VDA:

1. Inhabilite el modo FIPS de Windows.
2. Reinicie el VDA.

### Inhabilitar el modo FIPS en el servidor

Haga esto en cada servidor Universal Print Server:

1. Inhabilite el modo FIPS de Windows.
2. Ejecute este comando de PowerShell como administrador: `stop-service CitrixXTEServer , UpSvc`
3. Ejecute el script `Enable-UpsSsl.ps1` con los parámetros `-Enable -FIPSMode $false`.
4. Reinicie Universal Print Server.

## Configurar la versión del protocolo SSL/TLS

La versión predeterminada del protocolo SSL/TLS es TLS 1.2. TLS 1.2 es la única versión recomendada del protocolo SSL/TLS para su uso en producción. Para solucionar problemas que pueda haber, es posible que deba cambiar temporalmente la versión del protocolo SSL/TLS a un entorno que no sea de producción.

SSL 2.0 y SSL 3.0 no se admiten en Universal Print Server.

## Configurar la versión del protocolo SSL/TLS en el servidor

Haga esto en cada servidor Universal Print Server:

1. Ejecute este comando de PowerShell como administrador: `stop-service CitrixXTEServer , UpSvc`
2. Ejecute el script `Enable-UpsSsl.ps1` con los parámetros de versión `-Enable -SSLMinVersion`. Recuerde volver a revertir esto a “TLS 1.2” cuando haya terminado las pruebas.
3. Reinicie Universal Print Server.

## Configurar la versión del protocolo SSL/TLS en el cliente

Haga esto en cada VDA:

1. En Delivery Controller, asigne la versión de protocolo deseada en la configuración de directiva **Versión de protocolo SSL** y habilite la directiva.
2. El artículo de asistencia de Microsoft [TLS Registry Settings](#) (Configuración del Registro para TLS) describe la configuración del Registro para Microsoft SCHANNEL SSP. Habilite **TLS 1.0, TLS 1.1 o TLS 1.2** en el cliente mediante la configuración del Registro.

### Importante:

No se olvide de revertir la configuración del Registro a sus valores originales cuando haya terminado las pruebas.

3. Reinicie el VDA.

## Solución de problemas

Si se produce un error de conexión, compruebe el archivo de registros C:\Archivos de programa (x86)\Citrix\XTE\logs\error.log de Universal Print Server.

Si el protocolo de enlace SSL/TLS falla, aparece el mensaje de error **SSL handshake from client failed** en este archivo de registro. Errores como este pueden producirse si la versión del protocolo SSL/TLS del VDA y la de Universal Print Server no coinciden.

Utilice el FQDN de Universal Print Server en la siguiente configuración de directiva que contiene nombres de host de Universal Print Server:

- Impresoras de la sesión
- Asignaciones de impresora
- Universal Print Servers para equilibrio de carga

Compruebe que el reloj del sistema (fecha, hora y zona horaria) esté bien configurado en los servidores Universal Print Server y en los VDA.

## Seguridad de canales virtuales

January 25, 2022

De forma predeterminada, la función de lista de canales virtuales permitidos está inhabilitada. Al habilitarse, solo se pueden abrir los canales virtuales de Citrix en las sesiones de Virtual Apps and Desktops. Si hay necesidad de utilizar canales virtuales personalizados, ya sean internos o de un tercero, deben agregarse explícitamente a la lista de permitidos.

### Agregar canales virtuales a la lista de permitidos

Para agregar un canal virtual a la lista de permitidos, necesita lo siguiente:

1. El nombre del canal virtual tal y como se define en el código, que puede tener hasta 7 caracteres. Por ejemplo, `CTXCV1`.
2. Las rutas a los procesos que abren el canal virtual en la máquina VDA. Por ejemplo, `C:\Program Files\Application\run.exe`.

Una vez que tenga la información necesaria, deberá agregar el canal virtual a la lista de permitidos mediante la [configuración de la directiva Lista de canales virtuales permitidos](#). Para agregar un canal virtual a la lista, escriba el nombre del canal virtual seguido de una coma y, a continuación, la ruta del proceso que accede al canal virtual. Si hay varios procesos, estos se pueden agregar separados por comas.

**Nota:**

Después de hacer cambios en la directiva, reinicie el VDA para asegurarse de que los cambios surtan efecto.

Con los ejemplos anteriores, agregaría lo siguiente a la lista:

```
CTXCVC1,C:\Program Files\Application\run.exe
```

Si hay varios procesos, agregaría lo siguiente a la lista:

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application\run2.exe
```

## Consideraciones sobre canales virtuales Citrix

Todos los canales virtuales Citrix integrados son de confianza y se permite abrirlos sin ninguna configuración adicional. Sin embargo, hay dos funcionalidades que requieren entradas explícitas en la lista de permitidos debido a dependencias externas:

- Redirección multimedia
- HDX RealTime Optimization Pack para Skype Empresarial

### Redirección multimedia

Esta información es necesaria para la entrada en la lista de permitidos:

- Nombre del canal virtual: CTXMM
- Proceso: Ruta al reproductor multimedia utilizado en la máquina VDA. Por ejemplo, C:\Archivos de programa (x86)\Windows Media Player\wmplayer.exe
- Entrada en la lista de permitidos: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

### HDX RealTime Optimization Pack para Skype Empresarial

Esta información es necesaria para la entrada en la lista de permitidos:

- Nombre del canal virtual: CTXRMEP
- Proceso: Ruta al archivo ejecutable de Skype Empresarial en la máquina VDA, que puede variar según la versión de Skype Empresarial o si se ha usado una ruta de instalación personalizada. Por ejemplo, C:\Archivos de programa\Microsoft Office\root\Office16\lync.exe.
- Entrada en la lista de permitidos: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

## Obtener nombres y procesos de canales virtuales

La forma más sencilla de obtener el nombre del canal virtual y el proceso que lo abre en la máquina VDA es obtener la información del desarrollador o del proveedor tercero que proporcionó el canal virtual.

También puede obtener esta información aplicando los registros de la funcionalidad y siguiendo estos pasos:

1. Una vez establecidos los componentes del cliente y del servidor del canal virtual personalizado, inicie una aplicación virtual o un escritorio virtual.
2. En el registro de eventos del sistema de la máquina VDA, busque el nombre del canal virtual personalizado en el siguiente evento:
  - En un VDA de sesión única, ID de evento 2004 de Picadd de origen.
  - En un VDA multisesión, ID de evento 16 de Rpm de origen.
3. Cierre la sesión.
4. Agregue una entrada a la configuración de directiva Lista de canales virtuales permitidos para el canal virtual identificado, con solo el nombre del canal virtual.
5. Reinicie el VDA.
6. Inicie la aplicación virtual o el escritorio virtual.
7. En el registro de eventos del sistema de la máquina VDA, busque el proceso que intentó abrir el canal virtual en el siguiente evento:
  - En un VDA de sesión única, ID de evento 2002 de Picadd de origen.
  - En un VDA multisesión, ID de evento 14 de Rpm de origen.
8. Cierre la sesión.
9. Modifique la entrada en la configuración de directiva Lista de canales virtuales permitidos para incluir el proceso identificado.
10. Reinicie el VDA.
11. Inicie la aplicación virtual o el escritorio virtual para comprobar que el canal virtual personalizado se abre correctamente.

## Registro de la lista de canales virtuales permitidos

Los siguientes eventos se registran en el registro de eventos de la máquina VDA de sesión única:

---

---

Nombre de registro	Sistema
--------------------	---------

ID	2001
Origen	Picadd
Nivel	Información
Descripción	El proceso <processName> ha abierto el canal virtual personalizado <vcName>

---

---

Nombre de registro	Sistema
ID	2002
Origen	Picadd
Nivel	Advertencia
Descripción	El proceso <processName> no puede abrir el canal virtual personalizado <vcName>

---

---

Nombre de registro	Sistema
ID	2003
Origen	Picadd
Nivel	Información
Descripción	<username> abrió el canal virtual personalizado <vcName>

---

---

Nombre de registro	Sistema
ID	2004

---

---

Origen	Picadd
Nivel	Advertencia
Descripción	<username> intentó abrir el canal virtual personalizado <vcName>

---

Los siguientes eventos se registran en el registro de eventos de la máquina VDA multisesión:

---

Nombre de registro	Sistema
ID	13
Origen	Rpm
Nivel	Información
Descripción	El proceso <processName> ha abierto el canal virtual personalizado <vcName>

---

---

Nombre de registro	Sistema
ID	14
Origen	Rpm
Nivel	Advertencia
Descripción	El proceso <processName> no puede abrir el canal virtual personalizado <vcName>

---

---

Nombre de registro	Sistema
ID	15

---

Origen	Rpm
Nivel	Información
Descripción	<username> abrió el canal virtual personalizado <vcName>

---

---

Nombre de registro	Sistema
ID	16
Origen	Rpm
Nivel	Advertencia
Descripción	<username> intentó abrir el canal virtual personalizado <vcName>

---

### Canales virtuales de terceros conocidos

A continuación se indican soluciones de terceros conocidas que utilizan canales virtuales Citrix. Esta lista no incluye todas las soluciones que usan un canal virtual personalizado Citrix.

- Cerner
- Cisco WebEx Teams
- Cisco WebEx Meetings Virtual Desktop Software
- Epic Warp Drive
- Extensiones de cliente Midmark IQPath
- Extensiones de cliente Nuance PowerMic
- Nuance Dragon Medical Network Edition 360 vSync
- Zoom Meetings para VDI

Para obtener detalles sobre cómo agregar los canales virtuales asociados a la lista de permitidos, consulte a los proveedores de las soluciones. Como alternativa, siga los pasos descritos en la sección Obtener nombres y procesos de canales virtuales.

## Dispositivos

January 4, 2021

HDX proporciona una experiencia de usuario de alta definición en cualquier dispositivo y en cualquier ubicación. Los artículos en la sección Dispositivos describen estos dispositivos:

- [Dispositivo USB genérico](#)
- [Dispositivos móviles y de pantalla táctil](#)
- [Dispositivos en serie](#)
- [Teclados especiales](#)
- [Dispositivos TWAIN](#)
- [Cámaras web](#)

### Dispositivo USB optimizado y genérico

Un dispositivo USB optimizado es aquel para el cual la aplicación Citrix Workspace ofrece funcionalidades específicas. Por ejemplo, la capacidad de redirigir cámaras web mediante el canal virtual multimedia HDX. Un dispositivo genérico es un dispositivo USB para el que no hay ninguna funcionalidad específica en la aplicación Citrix Workspace.

De forma predeterminada, la redirección de USB genérico no puede redirigir dispositivos USB con funcionalidad optimizada para el canal virtual a menos que se coloquen en el modo Genérico.

En general, se obtiene un mejor rendimiento para dispositivos USB en el modo Optimizado que en el modo Genérico. Sin embargo, hay casos en que un dispositivo USB no tiene funcionalidad completa en el modo Optimizado. Puede que sea necesario cambiar al modo Genérico para obtener acceso completo a sus funciones.

Con dispositivos de almacenamiento masivo USB, puede utilizar la asignación de unidades del cliente, la redirección de USB genérico o ambos, controlados mediante directivas de Citrix. Las principales diferencias son:

Si la directiva de USB genérico y la directiva de asignación de unidades del cliente están ambas habilitadas y se inserta un dispositivo de almacenamiento masivo antes o después de iniciar una sesión, el dispositivo se redirigirá mediante la asignación de unidades del cliente.

Cuando se dan estas condiciones, el dispositivo de almacenamiento masivo se redirige mediante la redirección de USB genérico:

- Tanto la redirección de USB genérico como las directivas de asignación de unidades del cliente están habilitadas.
- Un dispositivo está configurado para la redirección automática.

- Se inserta un dispositivo de almacenamiento masivo antes o después de que se inicie sesión.

Para obtener más información, consulte <http://support.citrix.com/article/CTX123015>.

---

Función	Asignación de unidades del cliente	Redirección de USB genérico
Habilitada de forma predeterminada	Sí	No
Configuración para acceso de solo lectura	Sí	No
Acceso a dispositivo cifrado	Sí, si el cifrado se desbloquea antes de acceder al dispositivo en la sesión virtual.	Solo Citrix Virtual Desktops

---

## Dispositivos USB genéricos

April 19, 2024

La tecnología HDX ofrece **optimización** con los dispositivos USB más comunes. Estos dispositivos son:

- Monitores
- Mouse
- Teclados
- Teléfonos VoIP
- Auriculares con micro
- Cámaras web
- Escáneres
- Cámaras
- Impresoras
- Unidades
- Lectores de tarjetas inteligentes
- Tablet de dibujo
- Paneles táctiles de firma electrónica

La optimización ofrece una experiencia de usuario mejorada, con mejor rendimiento y eficiencia del ancho de banda en una conexión por red WAN. La optimización suele ser la mejor opción, sobre todo en entornos de alta latencia o cuando se requiera confidencialidad.

La tecnología HDX ofrece la **redirección de USB genérico** para dispositivos específicos sin optimización o cuando esta no es adecuada. Para obtener más información sobre la redirección de USB genérico, consulte [Redirigir USB genérico](#).

Para obtener más información sobre dispositivos USB y la aplicación Citrix Workspace para Windows, consulte [Configurar la redirección de dispositivos USB compuestos](#) y [Configurar la compatibilidad con USB].(/es-es/citrix-workspace-app-for-windows/configure/config-xdesktop/config-usb-support.html)

## Dispositivos móviles y de pantalla táctil

August 9, 2022

### Modo tableta para dispositivos de pantalla táctil mediante Windows Continuum

Continuum es una función de Windows 10 que se adapta al uso que se le da al dispositivo cliente. Esta versión de Continuum, incluido el cambio dinámico entre los diferentes modos, está disponible a partir de en la versión 7.16 de VDA y Citrix Receiver para Windows 4.10.

El VDA presente en Windows 10 detecta la presencia de un teclado o mouse en un cliente táctil y coloca al cliente en el modo escritorio. Si el teclado o el mouse no están presentes, el VDA de Windows 10 coloca al cliente en el modo móvil o tableta. Esta detección ocurre en la conexión y la reconexión. También ocurre al conectar o desconectar el teclado o el mouse.

Esta función está activada de forma predeterminada. Para inhabilitar esta versión de la funcionalidad, modifique las configuraciones de directiva [Alternar del modo tableta](#) en el artículo de configuraciones de la directiva ICA.

Para la versión de la funcionalidad que se incluye en XenApp 7.14 y 7.15 LTSR y XenDesktop 7.14 y 7.15 LTSR, use los parámetros de Registro para inhabilitar la función. Para obtener más información, consulte [Modo tableta para dispositivos de pantalla táctil](#).

El **modo tableta** ofrece una interfaz de usuario que se adapta mejor a las pantallas táctiles:

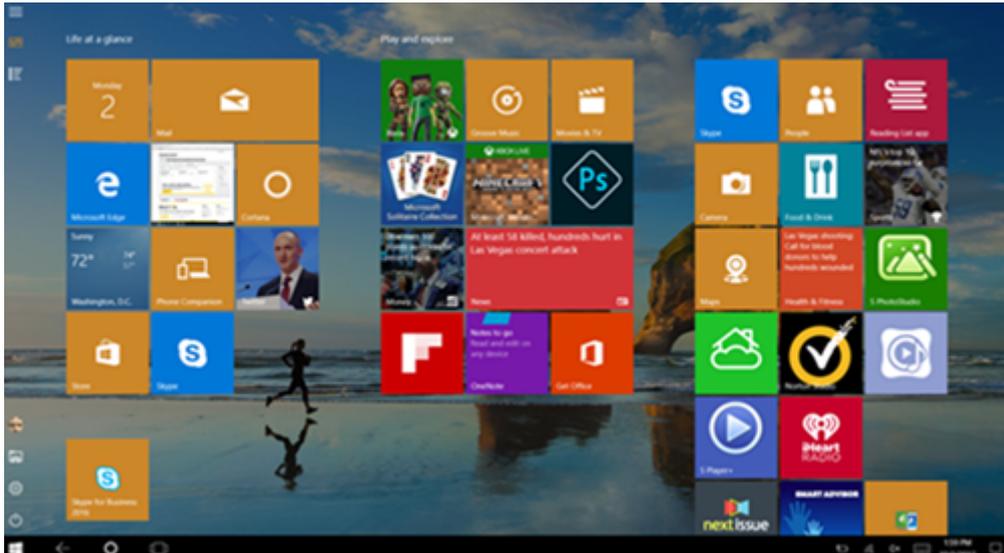
- Botones ligeramente más grandes.
- La pantalla de Inicio y cualquier aplicación que abra se inicia en modo de pantalla completa.
- La barra de tareas contiene el botón Atrás.
- Se han quitado iconos de la barra de tareas.

Puede utilizar el Explorador de archivos.

El **modo escritorio** ofrece la interfaz de usuario tradicional, donde se interactúa de la misma manera que con el PC, el teclado y el mouse.

El modo tableta requiere, como mínimo, la versión de Citrix Hypervisor 8.2 CU1 LTSR. Citrix Hypervisor se integra en el VDA de Citrix Virtual Desktops, con lo que el hipervisor cambia para permitir la configuración de firmware virtual para dispositivos 2 en 1. Windows 10 carga el controlador GPIO en la máquina virtual de destino basándose en esta BIOS actualizada. Se utiliza para alternar entre los modos escritorio y tableta dentro de la máquina virtual.

La aplicación Citrix Workspace para HTML5 (la versión ligera) no admite las funciones de Windows Continuum.



Ejecute el comando CLI de XenServer para permitir que se pueda cambiar entre el equipo portátil y la tableta:

**xe vm-param-set uuid=<VM\_UUID> platform:acpi\_laptop\_slate=1**

**Importante:**

Actualizar la imagen base de un catálogo existente de máquinas después de cambiar el parámetro de metadatos no afecta a las máquinas virtuales previamente aprovisionadas. Después de cambiar la imagen base de la VM de XenServer, cree un catálogo, seleccione la imagen base y aprovisiona una nueva máquina con Machine Creation Services (MCS).

**Antes de iniciar una sesión:**

Antes de iniciar una sesión, se recomienda que vaya a **Configuración > Sistema > Modo tableta** en el VDA y establezca las siguientes opciones en los menús de lista desplegable:

- Usar el modo adecuado para mi hardware
- No preguntarme y cambiar siempre

Si no configura estas opciones antes de iniciar la sesión, configúrelas después de iniciar la sesión y reinicie el VDA.

## Tablet mode

When I sign in

Use the appropriate mode for my hardware ▾

When this device automatically switches tablet mode on or off

Don't ask me and always switch ▾

### Lápices para Microsoft Surface Pro y Surface Book

Se admite la funcionalidad de lápiz estándar en aplicaciones basadas en Windows Ink. Esta funcionalidad requiere un Virtual Delivery Agent con al menos la versión 1809 de Microsoft Windows 10 y dispositivos cliente con la versión 1902 (como mínimo) de la aplicación Citrix Workspace para Windows. Se puede señalar, borrar y presionar con el lápiz, y se admiten las señales de Bluetooth y otras funciones que varían según el firmware del sistema operativo y el modelo del lápiz. Por ejemplo, la presión del lápiz puede ser de 4096 niveles como máximo. Esta función está habilitada de manera predeterminada.

Para obtener una demostración de Windows Ink y la funcionalidad del lápiz, haga clic en este gráfico:



## Requisitos del sistema

- Citrix Virtual Apps and Desktops 1903 (versión mínima)
- Aplicación Citrix Workspace para Windows 1902 (versión mínima)
- Microsoft Windows 10 (versión mínima 1809)

## Inhabilitar o habilitar

Para inhabilitar o habilitar esta función, configure el Registro de la siguiente manera:

HKEY\_LOCAL\_MACHINE\Software\Citrix\Citrix Virtual Desktop Agent\PenApi

Nombre: DisablePen

Tipo: DWORD

Valor:

1 (inhabilitada)

0 (habilitada)

## Puertos serie

March 21, 2023

La mayoría de los PC nuevos no tienen puertos serie integrados (COM). Es fácil agregar puertos mediante convertidores USB. Las aplicaciones adecuadas para los puertos serie suelen ser sensores, controladores, lectores antiguos de cheques, paneles táctiles, etc. Algunos dispositivos USB de puerto COM virtual utilizan controladores específicos del fabricante en lugar de los controladores que ofrece Windows (usbser.sys). Estos controladores permiten forzar el puerto COM virtual del dispositivo USB para que no cambie incluso aunque se conecte a otras ranuras USB. Se puede hacer desde **Administrador de dispositivos > Puertos (COM y LPT) > Propiedades** o desde la aplicación que controla el dispositivo.

La asignación de puertos COM del cliente permite utilizar los dispositivos conectados a los puertos COM del dispositivo de usuario durante las sesiones virtuales. Estas asignaciones se pueden utilizar de la misma forma que cualquier otra asignación de red.

Un controlador del sistema operativo asigna un nombre de enlace simbólico a cada puerto COM, como COM1 y COM2. Las aplicaciones usan ese enlace para acceder al puerto.

**Importante:**

El hecho de que un dispositivo se pueda conectar al dispositivo de punto final directamente por USB no significa que ese dispositivo se puede redirigir mediante la redirección de USB genérico. Algunos dispositivos USB funcionan como puertos COM virtuales, a los que las aplicaciones pueden acceder de la misma manera que al puerto serie físico. El sistema operativo puede abstraer puertos COM y tratarlos como archivos compartidos. Dos protocolos frecuentes para COM virtual son: CDC ACM o MCT. Cuando se conecta a través de un puerto RS-485, es posible que las aplicaciones no funcionen en absoluto. Debe obtener un convertidor de RS-485 a RS232 para usar RS-485 como puerto COM.

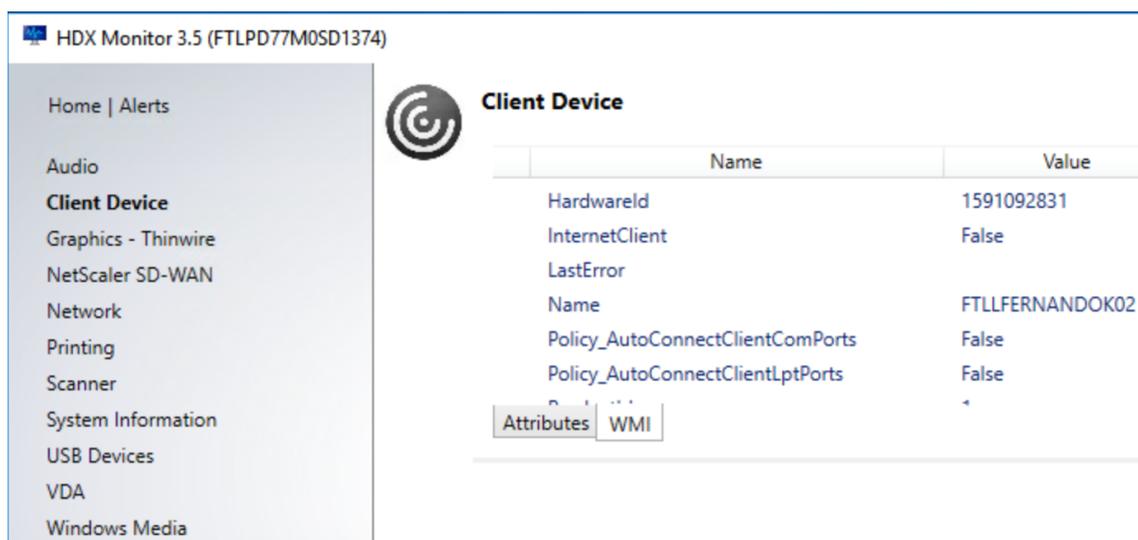
**Importante:**

Algunas aplicaciones reconocen el dispositivo (por ejemplo, un panel táctil de firmas) correctamente solo si está conectado a COM1 o COM2 en la estación de trabajo del cliente.

## Asignar un puerto COM de cliente a un puerto COM de servidor

Puede asignar los puertos COM del cliente a una sesión de Citrix de tres maneras:

- Directivas de Studio. Para obtener más información acerca de las directivas, consulte [Configuraciones de directiva de Redirección de puertos](#).
  - El símbolo del sistema del VDA.
  - Herramienta de configuración del escritorio remoto (Terminal Services).
1. Habilite las directivas **Redirección de puertos COM del cliente** y **Conectar automáticamente puertos COM del cliente de Studio**. Después de aplicarlas, se ofrece información en HDX Monitor.



HDX Monitor 3.5 (FTLPD77M0SD1374)

Home | Alerts

Audio

**Client Device**

Graphics - Thinwire

NetScaler SD-WAN

Network

Printing

Scanner

System Information

USB Devices

VDA

Windows Media

**Client Device**

Name	Value
HardwareId	1591092831
InternetClient	False
LastError	
Name	FTLLFERNANDOK02
Policy_AutoConnectClientComPorts	False
Policy_AutoConnectClientLptPorts	False
...	*

Attributes WMI

2. Si **Conectar automáticamente puertos COM del cliente** no puede asignar el puerto, puede

asignarlo manualmente o usar scripts de inicio de sesión. Inicie sesión en el VDA y, en una ventana de símbolo del sistema, escriba:

```
NET USE COMX: \\CLIENT\COMZ:
```

O bien:

```
NET USE COMX: \\CLIENT\CLIENTPORT:COMZ:
```

**X** es el número del puerto COM en el VDA (los puertos del 1 al 9 están disponibles para la asignación). **Z** es el número del puerto COM del cliente que quiere asignar.

Para confirmar que la operación se ha realizado correctamente, escriba **NET USE** en un símbolo del sistema de VDA. Aparecerá la lista de las unidades, puertos LPT y puertos COM asignados.

```
C:\Windows\system32>net use
New connections will be remembered.
```

Status	Local	Remote	Network
	COM3	\\Client\COM3:	Citrix Client Network

- Para utilizar este puerto COM en una sesión de aplicación o escritorio virtual, instale la aplicación del dispositivo de usuario y apúntela al nombre del puerto COM asignado. Por ejemplo, si asigna COM1 en el cliente a COM3 en el servidor, instale la aplicación del dispositivo de puerto COM en el VDA y apúntela a COM3 durante la sesión. Utilice este puerto COM asignado del mismo modo que lo haría con un puerto COM del dispositivo del usuario.

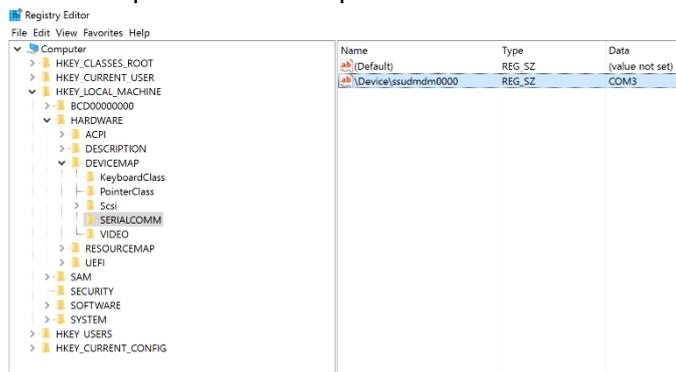
#### Importante:

La asignación de puertos COM no es compatible con TAPI. No puede asignar dispositivos Windows Telephony Application Programming Interface (TAPI) de Windows a los puertos COM del cliente. TAPI define una forma estándar que tienen las aplicaciones para controlar las funciones del teléfono para datos, fax y llamadas de voz. TAPI administra la señalización, incluido el marcado, la respuesta y la finalización de llamadas. Asimismo, gestiona servicios complementarios (como poner en espera, transferir y hacer llamadas de conferencia).

## Solución de problemas

- Compruebe que puede acceder al dispositivo directamente desde el dispositivo de punto final, sin pasar por Citrix. Mientras el puerto no se asigne al VDA, no podrá conectarse a una sesión de Citrix. Siga las instrucciones de solución de problemas incluidas con el dispositivo y primero compruebe que funciona localmente.  
Cuando un dispositivo se conecta a un puerto serie COM, se crea una clave de Registro en el

subárbol que se muestra aquí:



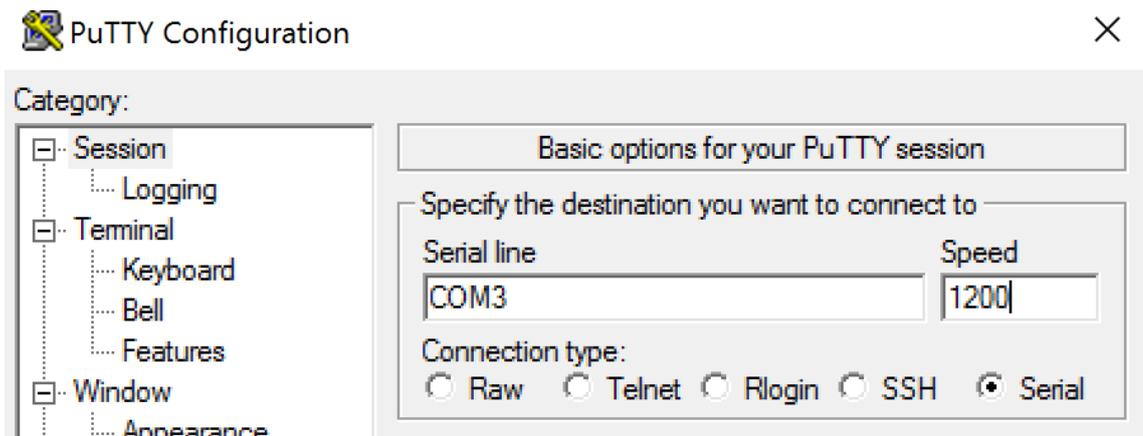
También puede encontrar esta información desde el símbolo del sistema ejecutando **chgpport /query**.

```
C:\Windows\system32\cmd.exe
C:\Users\fernandok>chgpport /query
COM3 = \Device\ssudmdm0000

C:\Users\fernandok>mode

Status for device COM3:
-----
      Baud:                1200
      Parity:               Even
      Data Bits:           7
      Stop Bits:           1
      Timeout:             OFF
      XON/XOFF:            OFF
      CTS handshaking:    OFF
      DSR handshaking:    OFF
      DSR sensitivity:    OFF
      DTR circuit:        ON
      RTS circuit:        ON
```

Si no dispone de instrucciones de solución de problemas para el dispositivo, intente solucionar problemas con una sesión PuTTY. Elija **Session** y, en **Serial line**, especifique su puerto COM.



Puede ejecutar **MODE** en una ventana de comando local. El resultado muestra el puerto COM en uso y los bits de parada, los bits de datos, la paridad y los baudios que necesita en su sesión PuTTY. Si se puede establecer la conexión con PuTTY, presione **Entrar** para ver la información que envíe el dispositivo. Los caracteres que escriba pueden repetirse en pantalla, o bien, puede recibir directamente respuesta a ellos. Sin este paso, no puede acceder al dispositivo desde una sesión virtual.

2. Asigne el puerto COM local al VDA (mediante directivas o **NET USE COMX: \\CLIENT\COMZ:**) y repita los mismos procedimientos de PuTTY que en el paso anterior, pero esta vez desde el PuTTY del VDA. Si PuTTY falla con el error **Unable to open connection to COM1. Unable to open serial port**, puede que otro dispositivo esté utilizando COM1.

3. Ejecute **chgpport /query**. Si el controlador serie de Windows integrado en el VDA asigna automáticamente \Device\Serial0 a un puerto COM1 del VDA, haga lo siguiente:

A. Abra CMD en el VDA y escriba **NET USE**.

B. Elimine cualquier asignación existente (por ejemplo, COM1) en el VDA.

#### **NET USE COM1 /DELETE**

C. Asigne el dispositivo al VDA.

#### **NET USE COM1: \\CLIENT\COM3:**

D. Apunte la aplicación en el VDA a COM3.

Por último, intente asignar su puerto COM local (por ejemplo, COM3) a otro puerto COM en el VDA (que no sea COM1 si no, por ejemplo, COM3). Compruebe que su aplicación apunta a él:

#### **NET USE COM3: \\CLIENT\COM3**

4. Si ahora ve el puerto asignado, PuTTY está funcionando, pero no pasa ningún dato, podría tratarse de una condición de carrera. La aplicación puede conectarse y abrir el puerto antes de que se asigne, con lo que se bloquea su asignación. Pruebe una de las siguientes soluciones:

- Abra una segunda aplicación publicada en el mismo servidor. Espere unos segundos para que se asigne el puerto y abra la aplicación que intenta usar el puerto.
- Habilite las directivas de redirección de puertos COM desde el Editor de directivas de grupo en Active Directory en lugar de Studio. Esas directivas son: **Redirección de puertos COM del cliente** y **Conectar automáticamente puertos COM del cliente**. Las directivas aplicadas de esta manera se pueden procesar antes de las directivas de Studio, lo que garantiza que el puerto COM se asigne. Las directivas de Citrix se envían al VDA y se almacenan en:

```
HKLN\SOFTWARE\Policies\Citrix \<user session ID\>
```

- Utilice este script de inicio de sesión para el usuario o, en lugar de publicar la aplicación, publique un script .bat que borre primero cualquier asignación en el VDA, vuelva a asignar el puerto COM virtual y luego inicie la aplicación:

```
@echo off
NET USE COM1 /delete
NET USE COM2 /delete
NET USE COM1: \\CLIENT\COM1:
NET USE COM2: \\CLIENT\COM2:
MODE COM1: BAUD=1200 (o el valor que necesite)
MODE COM2: BAUD=9600 PARITY=N Data=8 Stop=1 (o el valor que necesite)
START C:\Archivos de programa\<Ruta a su software>\
```

5. Process Monitor de Sysinternals es la herramienta de último recurso. Cuando ejecute la herramienta en el VDA, busque y filtre objetos como COM3, picaser.sys, CdmRedirector y, sobre todo, \<su\_aplicación>.exe. Los errores aparecen como “Acceso denegado” o similar.

## Limitaciones

- Los dispositivos del puerto COM deben estar conectados antes del inicio de sesiones ICA.
- La redirección del puerto COM durante la reconexión de ICA no proporciona una detección dinámica de puertos COM.
- Al conectarse desde un cliente con un dispositivo conectado a un puerto COM y, a continuación, mover por itinerancia un nuevo cliente sin un dispositivo conectado a un puerto COM, no se quita la asignación de puertos COM existente.

## Teclados especiales

April 19, 2024

## Teclados Bloomberg

### Advertencia

Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Citrix Virtual Apps and Desktops admite el teclado Starboard modelo 4 de Bloomberg (y el modelo anterior 3). Este teclado permite a los clientes del sector financiero utilizar funciones especiales en el teclado para poder acceder a datos del mercado financiero y realizar transacciones rápidamente.

Este teclado es compatible con los cuadros de conmutadores KVM y puede funcionar en dos modos:

- PC (un cable USB sin KVM)
- Modo KVM (dos cables USB con uno enrutado a través de KVM)

### Importante:

Se recomienda usar el teclado Bloomberg con una sola sesión. Es decir, no se recomienda utilizar este teclado con varias sesiones simultáneas (de un cliente a varias sesiones).

El teclado Bloomberg 4 es un dispositivo USB compuesto que consta de cuatro dispositivos USB en una carcasa física:

- Teclado.
- Lector de huellas dactilares.
- Dispositivo de sonido con teclas para aumentar y disminuir el volumen o silenciar el altavoz y el micrófono. Este dispositivo incluye altavoz, micrófono y conector integrado para el micrófono y los auriculares.
- Concentrador USB para conectar todos estos dispositivos al sistema.

### Requisitos:

- La sesión a la que se conecta la aplicación Citrix Workspace para Windows debe admitir dispositivos USB.
- La aplicación Citrix Workspace 1808 para Windows o Citrix Receiver para Windows 4.8, como mínimo, para admitir los modelos 3 y 4 del teclado Bloomberg.
- La aplicación Citrix Workspace 1808 para Windows o Citrix Receiver para Windows 4.12, como mínimo, para usar el modo KVM (dos cables USB con uno enrutado a través de KVM) para el modelo 4.

Para obtener información sobre cómo configurar los teclados Bloomberg en la aplicación Citrix Workspace para Windows, consulte [Configurar teclados Bloomberg](#).

### **Habilitar el teclado Bloomberg:**

De forma predeterminada, el teclado mejorado de Bloomberg está inhabilitado. Para habilitarlo, modifique esta entrada de Registro en la máquina cliente antes de iniciar una conexión.

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB

Nombre: **EnableBloombergHID** (dword)

Valor: 0 (Inhabilitar) 1 (Habilitar)

### **Comprobar que está disponible:**

Para determinar si el teclado Bloomberg está habilitado en la aplicación Citrix Workspace, compruebe si Desktop Viewer informa correctamente de los dispositivos del teclado Bloomberg.

En el escritorio:

Abra Desktop Viewer. Si el teclado Bloomberg está habilitado, Desktop Viewer muestra tres dispositivos debajo del icono USB:

- Escáner de huellas dactilares de Bloomberg
- Funciones del teclado de Bloomberg
- Bloomberg LP Keyboard 2013

Solo aplicación integrada:

Abra el menú Central de conexiones desde el icono del área de notificaciones de la aplicación Citrix Workspace. Si el teclado Bloomberg está habilitado, los tres dispositivos aparecen en el menú Dispositivos.

La marca de verificación situada junto a cada uno de estos dispositivos indica que están conectados remotamente a la sesión.

## **Dispositivos TWAIN**

September 22, 2021

### **Requisitos**

- El escáner debe ser compatible con TWAIN.
- Instale los controladores TWAIN en el dispositivo local. No son necesarios en el servidor.
- Conecte el escáner localmente (por ejemplo, por USB).
- Compruebe que el escáner esté utilizando el controlador TWAIN local, no el servicio Adquisición de imágenes de Windows.

- Compruebe que no se aplica ninguna directiva (por ejemplo, que limite el ancho de banda en la sesión ICA) a la cuenta de usuario que se utiliza para la prueba. Por ejemplo, la directiva Límite de ancho de banda de redirección de dispositivos USB del cliente.

Para obtener información acerca de las configuraciones de directiva, consulte [Configuraciones de directiva de Dispositivos TWAIN](#).

## Cámaras web

August 23, 2022

### Streaming por cámara web de alta definición

Las aplicaciones de videoconferencia que se ejecutan en la sesión virtual pueden utilizar cámaras web. La aplicación presente en el servidor selecciona el formato de cámara web y la resolución en función de los tipos de formato compatibles. Cuando se inicia una sesión, el cliente envía la información de la cámara web al servidor. Puede elegir una cámara web en la aplicación de videoconferencia. Si la cámara web y la aplicación admiten la generación de alta definición, la aplicación usa la resolución de alta definición. Admitimos resoluciones de cámara web hasta 1920 x 1080.

Esta función requiere Citrix Receiver para Windows, versión mínima 4.10. Para obtener una lista de las plataformas de aplicaciones Citrix Workspace que admiten la redirección de la cámara web HDX, consulte la [tabla de funciones de la aplicación Citrix Workspace](#).

Para obtener más información sobre el streaming de cámaras web de alta definición, consulte [HDX y los requisitos de las conferencias de vídeo para la compresión de vídeo de cámaras web](#).

#### ADVERTENCIA

Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Use el Editor del Registro bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Puede usar una clave de Registro para inhabilitar la función. Se usa la resolución predeterminada de 352 x 288:

HKEY\_LOCAL\_MACHINE\Software\Citrix\HDXRealTime

Nombre: Disable\_HighDefWebcam

Tipo: REG\_DWORD

Datos: 1 = Desactiva la distribución por streaming de la cámara web de alta definición

Puede usar claves de Registro en el cliente para configurar una resolución específica. Compruebe que la cámara admite la resolución especificada:

HKEY\_CURRENT\_USER\Software\Citrix\HDXRealTime

Nombre: DefaultWidth

Tipo: REG\_DWORD

Datos (decimales): Anchura deseada (por ejemplo, 1280)

Nombre: DefaultHeight

Tipo: REG\_DWORD

Datos (decimales): Altura deseada (por ejemplo, 720)

## Gráficos

September 22, 2021

Citrix HDX Graphics contiene un conjunto amplio de tecnologías de codificación y aceleración de gráficos que optimiza la entrega de aplicaciones con gráficos sofisticados desde Citrix Virtual Apps and Desktops. Estas tecnologías ofrecen la misma experiencia que con un escritorio físico cuando se trabaja de forma remota en aplicaciones virtuales de uso intensivo de gráficos.

Puede usar el software o el hardware para la generación de gráficos. La generación por software requiere una biblioteca de terceros que se denomina “rasterizador de software”. Por ejemplo, Windows incluye el rasterizador WARP para gráficos DirectX. En ocasiones, puede interesarle usar un elemento de representación alternativa por software. La representación por hardware (aceleración de hardware) requiere un procesador de gráficos (GPU).

Citrix HDX Graphics ofrece una configuración de cifrado predeterminado que está optimizada para los casos de uso más comunes. Con las directivas Citrix, los administradores de TI también pueden configurar varios parámetros relacionados con gráficos para cumplir los diferentes requisitos y ofrecer la experiencia de usuario pertinente.

### Thinwire

Thinwire es la tecnología predeterminada de Citrix para pantallas remotas que se utiliza en Citrix Virtual Apps and Desktops.

Las tecnologías de pantallas remotas permiten que los gráficos generados en una máquina se transmitan (normalmente a través de una red) a otra máquina para que se vean desde allí. Los gráficos se

generan como resultado de una entrada de usuario (por ejemplo, pulsaciones de teclado o acciones del mouse).

### **HDX 3D Pro**

Las capacidades HDX 3D Pro de Citrix Virtual Apps and Desktops permiten entregar escritorios y aplicaciones que rinden más gracias a una unidad de procesamiento de gráficos (GPU) para la aceleración de hardware. Estas aplicaciones incluyen gráficos 3D profesionales basados en OpenGL y DirectX. El VDA estándar solo admite la aceleración GPU de DirectX.

### **Aceleración de GPU para SO Windows de sesión única**

Cuando utiliza HDX 3D Pro, puede entregar aplicaciones de uso intensivo de gráficos como parte de escritorios o aplicaciones que se alojan en máquinas con SO de sesión única. HDX 3D Pro admite equipos host físicos (incluido el escritorio, blade y estaciones de trabajo en rack), así como GPU PassThrough y tecnologías de virtualización de GPU que ofrecen los hipervisores de XenServer, vSphere y Hyper-V (solo PassThrough).

Mediante GPU PassThrough, puede crear máquinas virtuales con acceso exclusivo a hardware de procesamiento de gráficos dedicado. Es posible instalar varias GPU en el hipervisor y asignar, una a una, diversas VM a cada GPU.

Con la virtualización de GPU, varias máquinas virtuales pueden acceder directamente a la capacidad de procesamiento de gráficos de una única GPU física.

### **Aceleración de GPU para SO Windows multisesión**

HDX 3D Pro permite que las aplicaciones con muchos gráficos que se ejecutan en sesiones de sistema operativo multisesión Windows se representen en la unidad de procesamiento de gráficos (GPU) del servidor. Al trasladar la representación de los gráficos de OpenGL, DirectX, Direct3D y Windows Presentation Foundation (WPF) a la GPU del servidor, la CPU del servidor no se ve ralentizada. Además, el servidor es capaz de procesar más gráficos, dado que la carga de trabajo se divide entre la CPU y la GPU.

### **Framehawk**

#### **Importante:**

A partir de Citrix Virtual Apps and Desktops 7 1903, Framehawk ya no se admite. En su lugar, utilice [Thinwire](#) con el [transporte adaptable](#) habilitado.

Framehawk es una tecnología de pantallas remotas para usuarios móviles con conexiones inalámbricas de banda ancha (redes de telefonía móvil Wi-Fi, 4G o LTE). Framehawk resuelve obstáculos como interferencias espectrales y propagaciones multitrayecto para ofrecer una experiencia de usuario fluida e interactiva a los usuarios de aplicaciones y escritorios virtuales.

### **Marca de agua de sesión basada en texto**

Las marcas de agua de la sesión basadas en texto ayudan a disuadir del robo de datos y rastrear los datos robados. Esta información rastreable aparece en el escritorio de la sesión como un elemento de disuasión para quienes usan fotografías y capturas de pantalla para robar datos. Puede especificar una marca de agua que sea una capa de texto. La marca de agua se puede mostrar en la pantalla de toda la sesión sin cambiar el contenido del documento original. Las marcas de agua de la sesión basadas en texto requieren que se admita el VDA.

## Información relacionada

- [HDX 3D Pro](#)
- [Aceleración de GPU para SO Windows de sesión única](#)
- [Aceleración de GPU para SO Windows multisesión](#)
- [Framehawk](#)
- [Thinwire](#)
- [Marca de agua de sesión basada en texto](#)

## HDX 3D Pro

September 22, 2021

Las capacidades HDX 3D Pro de Citrix Virtual Apps and Desktops permiten entregar escritorios y aplicaciones que rinden más gracias a una unidad de procesamiento de gráficos (GPU) para la aceleración de hardware. Estas aplicaciones incluyen gráficos 3D profesionales basados en OpenGL y DirectX. El VDA estándar solo admite la aceleración GPU de DirectX.

Para conocer las configuraciones de la directiva de HDX 3D Pro, consulte [Optimizar para cargas de trabajo de gráficos 3D](#),

Todas las aplicaciones Citrix Workspace compatibles se pueden usar con gráficos 3D. Para obtener el mejor rendimiento con cargas de trabajo complejas de 3D, monitores de alta resolución, configuraciones de varios monitores y aplicaciones con alta velocidad de fotogramas, se recomienda usar las versiones más recientes de la aplicación Citrix Workspace para Windows y la aplicación Citrix Workspace para Linux. Para obtener más información sobre las versiones compatibles de la aplicación Citrix Workspace, consulte [Lifecycle Milestones for Citrix Workspace app](#).

Los ejemplos de aplicaciones profesionales de 3D incluyen:

- Aplicaciones de ingeniería, fabricación y diseño asistidos por computadora (CAE/CAM/CAD)
- Software de sistema de información geográfica (GIS)
- Sistema de archivo y transmisión de imágenes (PACS) para la imagen médica

- Aplicaciones con las versiones más recientes de OpenGL, DirectX, NVIDIA CUDA y OpenCL y WebGL
- Aplicaciones no gráficas que consumen muchos recursos informáticos y que usan GPU CUDA (Compute Unified Device Architecture), la arquitectura de cálculo paralelo de NVIDIA, para el procesamiento paralelo

HDX 3D Pro ofrece la mejor experiencia de usuario en cualquier ancho de banda:

- En conexiones de red de área extensa (WAN). Entrega una experiencia de usuario interactiva en conexiones WAN con anchos de banda bajos, incluso hasta 1,5 Mbps.
- En conexiones de red de área local (LAN). Entrega una experiencia de usuario equivalente a la de un escritorio local en las conexiones LAN.

Puede reemplazar estaciones de trabajo complejas y costosas por dispositivos de usuario más simples, al mover el procesamiento de gráficos al centro de datos para una administración centralizada.

HDX 3D Pro ofrece la aceleración de GPU para las máquinas con sistema operativo de sesión única de Windows o multisesión de Windows. Para obtener más información, consulte [Aceleración de GPU para sistemas operativos de sesión única Windows](#) y [Aceleración de GPU para sistemas operativos multisesión Windows](#).

HDX 3D Pro es compatible con máquinas sin sistema operativo, además de las tecnologías de virtualización de GPU y GPU PassThrough que ofrecen los siguientes hipervisores:

- Citrix Hypervisor
  - GPU PassThrough con NVIDIA GRID, AMD e Intel GVT-d
  - Virtualización de GPU con NVIDIA GRID, AMD e Intel GVT-g
  - Consulte la compatibilidad de hardware en la [Lista de compatibilidad de hardware de Hypervisor](#).

La herramienta HDX Monitor permite validar la operación y la configuración de las tecnologías de visualización HDX, así como diagnosticar y solucionar problemas relacionados con HDX. Para descargar la herramienta y obtener más información acerca de ella, consulte <https://taas.citrix.com/hdx/download/>.

## **Aceleración de GPU para SO Windows multisesión**

September 22, 2021

HDX 3D Pro permite que las aplicaciones con muchos gráficos que se ejecutan en sesiones de sistema operativo multisesión Windows se representen en la unidad de procesamiento de gráficos (GPU) del

servidor. Al trasladar la representación de los gráficos de OpenGL, DirectX, Direct3D y Windows Presentation Foundation (WPF) a la unidad de procesamiento de gráficos (GPU) del servidor, la CPU del servidor no se ralentiza. Además, el servidor es capaz de procesar más gráficos, dado que la carga de trabajo se divide entre la CPU y la GPU.

Como Windows Server es un sistema operativo multiusuario, varios usuarios pueden compartir una GPU a la que se accede mediante Citrix Virtual Apps sin necesidad de virtualización de GPU (vGPU).

Para las instrucciones que impliquen modificar el Registro, tenga cuidado: si se modifica de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

## Compartir GPU

El uso compartido de GPU permite la generación por hardware de GPU de aplicaciones OpenGL y DirectX en las sesiones de escritorio remoto. Tiene las siguientes características:

- Se puede usar en máquinas físicas o virtuales para aumentar el rendimiento y la escalabilidad de las aplicaciones.
- Permite que varias sesiones simultáneas compartan los recursos de la GPU (la mayoría de los usuarios no necesitan el rendimiento de generación de gráficos que da una GPU dedicada).
- No necesita ninguna configuración especial.

Se puede asignar una GPU a la máquina virtual Windows Server en modo de PassThrough completo o GPU virtual (vGPU) siguiendo los requisitos del proveedor de GPU e hipervisor. También se admiten implementaciones bare metal en máquinas físicas con Windows Server.

El uso compartido de GPU no depende de ninguna tarjeta gráfica específica.

- Para máquinas virtuales, seleccione una tarjeta gráfica compatible con el hipervisor en uso. Para obtener una lista de compatibilidad de hardware de Citrix Hypervisor, consulte [Lista de compatibilidad de hardware de Hypervisor](#).
- Cuando se ejecuta directamente sobre el hardware (“bare metal”) se recomienda contar con un único adaptador de pantalla habilitado por el sistema operativo. Si hay varias GPU instaladas en el hardware, inhabilite todas menos una mediante Device Manager.

La escalabilidad mediante el uso compartido de GPU depende de varios factores:

- Las aplicaciones que se ejecuten
- La cantidad de memoria RAM de vídeo que consuman
- La capacidad de procesamiento de la tarjeta gráfica

Algunas aplicaciones administran la falta de memoria RAM de vídeo mejor que otras. Si el hardware se sobrecarga, esto puede provocar inestabilidad o incluso el bloqueo del controlador de la tarjeta gráfica. Limite el número de usuarios simultáneos para evitar esos problemas.

Para confirmar que está teniendo lugar la aceleración por GPU, use una herramienta de terceros, como GPU-Z. GPU-Z está disponible en <http://www.techpowerup.com/gpuz/>.

- Acceso a un codificador de vídeo de alto rendimiento para las GPU de NVIDIA y los procesadores gráficos de Intel Iris Pro. Una configuración de directiva (habilitada de forma predeterminada) controla esta funcionalidad y permite el uso de codificación por hardware para la codificación H.264 (si está disponible). Si no está disponible, el VDA recurre a la codificación basada en CPU con el códec de vídeo del software. Para obtener más información, consulte [Configuraciones de directiva de gráficos](#).

## Presentación de DirectX, Direct3D y WPF

La presentación de DirectX, Direct3D y WPF solo está disponible en servidores con una GPU que admita una interfaz de control de presentación (DDI), versión 9ex, 10 u 11.

- En Windows Server 2008 R2, DirectX y Direct3D no requieren ninguna configuración especial para usar una única GPU.
- En Windows Server 2016 y Windows Server 2012, las sesiones de Servicios de Escritorio remoto (RDS) en el servidor host de sesión de Escritorio remoto usan el Controlador de representación básica de Microsoft como el adaptador predeterminado. Para usar la GPU en sesiones de RDS en Windows Server 2012, habilite la configuración **Usar el adaptador de gráficos de hardware predeterminado para todas las sesiones de Servicios de Escritorio remoto** en la directiva de grupo **Directiva de equipo local > Configuración del equipo > Plantillas administrativas > Componentes de Windows > Servicios de Escritorio remoto > Host de sesión de Escritorio remoto > Entorno de sesión remota**.
- Para habilitar las aplicaciones WPF para que representen gráficos mediante la GPU del servidor, cree los siguientes parámetros en el Registro de Windows del servidor que ejecuta sesiones de SO multisesión Windows:
  - [HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit\_Dlls\Multiple Monitor Hook] "EnableWPFHook"=dword:00000001
  - [HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit\_Dlls\Multiple Monitor Hook] "EnableWPFHook"=dword:00000001

## Aceleración de GPU para aplicaciones OpenCL o CUDA

La aceleración de GPU para aplicaciones OpenCL y CUDA que se ejecutan en una sesión de usuario está inhabilitada de forma predeterminada.

Para usar las funcionalidades POC de aceleración de CUDA, habilite los siguientes parámetros de Registro:

- [HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\CtxHook\Applnit\_Dlls\Graphics Helper] “CUDA”=dword:00000001
- [HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\Applnit\_Dlls\Graphics Helper] “CUDA”=dword:00000001

Para usar las funcionalidades POC de aceleración de OpenCL, habilite los siguientes parámetros de Registro:

- [HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\CtxHook\Applnit\_Dlls\Graphics Helper] “OpenCL”=dword:00000001
- [HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\Applnit\_Dlls\Graphics Helper] “OpenCL”=dword:00000001

## **Aceleración de GPU para SO Windows de sesión única**

November 4, 2021

Con HDX 3D Pro, puede entregar aplicaciones de uso intensivo de gráficos como parte de escritorios o aplicaciones que se alojan en máquinas con SO de sesión única. HDX 3D Pro admite equipos host físicos (incluido el escritorio, blade y estaciones de trabajo en rack), así como GPU PassThrough y tecnologías de virtualización de GPU que ofrecen los hipervisores de Citrix Hypervisor, vSphere y Hyper-V (solo PassThrough).

Mediante GPU PassThrough, puede crear máquinas virtuales con acceso exclusivo a hardware de procesamiento de gráficos dedicado. Es posible instalar varias GPU en el hipervisor y asignar, una a una, diversas VM a cada GPU.

HDX 3D Pro ofrece las siguientes funciones:

- Compresión intensa y adaptable por H.264 o H.265 para un rendimiento WAN e inalámbrico óptimos. HDX 3D Pro utiliza la compresión H.264 de pantalla completa basada en CPU como técnica de compresión predeterminada para la codificación. La codificación por hardware con H.264 se puede usar con tarjetas de NVIDIA, Intel y AMD que admiten NVENC. La codificación por hardware con H.265 se puede usar con tarjetas de NVIDIA que admiten NVENC.
- La opción de compresión sin pérdida para casos de uso especiales. HDX 3D Pro también ofrece un códec sin pérdida basado en CPU para admitir las aplicaciones que necesitan gráficos de calidad perfecta, como, por ejemplo, la creación de imágenes para uso en medicina. La compresión sin pérdida solo se recomienda para casos de uso especializados, ya que consume más recursos de red y de procesamiento.

Cuando se utiliza la compresión sin pérdida:

- El indicador de compresión sin pérdida es un icono del área de notificaciones que avisa al usuario cuando la pantalla muestra fotogramas con o sin pérdida. Este icono ayuda cuando la configuración de directiva **Calidad visual** está definida como **Gradual sin pérdida**. El indicador sin pérdida se vuelve verde cuando los fotogramas se envían sin pérdida.
- La opción para cambiar la calidad sin pérdida permite que el usuario cambie al modo Siempre sin pérdida, en cualquier momento, dentro de la sesión. Para seleccionar o anular la selección de la **compresión sin pérdida en cualquier momento de la sesión**, haga clic con el botón secundario en el icono o use el atajo ALT+MAYÚS+1.

Para la compresión sin pérdida: HDX 3D Pro utiliza el códec de compresión sin pérdida, independientemente del códec seleccionado a través de la directiva.

Para la compresión con pérdida: HDX 3D Pro utiliza el códec original, o el predeterminado o el seleccionado a través de la directiva.

Los parámetros de la opción Cambiar calidad sin pérdida no se conservan para las sesiones subsiguientes. Para usar un códec de compresión sin pérdida en cada conexión, seleccione **Siempre sin pérdida** en la configuración de directiva **Calidad visual**.

- Puede reemplazar el acceso directo predeterminado, ALT + MAYÚS + 1, para seleccionar o anular la selección de la compresión sin pérdida en sesión. Configure un nuevo parámetro del Registro en HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator.
  - Nombre: HKEY\_LOCAL\_MACHINE\_HotKey, Tipo: String
  - El formato para configurar una combinación de acceso directo es: C=0 | 1, A=0 | 1, S=0 | 1, W=0 | 1, K=val. Las claves deben estar separadas por comas (,). El orden de las claves no importa.
  - A, C, S, W y K son teclas que equivalen a las teclas siguientes: C a Control, A a ALT, S a MAYÚS, W a Windows y K a una clave válida. Los valores permitidos para K van de 0 a 9 y de “a” a “z”, y son cualquier código de tecla virtual.
  - Por ejemplo:
    - \* Para F10, defina K = 0x79.
    - \* Para Ctrl + F10, defina C = 1, K = 0x79.
    - \* Para Alt + A, defina A = 1, K = a; o bien A = 1, K = A; o bien, K = A, A = 1.
    - \* Para Ctrl + Alt + 5, defina C = 1, A = 1, K = 5; o bien, A = 1, K = 5, C = 1.
    - \* Para Ctrl + Mayús + F5, defina A = 1, S = 1, K = 0x74.

### Precaución:

Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que oblig-

uen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

- Funcionalidad para varios monitores de alta resolución. Para máquinas con SO de sesión única, HDX 3D Pro es compatible con dispositivos de usuario de hasta cuatro monitores. Los usuarios pueden organizar sus monitores con la configuración que deseen y pueden mezclar monitores con resoluciones y orientaciones diferentes. La cantidad de monitores se ve limitada solamente por la capacidad de la GPU del equipo host, el dispositivo de usuario y el ancho de banda disponible. HDX 3D Pro admite todas las resoluciones de monitor. Solo la capacidad de la GPU en el equipo host limita el uso de ciertas resoluciones.

HDX 3D Pro también ofrece funcionalidad limitada para el acceso con monitor doble a escritorios Windows XP. Para obtener más información acerca de esta compatibilidad, consulte [Agentes VDA en máquinas con Windows XP o Windows Vista](#).

- Resolución dinámica. Puede cambiar el tamaño de la ventana de la aplicación o del escritorio virtual a cualquier resolución. **Nota:** El único método admitido para cambiar la resolución es cambiar el tamaño de la ventana de la sesión de VDA. No se admite el cambio de resolución desde dentro de la sesión de VDA (mediante el **Panel de control > Apariencia y Personalización > Pantalla > Resolución de pantalla**).
- Compatibilidad con la arquitectura de GPU virtual de NVIDIA. HDX 3D Pro es compatible con tarjetas de GPU virtual de NVIDIA. Para obtener información, consulte [Tecnología de GPU virtual de NVIDIA](#) para PassThrough y uso compartido de GPU. La GPU virtual de NVIDIA permite que múltiples máquinas virtuales tengan acceso directo y simultáneo a una única GPU física, mediante los mismos controladores de gráficos de NVIDIA que se implementan en sistemas operativos no virtualizados.
- Compatibilidad con VMware vSphere y VMware ESX mediante vDGA. Puede utilizar HDX 3D Pro con vDGA para cargas de trabajo RDS y VDI.
- Compatibilidad con VMware vSphere/ESX mediante GPU virtual de NVIDIA y MxGPU de AMD.
- Compatibilidad con Microsoft Hyper-V mediante la asignación de dispositivos diferenciados de Windows Server 2016.
- Compatibilidad con gráficos para centros de datos con la familia de procesadores Intel Xeon E3. HDX 3D Pro admite varios monitores (hasta 3), poner en blanco la consola, una resolución personalizada y una alta velocidad de fotogramas con la familia compatible de procesadores Intel. Para obtener más información, consulte <http://www.citrix.com/intel> y <http://www.intel.com/content/www/us/en/servers/data-center-graphics.html>.
- Compatibilidad con RapidFire de AMD en las tarjetas de servidor FirePro de serie S de AMD. HDX 3D Pro admite varios monitores (6 como máximo), consola vacía, resolución personalizada y

alta velocidad de fotogramas. Nota: La compatibilidad de HDX 3D Pro con MxGPU de AMD (virtualización de GPU) solo es posible con GPU virtuales de VMware vSphere. Citrix Hypervisor y Hyper-V son compatibles con PassThrough de GPU. Para obtener más información, consulte [AMD Virtualization Solution](#).

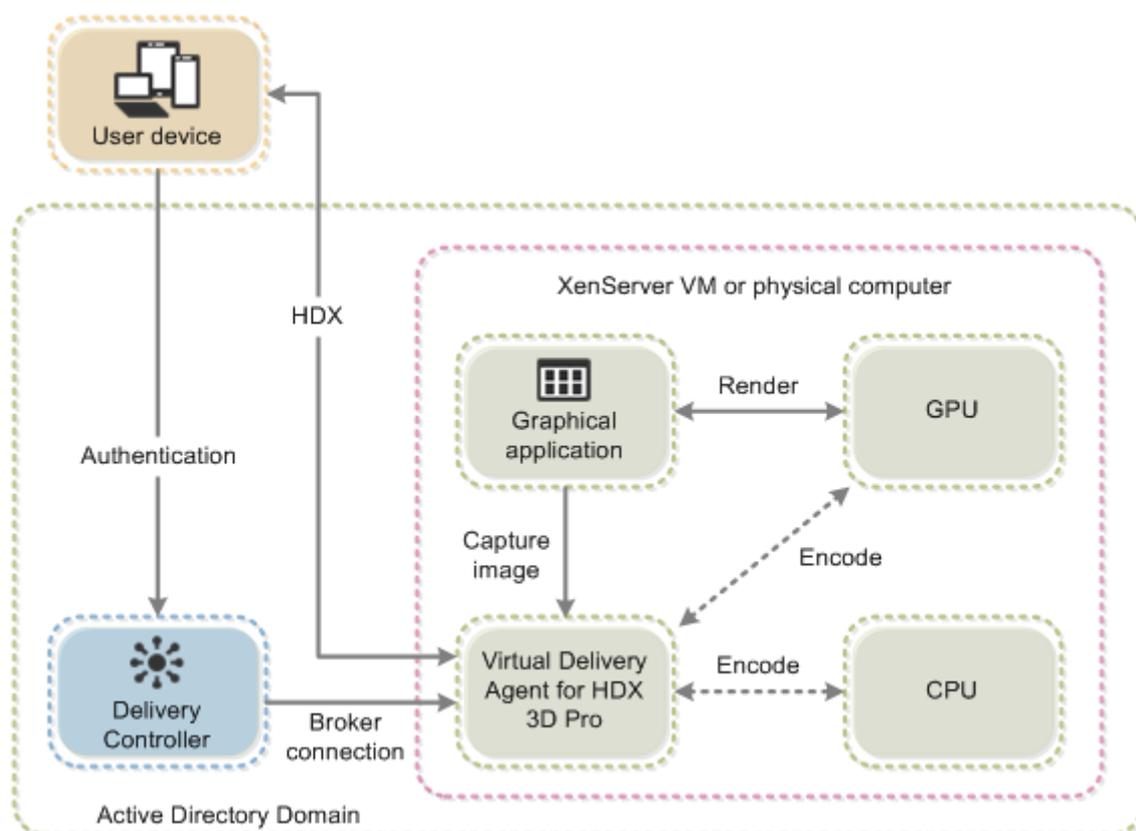
- Acceso a un codificador de vídeo de alto rendimiento para las GPU de NVIDIA, las de AMD y los procesadores gráficos de Intel Iris Pro. Una configuración de directiva (habilitada de forma predeterminada) controla esta función. Dicha función permite usar la codificación por hardware para la codificación H.264 (si está disponible). Si no está disponible, el VDA recurre a la codificación basada en CPU con el códec de vídeo del software. Para obtener más información, consulte [Configuraciones de directiva de gráficos](#).

Como se muestra en la siguiente imagen:

- Cuando un usuario inicia sesión en la aplicación Citrix Workspace y accede a la aplicación o escritorio virtual, el Controller autentica al usuario. A continuación, el Controller se pone en contacto con el VDA para HDX 3D Pro con el objetivo de establecer una conexión con el equipo que aloja la aplicación gráfica.

El VDA para HDX 3D Pro utiliza el hardware adecuado en el host para comprimir las vistas del escritorio completo o solamente de la aplicación gráfica.

- Las vistas de escritorio o aplicación y las interacciones del usuario con ellas se transmiten entre el equipo host y el dispositivo del usuario. Esta transmisión se realiza a través de una conexión HDX directa entre la aplicación Citrix Workspace y el VDA para HDX 3D Pro.



## Optimizar la experiencia del usuario de HDX 3D Pro

Para utilizar HDX 3D Pro con varios monitores, asegúrese de que el equipo host está configurado para, al menos, el número de monitores conectados a los dispositivos de usuario. Los monitores conectados al equipo host pueden ser físicos o virtuales.

No conecte un monitor (ya sea físico o virtual) a un equipo host mientras un usuario está conectado a la aplicación o escritorio virtual que proporciona la aplicación gráfica. Si lo hace, puede causar inestabilidad durante la sesión de un usuario.

Indique a los usuarios que no se admiten cambios en la resolución del escritorio (por ellos o una aplicación) mientras haya sesiones de aplicaciones gráficas en curso. Después de cerrar la sesión de la aplicación, el usuario puede cambiar la resolución de la ventana de Desktop Viewer en la aplicación Citrix Workspace: Preferencias de Desktop Viewer.

Cuando varios usuarios comparten una conexión con ancho de banda limitado (como los usuarios en una sucursal), se recomienda utilizar la configuración de directiva **Límite de ancho de banda global de la sesión** para limitar el ancho de banda disponible para cada usuario. Usar este parámetro garantiza que el ancho de banda disponible no fluctúe demasiado a medida que los usuarios inician y cierran sesiones. Como HDX 3D Pro se ajusta automáticamente para usar todo el ancho de banda

disponible, las grandes variaciones en el ancho de banda disponible durante el transcurso de las sesiones de usuario pueden afectar negativamente al rendimiento.

Por ejemplo, si 20 usuarios comparten una conexión de 60 Mbps, el ancho de banda disponible para cada usuario puede variar entre 3 y 60 Mbps, según la cantidad de usuarios simultáneos. Para optimizar la experiencia de usuario en este caso, determine el ancho de banda requerido por usuario en los períodos de mayor uso y limite los usuarios a esta cantidad siempre.

Para los usuarios de punteros 3D, se recomienda aumentar la prioridad del canal virtual Redirección de USB genérico a 0. Para obtener información sobre cómo cambiar la prioridad del canal virtual, consulte el artículo [CTX128190](#) de Knowledge Center.

## Thinwire

September 22, 2021

### Introducción

Thinwire es la tecnología predeterminada de Citrix para pantallas remotas que se utiliza en Citrix Virtual Apps and Desktops.

Las tecnologías de pantallas remotas permiten que los gráficos generados en una máquina se transmitan (normalmente a través de una red) a otra máquina para que se vean desde allí.

Una buena solución de pantallas remotas debe ofrecer una experiencia de usuario altamente interactiva que sea similar a la de un equipo local. Thinwire lo consigue porque utiliza un abanico de técnicas complejas y eficientes para la compresión y el análisis de imágenes. Thinwire maximiza la escalabilidad de los servidores y consume menos ancho de banda que otras tecnologías de pantallas remotas.

Gracias a este equilibrio, Thinwire cubre la mayoría de los casos de uso generales que pueda haber en una empresa, y se usa como la tecnología predeterminada para pantallas remotas en Citrix Virtual Apps and Desktops.

### Thinwire

Thinwire debería utilizarse para entregar cargas de trabajo típicas (por ejemplo, escritorios, aplicaciones de productividad de oficina o de explorador web). Thinwire también se recomienda para entornos de varios monitores, de alta resolución o con casos de configuración elevada de ppp, así como para cargas de trabajo con una mezcla de contenido de vídeo y no vídeo.

## HDX 3D Pro

En su configuración predeterminada, Thinwire puede entregar 3D o gráficos de interacción alta. Sin embargo, se recomienda habilitar el modo HDX 3D Pro desde la directiva **Optimizar para cargas de trabajo de gráficos 3D** de Citrix para casos en que hay unidades GPU. El modo HDX 3D Pro utiliza la GPU para la aceleración de hardware y configura Thinwire con los parámetros óptimos para los gráficos. Lo que ofrece una experiencia más fluida para gráficos 3D profesionales. Para obtener más información, consulte [HDX 3D Pro](#) y [Aceleración de GPU para SO Windows de sesión única](#).

## Requisitos y consideraciones

- Thinwire se ha optimizado para sistemas operativos modernos, como Windows Server 2012 R2, Windows Server 2016, Windows 7 y Windows 10. Para Windows Server 2008 R2, se recomienda el modo de gráficos antiguo. Utilice las [plantillas de directivas de Citrix](#) integradas, así como las plantillas “Alta escalabilidad de servidores para sistemas operativos antiguos” y “Optimización de redes WAN para sistemas operativos antiguos” para entregar las combinaciones de configuraciones de directiva que Citrix recomienda para estos casos de uso.

### Nota:

No se admite el modo de gráficos antiguo en esta versión. Este modo se incluye para la compatibilidad con versiones anteriores cuando se usa XenApp 7.15 LTSR y XenDesktop 7.15 LTSR, así como las versiones anteriores de VDA con Windows 7 y Windows 2008 R2.

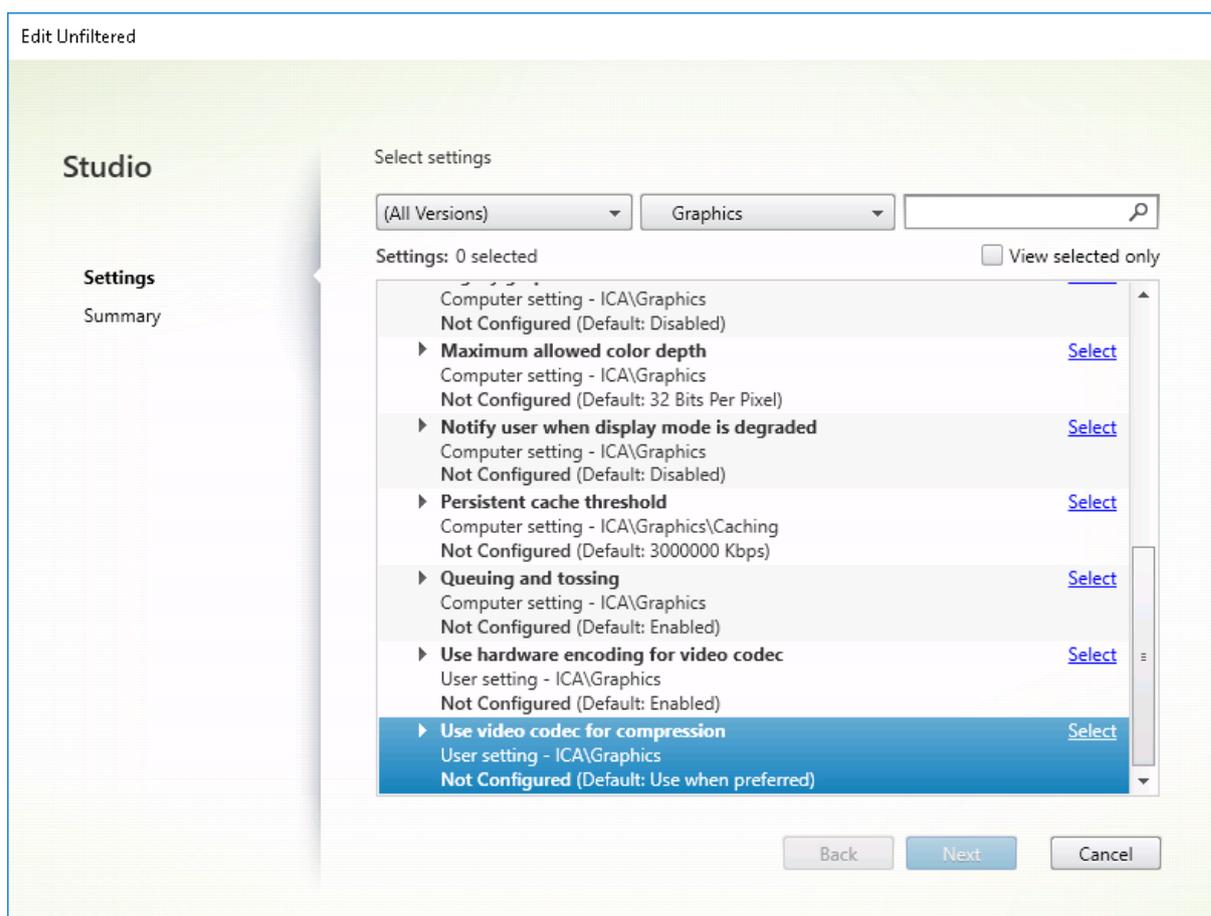
- La configuración de directiva que controla el comportamiento de Thinwire, **Usar códec de vídeo para compresión**, está disponible en las versiones de VDA de Citrix Virtual Apps and Desktops 7 1808 y versiones posteriores, así como XenApp y XenDesktop 7.6 FP3 y versiones posteriores. La opción **Usar códec de vídeo si se prefiere** es la configuración predeterminada en las versiones de VDA de Citrix Virtual Apps and Desktops 7 1808 o versiones posteriores, así como XenApp y XenDesktop 7.9 o versiones posteriores.
- Todas las aplicaciones Citrix Workspace admiten Thinwire. Sin embargo, algunas aplicaciones Citrix Workspace pueden admitir funciones de Thinwire que otras no admiten (por ejemplo, gráficos de 8 o 16 bits para reducir el uso del ancho de banda). La aplicación Citrix Workspace negocia automáticamente si admitir o no esas funciones.
- Thinwire usará más recursos de servidor (CPU, memoria) cuando haya varios monitores y una alta resolución de pantalla. Es posible ajustar la cantidad de recursos que utiliza Thinwire. Sin embargo, puede que eso provoque un aumento del uso de ancho de banda.
- En situaciones de poco ancho de banda y latencia alta, considere la posibilidad de habilitar gráficos de 8 o 16 bits para mejorar la interactividad, aunque ello afectará a la calidad visual, sobre todo en una profundidad de color de 8 bits.

## Configuración

Thinwire es la tecnología predeterminada de pantallas remotas.

La siguiente configuración de directiva de Gráficos establece las opciones predeterminadas y ofrece alternativas a diferentes casos de uso:

- [Usar códec de vídeo para compresión](#)
  - **Usar códec de vídeo si se prefiere.** Esta es la opción predeterminada. No se requiere ninguna configuración adicional. Si mantiene esta configuración como predeterminada, Thinwire se seleccionará para todas las conexiones de Citrix, y se optimizará para la escalabilidad, el ancho de banda y una calidad de imagen superior para cargas de trabajo típicas de escritorio.
- Las demás opciones de esta configuración de directiva seguirán mediante Thinwire combinado con otras tecnologías para diferentes casos de uso. Por ejemplo:
  - **Para áreas en cambio constante.** En Thinwire, la tecnología de pantalla adaptable identifica las imágenes en movimiento (vídeo, 3D en movimiento) y usa H.264 o H.265 solo en aquella parte de la pantalla donde se mueva la imagen.
  - **Para la pantalla entera.** Entrega Thinwire con H.264 o H.265 en pantalla completa para mejorar la experiencia del usuario y optimizar el ancho de banda, sobre todo cuando haya un uso intensivo de gráficos 3D.



Varias configuraciones de directiva más, incluidas las siguientes configuraciones de directiva de Presentación visual, se pueden usar para optimizar el rendimiento de la tecnología de pantallas remotas Thinwire las admite todas:

- [Profundidad de color preferida para gráficos simples](#)
- [Velocidad de fotogramas de destino](#)
- [Calidad visual](#)

Para conocer las combinaciones de configuraciones de directiva que Citrix recomienda para diferentes casos de uso en empresas, use las [plantillas de directivas de Citrix](#) integradas. Las plantillas **Alta escalabilidad de servidores** y **Experiencia de usuario de muy alta definición** usan Thinwire con las mejores combinaciones de configuraciones de directiva para las prioridades de la empresa y las expectativas de los usuarios.

## Supervisar Thinwire

Puede supervisar el uso y el rendimiento de Thinwire desde Citrix Director. La vista de detalles del canal virtual HDX ofrece información útil para la supervisión y la solución de problemas relacionados con Thinwire en cualquier sesión. Para ver las métricas relacionadas con Thinwire:

1. En Director, busque un usuario, una máquina o un dispositivo de punto final, abra una sesión activa y haga clic en **Detalles**. O bien, puede seleccionar **Filtros > Sesiones > Todas las sesiones**, abrir una sesión activa y hacer clic en **Detalles**.
2. Desplácese hacia abajo hasta el panel **HDX**.

**HDX**

Download System Report

	 Adobe® Flash®	Virtual channel: Idle Flash redirection: Inactive
	 Graphics - Framehawk	Virtual channel: Idle Current FPS: 0
	 Scanner	Virtual channel: Idle Compression level: Medium
	 Smart Cards	Virtual channel: Idle Number of devices: 0
	 Legacy Graphics	Virtual channel: Active Still image compression: Medium
	 Audio	Virtual channel: Idle Number of devices: 1
	 Graphics - Thinwire	Virtual channel: Active Current FPS: 1
	 Mapped Client Drives	Virtual channel: Idle Client drives available: 0
	 Network	Bandwidth used: 0% Average latency: 47 ms
	 Printing	Mapped printers: 4 Virtual channel: Idle
	 VDA	Version: Session ID: 3
	 Windows Media	Virtual channel: Idle Active streams: 2

3. Seleccione **Gráficos: Thinwire**.

Graphics - Thinwire

There are no alerts at this time.

▼ Status

Virtual channel state	Idle
Virtual channel priority	High
Monitors	1
Frames Per Second	1
Provider	Standard (RDS)
Video codec use	None
<b>Monitor 0</b>	
Monitor ID	0
Primary	True
Left	0
Top	0
Right	1280
Bottom	800

## Métodos de codificación

En XenApp y XenDesktop 7.16 y sus versiones anteriores, Thinwire ofrecía tres modos de codificación de mapas de bits, utilizados en la comunicación remota de gráficos para el VDA del sistema operativo multisesión y de sesión única:

- Pantalla completa H.264
- Thinwire Plus
- Thinwire Plus con H.264 selectivo

En la comunicación remota GDI antigua, se utilizaba el controlador remoto de XPDM, no un codificador Thinwire de mapa de bits.

En una sesión de escritorio estándar, la mayoría de las imágenes son gráficos simples o regiones de texto. Cuando se utiliza uno de los tres modos de codificación de mapas de bits mencionados, Thinwire selecciona estas áreas para la codificación sin pérdida mediante el códec 2DRLE. En el lado del cliente de la aplicación Citrix Workspace, esos elementos se decodifican mediante el decodificador 2DRLE del lado de la aplicación Citrix Workspace para mostrarlos en la sesión.

## Códec de compresión sin pérdida (MDRLE)

En XenApp y XenDesktop 7.17, hemos agregado un codificador MDRLE, con una razón de compresión más alta y menor consumo de ancho de banda que el códec 2DRLE en sesiones de escritorio estándar.

Por lo general, un menor consumo de ancho de banda implica una interactividad de sesión mejorada (especialmente en enlaces compartidos o restringidos) y costes reducidos. Por ejemplo, el consumo de ancho de banda previsto cuando se utiliza el códec MDRLE es, aproximadamente, entre un 10 y un 15 % más pequeño que con XenApp y XenDesktop 7.15 LTSR para cargas de trabajo estándar de Office.

No se requiere ninguna configuración para el códec MDRLE. Si la aplicación Citrix Workspace admite la decodificación MDRLE, el VDA utiliza su propia codificación de MDRLE y la decodificación MDRLE de la aplicación Citrix Workspace. En cambio, si la aplicación Citrix Workspace no admite la decodificación MDRLE, el VDA recurre automáticamente a la codificación 2DRLE.

### Requisitos de MDRLE

- Agentes VDA de Citrix Virtual Apps and Desktops 7 1808 (versión mínima)
- XenApp y XenDesktop: VDA 7.17 (versión mínima)
- Aplicación Citrix Workspace para Windows 1808 (versión mínima)
- Citrix Receiver para Windows 4.11 (versión mínima)

## Modo progresivo

La interactividad de la sesión puede degradarse en enlaces de latencia baja o poco ancho de banda. Por ejemplo, en enlaces con menos de 2 Mbps de ancho de banda o una latencia de más de 200 ms, el desplazamiento por una página web puede ralentizarse, dejar de responder o aparecer entrecortado. Las operaciones de teclado y mouse pueden retrasarse con respecto a las actualizaciones de gráficos.

Con la versión 7.17, se podían usar las directivas para reducir el consumo del ancho de banda configurando la calidad visual de la sesión en “Baja” o estableciendo una profundidad de color menor (gráficos de 16 u 8 bits). Sin embargo, se tenía que saber que un usuario tenía poca conectividad. HDX Thinwire no podía ajustar dinámicamente la calidad de la imagen estática en función de las condiciones de red.

En la versión 7.18, HDX Thinwire cambia de forma predeterminada a un modo de actualización progresiva cuando el ancho de banda disponible baja de 2 Mbps o la latencia de red excede los 200 ms. En este modo:

- Todas las imágenes estáticas se comprimen mucho.
- La calidad del texto se reduce.

Las imágenes transitorias (vídeo) se siguen gestionando con la pantalla adaptable o H.264 selectivo.

## Cómo se usa el modo progresivo

De forma predeterminada, el modo progresivo está en espera en las configuraciones de la directiva Calidad visual: Alta, Media (predeterminado) y Baja.

El modo progresivo se desactiva (no se usa) cuando:

- Calidad visual = Siempre sin pérdida o Gradual sin pérdida
- Preferencia de profundidad de color para gráficos sencillos = 8 bits
- Usar códec de vídeo para compresión = Para la pantalla entera (cuando quiere H.264 a pantalla completa)

Si el modo progresivo está en espera, se habilita de forma predeterminada cuando se da una de las siguientes condiciones:

- El ancho de banda disponible baja a menos de 2 Mbps
- La latencia de red aumenta por encima de 200 ms

Después de un cambio de modo, transcurre un mínimo de 10 segundos en ese modo, aunque las condiciones adversas de la red fueran temporales.

## Cambiar el comportamiento del modo progresivo

Puede cambiar el estado del modo progresivo con la siguiente clave de Registro:

[REG\_DWORD] HKEY\_LOCAL\_MACHINE\Software\Citrix\Graphics\ProgressiveDisplay

Valores:

0 = Siempre desactivado (no usar en ninguna circunstancia)

1 = Automático (alternar según las condiciones de la red, este es el valor predeterminado)

2 = Siempre activado

Cuando está en el modo automático (1), puede usar la siguiente clave de Registro para cambiar los umbrales en los que se alterna al modo progresivo:

[REG\_DWORD] HKEY\_LOCAL\_MACHINE\Software\Citrix\Graphics\ProgressiveDisplayBandwidthThreshold

Valor: <umbral en Kbps> (predeterminado = 2048)

Ejemplo: 4096 = Activa el modo progresivo si el ancho de banda baja de 4 Mbps

[REG\_DWORD] HKEY\_LOCAL\_MACHINE\Software\Citrix\Graphics\ProgressiveDisplayLatencyThreshold

Valor: <umbral en ms> (predeterminado = 200)

Ejemplo: 100 = Activa el modo progresivo si la latencia de la red baja de 100 ms.

## Marca de agua de sesión basada en texto

September 22, 2021

Las marcas de agua de la sesión basadas en texto ayudan a disuadir del robo de datos y rastrear los datos robados. Esta información rastreable aparece en el escritorio de la sesión como un elemento de disuasión para quienes usan fotografías y capturas de pantalla para robar datos. Puede especificar una marca de agua que sea una capa de texto y aparezca en toda la pantalla de la sesión, sin cambiar por ello el contenido del documento original. Las marcas de agua de la sesión basadas en texto requieren que se admita el VDA.

### Importante

La marca de agua de la sesión basada de texto no es una función de seguridad. Esta solución no impide por completo el robo de datos, pero ofrece cierto nivel de disuasión frente al robo de datos y rastreabilidad de los datos robados. Aunque no garantizamos una rastreabilidad completa de la información cuando se utiliza esta función, recomendamos combinar esta función con otras soluciones de seguridad, según corresponda.

La marca de agua de la sesión es texto y se aplica a la sesión que se entrega al usuario. La marca de agua de la sesión contiene información para rastrear datos robados. La información más importante es la identidad del usuario que inició la sesión en la que se realizó la captura de la pantalla. Para rastrear la filtración de datos de manera más efectiva, incluya otra información (como la hora de conexión y la dirección del protocolo de Internet del servidor o del cliente).

Para ajustar la experiencia del usuario, use las [configuraciones de directiva de Marca de agua](#) para definir la ubicación y la apariencia de la marca de agua en la pantalla.

#### **Requisitos:**

Agentes Virtual Delivery Agent:

SO multisesión 7.17

SO de sesión única 7.17

#### **Limitaciones:**

- No se admiten las marcas de agua en las sesiones donde se utiliza el acceso a aplicaciones locales, la redirección de Windows Media, MediaStream, la redirección de contenido del explorador web y la redirección de vídeo HTML5. Por tanto, para usar la marca de agua de la sesión, estas funciones deben estar inhabilitadas.
- No se admite la marca de agua de la sesión, y esta no aparece si la sesión se ejecuta en modos de aceleración de hardware en pantalla completa (codificación H.264 o H.265 en pantalla completa).
- Si configura estas directivas HDX, la configuración de la marca de agua no tendrá efecto y no se mostrará ninguna marca de agua en la pantalla de la sesión.

**Usar codificación por hardware para códec de vídeo en Habilitado**

**Usar códec de vídeo para compresión en Para la pantalla entera**

- Si configura estas directivas HDX, el comportamiento será desconocido y es posible que la marca de agua no aparezca.

**Usar codificación por hardware para códec de vídeo en Habilitado**

**Usar códec de vídeo para compresión en Usar códec de vídeo si se prefiere**

Para asegurarse de que la marca de agua aparezca, establezca **Usar codificación por hardware para códec de vídeo en Inhabilitado** o establezca **Usar códec de vídeo para compresión en Para áreas en cambio constante o No usar códec de vídeo.**

- La marca de agua de la sesión solo admite el modo gráfico de Thinwire, no Framehawk ni la redirección de composición del escritorio (DCR).
- Si usa la Grabación de sesiones, la sesión grabada no incluirá la marca de agua.
- Si usa la Asistencia remota de Windows, la marca de agua no aparece.

- Si un usuario presiona la tecla **Imprimir pantalla**, la pantalla capturada en el lado del VDA no incluirá las marcas de agua. Le recomendamos que tome las medidas oportunas para evitar que se copie la imagen capturada.

## Contenido multimedia

September 22, 2021

El conjunto de tecnologías HDX admite la entrega de aplicaciones multimedia a través de dos enfoques complementarios:

- Entrega de contenido multimedia generado en el servidor
- Redirección de contenido multimedia generado en el cliente

Esta estrategia le garantiza la entrega de una gama completa de formatos multimedia con una excelente experiencia del usuario, al mismo tiempo que maximiza la escalabilidad de los servidores para reducir el coste por usuario.

Con la entrega de contenido multimedia generado en el servidor, la aplicación decodifica y genera el contenido de audio y vídeo en el servidor de Citrix Virtual Apps and Desktops. Una vez recibido, el contenido se comprime y se entrega por protocolo ICA a la aplicación Citrix Workspace presente en el dispositivo del usuario. Este método proporciona la máxima compatibilidad con aplicaciones y formatos de medios distintos. Puesto que el procesamiento de vídeo consume muchos recursos de procesamiento, la entrega multimedia generada en el servidor aprovecha considerablemente la aceleración integrada de hardware. Por ejemplo, la aceleración de vídeo DirectX (DXVA) reduce la carga en la CPU porque realiza la decodificación H.264 en otro hardware aparte. Las tecnologías Intel Quick Sync, AMD RapidFire y NVIDIA NVENC proporcionan la codificación H.264 acelerada por hardware.

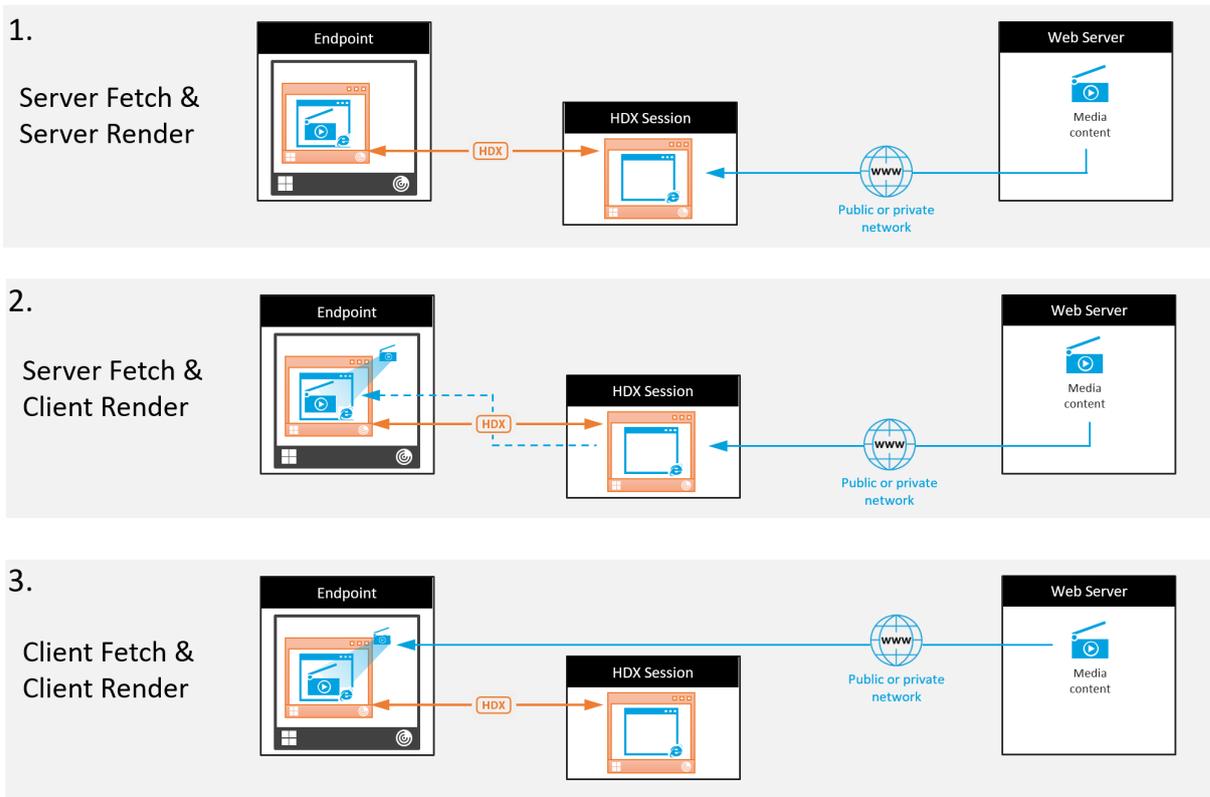
Puesto que la mayoría de los servidores no ofrecen ninguna aceleración de hardware para la compresión de vídeo, la escalabilidad de servidor se ve afectada negativamente si todo el procesamiento de vídeo se realiza en el servidor de la CPU. Para mantener una alta escalabilidad de servidor, redirija muchos formatos multimedia al dispositivo del usuario para su generación local.

- La redirección de Windows Media reduce la carga del servidor cuando se trata de una amplia variedad de formatos de medios normalmente asociados al Reproductor de Windows Media.
- El vídeo HTML5 se ha vuelto popular, y Citrix presentó una tecnología de redirección para este tipo de contenido. Recomendamos el redireccionamiento de contenido de explorador para sitios web que utilizan HTML5, HLS, DASH o WebRTC.
- Puede aplicar tecnologías generales de redirección del host al cliente y el acceso a aplicaciones locales para el contenido multimedia.

Si combina estas dos tecnologías pero no configura la redirección, HDX genera el contenido en el servidor.

En cambio, si configura la redirección, HDX utiliza la opción “obtener en el servidor y generar en el cliente” u “obtener en el cliente y generar en el cliente”. Si se producen fallos cuando utiliza estos métodos, HDX recurre a la generación en el servidor cuando sea necesario y se rige por la directiva de prevención de reserva.

## Casos de ejemplo



### Caso 1. (Obtener en servidor y generar en servidor):

1. El servidor obtiene el archivo multimedia desde su origen, lo decodifica y, a continuación, presenta su contenido a un dispositivo de sonido o un dispositivo de pantalla.
2. El servidor extrae la imagen o el sonido presentados del dispositivo de pantalla o del dispositivo de sonido respectivamente.
3. El servidor puede comprimirlo y, a continuación, lo transmite al cliente.

Este enfoque implica un alto consumo de CPU, de alto ancho de banda (si la imagen o el sonido extraídos no se comprimen eficazmente), y tiene una escalabilidad de servidor baja.

Thinwire y los canales virtuales de sonido se ocupan de este enfoque. La ventaja de este enfoque

es que reduce los requisitos de hardware y software para los clientes. Con este enfoque, la decodificación ocurre en el servidor y funciona para una mayor variedad de dispositivos y formatos.

**Caso 2. (Obtener en servidor y generar en cliente):**

Este enfoque necesita poder interceptar el contenido multimedia antes de que se decodifique y se presente al dispositivo de sonido o de pantalla. El contenido de audio o vídeo comprimidos se envía al cliente, donde se decodifica y se presenta localmente. La ventaja de este enfoque es que se transmite a los dispositivos cliente, con lo que se ahorran ciclos de CPU en el servidor.

Sin embargo, conlleva algunos requisitos de hardware y software adicionales para el cliente. El cliente debe poder decodificar todos los formatos que pueda recibir.

**Caso 3. (Obtener en cliente y generar en cliente):**

Este enfoque se basa en la capacidad de interceptar la URL del contenido multimedia antes de que se obtenga desde el origen. La dirección URL se envía al cliente, donde el contenido multimedia se obtiene, se decodifica y se presenta localmente. Este enfoque es conceptualmente simple. Su ventaja es que ahorra ancho de banda y ciclos de CPU en el servidor, porque el servidor solo envía comandos de control. No obstante, el contenido multimedia no siempre está disponible para los clientes.

**Entorno y plataforma:**

Los sistemas operativos de sesión única (Windows, Mac OS X y Linux) ofrecen entornos multimedia que permiten un desarrollo más rápido de aplicaciones multimedia. En esta tabla se muestran algunos de los entornos multimedia más comunes. En cada entorno se divide el procesamiento multimedia en varias etapas y se usa una arquitectura adaptada.

---

Framework	Platform
DirectShow	Windows (98 y versiones posteriores)
Media Foundation	Windows (Vista y versiones posteriores)
Gstreamer	Linux
QuickTime	Mac OS X

---

**Funcionalidad de doble salto con tecnologías de redirección multimedia**

---

---

	Redirección de sonido	No
	Redirección de contenido de explorador web	No

---

Redirección de cámara web HDX	Sí
Redirección de vídeo HTML5	Sí
Redirección de Windows Media	Sí

---

## Funciones de audio

September 21, 2022

Puede configurar y agregar las siguientes configuraciones de directiva de Citrix a una directiva que optimice las funciones de audio de HDX. Para obtener información acerca del uso, las relaciones y las dependencias con otras configuraciones de directiva, consulte [Configuraciones de directiva de audio](#), [Configuraciones de directiva de ancho de banda](#) y [Configuraciones de directiva de conexiones de multisequencia](#).

### Importante:

Recomendamos entregar el audio mediante el protocolo de datagramas de usuario (UDP) en lugar de TCP. Solo Virtual Delivery Agent (VDA) de Windows admite audio por UDP.

El cifrado de audio por UDP mediante DTLS solo está disponible entre Citrix Gateway y la aplicación Citrix Workspace. Por lo tanto, a veces puede ser preferible utilizar el transporte TCP. TCP admite el cifrado TLS de punto a punto desde el VDA a la aplicación Citrix Workspace.

## Calidad de audio

En general, un audio de mayor calidad consume más ancho de banda y utiliza más recursos de CPU del servidor, al enviar más datos de audio a los dispositivos de los usuarios. La compresión de audio permite llegar a un equilibrio entre calidad de audio y rendimiento general de la sesión; use las configuraciones de directiva de Citrix para configurar los niveles de compresión que se deben aplicar a los archivos de audio.

De forma predeterminada, la configuración de **la directiva Calidad de audio** está establecida en “Alta: audio de alta definición” cuando se utiliza el transporte TCP. En cambio, la directiva “Calidad de audio” se establece en “Medio: optimizado para voz” cuando se utiliza el transporte UDP (opción recomendada). El parámetro **Alta: audio de alta definición** ofrece audio estéreo de alta fidelidad, pero consume más ancho de banda que los demás parámetros de calidad. No use este nivel de calidad de

audio para aplicaciones de videochat o chat de voz no optimizadas (por ejemplo, programas de soft-phone). Puede provocar unos niveles de latencia en la ruta de audio que no son adecuados para las comunicaciones en tiempo real. Se recomienda la configuración de directiva “Medio: optimizado para voz” para audio en tiempo real, independientemente del protocolo de transporte seleccionado.

Cuando el ancho de banda es limitado (conexiones por satélite o acceso telefónico), reducir la calidad del audio a **Baja** consume el menor ancho de banda posible. En este caso, deberá crear directivas distintas para los usuarios en las conexiones de poco ancho de banda para que los usuarios que disponen de conexiones con buen ancho de banda no se vean afectados negativamente.

Para obtener más información acerca de la configuración, consulte [Configuraciones de directiva de audio](#). Recuerde que debe habilitar “Parámetros de audio del cliente” en el dispositivo del usuario.

Directrices sobre ancho de banda para la reproducción y grabación de audio:

- Alta calidad (valor predeterminado)
  - Velocidad de bits: ~ 100 kbps (mín. 75, máx. 175 kbps) para reproducción / ~ 70 kbps para captura de micrófono
  - Número de canales: 2 (estéreo) para reproducción, 1 (mono) para captura de micrófono
  - Frecuencia: 44100 Hz.
  - Profundidad de bits: 16 bits
- Calidad media (recomendada para VoIP)
  - Velocidad de bits: ~ 16 kbps (mín. 20, máx. 40 kbps) para reproducción, ~ 16 kbps para captura de micrófono
  - Número de canales: 1 (Mono) para reproducción y captura
  - Frecuencia: 16000 Hz (banda ancha)
  - Profundidad de bits: 16 bits
- Calidad baja
  - Velocidad de bits: ~ 11 kbps (mín. 10, máx. 25 kbps) para reproducción, ~ 11 kbps para captura de micrófono
  - Número de canales: 1 (Mono) para reproducción y captura
  - Frecuencia: 8000 Hz (banda estrecha)
  - Profundidad de bits: 16 bits

## Redirección de audio del cliente

Para permitir que los usuarios reciban audio desde una aplicación en un servidor mediante los altavoces u otros dispositivos de audio en sus dispositivos de usuario, deje la configuración **Redirección de audio del cliente** en **Permitida**. Esta es la opción predeterminada.

La asignación de audio del cliente genera una carga adicional para los servidores y para la red. Cuando la Redirección de audio del cliente está Prohibida, toda la función de audio de HDX queda inhabilitada.

Para obtener más información acerca de la configuración, consulte [Configuraciones de directiva de audio](#). Recuerde que debe habilitar “Parámetros de audio del cliente” en el dispositivo del usuario.

### **Redirección de micrófonos del cliente**

Para permitir que los usuarios graben audio por medio de dispositivos de entrada (por ejemplo, micrófonos) en sus dispositivos, deje el parámetro **Redirección de micrófonos del cliente** en su opción predeterminada (Permitida).

Por motivos de seguridad, se alerta a los usuarios si un servidor en el que no confía el dispositivo de usuario intenta acceder a su micrófono. El usuario puede elegir entre aceptar o rechazar dicho acceso, antes de usar el micrófono. Los usuarios pueden inhabilitar esta alerta en la aplicación Citrix Workspace.

Para obtener más información acerca de la configuración, consulte [Configuraciones de directiva de audio](#). Recuerde que debe habilitar “Parámetros de audio del cliente” en el dispositivo del usuario.

### **Audio Plug and Play**

La configuración de directiva Audio Plug and Play controla si se permite o se impide el uso de varios dispositivos de audio para grabar y reproducir audio. Esta configuración está **habilitada** de forma predeterminada. Audio Plug N Play permite reconocer los dispositivos de audio. Los dispositivos se reconocen aunque no estén conectados hasta después de que se haya iniciado la sesión de usuario.

Esta configuración solo se aplica a máquinas de SO multisesión Windows.

Para obtener más información acerca de la configuración, consulte [Configuraciones de directiva de audio](#).

### **Límite de ancho de banda de redirección de audio y Porcentaje límite de ancho de banda de redirección de audio**

La configuración de directiva Límite de ancho de banda de redirección de audio especifica el ancho de banda máximo (en kilobits por segundo) que se puede usar para la reproducción y grabación de audio en una sesión.

La configuración Porcentaje límite de ancho de banda de redirección de audio especifica el ancho de banda máximo que se puede usar para la redirección de audio, expresado como un porcentaje del ancho de banda total disponible.

De manera predeterminada, el valor para ambos es cero (no hay máximo). Si se han configurado ambos parámetros, se usará aquél que ofrezca la menor limitación de ancho de banda.

Para obtener más información acerca de la configuración, consulte [Configuraciones de directiva de ancho de banda](#). Recuerde que debe habilitar “Parámetros de audio del cliente” en el dispositivo del usuario.

## Transporte de audio en tiempo real por UDP e Intervalo de puertos UDP de audio

De manera predeterminada, la opción “Transporte de audio en tiempo real por UDP” está “Permitida” (si se selecciona en el momento de la instalación). Esa opción abre un puerto UDP en el servidor para las conexiones que usan el transporte de audio en tiempo real por UDP. En caso de una congestión de red o pérdida de paquetes, se recomienda configurar UDP/RTP para el audio para garantizar la mejor experiencia de usuario. Para cualquier audio en tiempo real típico de aplicaciones softphone, se prefiere el audio UDP antes que EDT. UDP permite la pérdida de paquetes sin retransmisión, con lo que no se agrega latencia en las conexiones con pérdidas grandes de paquetes.

### Importante:

Cuando Citrix Gateway no está en la ruta, los datos de audio transmitidos por UDP no se cifran. Si Citrix Gateway está configurado para acceder a los recursos de Citrix Virtual Apps and Desktops, el tráfico de audio entre el dispositivo de punto final y Citrix Gateway se protege mediante el protocolo DTLS.

El “Intervalo de puertos UDP de audio” especifica el intervalo de números de puerto que Windows VDA utiliza para intercambiar datos de paquetes de audio con el dispositivo de usuario.

De manera predeterminada, el intervalo es de 16500 a 16509.

Para obtener más información sobre el Transporte de audio en tiempo real por UDP, consulte [Configuraciones de directiva de audio](#). Para obtener más información sobre el Intervalo de puertos UDP de audio, consulte [Configuraciones de directiva de conexiones de multisequencia](#). Recuerde que debe habilitar “Parámetros de audio del cliente” en el dispositivo del usuario.

El audio por UDP requiere el Windows VDA. Para obtener información sobre las directivas compatibles en Linux VDA, consulte [Lista de directivas disponibles](#).

## Configuraciones de directiva de audio para los dispositivos de usuario

1. Cargue las plantillas de directiva de grupo siguiendo las instrucciones de [Configurar la plantilla administrativa de objeto de directiva de grupo](#).
2. En el Editor de directivas de grupo, expanda **Plantillas administrativas > Componentes de Citrix > Citrix Workspace > Experiencia de usuario**.

3. En **Configuración del audio del cliente**, seleccione **No configurada**, **Habilitada** o **Inhabilitada**.
  - **No configurada**. De forma predeterminada, la redirección de audio está habilitada con alta calidad de audio, o con los parámetros de audio personalizados configurados previamente.
  - **Habilitada**. Habilita la redirección de audio mediante las opciones seleccionadas.
  - **Inhabilitado**. Inhabilita la redirección de audio.
4. Si ha seleccionado **Habilitada**, elija una calidad de audio. Para el audio UDP, use solo la calidad de audio **media** (la predeterminada).
5. Para el audio UDP solamente, seleccione **Enable Real-Time Transport** y configure el intervalo de puertos de entrada que se abrirán en el Firewall de Windows local.
6. Para utilizar el audio UDP con Citrix Gateway, seleccione **Permitir transporte en tiempo real a través de NetScaler Gateway**. Configure Citrix Gateway con DTLS. Para obtener más información, consulte [este artículo](#).

Como administrador, si no tiene control sobre los dispositivos de punto final para hacer estos cambios, use los atributos del archivo default.ica de StoreFront para habilitar el audio UDP. Por ejemplo, en el caso de dispositivos que son propiedad de los usuarios (Bring Your Own Device) o equipos domésticos.

1. En la máquina de StoreFront, abra C:\inetpub\wwwroot\Citrix\\App\_Data\default.ica con un editor de texto como el Bloc de notas.
2. Cree estas entradas en la sección [Aplicación].
  - ; Este texto permite el transporte en tiempo real  
EnableRtpAudio=true
  - ; Este texto permite el transporte en tiempo real a través de la puerta de enlace  
EnableUDPThroughGateway=true
  - ; Este texto establece la calidad del audio en Media  
AudioBandwidthLimit=1
  - ; Intervalo de puertos UDP  
RtpAudioLowestPort=16500  
RtpAudioHighestPort=16509

Si el audio UDP se habilita mediante la edición de default.ica, el audio UDP estará habilitado para todos los usuarios que utilicen ese almacén.

## Evitar eco durante conferencias multimedia

Los usuarios de conferencias de audio o de vídeo pueden escuchar un eco. El eco normalmente ocurre cuando los altavoces están muy cerca del micrófono. En estos casos, se recomiendan auriculares para conferencias con audio y vídeo.

HDX ofrece una opción de eliminación de ecos (habilitada de forma predeterminada), que permite minimizarlos. La eficacia de la eliminación del eco depende de la distancia entre los altavoces y el micrófono. Los dispositivos no deben estar demasiado cerca ni demasiado lejos el uno del otro.

La eliminación de eco se puede inhabilitar mediante un parámetro de Registro.

### Advertencia

Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

1. En el Editor del Registro, vaya a una de estas ubicaciones:

- Equipos de 32 bits: HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced
- Equipos de 64 bits: HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio\EchoCancellation

2. Cambie el campo **Información del valor** a FALSE.

## Softphone

Una aplicación softphone es un software que actúa como una interfaz de teléfono. Se utiliza un software softphone para realizar llamadas por Internet desde un equipo o una tableta, por ejemplo. Con softphone, puede marcar números de teléfono y llevar a cabo otras funciones relacionadas con el teléfono a través de una pantalla.

Citrix Virtual Apps and Desktops admiten varias alternativas para la entrega de aplicaciones softphone.

- **Modo de control.** La aplicación softphone alojada controla un teléfono físico configurado. En este modo, no hay tráfico de audio que pase por el servidor de Citrix Virtual Apps and Desktops.
- **Optimización de HDX RealTime para softphone (recomendado).** El motor de medios se ejecuta en el dispositivo de usuario, y el tráfico VoIP (Voice over Internet Protocol) pasa de un homónimo a otro. Para ver ejemplos, consulte:
  - [Optimización para Microsoft Teams](#)

- [HDX RealTime Optimization Pack](#), que optimiza la entrega de Skype Empresarial de Microsoft
  - [Cisco Jabber Softphone para VDI](#) (anteriormente conocido como VXME)
  - [Reuniones de Cisco Webex para VDI](#)
  - [Avaya VDI Equinox](#) (antes conocido como VDI Communicator)
  - [Plugin Zoom para entornos VDI](#)
  - [Genesys PureEngage Cloud](#)
  - [Dispositivo de dictado Nuance PowerMic para Dragon](#)
- **Acceso a aplicaciones locales.** Una función de Citrix Virtual Apps and Desktops que permite que una aplicación softphone se ejecute localmente en el dispositivo Windows del usuario, al mismo tiempo que aparece perfectamente integrada en el escritorio virtual o publicado. Con esta función, toda la carga del procesamiento de audio pasa al dispositivo del usuario. Para obtener más información, consulte [Acceso a aplicaciones locales y redirección de URL](#).
  - **Funcionalidad genérica de HDX RealTime para softphone.** VoIP por ICA.

### ***Funcionalidad genérica para softphone***

La funcionalidad genérica para softphone permite alojar un softphone no modificado en el centro de datos de XenApp o XenDesktop. El tráfico de audio se dirige mediante el protocolo ICA de Citrix (preferentemente por UDP/RTP) al dispositivo de usuario que ejecuta la aplicación Citrix Workspace.

La funcionalidad genérica para softphone es una función de HDX RealTime. Este enfoque a la entrega de softphone es especialmente útil para:

- La solución optimizada para entregar el softphone no está disponible y el usuario no está en un dispositivo Windows donde se pueda utilizar el Acceso a aplicaciones locales.
- El motor de medios necesario para la entrega optimizada del softphone no se ha instalado en el dispositivo de usuario o no está disponible para la versión de sistema operativo que ejecuta el dispositivo del usuario. En este caso, HDX RealTime genérico ofrece una buena solución a la que recurrir.

Existen dos aspectos a tener en cuenta en la entrega de softphone con Citrix Virtual Apps and Desktops:

- ¿Cómo se entrega la aplicación softphone al escritorio virtual o publicado?
- ¿Cómo se entrega el audio desde y hacia los auriculares, el micrófono y el altavoz o el set USB para teléfonos del usuario?

Citrix Virtual Apps and Desktops contiene numerosas tecnologías para ofrecer la entrega genérica de softphone:

- Códec optimizado para voz si quiere codificar rápidamente audio en tiempo real y quiere un uso eficiente del ancho de banda.

- Pila de audio para latencia baja.
- Búfer de vibración en el servidor para suavizar el audio cuando fluctúa la latencia de red.
- Etiquetado de paquetes (DSCP y WMM) para la calidad de servicio.
  - Etiquetado de DSCP para paquetes RTP (Layer 3)
  - Etiquetado de WMM para Wi-Fi

Las versiones de la aplicación Citrix Workspace para Mac, Windows, Linux y Chrome también admiten VoIP. La aplicación Citrix Workspace para Windows ofrece estas funciones:

- Búfer de vibración en el cliente: Suaviza el audio incluso cuando fluctúa la latencia de red.
- Eliminación de eco: Permite mayor variación en la distancia entre el micrófono y los altavoces para usuarios que no disponen de auriculares con micrófono.
- Audio Plug and Play: Los dispositivos de audio no necesitan estar conectados antes de iniciar una sesión. Se pueden conectar en cualquier momento.
- Redirección de dispositivos de audio: Los usuarios pueden dirigir tonos a los altavoces, mientras que la voz va a sus auriculares.
- ICA de multisequencia: Permite la redirección flexible basada en la calidad de servicio (QoS) a través de la red.
- ICA admite cuatro flujos TCP y dos UDP. Uno de los flujos UDP admite el audio en tiempo real por RTP.

Para ver un resumen de las funciones de la aplicación Citrix Workspace, consulte la [Tabla de funciones de Citrix Receiver](#).

### **Recomendaciones de configuración del sistema**

Hardware y software del cliente:

Para una calidad óptima del sonido, le recomendamos la versión más reciente de la aplicación Citrix Workspace y unos auriculares de buena calidad con eliminación de eco acústico (AEC). Las versiones de la aplicación Citrix Workspace para Windows, Linux y Mac admiten VoIP. Además, Dell Wyse ofrece compatibilidad con VoIP en ThinOS (WTOS).

Consideraciones sobre CPU:

Supervise el consumo de CPU en el VDA para determinar si es necesario asignar dos CPU virtuales a cada máquina virtual. La transmisión de voz y vídeo en tiempo real consumen muchos recursos. Configurar dos CPU virtuales reduce la latencia generada por cambiar de subprocesos. Por lo tanto, se recomienda configurar dos unidades CPU virtuales en un entorno de VDI de Citrix Virtual Desktops.

Tener dos CPU virtuales no significa necesariamente doblar la cantidad de unidades CPU físicas, porque las CPU físicas existentes pueden compartirse entre varias sesiones.

Citrix Gateway Protocol (CGP), que se utiliza para la función de fiabilidad de la sesión, también aumenta el consumo de CPU. Puede inhabilitar esta función para reducir el consumo de CPU en el VDA

cuando se trate de conexiones de red de alta calidad. Ninguno de los pasos anteriores es necesario en un servidor potente.

#### Audio UDP:

El audio por UDP ofrece una tolerancia excelente frente a la congestión de red y a la pérdida de datos. Se recomienda UDP en lugar de TCP cuando esté disponible.

#### Configuración de LAN o WAN:

Configurar correctamente la red es fundamental para una buena calidad de audio en tiempo real. Por lo general, debe configurar LAN virtuales (vLAN) porque demasiados paquetes de difusión pueden provocar vibración. Los dispositivos habilitados con IPv6 pueden generar una gran cantidad de paquetes de difusión. Si no se necesita compatibilidad con IPv6, puede inhabilitar IPv6 en esos dispositivos. Configure esta funcionalidad para admitir la calidad de servicio.

#### Parámetros para usar conexiones WAN:

Puede usar el chat de voz a través de conexiones LAN y WAN. En una conexión WAN, la calidad del audio depende de la latencia, la pérdida de paquetes y la vibración existentes en la conexión. Si entrega aplicaciones softphone a los usuarios por una conexión WAN, se recomienda usar NetScaler SD-WAN entre el centro de datos y la oficina remota. Así, se mantiene una alta calidad de servicio (QoS). NetScaler SD-WAN admite ICA de multisequencia, incluido UDP. Además, en caso de un único flujo TCP, puede establecer prioridades distintas para los diferentes canales virtuales ICA para garantizar que los datos de audio en tiempo real de alta prioridad se traten de manera preferente.

Use Director o [HDX Monitor](#) para validar la configuración de HDX.

#### Conexiones de usuarios remotos:

Citrix Gateway admite DTLS para entregar el tráfico UDP/RTP de forma nativa (sin encapsulación en TCP).

Abra los firewalls en los dos sentidos para el tráfico UDP en el puerto 443.

#### Selección de códecs y consumo de ancho de banda:

Entre el dispositivo de usuario y el VDA del centro de datos, se recomienda usar el parámetro de códec **optimizado para voz**, también conocido como calidad de audio media. Entre la plataforma VDA y la PBX de IP, el softphone utiliza el códec configurado o negociado. Por ejemplo:

- G711 ofrece una calidad de voz muy buena, pero presenta un requisito de ancho de banda de 80 a 100 kilobits por segundo y por llamada (según la sobrecarga de Network Layer2).
- G729 ofrece una buena calidad de voz y presenta un requisito de ancho de banda de 30 a 40 kilobits por segundo y por llamada (según la sobrecarga de Network Layer2).

#### ***Entregar aplicaciones softphone al escritorio virtual***

Existen dos métodos para entregar una aplicación softphone al escritorio virtual XenDesktop:

- La aplicación puede instalarse en la imagen del escritorio virtual.

- La aplicación puede distribuirse por streaming al escritorio virtual mediante Microsoft App-V. Este enfoque ofrece ventajas de capacidad de administración, porque la imagen del escritorio virtual se mantiene limpia. Después de distribuirse por streaming al escritorio virtual, la aplicación se ejecuta en ese entorno como si se hubiera instalado de la forma habitual. No todas las aplicaciones son compatibles con App-V.

### ***Entregar audio desde y hacia el dispositivo de usuario***

HDX RealTime genérico admite dos métodos para entregar audio desde y hacia el dispositivo de usuario:

- **Citrix Audio Virtual Channel.** Por lo general, se recomienda Citrix Audio Virtual Channel porque se ha diseñado específicamente para el transporte de audio.
- **Redirección de USB genérico.** Admite dispositivos de audio que tienen botones y/o pantalla o es un dispositivo de interfaz humana (HID) si el dispositivo del usuario se encuentra en una LAN (o una conexión de este tipo) al servidor de Citrix Virtual Apps and Desktops.

### ***Citrix Audio Virtual Channel***

Citrix Audio Virtual Channel (CTXCAM) bidireccional permite la entrega de audio de forma eficiente en la red. HDX RealTime genérico toma el audio desde los auriculares o el micrófono del usuario y lo comprime. Luego, lo envía por ICA a la aplicación softphone presente en el escritorio virtual. Del mismo modo, el audio resultante de la aplicación softphone se comprime y se envía en la dirección opuesta, hacia los auriculares o los altavoces del usuario. Esta compresión no depende de la compresión utilizada por el sistema softphone en sí (por ejemplo, G.729 o G.711). Se lleva a cabo mediante el códec optimizado para voz (calidad media). Sus funciones son ideales para VoIP. Presenta un tiempo muy pequeño de codificación y consume aproximadamente solo 56 Kilobits por segundo del ancho de banda de red (28 Kbps en cada dirección) en las horas punta. Este códec debe seleccionarse explícitamente en la consola de Studio porque no es el códec predeterminado de audio. La opción predeterminada es el códec de audio HD (calidad alta). Ese códec es ideal para melodías en estéreo de alta fidelidad, pero es más lento para codificar en comparación con el códec optimizado para voz.

### ***Redirección de USB genérico***

La tecnología de redirección de USB genérico de Citrix (canal virtual CTXGUSB) ofrece un medio genérico para comunicar dispositivos USB remotos, incluidos los dispositivos compuestos (audio más HID) y los dispositivos USB isócronos. Este enfoque está limitado a los usuarios conectados por LAN. Ya que el protocolo USB tiende a ser sensible a la latencia de red y requiere un ancho de banda considerable. La redirección de USB isócrono funciona bien cuando se usan determinadas aplicaciones softphone. Esta redirección ofrece una calidad de voz excelente y una latencia baja. Sin embargo, se prefiere Citrix Audio Virtual Channel porque está optimizado para el tráfico de audio. La excepción principal es cuando se usa un dispositivo de audio con botones. Por ejemplo, un teléfono USB conectado al dispositivo de usuario que está conectado a su vez a la central de datos por LAN. En este caso, la redirección de USB genérico admite botones en el teléfono o en los auriculares,

utilizados para controlar las funciones por el envío de señales a la aplicación softphone. Este no es un problema con los botones que funcionan de forma local en el dispositivo.

## Limitación

### Advertencia

Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Cuando instala un dispositivo de audio en el cliente y habilita la redirección de audio e inicia una sesión RDS: Es posible que los archivos de audio no se reproduzcan y aparezca un mensaje de error.

Como solución alternativa, agregue esta clave al Registro en la máquina RDS y reiniciela:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SCMConfig

Nombre: EnableSvchostMitigationPolicy

Tipo: REG\_DWORD

Datos: 0

## Redirección de contenido de explorador web

March 15, 2022

Redirigir el contenido del explorador web impide que las páginas web incluidas en la lista de permitidos se generen en el lado del agente VDA. Esta función utiliza la aplicación Citrix Workspace para crear una instancia de motor de generación correspondiente en el lado del cliente, que obtiene el contenido HTTP y HTTPS a partir de la URL.

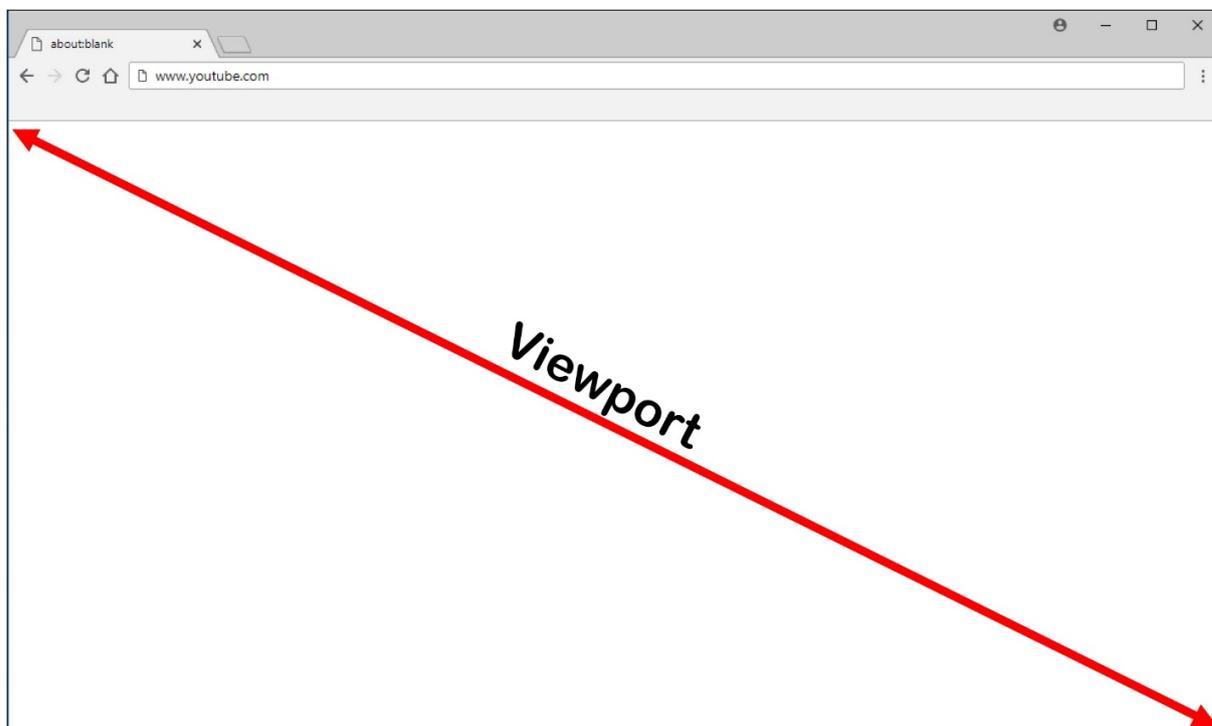
### Nota:

Puede especificar que las páginas web se redirijan al lado del VDA (no al lado del cliente) mediante una lista de bloqueados.

Este motor web de distribución superpuesta se ejecuta en el dispositivo de punto final, en lugar de ejecutarse en el VDA, y utiliza la CPU, la GPU, la memoria RAM y la red del dispositivo de punto final.

Solo se redirige la ventanilla del explorador web. La ventanilla es el área rectangular del explorador web donde aparece el contenido. La ventanilla no incluye elementos como la barra de direcciones, la

barra de favoritos ni la barra de estado. Esos elementos están en la interfaz de usuario, que todavía se ejecutan en el explorador en el VDA.



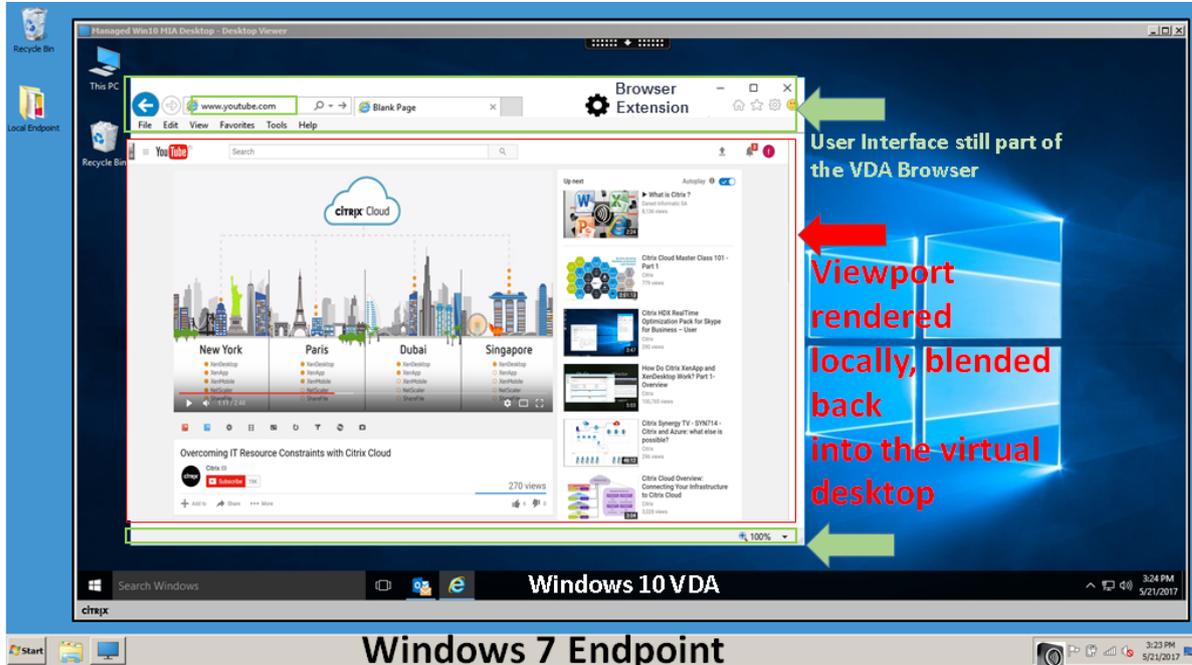
1. Configure una directiva de Studio que especifique una lista de control de acceso que contenga las URL incluidas en la lista de permitidos para permitir redirecciones o la lista de bloqueados para inhabilitar la redirección de URL específicas. Para que el explorador web presente en el VDA detecte que la URL a la que se dirige el usuario está incluida en la lista de permitidos o en la lista de bloqueados, la extensión del explorador web busca la URL en esas listas. La extensión del explorador web (BHO) para Internet Explorer 11 está incluida en los medios de instalación y se instala automáticamente. Para Chrome, la extensión del explorador está disponible en Chrome Web Store y puede implementarla mediante las directivas de grupo y los archivos ADMX. Las extensiones de Chrome se instalan basándose en el usuario. No es necesario actualizar una imagen maestra para agregar o eliminar una extensión.
2. Si se encuentra una coincidencia en la lista de permitidos (por ejemplo <https://www.mycompany.com/>), y no hay ninguna coincidencia en la lista de bloqueados (por ejemplo <https://www.mycompany.com/engineering>), un canal virtual (CTXCSB) indica a la aplicación Citrix Workspace que se requiere una redirección y transmite la URL. La aplicación Citrix Workspace crea una instancia de motor de generación local y muestra el sitio web.
3. La aplicación Citrix Workspace introduce el sitio web en el área de contenido del explorador web que tenga el escritorio virtual.

El color del logotipo especifica el estado de la extensión de Chrome. Es uno de estos tres colores:

- Verde: Activo y conectado.

- Gris: No activo/inactivo en la ficha actual.
- Rojo: No funciona.

Puede depurar el registro mediante **Opciones**, en el menú de extensiones.



### Importante:

Los parámetros siguientes solo se aplican a 1912 LTSR CU1 o a versiones posteriores.

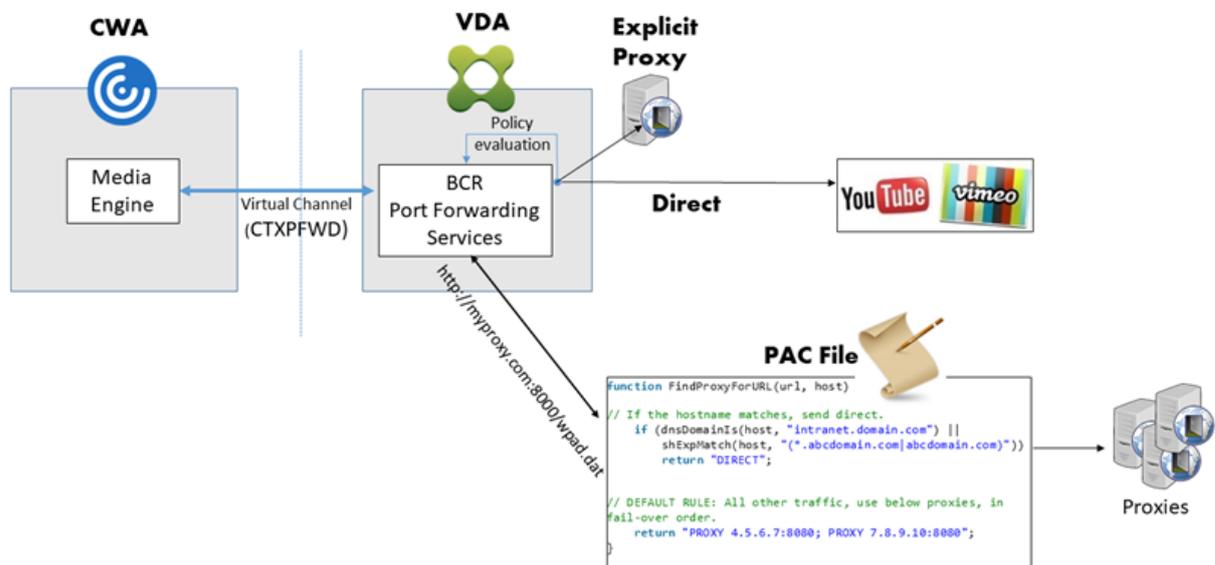
La aplicación Citrix Workspace obtiene el contenido de estas maneras:

- **Obtención en el servidor y generación en el servidor:** No hay redirección porque el sitio no consta en la lista de permitidos o la redirección ha fallado. Se recurre a la generación de la página web en el VDA y se usa Thinwire para generar remotamente los gráficos. Se usan directivas para controlar el comportamiento cuando se recurre al mecanismo alternativo. Alto consumo de CPU, memoria RAM y ancho de banda en el VDA.
- **Obtención en el servidor y generación en el cliente:** La aplicación Citrix Workspace se comunica con el servidor web y obtiene el contenido desde este a través del VDA mediante un canal virtual (CTXPFW). Esta opción es útil cuando el cliente no tiene acceso a Internet (por ejemplo, clientes ligeros). Bajo consumo de CPU y RAM en el VDA, pero se consume ancho de banda para el canal virtual ICA.

Hay tres modos de funcionamiento para este caso. El término proxy hace referencia a un dispositivo proxy al que accede el VDA para obtener acceso a Internet.

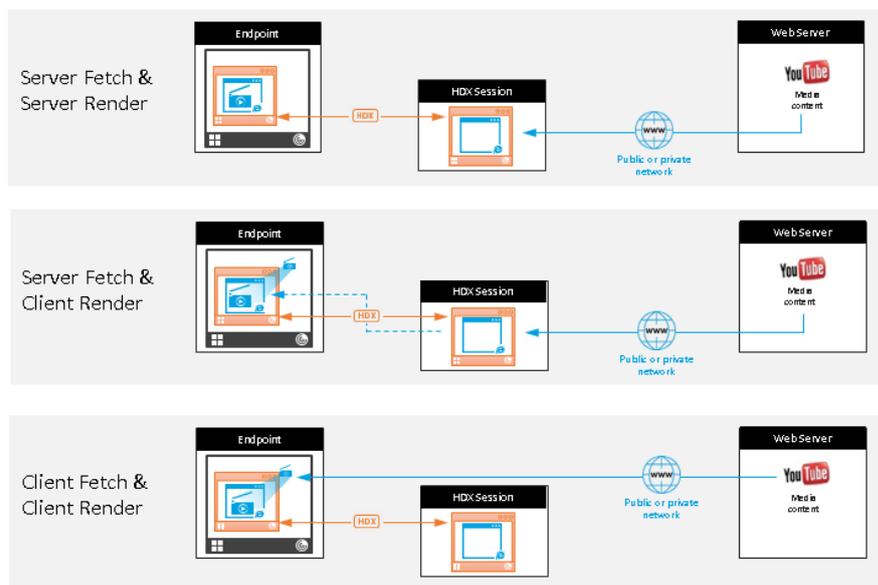
Qué opción de directiva elegir:

- Proxy explícito: Si tiene un solo proxy explícito en su centro de datos. Redirige el tráfico de la redirección de contenido del explorador a través del VDA y lo reenvía al proxy web especificado.
- Directo o transparente: Si no tiene proxies o si utiliza proxies transparentes. Redirige el tráfico de la redirección de contenido del explorador a través del VDA y lo reenvía directamente al servidor web que aloja el contenido.
- Archivos PAC: Si confía en archivos PAC, los exploradores del VDA pueden elegir automáticamente el servidor proxy apropiado para obtener la URL especificada. Redirige el tráfico de la redirección de contenido del explorador a través del VDA y lo reenvía al proxy web determinado mediante la evaluación del archivo PAC especificado.



- **Obtención en el cliente y generación en el cliente:** Como la aplicación Citrix Workspace se comunica directamente con el servidor web, requiere acceso a Internet. En este caso, no se consume la red, la CPU ni la memoria RAM del sitio de XenApp y XenDesktop.

## Redirection scenarios



### Benefits:

- Better end user experience (Adaptive Bit Rate (ABR))
- Reduced VDA resource usage (CPU/RAM/IO)
- Reduced bandwidth consumption

### Mecanismo alternativo:

La redirección de cliente puede fallar a veces. Por ejemplo, si la máquina cliente no tiene acceso directo a Internet, el VDA puede recibir una respuesta de error. En tales casos, el explorador presente en el VDA puede volver a cargar la página web y generarla en el servidor.

Puede impedir la generación de elementos de vídeo en el lado del servidor mediante la directiva existente **Prevención de reserva de Windows Media**. Establezca esta directiva en **Reproducir todo el contenido solo en el cliente** o **Reproducir solo el contenido accesible por el cliente en el cliente**. Estas configuraciones bloquean la reproducción de elementos de vídeo en el servidor si hay fallos en la redirección de cliente. Esta directiva tiene efecto solo cuando la redirección de contenido del explorador web está habilitada y la directiva **Lista de control de acceso** contiene la URL alternativa. La URL no puede constar en la directiva de listas de bloqueados.

### Requisitos del sistema:

Dispositivos de punto final de Windows:

- Windows 7, 8.x, o 10
- Aplicación Citrix Workspace para Windows 1809 o versiones posteriores
- Citrix Receiver para Windows 4.10 o versiones posteriores

### Nota:

La aplicación Citrix Workspace 1912 LTSR para Windows, así como todas las actualizaciones acumulativas de la aplicación Citrix Workspace 1912 LTSR no admiten la redirección de contenido del explorador.

#### Dispositivos de punto final de Linux:

- Aplicación Citrix Workspace 1808 para Linux o versiones posteriores
- Citrix Receiver para Linux 13.9 o versiones posteriores
- Los terminales de clientes ligeros deben incluir WebKitGTK+

#### Citrix Virtual Apps and Desktops 7 1808; XenApp y XenDesktop 7.15 CU5, 7.18, 7.17, 7.16:

- Sistema operativo del VDA: Windows 10 (versión mínima 1607), Windows Server 2012 R2, Windows Server 2016
- Explorador en el VDA:
  - Google Chrome v66 o versiones posteriores (Chrome requiere la aplicación Citrix Workspace 1809 para Windows en el dispositivo de punto final del usuario, Citrix Virtual Apps and Desktops 7 1808 VDA y la extensión de redirección de contenido de explorador)
  - Internet Explorer 11 con estas opciones configuradas:
    - \* Desmarque **Modo protegido mejorado** en: **Opciones de Internet > Avanzado > Seguridad**.
    - \* Marque **Habilitar extensiones de explorador de terceros** en: **Opciones de Internet > Avanzado > Exploración**

#### Solución de problemas:

Para obtener información sobre la resolución de problemas, consulte <https://support.citrix.com/article/CTX230052>

#### Extensión de Chrome de redirección de contenido de explorador web

Para usar la redirección de contenido de explorador con Chrome, agregue la extensión de redirección de contenido de explorador desde Chrome Web Store. Haga clic en **Añadir a Chrome** en el entorno de Citrix Virtual Apps and Desktops.

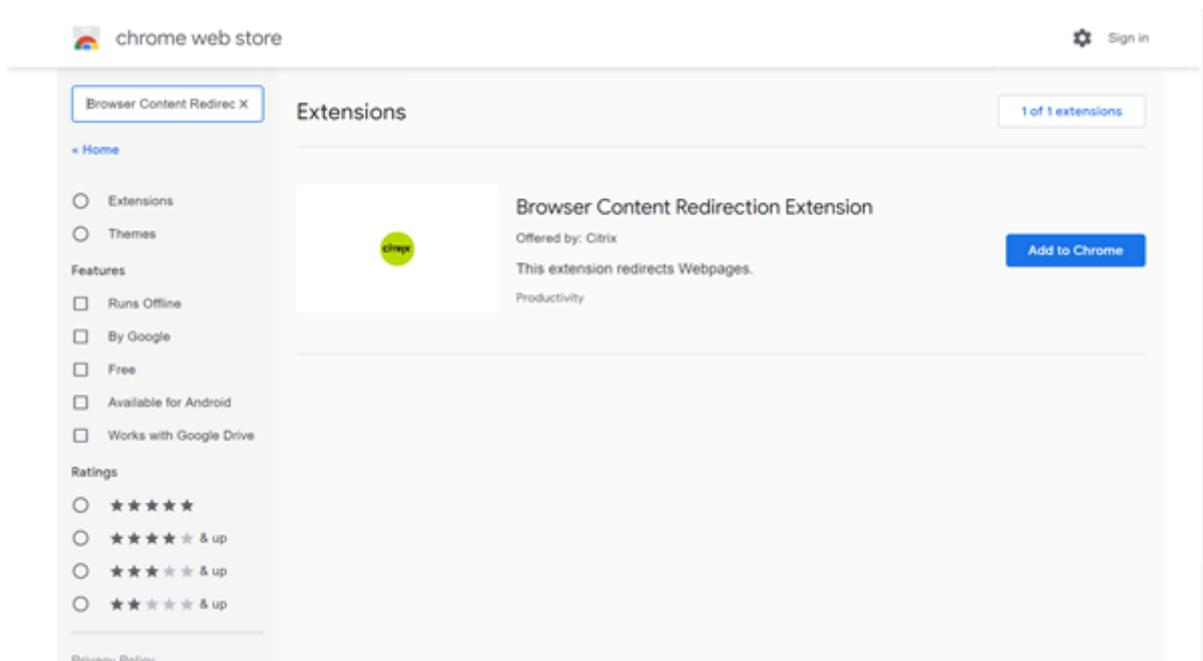
La extensión **no** se requiere en la máquina cliente del usuario, solo en el VDA.

#### Requisitos del sistema

- Chrome v66 o versiones posteriores
- Extensión de redirección de contenido de explorador web
- Citrix Virtual Apps and Desktops 7 1808 o versiones posteriores
- Aplicación Citrix Workspace para Windows 1809 o versiones posteriores

**Nota:**

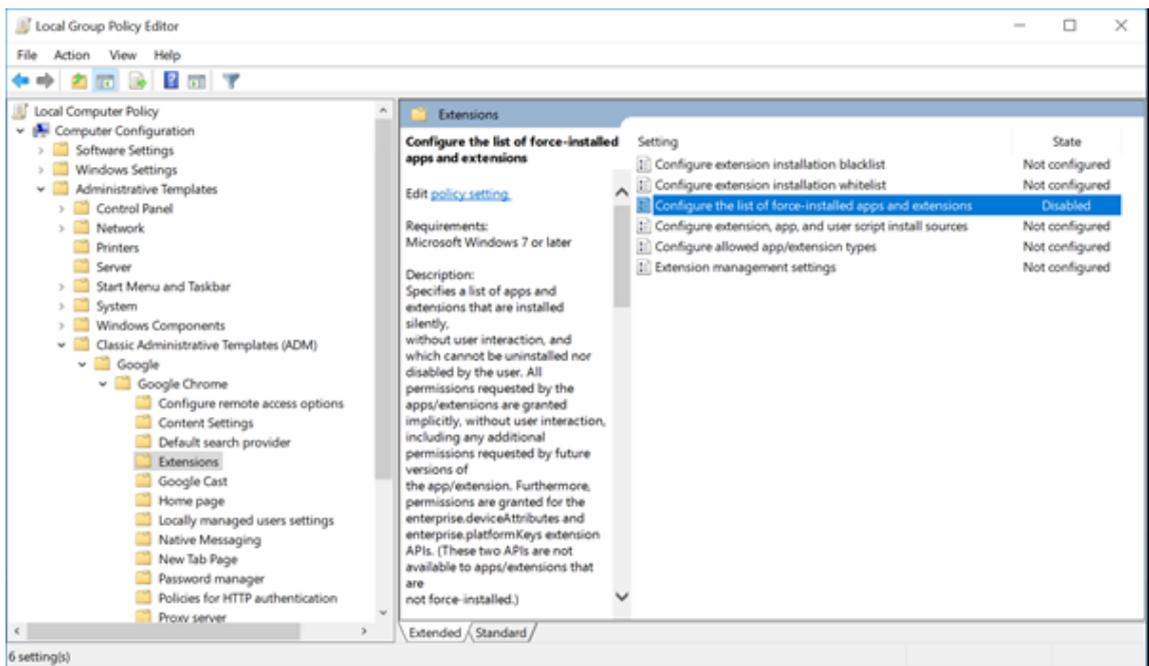
La aplicación Citrix Workspace 1912 LTSR para Windows, así como todas las actualizaciones acumulativas de la aplicación Citrix Workspace 1912 LTSR no admiten la redirección de contenido del explorador.



Este método funciona para usuarios individuales. Para implementar la extensión a un gran grupo de usuarios en su organización, implemente la extensión mediante la directiva de grupo.

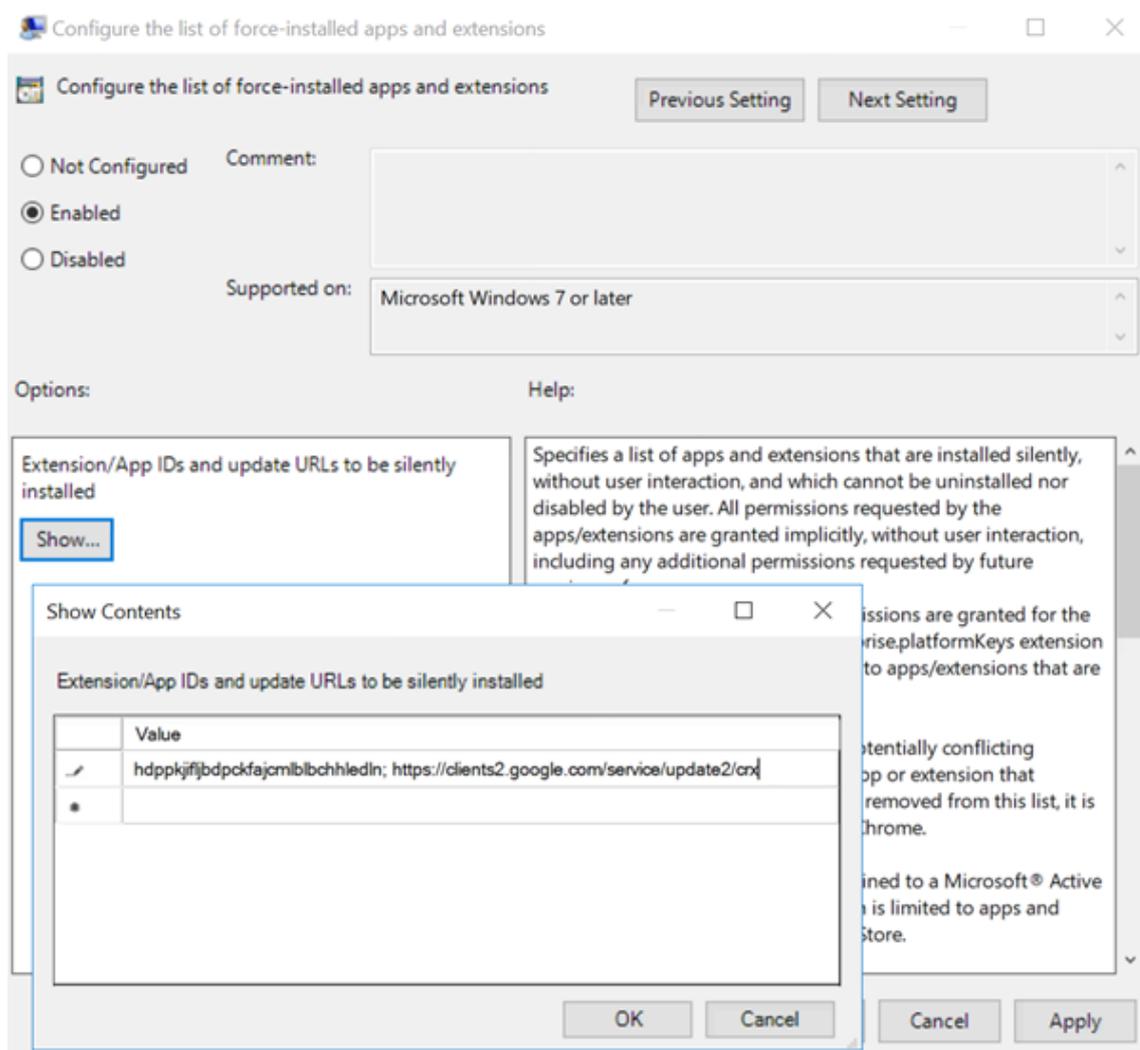
**Implementar la extensión mediante la directiva de grupo**

1. Importe los archivos ADMX de Google Chrome a su entorno. Para obtener información sobre cómo descargar plantillas de directivas, e instalar y configurar las plantillas en su editor de directivas de grupo, consulte <https://support.google.com/chrome/a/answer/187202?hl=en>.
2. Abra su Consola de administración de directivas de grupo y vaya a **Configuración de usuario\Plantillas administrativas\Plantillas administrativas clásicas (ADM)\Google\Google Chrome\Extensiones**. Habilite el parámetro **Configurar la lista de aplicaciones y extensiones con instalación forzada**.



3. Haga clic en **Mostrar** y escriba la siguiente cadena, que corresponde a la ID de extensión. Actualice la URL de la extensión de redirección de contenido de explorador web.

hdppkjifljbdpckfajcmlblbchhledln; <https://clients2.google.com/service/update2/crx>



4. Aplique el parámetro y después de actualizar **gpupdate**, el usuario recibe automáticamente la extensión. Si inicia el explorador Chrome en la sesión del usuario, la extensión ya está aplicada y no pueden quitarla.

Todas las actualizaciones de la extensión se instalan automáticamente en las máquinas de los usuarios a través de la URL de actualización que especificó en la configuración.

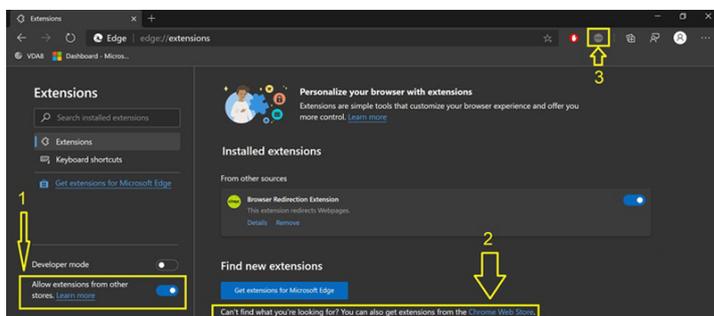
Si el parámetro **Configurar la lista de aplicaciones y extensiones con instalación forzada** se establece en **Inhabilitado**, la extensión se elimina automáticamente de Chrome para todos los usuarios.

### Extensión de Edge Chromium de redirección de contenido de explorador web

Para instalar la extensión de redirección de contenido de explorador web en Edge, compruebe que tiene instalada la versión **83.0.478.37** o una posterior del explorador Edge.

1. Haga clic en la opción **Extensiones** del menú y active **Permitir extensiones de otras tiendas**.
2. Haga clic en el enlace **Chrome Web Store** y la extensión aparecerá en la barra de la parte superior derecha.

Para obtener más información sobre las extensiones de Microsoft Edge, consulte [Extensions](#).



## PPP y redirección de contenido del explorador

### Advertencia:

Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Cuando se utiliza la redirección de contenido del explorador con los PPP (escalado) establecidos por encima del 100% en el equipo del usuario, la pantalla de contenido del explorador redirigido se muestra incorrectamente. Para evitar este problema, no establezca los PPP cuando utilice la redirección de contenido del explorador. Otra forma de evitar el problema es inhabilitar la aceleración de la GPU en la redirección del contenido del explorador para Chrome. Para ello, cree la siguiente clave de Registro en la máquina del usuario:

```
\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxMediaStream
```

Nombre: GPU

Tipo: DWORD

Datos: 0

## Conferencias de vídeo de HDX y compresión de vídeo para cámaras web de HDX

September 22, 2021

### Advertencia:

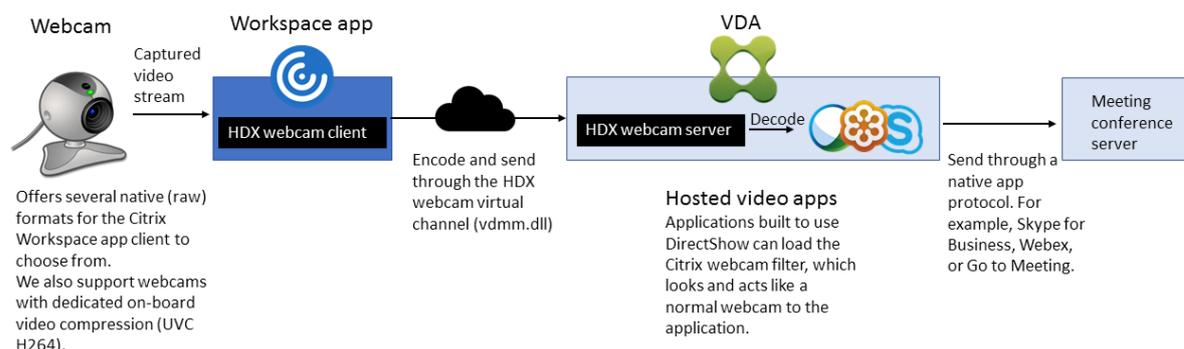
Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Las aplicaciones que se ejecutan en la sesión virtual pueden utilizar cámaras web. Para ello, se debe definir la compresión de vídeo de cámaras web de HDX o la redirección de USB genérico Plug-n-Play de HDX. Para cambiar de modo, vaya a la **aplicación Citrix Workspace > Preferencias > Dispositivos**. Citrix recomienda que siempre use la compresión de vídeo de cámaras web de HDX si es posible. Para evitar que los usuarios cambien la compresión de vídeo de cámaras web de HDX, inhabilite la redirección de dispositivos USB desde las configuraciones de la directiva ICA > configuraciones de la directiva Dispositivos USB. Los usuarios de la aplicación Citrix Workspace pueden supeditar este comportamiento predeterminado. Para ello, deben seleccionar el parámetro **No usar mi micrófono ni mi cámara web** en **Micrófono y cámara web de Desktop Viewer**.

### Compresión de vídeo de cámaras web de HDX

La compresión de vídeo de cámaras web de HDX también se llama modo de cámara web **optimizado**. Este tipo de compresión de vídeo de la cámara web utiliza la tecnología de framework multimedia que forma parte del sistema operativo cliente para interceptar el vídeo de los dispositivos de captura, transcodificarlo y comprimirlo. Los fabricantes de los dispositivos de captura suministran controladores que complementan la arquitectura de streaming del kernel del sistema operativo.

El cliente gestiona la comunicación con la cámara web. El cliente envía el vídeo solo al servidor que puede mostrarlo correctamente. El servidor no trata directamente con la cámara web, pero está integrado, con lo que el usuario recibe la misma experiencia en el escritorio que un tratamiento directo. La aplicación Workspace comprime el vídeo para ahorrar ancho de banda y proporcionar una mejor capacidad de recuperación en conexiones WAN.



La compresión de vídeo de cámaras web de HDX requiere que las siguientes configuraciones de directiva estén habilitadas (están todas habilitadas de forma predeterminada).

- Conferencia multimedia
- Redirección de Windows Media

Si una cámara web es compatible con la codificación por hardware, la compresión de vídeo de HDX utiliza la codificación por hardware de manera predeterminada. La codificación por hardware puede consumir más ancho de banda que la codificación por software. Para forzar la compresión de software, agregue el siguiente valor de clave DWORD a la clave de Registro:

HKEY\_CURRENT\_USER\Software\Citrix\HdxRealTime: DeepCompress\_ForceSWEncode=1

### Requisitos para la compresión de vídeo de cámaras web de HDX

Cientes admitidos: La aplicación Citrix Workspace para Windows, la aplicación Citrix Workspace para Mac, la aplicación Citrix Workspace para Chrome y la aplicación Citrix Workspace para Linux.

#### Nota:

Solo la aplicación Citrix Workspace para Windows, la aplicación Citrix Workspace para Chrome y la aplicación Citrix Workspace para Mac 2006 o posterior admiten la redirección de cámaras web para aplicaciones de 64 bits.

Aplicaciones de conferencias de vídeo compatibles (32 y 64 bits):

- Adobe Connect
- Cisco Webex y Webex Teams
- GoToMeeting
- Google Hangouts y Hangouts Meet
- IBM Sametime
- Microsoft Skype Empresarial 2015
- Microsoft Lync 2010 y 2013

- Microsoft Skype 7 o posterior
- Aplicaciones de vídeo basadas en Media Foundation en Windows 8.x o posterior, Windows Server 2012 R2 y posterior

Para usar Skype en un cliente Windows, modifique el Registro en el cliente y en el servidor:

- Clave del Registro de cliente HKEY\_CURRENT\_USER\Software\Citrix\HdxRealTime
  - Nombre: DefaultHeight
  - Tipo: REG\_DWORD
  - Datos: 240
  - Nombre: DefaultWidth, Tipo: REG\_DWORD
  - Datos: 320
- Clave del Registro de servidor HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\Vd3d\Compatibility
  - Nombre: skype.exe
  - Tipo: REG\_DWORD
  - Datos: Establecido en 0

Otros requisitos del dispositivo de usuario:

- Hardware adecuado para reproducir sonido.
- Cámara web compatible con DirectShow (use la configuración predeterminada de la cámara web). Las cámaras web que pueden codificar hardware reducen el uso de la CPU en el lado del cliente.
- Para la compresión de vídeo de cámaras web de HDX, instale los controladores de cámara web en el cliente, obtenidos del fabricante de la cámara, si es posible.

## **Streaming por cámara web de alta definición**

La aplicación de videoconferencias presente en el servidor selecciona el formato de cámara web y la resolución en función de los tipos de formato compatibles. Cuando se inicia una sesión, el cliente envía la información de la cámara web al servidor. Usted elige la cámara web desde la aplicación. Si la cámara web y la aplicación admiten la generación de alta definición, la aplicación usa la resolución de alta definición. Admitimos resoluciones de cámara web hasta 1920 x 1080.

Esta función requiere la aplicación Citrix Workspace para Windows (versión mínima 1808) o Citrix Receiver para Windows (versión mínima 4.10).

Puede usar una clave de Registro para inhabilitar la función. Se usa la resolución predeterminada de 352 x 288:

HKEY\_LOCAL\_MACHINE\Software\Citrix\HDXRealTime

Nombre: Enable\_HighDefWebcam

Tipo: REG\_DWORD

Datos: 0 = Desactiva la distribución por streaming de la cámara web de alta definición

Puede usar claves de Registro en el cliente para configurar una resolución específica. Compruebe que la cámara admite la resolución especificada:

HKEY\_CURRENT\_USER\Software\Citrix\HDXRealTime

Nombre: DefaultWidth

Tipo: REG\_DWORD

Datos (decimales): Anchura deseada (por ejemplo, 1280)

Nombre: DefaultHeight

Tipo: REG\_DWORD

Datos (decimales): Altura deseada (por ejemplo, 720)

## Redirección de USB genérico Plug-n-Play de HDX

La redirección de USB genérico Plug-n-Play de HDX (isócrona) también se denomina modo de cámara web **genérico**. La ventaja de la redirección de USB genérico de HDX Plug-n-Play es que no es necesario instalar controladores en el cliente ligero o el dispositivo de punto final. La pila USB está virtualizada, de modo que todo lo que conecte al cliente local se envía a la máquina virtual remota. El escritorio remoto actúa como si lo hubiera conectado al entorno nativo. El escritorio Windows se ocupa de toda la interacción con el hardware, y se ejecuta siguiendo la lógica Plug-n-Play para buscar los controladores correctos. La mayoría de las cámaras web funcionan si los controladores existen y pueden funcionar sobre ICA. El modo genérico de cámara web consume mucho más ancho de banda (muchos megabits por segundo) porque se envían vídeos sin comprimir con el protocolo USB a través de la red.

## Redirección multimedia HTML5

June 27, 2024

La redirección multimedia HTML5 amplía las funciones de redirección multimedia de HDX MediaStream para incluir audio y vídeo de HTML5. Debido al aumento de la distribución en línea de contenido multimedia, sobre todo para dispositivos móviles, la industria de exploración ha desarrollado métodos más eficientes para presentar audio y vídeo.

Flash ha sido el estándar, pero requiere un complemento, no funciona en todos los dispositivos y resulta en un mayor uso de batería en los dispositivos móviles. Empresas como YouTube o Netflix, y versiones más recientes de los exploradores de Mozilla, Google y Microsoft están migrando a HTML5, con lo que HTML5 se convierte en el nuevo estándar.

El contenido multimedia basado en HTML5 presenta muchas ventajas frente los plug-ins propietario, incluidos:

- Estándares independientes de empresas (W3C)
- Flujo de trabajo simplificado para la administración de los derechos digitales (DRM)
- Mejor rendimiento sin los problemas de seguridad que implican los complementos

### **Descargas progresivas HTTP**

La descarga progresiva HTTP es un método de semidistribución por streaming basado en HTTP que admite HTML5. En una descarga progresiva, el explorador web reproduce un solo archivo (codificado con una sola calidad) mientras ese archivo se descarga desde un servidor web HTTP. El vídeo se almacena en el disco tal cual se recibe, y se reproduce desde ese disco. Si vuelve a reproducir el vídeo, el explorador web puede cargar el vídeo desde la memoria caché.

Para ver un ejemplo de descarga progresiva, consulte la [página para pruebas de redirección de vídeo HTML5](#). Utilice las herramientas de desarrollo que facilita su explorador web para inspeccionar los elementos de vídeo en la página web y buscar los orígenes (un formato de contenedor mp4) en la etiqueta de vídeos HTML5:

### **Comparación entre HTML5 y Flash**

---

Función	HTML5	Flash
Requiere un reproductor propietario	No	Sí
Se ejecuta en dispositivos móviles	Sí	Algunos
Velocidad de ejecución en distintas plataformas	Alto	Lento
Compatible con iOS	Sí	No
Consumo de recursos	Menos	Más
Carga más rápida	Sí	No

---

## Requisitos

Solo se admite la redirección para las descargas progresivas en formato mp4. No se admiten tecnologías de streaming WebM y Adaptive bitrate, como DASH/HLS.

Se admite lo siguiente, y se utilizan directivas para controlarlo. Para obtener más información, consulte [Configuraciones de directiva Multimedia](#).

- Generación en el lado del servidor
- Obtención en servidor, generación en cliente
- Obtención y generación en el lado del cliente

Versiones mínimas de la aplicación Citrix Workspace y Citrix Receiver:

- Aplicación Citrix Workspace para Windows 1808
- Citrix Receiver para Windows 4.5
- Aplicación Citrix Workspace 1808 para Linux
- Citrix Receiver para Linux 13.5

---

Versión mínima del explorador web en el VDA	SO Windows versión/compilación/SP
Internet Explorer 11.0	Windows 10 x86 (1607 RS1) y x64 (1607 RS1); Windows 7 x86 y x64; Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2
Firefox 47 Debe agregar manualmente los certificados al almacén de certificados de Firefox o configurar Firefox para buscar certificados provenientes de un almacén de certificados de confianza de Windows. Para obtener más información, consulte <a href="https://wiki.mozilla.org/CA:AddRootToFirefox">https://wiki.mozilla.org/CA:AddRootToFirefox</a>	Windows 10 x86 (1607 RS1) y x64 (1607 RS1); Windows 7 x86 y x64; Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2
Chrome 51	Windows 10 x86 (1607 RS1) y x64 (1607 RS1); Windows 7 x86 y x64; Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2

---

## Componentes de la solución de redirección de vídeo HTML5

- **HdxVideo.js:** Enlace de JavaScript que intercepta los comandos vídeo en el sitio web. HdxVideo.js se comunica con WebSocketService mediante Secure WebSockets (SSL/TLS).
- **Certificados SSL de WebSocket**

- Para la CA (raíz): **Citrix XenApp/XenDesktop HDX In-Product CA** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX In-Product CA)  
Ubicación: Certificados (Equipo local) > Entidades de certificación raíz de confianza > Certificados.
  - Para la entidad final (hoja): **Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX Service)  
Ubicación: Certificados (Equipo local) > Personal > Certificados.
- **WebSocketService.exe:** Se ejecuta en el sistema local y realiza la terminación SSL y la asignación de sesiones de usuario. TLS Secure WebSocket escucha en 127.0.0.1 en el puerto 9001.
  - **WebSocketAgent.exe:** Se ejecuta en la sesión del usuario y genera el vídeo según las instrucciones de los comandos de WebSocketService.

## Cómo habilito la redirección de vídeo HTML5

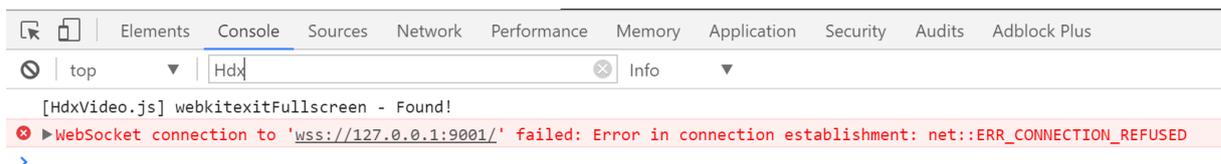
En esta versión, esta funcionalidad está disponible solo para las páginas web controladas. Requiere que se agregue HdxVideo.js de JavaScript (incluido en los medios de instalación de Citrix Virtual Apps and Desktops) a las páginas web donde está disponible el contenido multimedia HTML5. Por ejemplo: vídeos en un sitio de formación interna.

Los sitios como youtube.com, que están basados en tecnologías de velocidad de bits adaptable, como HTTP Live Streaming (HLS) y Dynamic Adaptive Streaming over HTTP (DASH), no se admiten.

Para obtener más información, consulte [Configuraciones de directiva Multimedia](#).

## Sugerencias para solucionar problemas

Pueden producirse errores cuando la página web intenta ejecutar HdxVideo.js. Si JavaScript no se puede cargar, se produce un error en el mecanismo de redirección de HTML5. Debe comprobar que no hay errores relacionados con HdxVideo.js. Para ello, examine la consola en las ventanas de herramientas de desarrolladores del explorador web. Por ejemplo:



## Optimización para Microsoft Teams

June 27, 2024

**Importante:**

La optimización para Microsoft Teams requiere la versión 1.2.00.31357 de Microsoft Teams o una posterior.

Citrix ofrece la optimización para Microsoft Teams de escritorio mediante Citrix Virtual Apps and Desktops y la aplicación Citrix Workspace. De forma predeterminada, agrupamos todos los componentes necesarios en la aplicación Citrix Workspace y en Virtual Delivery Agent (VDA).

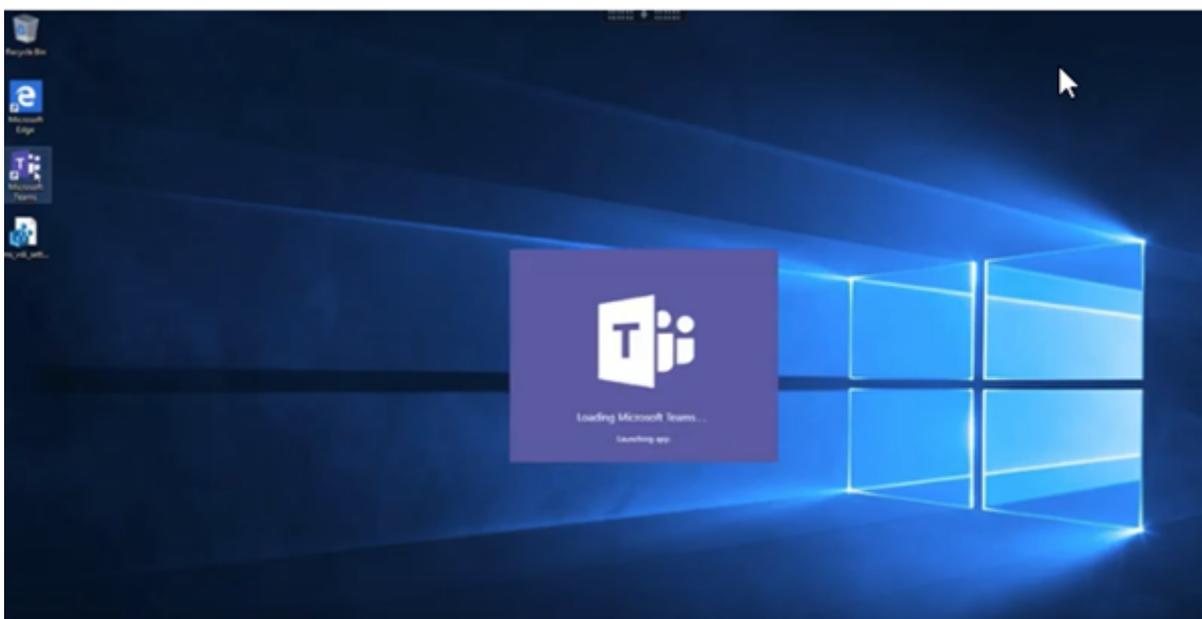
Nuestra optimización para Microsoft Teams contiene una API y servicios de HDX del lado de VDA para interactuar con la aplicación alojada Teams y recibir comandos. Estos componentes abren un canal virtual de control (CTXMTOP) en el motor de medios de la aplicación Citrix Workspace. El dispositivo de punto final descodifica y genera el contenido multimedia de manera local, y devuelve la ventana de la aplicación Citrix Workspace a la aplicación Microsoft Teams alojada.

La autenticación y la señalización se producen de forma nativa en la aplicación alojada de Microsoft Teams, al igual que los demás servicios de Microsoft Teams (por ejemplo, el chat o la colaboración). La redirección de audio/vídeo no les afecta.

**CTXMTOP** es un canal virtual de comando y control. Esto significa que los medios no se intercambian entre la aplicación Citrix Workspace y el VDA.

Solo la obtención del cliente/generación del cliente está disponible.

Este vídeo de demostración le da una idea de cómo funciona Microsoft Teams en un entorno virtual Citrix.



## Instalación de Microsoft Teams

### Nota:

Recomendamos instalar el VDA antes de instalar Teams en la imagen dorada. Este orden de instalación es necesario para que el indicador **ALLUSER=1** surta efecto. Si la máquina virtual tenía Teams instalado antes de instalar el VDA, desinstale Teams y vuelva a instalarlo. Si utiliza App Layering, consulte las instrucciones de App Layering al final de esta sección para obtener más detalles.

Le recomendamos que siga las [directrices de instalación para toda la máquina de Microsoft Teams](#) y que no utilice el instalador .exe que instala Teams en AppData. En su lugar, instálelo en `C:\Program Files (x86)\Microsoft\Teams` con el indicador **ALLUSER=1** desde la línea de comandos.

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1  
ALLUSERS=1
```

En este ejemplo también se utiliza el parámetro **ALLUSERS=1**. Al establecer este parámetro, el instalador de Teams a nivel de equipo aparece en **Programas y características** en el Panel de control y en **Aplicaciones y características** en Configuración de Windows para todos los usuarios del equipo. Todos los usuarios pueden desinstalar Teams si tienen credenciales de administrador. Es importante entender la diferencia entre **ALLUSERS=1** y **ALLUSER=1**. Puede utilizar el parámetro **ALLUSERS=1** en entornos VDI y no VDI. Utilice el parámetro **ALLUSER=1** solo en entornos VDI para especificar una instalación por máquina.

En el modo **ALLUSER=1**, la aplicación Teams no se actualiza automáticamente cuando hay una nueva

versión. Recomendamos este modo para entornos no persistentes. Por ejemplo, aplicaciones o escritorios compartidos alojados fuera de catálogos aleatorios/agrupados de Windows Server o Windows 10. Para obtener más información, consulte [Instalar Microsoft Teams mediante MSI](#) (sección Instalación de VDI).

Tiene entornos VDI persistentes dedicados en Windows 10. Quiere que la aplicación Teams se actualice automáticamente y preferiría que Teams se instalara por usuario en `Appdata/Local`, utilice el instalador `.exe` o MSI sin **ALLUSER=1**.

### Para App Layering:

#### ADVERTENCIA:

Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Cree una clave de Registro vacía llamada `PortICA` (deje el nombre, el tipo y los datos predeterminados).

Si utiliza Citrix App Layering para administrar instalaciones de VDA y Microsoft Teams en diferentes capas, implemente esta clave de Registro en Windows antes de instalar Teams con **ALLUSER =1**:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA
```

O bien:

```
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\PortICA
```

## Recomendaciones para Profile Management

Se recomienda utilizar el instalador a nivel de equipo para entornos Windows Server y VDI agrupados de Windows 10.

Cuando el indicador **ALLUSER =1** se transfiere al MSI desde la línea de comandos (instalador a nivel de equipo), la aplicación Teams se instala en `C:\Program Files (x86)` (~ 300 MB). La aplicación utiliza `AppData\Local\Microsoft\TeamsMeetingAddin` para los registros y `AppData\Roaming\Microsoft\Teams` (~600–700 MB) para configuraciones específicas de usuario, almacenamiento en caché de elementos de la interfaz de usuario, etc.

### Instalador a nivel de equipo

A continuación, se muestra un ejemplo de carpetas, accesos directos de escritorio y registros creados al instalar el instalador a nivel de equipo de Teams en una máquina virtual Windows Server 2016 de

64 bits:

*Carpeta:*

- C:\Program Files (x86)\Microsoft\Teams
- C:\Users\\AppData\Roaming\Microsoft\Teams

*Acceso directo de escritorio:*

C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe

*Registro:*

- HKEY\_LOCAL\_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run
- HKEY\_LOCAL\_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKEY\_CURRENT\_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run

## Recomendaciones

- Recomendamos inhabilitar el inicio automático eliminando las claves de Registro de Teams. Al hacerlo, se evita el repunte de “avalanchas de inicio de sesión de las 8 de la mañana” en la CPU de la máquina virtual.
- Si el escritorio virtual no tiene una GPU/vGPU, se recomienda **Deshabilitar la aceleración de hardware de GPU** en la **Configuración** de Teams para mejorar el rendimiento. Esta configuración ("**disableGpu**":**true**) se almacena %Appdata%\Microsoft\Teams, en el archivo `desktop-config.json`. Puede utilizar un script de inicio de sesión para modificar ese archivo y establecer el valor en true.
- Si utiliza Citrix Workspace Environment Management (WEM), habilite la **protección contra picos de CPU** para administrar el consumo de procesador para Teams.

### Importante:

Si no transfiere el indicador **ALLUSER=1**, el MSI coloca el instalador Teams.exe y `setup.json` en C:\Program Files (x86)\Teams Installer.

Se agrega una clave del Registro (TeamsMachineInstaller) en:

```
HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run
```

Un inicio de sesión de usuario posterior desencadena la instalación final en **AppData** en su lugar.

## Instalador por usuario

Al usar el instalador `.exe`, el proceso de instalación cambia significativamente y todos los archivos se colocan en AppData.

*Carpeta:*

- `C:\Users\\AppData\Local\Microsoft\Teams`
- `C:\Users\\AppData\Local\Microsoft\TeamsPresenceAddin`
- `C:\Users\\AppData\Local\Microsoft\TeamsMeetingAddin`
- `C:\Users\\AppData\Local\SquirrelTemp`
- `C:\Users\\AppData\Roaming\Microsoft\Teams`

*Acceso directo de escritorio:*

```
C:\Users\\AppData\Local\Microsoft\Teams\Update.exe --processStart "Teams.exe"
```

*Registro:*

```
HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

## **Prácticas recomendadas**

Las recomendaciones se basan en supuestos de casos de uso.

El uso de Teams con una configuración no persistente requiere un administrador de almacenamiento en caché de perfiles para una sincronización eficiente de los datos de runtime de Teams. Un administrador de almacenamiento en caché de perfiles garantiza que la información específica del usuario necesaria (por ejemplo, datos de usuario, perfil y configuración) se almacene en caché durante la sesión de usuario. Asegúrese de sincronizar los datos de estas dos carpetas:

- `C:\Users\\AppData\Local\Microsoft\IdentityCache`
- `C:\Users\\AppData\Roaming\Microsoft\Teams`

## **Lista de exclusión de contenido almacenado en caché de Teams para una configuración no persistente:**

Excluya los siguientes elementos de la carpeta de almacenamiento en caché de Teams: `%AppData%\Microsoft\Teams`. Excluir estos elementos ayuda a reducir el tamaño del almacenamiento en caché del usuario para optimizar aún más la configuración no persistente.

Lista de exclusión de archivos

- `Roaming\Microsoft\Teams\* .txt`

Lista de exclusión de directorios

- `Roaming\Microsoft\Teams\Logs`
- `Roaming\Microsoft\Teams\media-stack`
- `Roaming\Microsoft\Teams\Service Worker\CacheStorage`
- `Roaming\Microsoft\Teams\Application Cache`

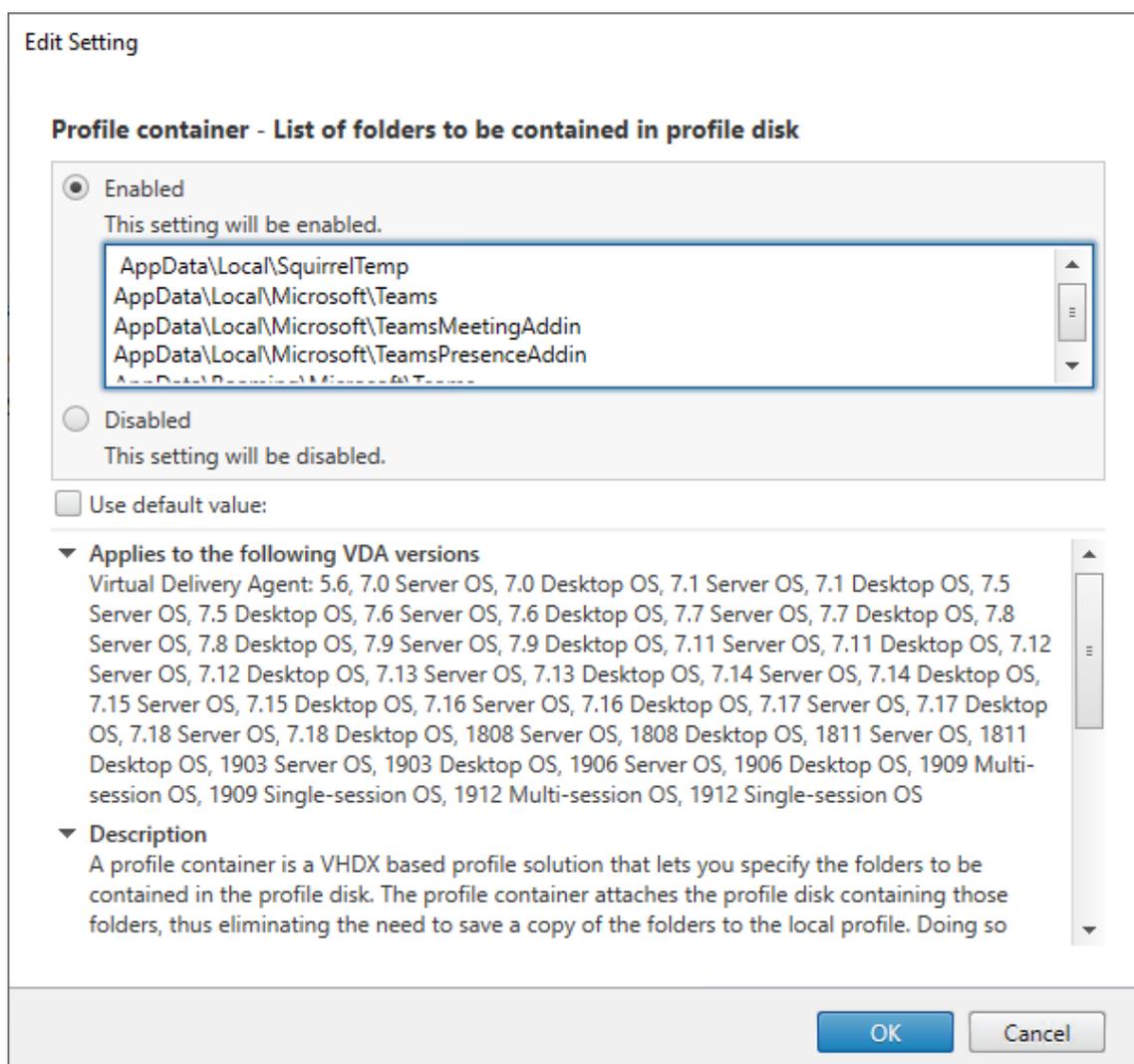
- Roaming\Microsoft\Teams\Cache
- Roaming\Microsoft\Teams\GPUCache
- Roaming\Microsoft\Teams\meeting-addin\Cache (esencial cuando falta el complemento en Outlook)

#### **Caso de uso: supuesto de sesión única:**

En este caso, el usuario final utiliza Microsoft Teams en una ubicación cada vez. No es necesario ejecutar Teams en dos sesiones diferentes de Windows simultáneamente. Por ejemplo, en una implementación de escritorio virtual común, cada usuario se asigna a un escritorio y Teams se implementa dentro del escritorio virtual como una aplicación.

Se recomienda habilitar el contenedor de perfiles de Citrix y redirigir los directorios “por usuario” mencionados anteriormente al contenedor.

1. Implemente el instalador a nivel de equipo de Microsoft Teams (**ALLUSER=1**) en la imagen maestra.
2. Habilite Citrix Profile Management y configure el almacén de perfiles de usuario con los permisos adecuados.
3. Habilite la siguiente configuración de directiva de Profile Management: **Sistema de archivos > Sincronización > Contenedor de perfiles —Lista de carpetas que se incluirán en el disco de perfiles.**



Indique todas las carpetas mencionadas anteriormente en esta configuración. También puede configurar estas opciones a través del servicio Citrix Workspace Environment Management (WEM).

4. Aplique la configuración al grupo de entrega correspondiente.
5. Inicie sesión para validar la implementación.

## Requisitos del sistema

**Versión mínima recomendada: Delivery Controller (DDC) 1906.2 (si utiliza una versión anterior, consulte [Habilitar la optimización de Microsoft Teams](#)):**

Sistemas operativos compatibles:

- Windows Server 2019, 2016, 2012R2 ediciones Standard y Datacenter, y con opción Server Core

### **Versión mínima: Virtual Delivery Agent (VDA) 1906.2:**

Sistemas operativos compatibles:

- Windows 10 de 64 bits, versión 1607 y versiones posteriores. (Las aplicaciones alojadas en VM no son compatibles).
- Windows Server 2019, 2016 y 2012 R2 (ediciones Standard y Datacenter).

Requisitos:

- BCR\_x64.msi: El MSI que contiene el código de optimización de Microsoft Teams y se inicia automáticamente desde la GUI. Si utiliza la interfaz de línea de comandos para la instalación de VDA, no la excluya.

### **Versión recomendada: aplicación Citrix Workspace 2006.1 para Windows; versión mínima: aplicación Citrix Workspace 1907 para Windows:**

- Windows 7, 8 y 10 (ediciones de 32 y 64 bits, incluida las ediciones Embedded)
- Windows 10 IoT Enterprise 2016 LTSB (versión 1607) y 2019 LTSC (versión 1809)
- Arquitecturas de procesador (CPU) compatibles: x86 y x64 (ARM no es compatible)
- Requisito del dispositivo de punto final: CPU dual de aproximadamente 2,2-2,4 GHz que puede admitir una resolución HD de 720p durante una llamada de conferencia en vídeo de punto a punto.
- CPU de núcleo doble o cuádruple con velocidades base más bajas (unos 1,5 GHz) equipadas con Intel Turbo Boost o AMD Turbo Core que pueden aumentar hasta al menos 2,4 GHz.
- Clientes ligeros HP verificados: t630/t640, t730/t740, mt44/mt45.
- Clientes ligeros Dell verificados: 5070/5470 Mobile TC.
- Clientes ligeros 10ZiG verificados: 4510 y 5810q.
- Para obtener una lista completa de dispositivos de punto final verificados, consulte [Clientes ligeros](#).
- La aplicación Citrix Workspace requiere un mínimo de 600 MB de espacio libre en el disco y 1 GB de RAM.
- El requisito mínimo de Microsoft .NET Framework es la versión 4.6.2. La aplicación Citrix Workspace descarga e instala automáticamente .NET Framework si no está presente en el sistema.

### **Versión mínima: Aplicación Citrix Workspace 2006 para Linux:**

Para obtener más información, consulte la sección [Optimización para Microsoft Teams](#) en la documentación de la aplicación Citrix Workspace para Linux.

Software:

- GStreamer 1.0 o una versión posterior o Cairo 2
- libc++-9.0 o una versión posterior
- libgdk 3.22 o una versión posterior

- OpenSSL 1.1.1d
- Distribución de Linux x64

Hardware:

- Como mínimo una CPU de doble núcleo de 1,8 GHz que admita una resolución de 720p HD durante llamadas de conferencias en vídeo de punto a punto.
- CPU de doble o cuádruple núcleo con una velocidad base de 1,8 GHz y una velocidad Intel Turbo Boost alta de al menos 2,9 GHz.

Para obtener más información, consulte [Requisitos previos para instalar la aplicación Citrix Workspace](#).

### **Versión mínima: Aplicación Citrix Workspace 2012 para Mac:**

Sistemas operativos compatibles

- macOS Catalina (10.15)
- macOS Big Sur Beta 8 solo en entornos de prueba. No utilizar en entornos de producción.

Funciones compatibles:

- Audio
- Vídeo
- Optimización para compartir pantalla (entrante y saliente)

La optimización para Teams funciona de forma predeterminada si el usuario tiene la aplicación Citrix Workspace 2012 o una versión posterior y macOS 10.15.

Si quiere desactivar la optimización de Teams, ejecute este comando en el terminal y reinicie la aplicación Workspace:

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

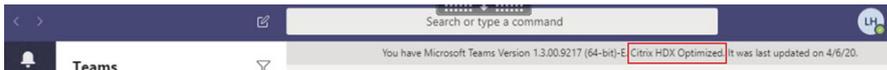
### **Habilitar la optimización de Microsoft Teams**

Para habilitar la optimización de Microsoft Teams, utilice la directiva de Studio descrita en la [directiva de redirección de Microsoft Teams](#) (está **ACTIVADA** de forma predeterminada). Además de habilitar esta directiva, HDX comprueba si la versión de la aplicación Citrix Workspace es igual o mayor que la versión mínima requerida. Si se ha habilitado la directiva y se admite la versión de la aplicación Citrix Workspace, **HKEY\_CURRENT\_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupport** se establece en **1** automáticamente en el VDA. La aplicación Microsoft Teams lee la clave para cargar en modo VDI.

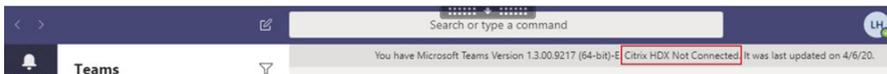
**Nota:**

Aunque utilice agentes VDA con la versión 1906.2 o una posterior con versiones anteriores de Controller (por ejemplo, la versión 7.15), que no tienen la directiva disponible en Studio, puede seguir utilizando la optimización HDX para Microsoft Teams porque está habilitada de forma predeterminada en el VDA.

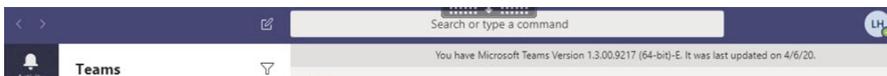
Si hace clic en **Acerca de > Versión**, aparecerá la leyenda **Optimizado para Citrix HDX**:



Si en su lugar aparece que **Citrix HDX no está conectado**, la API de Citrix se carga en Teams (que es el primer paso hacia la redirección), pero se produjo un error en secciones posteriores de la pila. Es muy probable que el error esté en los servicios de VDA o en la aplicación Citrix Workspace.



Si no aparece ninguna leyenda, Teams no pudo cargar la API de Citrix. Salga de Teams haciendo clic con el botón secundario en el icono del área de notificaciones y reinicie. Asegúrese de que la directiva de Studio no esté establecida en **Prohibido** y de que la versión de la aplicación Citrix Workspace sea compatible.



## Requisitos de la red

Microsoft Teams se basa en servidores Media Processor (procesador de multimedia) en Office 365 para las reuniones o llamadas con múltiples participantes. Microsoft Teams se basa en Transport Relay (traspaso de transporte) de Office 365 para los siguientes supuestos:

- Dos pares en una llamada punto a punto sin conectividad directa
- Un participante no tiene conectividad directa con el procesador de multimedia.

Por lo tanto, el estado de la red entre el par y la nube de Office 365 determina el rendimiento de la llamada.

Se recomienda analizar el entorno para identificar los riesgos y los requisitos que puedan influir en la implementación general de voz y vídeo en la nube.

Utilice la [Herramienta de evaluación de la red de Skype Empresarial](#) para comprobar si la red está lista para Microsoft Teams. Para obtener información sobre asistencia, consulte [Asistencia](#).

### Resumen de las recomendaciones de red clave para el tráfico con protocolo de transporte en tiempo real (RTP):

- Conéctese a la red de Office 365 de la forma más directa posible desde la sucursal.
- Si debe utilizar cualquiera de las siguientes opciones en la sucursal, asegúrese de que el tráfico RTP/UDP de Teams no tenga obstáculos. HdxTeams.exe no respeta los proxies explícitos configurados en el dispositivo de punto final.
  - Omitir servidores proxy
  - Interceptación SSL de red
  - Dispositivos de inspección profunda de paquetes (PPP)
  - Bifurcaciones VPN (utilice túnel dividido si es posible)
- Planifique y proporcione suficiente ancho de banda.
- Compruebe la conectividad y la calidad de la red en cada sucursal.

El motor multimedia WebRTC en la aplicación Workspace (HdxTeams.exe) utiliza el protocolo de transporte seguro en tiempo real (SRTP) para transmisiones multimedia que se descargan en el cliente. SRTP proporciona confidencialidad y autenticación a RTP mediante el uso de claves simétricas (128 bits) para cifrar el contenido multimedia y los mensajes de control, y utiliza el cifrado AES con modo de contador.

Para garantizar una experiencia de usuario positiva, se recomiendan las siguientes métricas:

Métrica	Dispositivo de punto final a Office 365
Latencia (ida)	< 50 ms
Latencia (RTT)	< 100 ms
Pérdida de paquetes	< 1% durante cada intervalo de 15 segundos
Fluctuación entre la llegada de paquetes	< 30 ms durante cada intervalo de 15 segundos

Para obtener más información, consulte [Preparación de la red de la organización para Microsoft Teams](#).

En cuanto a requisitos de ancho de banda, la optimización para Microsoft Teams puede utilizar una amplia variedad de códecs para audio (OPUS/G.722/PCM G711) y vídeo (H264/VP9).

Los pares negocian estos códecs durante el proceso de establecimiento de llamadas mediante la oferta/respuesta de Session Description Protocol (SDP).

Las recomendaciones mínimas de Citrix por usuario son:

Tipo	Ancho de banda	Códec
Audio (en cada sentido)	~ 90 Kbps	G.722

---

Tipo	Ancho de banda	Códec
Audio (en cada sentido)	~ 60 Kbps	Opus*
Vídeo (en cada sentido)	~ 700 Kbps	H264 360p @ 30 fps 16:9
Vídeo (en cada sentido)	~ 2500 Kbps	VP9 720p @ 30 fps 16:9
Pantalla compartida	~ 300 Kbps	H.264 1080p @ 15 fps

---

\* Opus admite codificación de velocidad de bits constante y variable desde 6 kbps hasta 510 kbps.

Opus y VP9 son los códecs preferidos para llamadas de punto a punto entre dos usuarios VDI optimizados.

G.722 y H264 son los códecs preferidos para un usuario de VDI que se une a una reunión.

### Citrix Gateway

La presencia de Citrix Gateway local o Citrix Gateway Service como proxy HDX no afecta a la optimización de Microsoft Teams. Esto se debe a que solo hay un canal virtual de comando y control establecido entre la aplicación Workspace y el VDA.

Todas las transmisiones de audio o vídeo se descargan al cliente para su procesamiento local. Como resultado, no hay generación en el lado del servidor.

Según la configuración de su entorno, el canal virtual de comando y control fluye a través de Citrix Gateway mediante uno de estos métodos:

- TLS para TCP
- DTLS para EDT

Si también usa Citrix Gateway para VPN, asegúrese de permitir que la máquina cliente contacte directamente con los servidores de Microsoft Teams de O365. Esto se puede lograr mediante túneles divididos u otros métodos.

### Servidores proxy

Según la ubicación del proxy, tenga en cuenta lo siguiente:

- Configuración del proxy en el VDA:

Si configura un servidor proxy explícito en el VDA y dirige las conexiones al host local a través de un proxy, la redirección falla. Para configurar el proxy correctamente, debe seleccionar la configuración **Omitir servidor proxy para las direcciones locales** en **Opciones**

**de Internet > Conexiones > Configuración de LAN > Servidores proxy** y comprobar que 127.0.0.1:9002 se omite.

Si utiliza un archivo PAC, el script de configuración del proxy de VDA del archivo PAC debe devolver **DIRECT** para `wss://127.0.0.1:9002`. Si no, la optimización falla. Para asegurarse de que el script devuelva **DIRECT**, utilice `shExpMatch(url, "wss://127.0.0.1:9002/*")`.

- Configuración del proxy en la aplicación Citrix Workspace:

Si la sucursal está configurada para acceder a Internet a través de un proxy, la versión 2012 de la aplicación Citrix Workspace para Windows (Negotiate/Kerberos, NTLM, Basic y Digest), la versión 2101 de la aplicación Citrix Workspace para Linux (autenticación anónima) y la versión 2104 de la aplicación Citrix Workspace para Mac (autenticación anónima) admite servidores proxy. Los dispositivos cliente con versiones anteriores de la aplicación Citrix Workspace no pueden leer configuraciones de proxy. Estos dispositivos envían tráfico directamente a los servidores TURN de Office 365.

**Importante:**

Compruebe que el dispositivo cliente se puede conectar al servidor DNS para llevar a cabo resoluciones DNS. Un dispositivo cliente debe poder resolver tres FQDN del servidor TURN de Microsoft Teams: `worldaz.turn.teams.microsoft.com`, `usaz.turn.teams.microsoft.com` y `euaz.turn.teams.microsoft.com`.

## Establecimiento de llamadas y rutas de flujo de medios

Cuando sea posible, el motor de medios HDX de la aplicación Citrix Workspace (HdxTeams.exe) intenta establecer una conexión SRTP (protocolo de transporte seguro en tiempo real) de red directa mediante el protocolo de datagramas de usuario (UDP) en una llamada de un par homólogo a otro. Si los puertos UDP están bloqueados, el motor de medios recurre a TCP 443.

El motor de contenido multimedia HDX admite ICE, el protocolo STUN (Session Traversal Utilities for NAT) y el protocolo TURN (Traversal Using Relays around NAT) para la detección de candidatos y el establecimiento de conexiones.

Si no hay una ruta directa entre los dos pares o entre un par y un servidor de conferencias (si el usuario se une a una reunión o llamada con múltiples participantes), HdxTeams.exe utiliza un servidor de traspaso de transporte de Microsoft Teams en Office 365 para llegar al otro par o al procesador de multimedia (donde se alojan las reuniones). La máquina cliente del usuario debe tener acceso a dos intervalos de direcciones IP de subred de Office 365 y a 4 puertos UDP. Para obtener más información, consulte el diagrama de arquitectura en la sección “Configuración de llamadas” más adelante y [Direcciones URL e intervalos de direcciones IP de ID 11 para Office 365](#).

ID	Categoría	Direcciones	Puertos de destino
11	Precisa optimización	13.107.64.0/18, 52.112.0.0/14, 52.120.0.0/14	<b>UDP:</b> 3478, 3479, 3480, 3481, <b>TCP:</b> 443 (reserva)

Estos intervalos contienen tanto servidores de traspaso de transporte como procesadores de multimedia.

Los servidores de traspaso de transporte de Teams proporcionan funciones STUN y TURN, pero no son dispositivos de punto final ICE. Además, los servidores de traspaso de transporte de Teams no finalizan el contenido multimedia ni realizan ninguna transcodificación. Pueden puentear TCP (si HdxTeams.exe utiliza TCP) a UDP cuando reenvían tráfico a otros pares o procesadores de multimedia.

HdxTeams.exe conecta con el servidor de traspaso de transporte de Microsoft Teams más cercano en la nube de Office 365. HdxTeams.exe utiliza la técnica IP Anycast y los puertos UDP 3478 a 3481 (puertos UDP diferentes por carga de trabajo, aunque puede haber multiplexación) o el puerto TCP 443 con TLS 1.2 de reserva. La calidad de la llamada depende del protocolo de red subyacente. Debido a que siempre se recomienda UDP antes que TCP, se recomienda diseñar las redes para dar cabida al tráfico UDP en la sucursal.

Si Teams se carga en modo optimizado y HdxTeams.exe se está ejecutando en el terminal, los errores de establecimiento interactivo de conectividad (ICE) pueden provocar un error de configuración de llamada o transmisión de audio/vídeo en una sola dirección. Cuando no se pueda completar una llamada o las secuencias multimedia no sean dúplex completo, compruebe primero la **traza Wireshark** en el dispositivo de punto final.

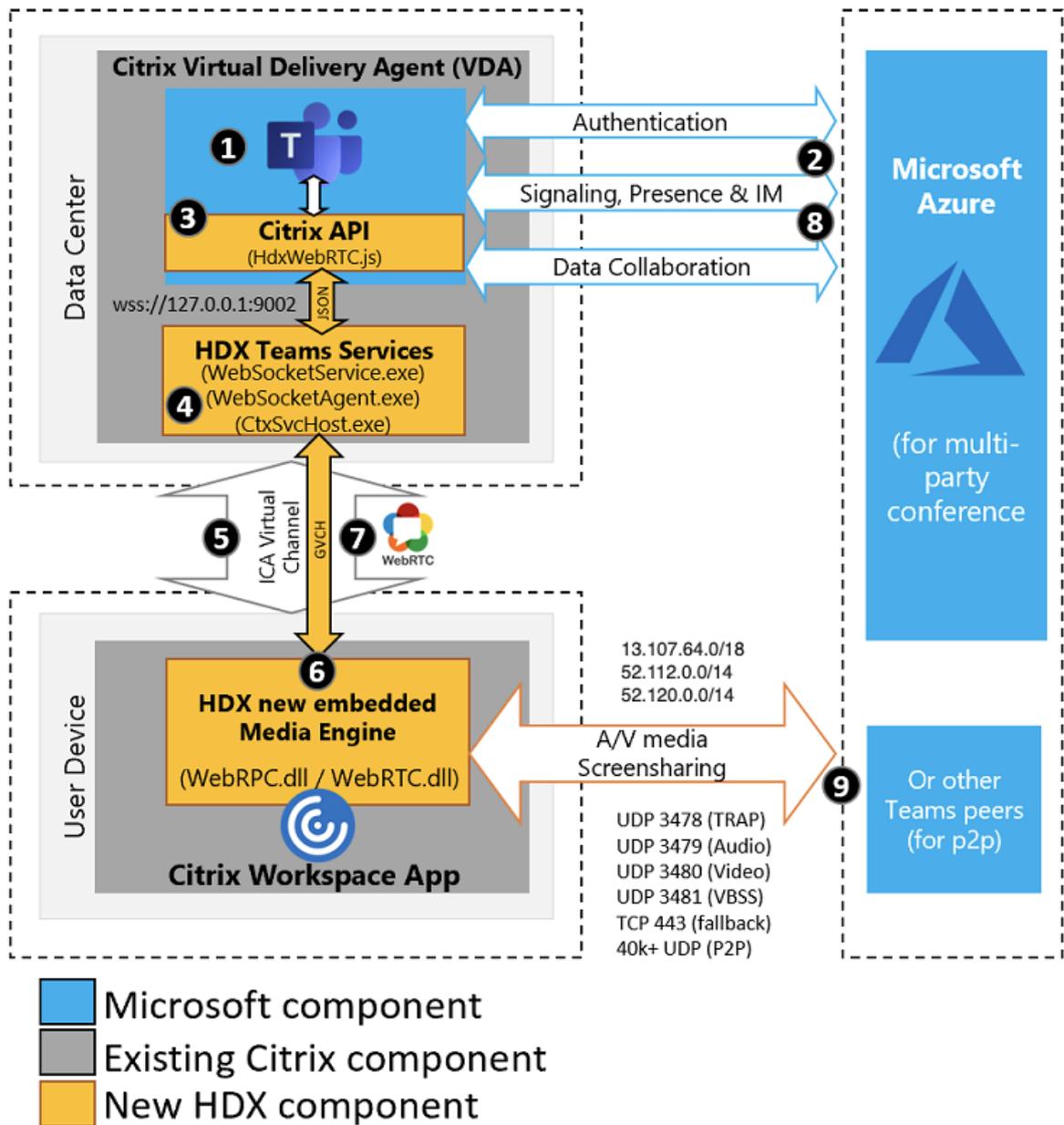
**Nota:**

Si los dispositivos de punto final no tienen acceso a Internet, es posible que el usuario solo pueda realizar una llamada de un par homólogo a otro si están en la misma red de área local (LAN). Las reuniones no funcionan. En este caso, hay un tiempo de espera de 30 segundos antes de que comience la configuración de la llamada.

**Configuración de llamadas**

Utilice este diagrama de arquitectura como referencia visual para la secuencia del flujo de llamadas. Los pasos correspondientes se indican en el diagrama.

**Arquitectura:**



1. Inicie Microsoft Teams.
2. Teams se autentica en O365. Las directivas de arrendatario se envían al cliente de Teams, y la información pertinente del canal de señalización y del protocolo TURN se transmite a la aplicación.
3. Teams detecta que se ejecuta en un VDA y realiza llamadas API a la API de JavaScript de Citrix.
4. JavaScript de Citrix en Teams abre una conexión WebSocket segura con WebSocketService.exe en el VDA (127.0.0.1:9002), que genera WebSocketAgent.exe dentro de la sesión de usuario.
5. WebSocketAgent.exe crea una instancia de un canal virtual genérico mediante una llamada al servicio de redirección de Teams para Citrix HDX (CtxSvcHost.exe).

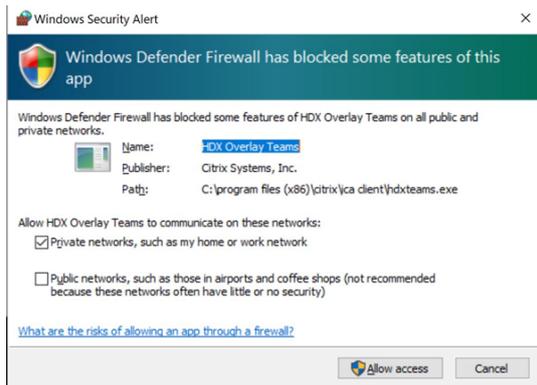
6. El archivo wfica32.exe (motor de HDX) de la aplicación Citrix Workspace genera un nuevo proceso denominado HdxTeams.exe, que es el nuevo motor de WebRTC utilizado para la optimización de Teams.
7. HdxTeams.exe y Teams.exe tienen una ruta bidireccional de canales virtuales y pueden comenzar a procesar solicitudes multimedia.  
  
——Llamadas de usuario——
8. El **interlocutor A** hace clic en el botón de **llamada**. Teams.exe se comunica con los servicios de Teams de Office 365 y establece una ruta de señalización de extremo a extremo con el **interlocutor B**. Teams solicita a HdxTeams una serie de parámetros de llamada admitidos (códecs, resoluciones, etc., lo que se conoce como una oferta de protocolo de descripción de sesiones o SDP). A continuación, estos parámetros de llamada se retransmiten mediante la ruta de señalización a los servicios de Teams en Office 365 y, desde allí, al otro interlocutor.
9. La oferta/respuesta SDP (negociación de paso único) tiene lugar a través del canal de señalización, y las comprobaciones de conectividad de ICE (recorrido de NAT y firewalls mediante el protocolo STUN) se completan. A continuación, el contenido multimedia con Secure Real-Time Transport Protocol (SRTP) circula directamente entre HdxTeams.exe y el otro interlocutor (o servidores de conferencia de Office 365 si se trata de una reunión).

## Sistema telefónico de Microsoft

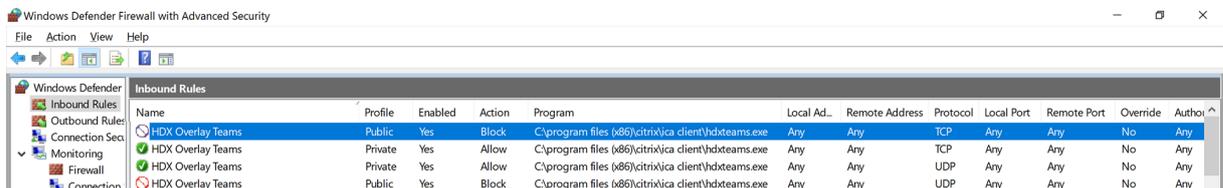
Sistema telefónico es la tecnología de Microsoft que permite el control de llamadas y las capacidades de central de conmutación (PBX) en la nube de Office 365 con Microsoft Teams. La optimización para Microsoft Teams es compatible con el sistema telefónico mediante planes de llamada de Office 365 o enrutamiento directo. Con Enrutamiento directo, puede conectar su propio controlador de borde de sesión (SBC) compatible directamente al sistema telefónico de Microsoft sin necesidad de software local adicional.

## Consideraciones sobre el firewall

Cuando los usuarios inician una llamada optimizada mediante el cliente de Microsoft Teams por primera vez, es posible que aparezca una advertencia relacionada con la configuración del **firewall de Windows**. En la advertencia, se pide a los usuarios que permitan la comunicación para HdxTeams.exe (HDX Overlay Teams).



Las cuatro entradas siguientes se agregan en **Reglas de entrada**, en la consola **Firewall de Windows Defender > Seguridad avanzada**. Puede aplicar reglas más restrictivas si lo quiere.

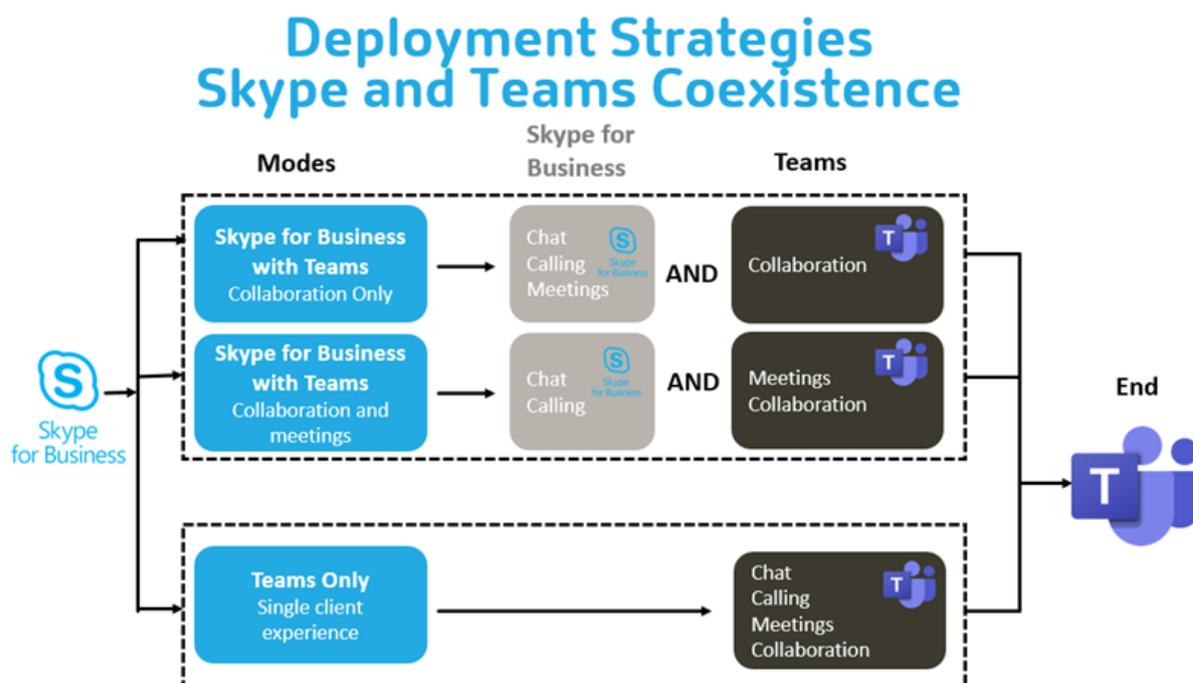


## Coexistencia de Microsoft Teams y Skype Empresarial

Puede implementar Microsoft Teams y Skype Empresarial en paralelo, como dos soluciones independientes con capacidades superpuestas. Para obtener más información, consulte [Coexistencia e interoperabilidad de Microsoft Teams y Skype Empresarial](#).

Citrix RealTime Optimization Pack y la optimización HDX para los motores multimedia de Teams respetan la configuración establecida en su entorno (por ejemplo, modos de isla, colaboración de Skype Empresarial con Teams, colaboración de Skype Empresarial con Teams, colaboración y reuniones de Skype Empresarial con Teams).

El acceso periférico solo se puede conceder a una sola aplicación a la vez. Por ejemplo, el acceso a la cámara web de parte de RealTime Media Engine durante una llamada bloquea el dispositivo de imágenes durante dicha llamada. Cuando el dispositivo se lanza, estará disponible para Teams.



### Citrix SD-WAN: conectividad de red optimizada para Microsoft Teams

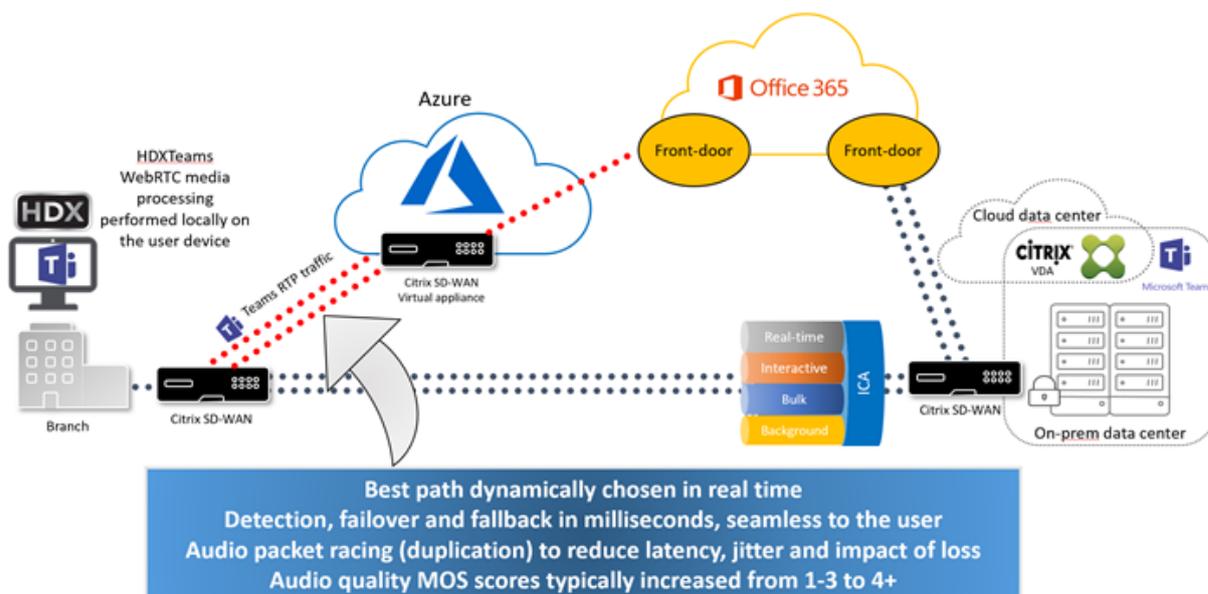
Para lograr una calidad de audio y vídeo óptima, se requiere una conexión de red a la nube de Office 365 que tenga baja latencia, baja vibración y baja pérdida de paquetes. El uso de una red de retorno (backhaul) para canalizar el tráfico RTP de audio y vídeo de Microsoft Teams desde los usuarios de la aplicación Citrix Workspace que se encuentran en sucursales a un centro de datos antes de dirigirlo a Internet puede agregar una latencia excesiva y también puede causar congestión en los vínculos WAN. Citrix SD-WAN optimiza la conectividad para Microsoft Teams siguiendo los principios de conectividad de red de Microsoft Office 365. Citrix SD-WAN utiliza la dirección IP y el servicio web de Office 365 basados en REST de Microsoft y DNS próximo para identificar, clasificar y dirigir el tráfico de Microsoft Teams.

Las conexiones de banda ancha empresarial de Internet en muchas áreas sufren pérdida intermitente de paquetes, períodos de vibración excesiva e interrupciones.

Citrix SD-WAN ofrece dos soluciones para preservar la calidad de audio y vídeo de Microsoft Teams cuando la red tiene un estado variable o degradado.

- Si utiliza Microsoft Azure, un dispositivo virtual Citrix SD-WAN (VPX) implementado en la red virtual de Azure ofrece optimizaciones de conectividad avanzadas. Estas optimizaciones incluyen conmutación por error de enlaces y duplicación de paquetes de audio.
- Como alternativa, los clientes de Citrix SD-WAN pueden conectarse a Office 365 a través del servicio Citrix Cloud Direct. Este servicio garantiza una entrega fiable y segura de todo el tráfico de Internet.

Si la calidad de la conexión a Internet de la sucursal no es un problema, puede ser suficiente para minimizar la latencia, al dirigir el tráfico de Microsoft Teams directamente desde el dispositivo de sucursal Citrix SD-WAN a la puerta delantera de Office 365 más próxima. Para obtener más información, consulte [Optimización de Citrix SD-WAN Office 365](#).



## Vista de galería y participantes activos en Microsoft Teams

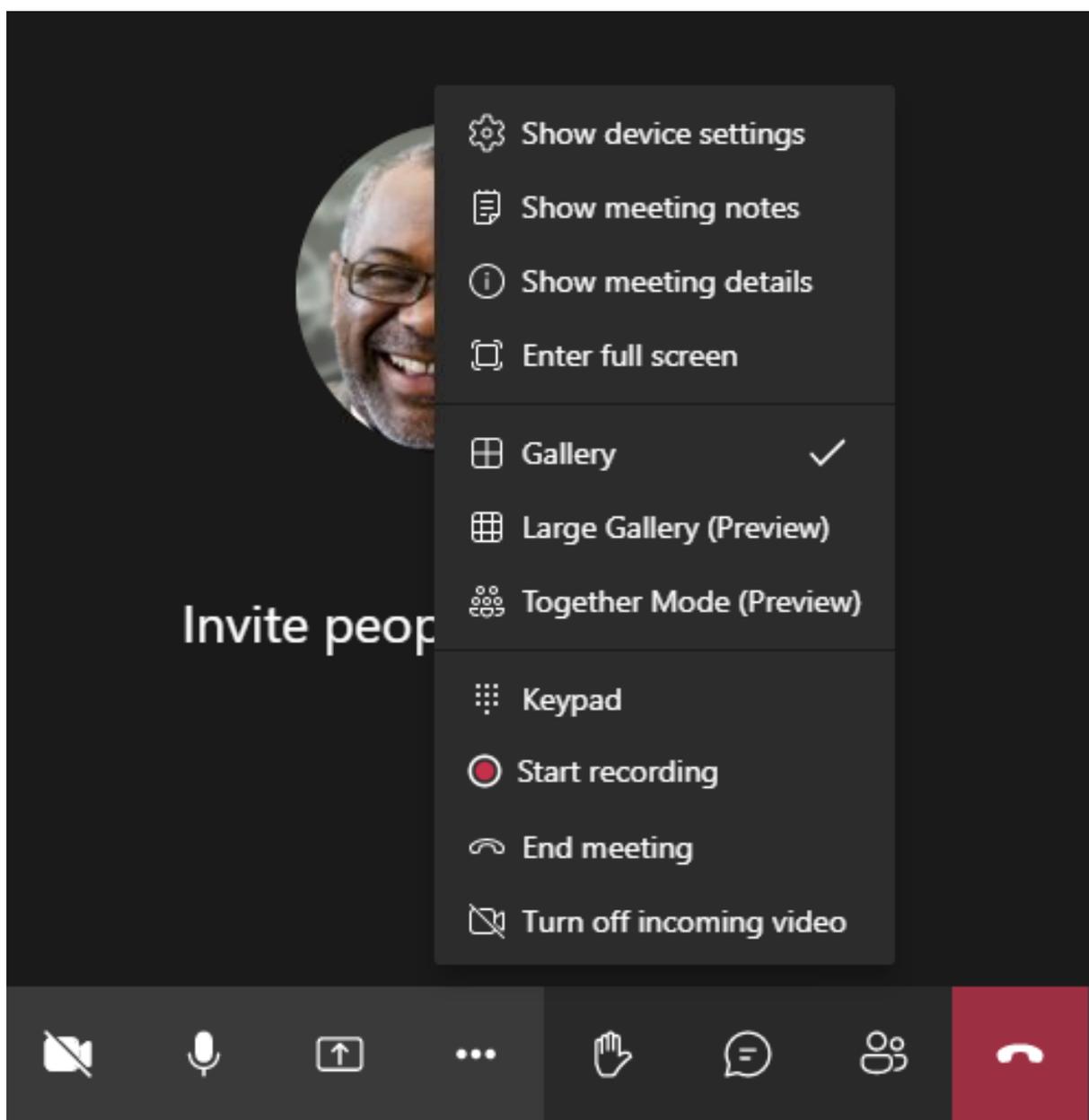
Microsoft Teams permite los modos **Gallery**, **Large Gallery** y **Together**.

Microsoft Teams muestra una cuadrícula 2x2 con secuencias de vídeo de cuatro participantes (denominada Gallery). En este caso, Teams envía 4 secuencias de vídeo individuales al dispositivo cliente para su decodificación. Cuando hay más de cuatro participantes que comparten vídeo, solo aparecen los últimos cuatro participantes más activos en la pantalla.

Microsoft Teams también ofrece la vista Large Gallery con una cuadrícula de hasta 7x7. Como resultado, el servidor de conferencias de Teams compone un único feed de vídeo y lo envía al dispositivo cliente para su decodificación, lo que reduce el consumo de CPU. Es posible que este único feed con cuadrículas también incluya el vídeo de autoprevisualización del usuario.

Por último, Microsoft Teams permite el modo Together, que forma parte de la nueva experiencia de las reuniones. Con la tecnología de segmentación de IA para colocar digitalmente a los participantes en un fondo compartido, Teams coloca a todos los participantes en el mismo auditorio.

El usuario puede controlar estos modos durante una llamada de conferencia con seleccionar los modos **Gallery**, **Large Gallery** o **Together** en el menú de puntos suspensivos.

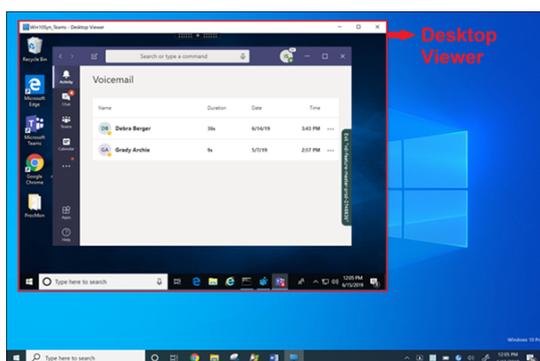


## Uso compartido de la pantalla en Microsoft Teams

Microsoft Teams utiliza el uso compartido de la pantalla basado en vídeo (VBSS), que codifica el escritorio que se comparte con códecs de vídeo, como H264, y crea un flujo de alta definición. Con la optimización HDX, la pantalla compartida entrante se trata como una transmisión de vídeo. Por lo tanto, si está en medio de una videollamada y el otro participante comienza a compartir el escritorio, la fuente de vídeo de la cámara original se pone en pausa. En su lugar, se muestra la fuente de vídeo de la pantalla compartida. A continuación, el participante debe reanudar manualmente el uso compartido de la cámara.

El uso compartido de la pantalla saliente también se optimiza y se descarga en la aplicación Citrix Workspace (versión 1907 o una posterior). En este caso, HdxTeams.exe captura y transmite solo la ventana de Citrix Desktop Viewer (CDViewer.exe). Si quiere compartir una aplicación local que se ejecute en su equipo cliente, puede superponerla sobre CDViewer y también se captura.

Multimonitor: En los casos en que CDViewer está en modo de pantalla completa y se extiende por varios monitores, solo se comparte el monitor principal. Los usuarios deben arrastrar la aplicación en cuestión al escritorio virtual del monitor principal para que el otro participante de la llamada la pueda ver.

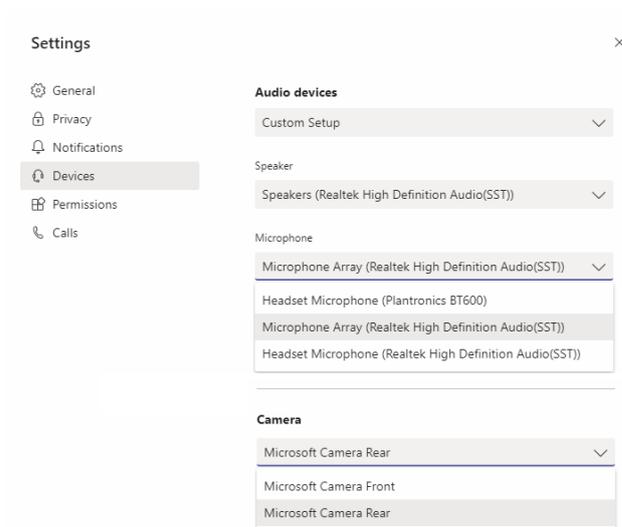


#### Nota:

Si publica Teams como aplicación independiente integrada, el uso compartido de pantalla captura el escritorio local del terminal físico en la versión mínima de la aplicación Citrix Workspace 1909.

### Periféricos en Microsoft Teams

Cuando la optimización para Microsoft Teams está activa, la aplicación Citrix Workspace accede a los periféricos (auriculares, micrófono, cámaras, altavoces...). A continuación, los periféricos se indican correctamente en la IU de Microsoft Teams (**Configuración > Dispositivos**).



Microsoft Teams no accede directamente a los dispositivos. En su lugar, se basa en HdxTeams.exe para adquirir, capturar y procesar los archivos multimedia. Microsoft Teams indica los dispositivos que debe seleccionar el usuario.

### Recomendaciones:

- [Auriculares con micrófono certificados por Microsoft Teams](#) con eliminación de eco integrada. En configuraciones con varios periféricos, donde el micrófono y los altavoces se encuentran en dispositivos separados, puede producirse eco. Por ejemplo, una cámara web con un micrófono incorporado y un monitor con altavoces. Cuando utilice altavoces externos, colóquelos lo más lejos posible del micrófono y de cualquier superficie que pueda refractar el audio hacia el micrófono.
- [Cámaras certificadas por Microsoft Teams](#), aunque los [periféricos certificados por Skype Empresarial](#) son compatibles con Microsoft Teams.
- HdxTeams.exe no puede aprovechar la descarga de CPU con cámaras web que emplean codificación H.264 integrada -UVC 1.1 y 1.5.

### Nota:

HdxTeams.exe solo admite estos formatos específicos de dispositivo de sonido (canales, profundidad de bits y tasa de muestreo):

- Dispositivos de reproducción: Hasta 2 canales, 16 bits, frecuencias de hasta 96 000 Hz
- Dispositivos de grabación: Hasta 4 canales, 16 bits, frecuencias de hasta 96 000 Hz

Aunque un solo altavoz o micrófono no tenga la configuración prevista, la enumeración de dispositivos en Teams falla y aparece **Ninguno** en **Configuración > Dispositivos**.

**Webrpc:** Sus registros en **HdxTeams.exe** muestran este tipo de información:

```
Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing  
...
```

```
Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't  
create audio module!
```

Como solución temporal, abra el **Panel de control de Sonido** (mmsys.cpl), seleccione el dispositivo de reproducción o grabación, abra **Propiedades > Avanzadas** y cambie la configuración a un modo compatible. También puede inhabilitar el dispositivo específico.

## Modo de reserva

Si Microsoft Teams no se carga en el modo VDI optimizado, el VDA recurre a tecnologías HDX heredadas, como la redirección de la cámara web y la redirección de audio y micrófono del cliente. En el modo no optimizado, los periféricos se asignan al VDA. Los periféricos aparecen en la aplicación Microsoft Teams como si estuvieran conectados localmente al escritorio virtual.

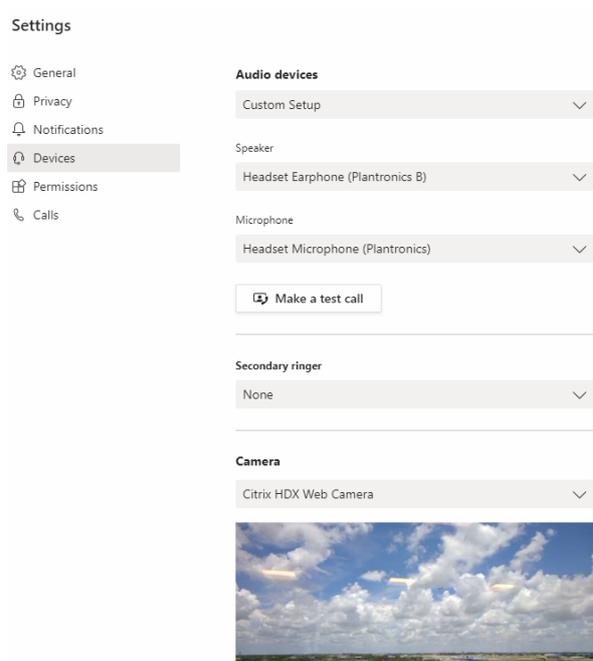
Ahora puede controlar granularmente el mecanismo de reserva (recurrir a un elemento cuando no se tiene el indicado). Para ello, establezca uno de los siguientes valores DWORD del Registro en el VDA:

```
HKLM\SOFTWARE\Microsoft\Teams\DisableFallback
```

```
HKCU\SOFTWARE\Microsoft\Office\Teams\DisableFallback
```

Para desactivar el modo de reserva, establezca el valor en 1. Para habilitar solo audio, establezca el valor en 2. Si el valor no está presente o está establecido en 0, se habilita el modo de reserva. Esta función requiere Teams 1.3.0.13565 o una versión posterior.

Para determinar si está en el modo optimizado o no en la ficha **Configuración > Dispositivos** en Teams, la diferencia más significativa es el nombre de la cámara. Si Microsoft Teams se carga en modo no optimizado, se inician las tecnologías HDX antiguas. El nombre de la cámara web tiene el sufijo **Citrix HDX**, como se muestra en el gráfico siguiente. Es posible que los nombres de los altavoces y del micrófono sean ligeramente distintos (o estar truncados) si se comparan con sus nombres en el modo optimizado.



Cuando se utilizan tecnologías HDX heredadas, Microsoft Teams no descarga el procesamiento de audio, vídeo y uso compartido de la pantalla al motor multimedia WebRTC de la aplicación Citrix Workspace del dispositivo de punto final. En su lugar, las tecnologías HDX emplean la generación de contenido del lado del servidor. Espere un alto consumo de CPU en el VDA cuando active vídeo. Es posible que el rendimiento del audio en tiempo real no sea óptimo.

## Limitaciones conocidas

### Limitaciones de Citrix

Limitaciones en la aplicación Citrix Workspace:

- No se admiten tonos DTMF.
- Botones HID: Respuesta y finalización de llamada no disponibles. Compatible con subir y bajar el volumen.
- Al hacer uso compartido de pantalla en configuraciones de varios monitores, solo se comparte el monitor principal.
- Solo admitimos una secuencia de vídeo desde una cámara entrante o una transmisión compartida de pantalla. Cuando hay un recurso compartido de pantalla entrante, ese recurso se muestra en lugar del vídeo del altavoz dominante.
- No está disponible el timbre secundario (**Teams > Parámetros > Dispositivos**).
- Los parámetros de calidad de servicio que ofrece el Centro de administración de Microsoft Teams no se aplican a los usuarios de VDI.

- El complemento de la función de protección de aplicaciones que ofrece la aplicación Citrix Workspace impide compartir pantalla saliente.
- No está disponible la función de zoom en Teams.

Limitación en el VDA:

- Al configurar el parámetro PPP elevado de la aplicación Citrix Workspace en **Sí** o **No, usar la resolución nativa**, la ventana de vídeo redirigido aparece fuera de lugar cuando el factor de escalado de PPP del monitor está configurado en más del 100%.

Limitaciones en la aplicación Citrix Workspace y el VDA:

- Compartir pantalla saliente: No se admite compartir aplicaciones.
- Solo se puede controlar el volumen de una llamada optimizada desde la barra de volumen presente en la máquina cliente, no en el VDA.

### Limitaciones de Microsoft

- No se ofrecen las opciones para desenfocar o personalizar el fondo de pantalla.
- No se ofrece la vista de galería 3x3. Dependencia de Teams: Póngase en contacto con Microsoft para saber cuándo esperar una cuadrícula 3x3.
- La interoperabilidad con Skype Empresarial se limita a llamadas de audio, sin modalidad de vídeo.
- La resolución máxima de transmisión de vídeo entrante y saliente es 720p. Dependencia de Teams: Póngase en contacto con Microsoft para saber cuándo esperar el modo 1080p.
- No se admite el tono de espera de las llamadas RTC.
- No se admite la omisión de medios para enrutamiento directo.

### Limitaciones de Citrix y Microsoft

- Al hacer uso compartido de pantalla, la opción de **Incluir audio del sistema** no está disponible.
- No está disponible el chat emergente (también conocido como chat multiventana o la nueva experiencia de reunión).
- Se pueden utilizar grupos de trabajo para los participantes de VDI. Teams no admite grupos de trabajo si el organizador es un usuario de VDI.
- Dar el control y tomar el control: No está disponible durante sesiones de uso compartido de la pantalla o de aplicaciones. Se admite solo durante una [sesión de uso compartido de PowerPoint](#).
- No están disponibles ni E911 (911 mejorado) ni LBR (redirección por ubicación).

## Próximo fin de vida (EOL) de la función de ventana única en Microsoft Teams

El 31 de enero de 2024, Microsoft retirará la compatibilidad de Microsoft Teams con la interfaz de usuario de ventana única cuando se utilice la optimización de Microsoft Teams en entornos de imagen de disco virtual (VDI) y solo admitirá la experiencia multiventana. Microsoft notificó esta retirada el 8 de septiembre de 2023 en el Centro de administración de M365 (ID de publicación: MC674419).

Los detalles sobre la función de multiventana se encuentran en el artículo [New Meeting and Calling Experience in Microsoft Teams](#) de Tech Community.

Para seguir usando Microsoft Teams en modo optimizado para compartir pantallas y vídeo, debe actualizar su VDA y la aplicación Citrix Workspace a las versiones compatibles. Si no actualiza su infraestructura y dispositivos de punto final para que admitan el modo multiventana, solo podrá establecer llamadas de audio. No podrá usar la funcionalidad optimizada de vídeo y pantalla compartida.

En la siguiente tabla se muestran las versiones mínima, LTSR y recomendada de VDA y la aplicación Citrix Workspace necesarias para seguir usando las llamadas optimizadas en Microsoft Teams con Citrix VDI:

Componente	Versión mínima	Versión LTSR compatible	Versión recomendada
Microsoft Teams	1.5.00.11865	No aplicable	Más reciente
VDA	1912 CU6 LTSR, 2112 CR	1912 CU7+, 2203 CU2+	2308 CR+
Aplicación Citrix Workspace para Windows	2205 CR	2203 CU2+	2309 CR+
Aplicación Citrix Workspace para Mac	2209 CR	No aplicable	2308 CR+
Aplicación Citrix Workspace para Linux	2209 CR	No aplicable	2308 CR+
Aplicación Citrix Workspace para ChromeOS o HTML5	2303 CR	No aplicable	2309 CR+

## Anuncio de obsolescencia del formato SDP (Plan B) en WebRTC

Citrix tiene previsto retirar la compatibilidad con el formato SDP (Plan B) en WebRTC en versiones futuras. Para poder hacer uso de las funcionalidades optimizadas de Microsoft Teams, deberá usar Unified Plan en WebRTC.

## Productos afectados

En una de las versiones futuras de la aplicación Citrix Workspace, no se admitirán las llamadas entre dispositivos de punto final con la próxima versión de la aplicación Citrix Workspace y dispositivos de punto final con la aplicación Citrix Workspace 2108 o versiones anteriores. Esta incompatibilidad en las llamadas incluye a los clientes de la aplicación Citrix Workspace (CWA) 1912 LTSR. Los siguientes clientes de CWA se ven afectados:

- Aplicación Citrix Workspace para Windows
- Aplicación Citrix Workspace para Linux
- Aplicación Citrix Workspace para Mac
- Aplicación Citrix Workspace para Chrome

## Reemplazo para el Plan B

Si utiliza una versión de la aplicación Citrix Workspace anterior a 2109, debe actualizar a una versión compatible (preferiblemente, la última versión Current Release). De lo contrario, no se conectarán las llamadas con una versión futura o dispositivos de punto final más recientes. Es posible que las llamadas entre versiones futuras y sus socios de comunicación federados tampoco se completen si el socio federado no ha actualizado su versión de Citrix Workspace.

La versión 2108 de la aplicación Citrix Workspace dejó recibir asistencia en marzo de 2023 y debe actualizarse a una versión más reciente. Para obtener más información sobre la compatibilidad de versiones, consulte la [aplicación Workspace](#).

Para obtener más información sobre la retirada del Plan B, consulte la documentación de [WebRTC](#).

## Información adicional

- [Supervisión, solución de problemas y asistencia para Microsoft Teams](#)
- [Implementar la aplicación de escritorio de Teams en la VM](#)
- [Instalar Microsoft Teams mediante MSI \(sección Instalación de VDI\)](#)
- [Clientes ligeros](#)
- [Herramienta de evaluación de la red de Skype Empresarial](#)
- [Coexistencia e interoperabilidad de Microsoft Teams y Skype Empresarial](#)

## Supervisión, solución de problemas y asistencia para Microsoft Teams

March 10, 2022

## Supervisar Teams

En esta sección, se ofrecen líneas generales para supervisar la optimización de Microsoft Teams con HDX.

Si el usuario se está ejecutando en modo optimizado y `HdxTeams.exe` se está ejecutando en la máquina cliente, hay un proceso en el VDA llamado `WebSocketAgent.exe` que se ejecuta en la sesión. Utilice **Administrador de actividades** en Director para ver la aplicación.

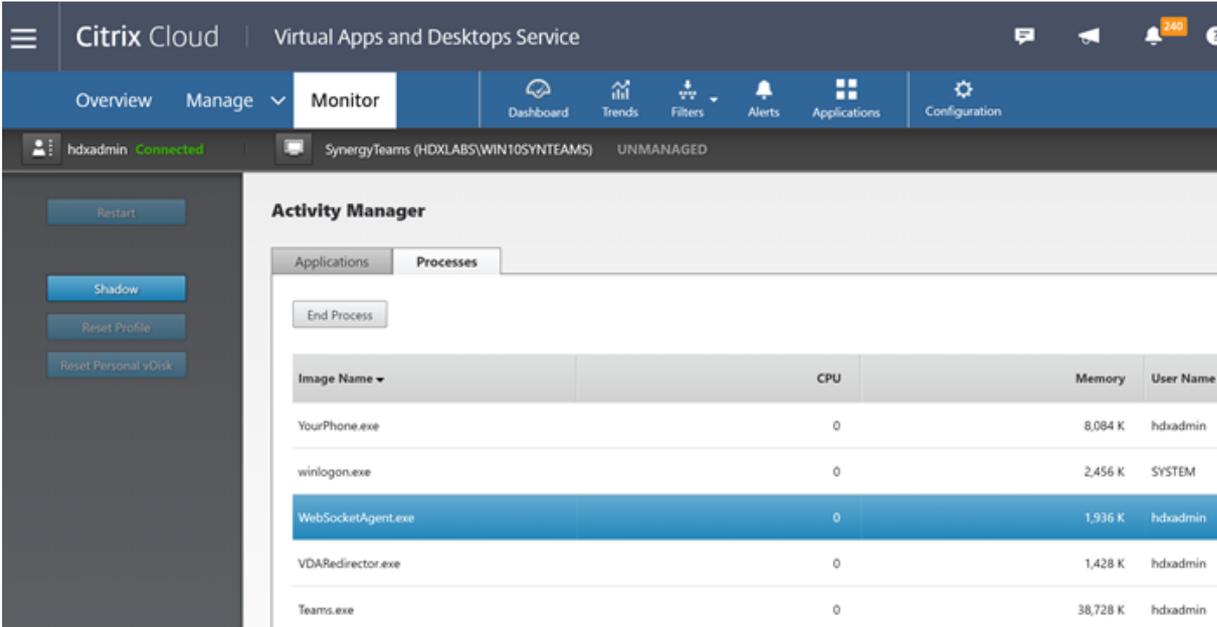


Image Name	CPU	Memory	User Name
YourPhone.exe	0	8,084 K	hdxadmin
winlogon.exe	0	2,456 K	SYSTEM
WebSocketAgent.exe	0	1,936 K	hdxadmin
VDARedirector.exe	0	1,428 K	hdxadmin
Teams.exe	0	38,728 K	hdxadmin

Con la versión mínima de VDA 1912, puede supervisar las llamadas activas de Teams a través de Citrix HDX Monitor (versión mínima 3.11). La imagen ISO del producto Citrix Virtual Apps and Desktops contiene la última versión de `hdxmonitor.msi` en la carpeta `layout\image-full\Support\HDX Monitor`.

Para obtener más información, consulte *Supervisión* en el artículo [CTX253754](#) de Knowledge Center.

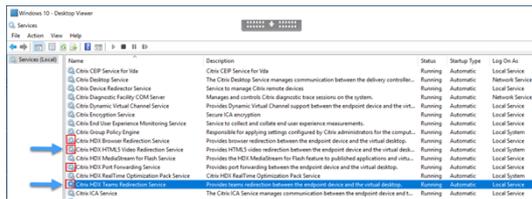
## Solucionar problemas técnicos

En esta sección se proporcionan sugerencias para solucionar problemas que pueden surgir al usar la optimización para Microsoft Teams.

Encontrará más información en [CTX253754](#).

## En el Virtual Delivery Agent

Hay cuatro servicios instalados por `BCR_x64.msi`. Solo dos son responsables de la redirección de Microsoft Teams en el VDA.



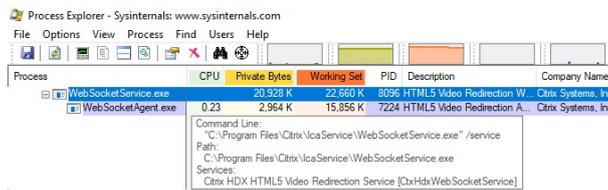
- **Citrix HDX Teams Redirection Service** establece el canal virtual utilizado en Microsoft Teams. El servicio se basa en CtxSvcHost.exe.
- **Citrix HDX HTML5 Video Redirection Service** se ejecuta como WebSocketService.exe y escucha el puerto TCP 127.0.0.1:9002. WebSocketService.exe realiza dos funciones principales:
  - i. La **finalización de TLS para WebSockets seguros** recibe una conexión WebSocket segura desde vdiCitrixPeerConnection.js, que es un componente de la aplicación Microsoft Teams. Puede hacer un seguimiento de esto con Process Monitor. Para obtener más información sobre los certificados, consulte la sección “TLS, la redirección de vídeo HTML5 y la redirección de contenido del explorador web” en [Comunicación entre Controller y VDA](#).

Algunos antivirus y software de seguridad de escritorio interfieren con el correcto funcionamiento de `WebSocketService.exe` y sus certificados. Aunque es posible que el servicio de Redirección de vídeo HTML5 de Citrix HDX se esté ejecutando en la consola de `services.msc`, el socket TCP de localhost 127.0.0.1:9002 nunca está en modo de escucha como se ve en netstat. Intentar reiniciar el servicio hace que se bloquee (“Deteniendo...”).

Asegúrese de que aplica las exclusiones adecuadas para el proceso `WebSocketService.exe`.



- ii. **Asignación de sesiones de usuario.** Cuando se inicia la aplicación Microsoft Teams, `WebSocketService.exe` inicia el proceso `WebSocketAgent.exe` en la sesión del usuario en el VDA. `WebSocketService.exe` se ejecuta en la sesión 0 como una cuenta `LocalSystem`.



Puede utilizar `netstat` para comprobar si el servicio `WebSocketService.exe` se encuentra en un estado de escucha activa en el VDA.

Ejecute `netstat -anob -p tcp` desde una ventana elevada de símbolo del sistema:

```
TCP 127.0.0.1:9001 0.0.0.0:0 LISTENING 11740
[WebSocketService.exe]
TCP 127.0.0.1:9002 0.0.0.0:0 LISTENING 11740
[WebSocketService.exe]
```

En una conexión correcta, el estado cambia a ESTABLECIDO:

```
TCP 127.0.0.1:9002 127.0.0.1:58069 ESTABLISHED 8096
[WebSocketService.exe]
TCP 127.0.0.1:58069 127.0.0.1:9002 ESTABLISHED 748
[Teams.exe]
```

### Importante:

WebSocketService.exe escucha dos sockets TCP: 127.0.0.1:9001 y 127.0.0.1:9002. El puerto 9001 se utiliza para la redirección de contenido del explorador y la redirección de vídeo HTML5. El puerto 9002 se utiliza para la redirección de Microsoft Teams. No debe tener ninguna configuración de proxy en el sistema operativo Windows del VDA que pueda impedir una comunicación directa entre Teams.exe y WebSocketService.exe. A veces, al configurar un proxy explícito en Internet Explorer 11 (**Opciones de Internet > Conexiones > Configuración de LAN > Servidor proxy**), es posible que las conexiones circulen por un servidor proxy asignado. Compruebe que la opción **Omitir servidor proxy para las direcciones locales** esté activada cuando utilice una configuración de proxy manual y explícita.

## Ubicaciones y descripciones de servicios

Servicio	Ruta al archivo ejecutable en el SO de servidor Windows	Iniciar sesión como	Descripción
Servicio de redirección de vídeo para Citrix HTML5	“C:\Archivos de programa (x86)\Citrix\System32\WebSocketService.exe” /service	Cuenta del sistema local	Proporciona varios servicios HDX Multimedia con el marco inicial necesario para realizar la redirección multimedia entre el escritorio virtual y el dispositivo de punto final.
Servicio de redirección de explorador para Citrix HDX	“C:\Archivos de programa (x86)\Citrix\System32\CtxSvcHost.exe” -g BrowserRedirSvcs	Esta cuenta (servicio local)	Permite redirigir el contenido del explorador entre el dispositivo de punto final y el escritorio virtual.

Servicio	Ruta al archivo ejecutable en el SO de servidor Windows	Iniciar sesión como	Descripción
Servicio de reenvío de puertos para Citrix	“C:\Archivos de programa (x86)\Citrix\System32\CtxSvcHost.exe” -g PortFwdSvcs	Esta cuenta (servicio local)	Permite reenviar puertos entre el dispositivo de punto final y el escritorio virtual para la redirección de contenido del explorador web.
Servicio de redirección de Teams para Citrix HDX	“C:\Archivos de programa (x86)\Citrix\System32\CtxSvcHost.exe” -g TeamsSvcs	Cuenta del sistema local	Permite redirigir Microsoft Teams entre el dispositivo de punto final y el escritorio virtual.

### Aplicación Citrix Workspace

En el dispositivo de punto final del usuario, la aplicación Citrix Workspace para Windows crea una instancia de un nuevo servicio denominado HdxTeams.exe. Lo hace cuando Microsoft Teams se inicia en el VDA y el usuario intenta llamar o acceder a periféricos en la vista previa automática. Si no ve este servicio, compruebe lo siguiente:

1. Debe haber instalado como mínimo la versión 1905 de la aplicación Workspace para Windows. ¿Ve HdxTeams.exe y los binarios de webrpc.dll en la ruta de instalación de la aplicación Workspace?
2. Si validó el paso 1, haga lo siguiente para comprobar si se va a iniciar HdxTeams.exe.
  - a) Salga de Microsoft Teams en el VDA.
  - b) Inicie services.msc en el VDA.
  - c) Detenga Citrix HDX Teams Redirection Service.
  - d) Desconecte la sesión ICA.
  - e) Conecte la sesión ICA.
  - f) Inicie Citrix HDX Teams Redirection Service.
  - g) Reinicie Citrix HDX HTML5 Video Redirection Service.
  - h) Inicie Microsoft Teams en el VDA.
3. Si aún no ve que HdxTeams.exe se inicia en el dispositivo de punto final del cliente, haga lo siguiente:

- a) Reinicie el VDA.
- b) Reinicie el dispositivo de punto final del cliente.

## Asistencia

Citrix y Microsoft ofrecen soporte conjunto a la entrega de Microsoft Teams desde Citrix Virtual Apps and Desktops mediante la optimización para Microsoft Teams. Este soporte conjunto es el resultado de una estrecha colaboración entre ambas empresas. Si tiene contratos de soporte válidos y sufre problemas con esta solución, abra un tíquet de asistencia con el proveedor cuyo código sospeche que está causando el problema. Es decir, Microsoft si se trata de Teams o Citrix si se trata de los componentes de optimización.

Citrix o Microsoft reciben el tíquet, evalúan el problema y lo escalan según corresponda. No es necesario que se ponga en contacto con el equipo de asistencia de cada empresa.

Cuando tenga un problema, le recomendamos que haga clic en **Ayuda > Informar de un problema** en la interfaz de usuario de Teams. Los registros del lado del VDA se comparten automáticamente entre Citrix y Microsoft para resolver los problemas técnicos con mayor rapidez.

## Recopilar registros

Los registros del motor de medios HDX se pueden encontrar en la máquina del usuario (no en el VDA). Si ocurre algún problema, adjunte los registros al caso de asistencia técnica.

### Registros de Windows:

Los registros de Windows se encuentran en %TEMP%, dentro de la carpeta **HDXTeams** (AppData/Local/Temp/HDXTeams o AppData/Local/Temp/HdxRtcEngine). Busque un archivo TXT llamado `webrpc_día_mes_hora_año.txt`. Si utiliza versiones más recientes de la aplicación Citrix Workspace, por ejemplo, la aplicación Citrix Workspace 2009.5 o una versión posterior, guarde los registros en `AppData\Local\Temp\HdxRtcEngine`.

Cada sesión crea una carpeta independiente para los registros.

### Registros de Mac:

1. Registro VDWEBRTC: Registra la ejecución del canal virtual.

Ubicación: `/Users/<User Name>/Library/Logs/Citrix Workspace/CitrixViewer_<Y_M_D_H_M_S>.txt`

2. Registro HdxRtcEngine: Registra la ejecución de los procesos en HdxRtcEngine.

Ubicación: `$TMPDIR/hdxrtcengine/<W_M_D_H_M_S_Y>/hdxrtcengine.log`

El registro HdxRtcEngine está habilitado de forma predeterminada.

**Registros de Linux:**

Los registros de Linux se encuentran en el directorio `/tmp/webrpc/<current date>/` and `/tmp/hdxrtcengine/<current date>/`.

Al establecer una llamada, se requieren estas cuatro fases ICE:

- Recopilación de candidatos
- Intercambio de candidatos
- Comprobaciones de conectividad (solicitudes de enlace STUN)
- Promoción de candidatos

En los registros de HdxTeams.exe, las siguientes entradas son las entradas pertinentes del establecimiento interactivo de conectividad (ICE). Estas entradas deben estar allí para que una configuración de llamada se lleve a cabo correctamente (consulte este fragmento de ejemplo para la fase de recopilación):

```

1  RPCStubs Info: -> device id = \\?\display#int3470#4&1835d135&0&uid13424
   #{
2  65e8773d-8f56-11d0-a3b9-00a0c9223196 }
3  {
4  bf89b5a5-61f7-4127-a279-e187013d7caf }
5  label = Microsoft Camera Front groupId =
6
7  webrtcapi.RTCPeerConnection Info: createOffer. audio = 1 video = 1
8  webrtcapi.RTCPeerConnection Info: setLocalDescription.
9  >>> begin:sdp
10 [...]
11
12 webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
   HaveLocalOffer
13
14 webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state =
   Gathering
15
16 [...]
17 >>> begin:sdp
18 candidate:840548147 1 udp 2122194687 10.108.124.215 56927 typ host
   generation 0 ufrag oVk6 network-id 1
19 <<< end:sdp
20 [...]
21 >>> begin:sdp
22 candidate:1938109490 1 udp 24911871 52.114.xxx.xxx 52786 typ relay
   raddr 73.205.xxx.x rport 25651 generation 0 ufrag dDML network-id 1
   network-cost 10
23 <<< end:sdp
24 [...]
25 >>> begin:sdp
26 candidate:4271145120 1 udp 1685987071 66.xxx.xxx.xxx 55839 typ srflx
   raddr 10.108.124.215 rport 55839 generation 0 ufrag uAVH network-id
   1

```

```
27 <<< end:sdp
28 [...]
29
30 webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state =
    Complete webrtcapi.RTCPeerConnection Info: setRemoteDescription.
31 >>> begin:sdp
32 [...]
33
34 webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
    HaveRemoteOffer
35
36 <!--NeedCopy-->
```

Si hay varios candidatos de ICE, el orden de preferencia es el siguiente:

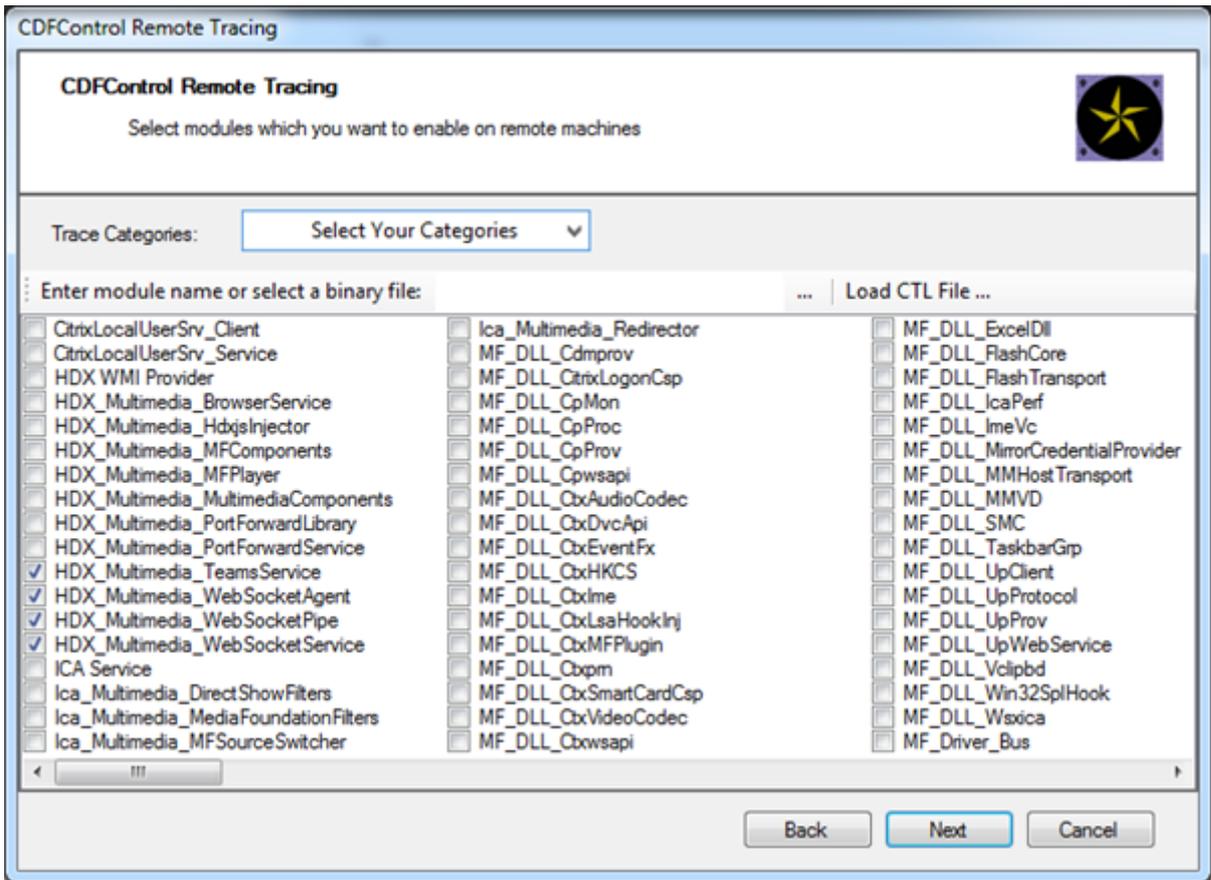
1. host
2. par reflexivo
3. servidor reflexivo
4. traspaso de transporte

Si encuentra un problema y puede reproducirlo, le recomendamos que haga clic en **Ayuda > Informar de un problema** en Teams. Citrix y Microsoft comparten los registros para resolver los problemas técnicos si abre un caso con Microsoft.

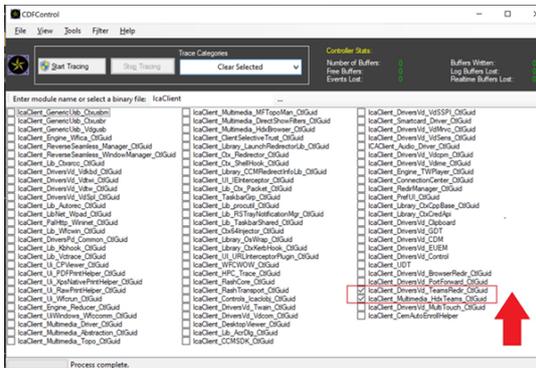
La captura de rastros CDF antes de ponerse en contacto con Citrix Support también puede resultar beneficiosa. Para obtener más información, consulte el artículo [CDFcontrol](#) de Knowledge Center.

Para obtener recomendaciones para recopilar trazas CDF, consulte el artículo [Recommendations for Collecting the CDF Traces](#) de Knowledge Center.

**Rastros CDF del lado de VDA. Habilite los siguientes proveedores de rastros CDF:**



Rastros CDF del lado de la aplicación Workspace. Habilite los siguientes proveedores de rastros CDF:



## Redirección de Windows Media

September 22, 2021

La Redirección de Windows Media controla y optimiza el modo en que los servidores entregan a los usuarios sonido y vídeo por streaming. Al reproducir los archivos en tiempo de ejecución multimedia

en el dispositivo del usuario y no en el servidor, la Redirección de Windows Media reduce los requisitos de ancho de banda para reproducir archivos multimedia. La Redirección de Windows Media mejora el rendimiento del Reproductor de Windows Media y de los reproductores compatibles que se ejecutan en escritorios virtuales Windows.

Si no se cumplen los requisitos de Windows Media para la obtención de contenido en el cliente, la entrega de contenido multimedia pasa automáticamente a utilizar la obtención en el servidor. Este método es transparente para los usuarios. Puede usar Citrix Scout para rastrear el método utilizado con Citrix Diagnosis Facility (CDF) desde HostMMTransport.dll. Para obtener más información, consulte [Citrix Scout](#).

La Redirección de Windows Media intercepta los procesos multimedia del servidor host, captura los datos multimedia en el formato nativo comprimido y redirige el contenido al dispositivo cliente. A continuación, el dispositivo cliente vuelve a crear los procesos multimedia para descomprimir y generar los datos multimedia recibidos de parte del servidor host. La Redirección de Windows Media funciona bien en dispositivos cliente que ejecutan un sistema operativo Windows. Esos dispositivos disponen del marco multimedia necesario para reconstruir los procesos multimedia que existen en el servidor host. Los clientes Linux usan marcos multimedia similares de código abierto para reconstruir los procesos multimedia.

La configuración **Redirección de Windows Media** controla esta función y está establecida en **Permitida** de forma predeterminada. Por lo general, esta configuración aumenta la calidad de sonido y vídeo que se generan desde el servidor a un nivel comparable al del sonido y el vídeo reproducidos localmente en un dispositivo cliente. En casos contados, la reproducción multimedia con la Redirección de Windows Media resulta ser peor que cuando se genera mediante la compresión básica de ICA y el sonido normal. Para inhabilitar esta función, agregue la configuración **Redirección de Windows Media** a una directiva y establezca su valor en **Prohibida**.

Para obtener más información sobre las configuraciones de directiva, consulte [Configuraciones de directiva de Multimedia](#).

#### **Limitación:**

Cuando usa Windows Media Player con Remote Audio & Video Extensions (RAVE) habilitado dentro de una sesión, puede aparecer una pantalla en negro. Esta pantalla en negro puede aparecer si hace clic con el botón secundario en el vídeo y selecciona **Reproducción en curso siempre visible**.

## **Redirección de contenido general**

February 6, 2020

La redirección de contenido permite controlar si los usuarios acceden a la información desde aplicaciones publicadas en servidores o desde aplicaciones que se ejecutan localmente en dispositivos de usuario.

### Redirección de carpetas del cliente

La redirección de carpetas del cliente cambia el modo en que los archivos del lado del cliente son accesibles desde la sesión en el host.

- Cuando se habilita solo la asignación de unidades del cliente en el servidor, se asignan automáticamente volúmenes completos del cliente a las sesiones como enlaces UNC (Universal Naming Convention).
- Cuando se habilita la redirección de carpetas del cliente en el servidor y, a continuación, el usuario lo configura en el dispositivo de escritorio Windows, solo se redirige la parte del volumen local que especifique el usuario.

### Redirección del host al cliente

La redirección del host al cliente resulta útil para casos concretos y poco frecuentes. En la mayoría de los casos, existen formas mejores de redirigir el contenido. Solo admitimos este tipo de redirección en los VDA con SO multisesión, y no en los VDA con SO de sesión única.

### Acceso a aplicaciones locales y redirección de URL

El acceso a aplicaciones locales integra sin problemas las aplicaciones de Windows instaladas localmente en un entorno de escritorio alojado. Lo hace sin cambiar de un equipo a otro.

La tecnología HDX ofrece la **redirección de USB genérico** para dispositivos específicos sin optimización o cuando esta no es adecuada.

## Redirección de carpetas del cliente

February 6, 2020

La redirección de carpetas del cliente cambia el modo en que los archivos del lado del cliente son accesibles desde la sesión en el host. Si se habilita solamente la asignación de unidades del cliente en el servidor, se asignan automáticamente volúmenes completos del cliente a las sesiones como enlaces UNC (Universal Naming Convention). Cuando se habilita la redirección de carpetas del cliente en el servidor y, a continuación, el usuario lo configura en el dispositivo de usuario, solo se redirige la parte del volumen local que especifique el usuario.

Solo las carpetas especificadas por el usuario aparecen como enlaces UNC dentro de las sesiones. Es decir, en lugar del sistema de archivos completo en el dispositivo del usuario. Si se inhabilitan los

enlaces UNC mediante el Registro, las carpetas del cliente aparecen como unidades asignadas dentro de la sesión.

La redirección de carpetas del cliente solo se admite en máquinas con SO de sesión única Windows.

La redirección de carpetas del cliente para una unidad USB externa no se guarda al desconectar y volver a conectar el dispositivo.

Habilite la redirección de carpetas del cliente en el servidor. Luego, en el dispositivo cliente, especifique qué carpetas redirigir. La aplicación que se utiliza para especificar las opciones de carpeta del cliente está incluida en la aplicación Citrix Workspace proporcionada con esta versión.

### **Requisitos:**

Para servidores:

- Windows Server 2019, Standard y Datacenter Edition
- Windows Server 2016, Standard y Datacenter Edition
- Windows Server 2012 R2, Standard y Datacenter Edition

Para clientes:

- Windows 10, ediciones de 32 y 64 bits (versión mínima: 1607)
- Windows 8.1, ediciones de 32 y 64 bits (y Embedded)
- Windows 7, ediciones de 32 y 64 bits (incluida la Embedded Edition)

### **Advertencia**

Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

#### **1. En el servidor:**

- a) Cree una clave: HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection.
- b) Cree un valor REG\_DWORD.
  - Nombre: CFROnlyModeAvailable
  - Tipo: REG\_DWORD
  - Datos: Establézcalo en 1.

#### **2. En el dispositivo de usuario:**

- a) Compruebe que está instalada la versión más reciente de la aplicación Citrix Workspace.
- b) En el directorio de instalación de la aplicación Citrix Workspace, inicie CtxCFRUI.exe.

- c) Seleccione el botón de opción **Personalizada** y agregue, modifique o quite carpetas.
- d) Desconecte y vuelva a conectar sus sesiones para que la configuración tenga efecto.

## Redirección del host al cliente

September 22, 2021

La redirección del host al cliente permite que las URL, incrustadas como enlaces en las aplicaciones que se ejecutan en una sesión de Citrix, se abran mediante la aplicación correspondiente en el dispositivo de punto final del usuario. Algunos casos de uso comunes para la redirección del host al cliente incluyen:

- Redirección de sitios web en los casos en que el servidor Citrix no tiene acceso a Internet o de red al origen.
- Por motivos de seguridad, rendimiento, compatibilidad o escalabilidad, no se quiere redireccionar los sitios web cuando se ejecuta un explorador web en la sesión de Citrix.
- Redirección de tipos de URL específicos en los casos en que las aplicaciones requeridas para abrir la URL no están instaladas en el servidor Citrix.

La redirección del host al cliente no está pensada para URL a las que accede en una página web o se introducen en la barra de direcciones del explorador web que se ejecuta en la sesión de Citrix. Para obtener información sobre la redirección de URL en exploradores web, consulte [Redirección bidireccional de URL](#) o [Redirección de contenido del explorador web](#).

### Requisitos del sistema

- VDA de SO multisesión
- Clientes compatibles:
  - Aplicación Citrix Workspace para Windows
  - Aplicación Citrix Workspace para Mac
  - Aplicación Citrix Workspace para Linux
  - Aplicación Citrix Workspace para HTML5
  - Aplicación Citrix Workspace para Chrome

El dispositivo cliente debe tener instalada y configurada una aplicación para gestionar la redirección de los tipos de URL.

## Configuración

Utilice la directiva de Citrix [Redirección del host al cliente](#) para habilitar esta funcionalidad. La **redirección del host al cliente** está inhabilitada de forma predeterminada. Después de habilitar la directiva de redirección del host al cliente, la aplicación Citrix Launcher se registra en el servidor Windows para asegurarse de que puede interceptar URL y enviarlas al dispositivo cliente.

A continuación, deberá configurar la directiva de grupo de Windows para utilizar Citrix Launcher como aplicación predeterminada para los tipos de URL requeridos. En el VDA de servidor Citrix, cree el archivo ServerFTAdefaultPolicy.xml e inserte el siguiente código XML.

```
1 <?xml version="1.0" encoding="UTF-8"?>
2
3 <DefaultAssociations>
4
5 <Association Identifier="http" ProgId="ServerFTAHTML" ApplicationName="
   ServerFTA" />
6
7 <Association Identifier="https" ProgId="ServerFTAHTML" ApplicationName="
   ServerFTA" />
8
9 </DefaultAssociations>
10 <!--NeedCopy-->
```

En la Consola de administración de directivas de grupo, vaya a **Configuración del equipo > Plantillas administrativas > Componentes de Windows > Explorador de archivos > Definir un archivo de configuración de asociaciones predeterminadas** y guarde el archivo ServerFTAdefaultPolicy.xml.

### Nota:

Si un servidor Citrix no tiene la configuración de directiva de grupo, Windows pide a los usuarios que seleccionen una aplicación para abrir las URL.

De forma predeterminada, se admite la redirección de los siguientes tipos de URL:

- HTTP
- HTTPS
- RTSP
- RTSPU
- PNM
- MMS

Para incluir otros tipos de URL estándar o personalizados en la lista para redirección, cree una nueva línea de **identificador de asociación** en el archivo ServerFTAdefaultPolicy.xml al que se hace referencia anteriormente. Por ejemplo:

```
<Association Identifier="ftp"ProgId="ServerFTAHTML"ApplicationName="
ServerFTA"/>
```

```
<Association Identifier="mailto"ProgId="ServerFTAHTML"ApplicationName="ServerFTA"/>
```

```
<Association Identifier="customtype1"ProgId="ServerFTAHTML"ApplicationName="ServerFTA"/>
```

```
<Association Identifier="customtype2"ProgId="ServerFTAHTML"ApplicationName="ServerFTA"/>
```

La adición de tipos de URL a la lista también requiere la configuración del cliente. Cree la siguiente clave y valores del Registro en el cliente Windows.

**Nota:**

Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

- Clave: HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- Nombre del valor: ExtraURLProtocols
- Tipo de valor: REG\_SZ
- Información del valor: Especifique los tipos de URL requeridos separados por punto y coma. Incluya todo antes de la sección de autoridad de la URL. Por ejemplo:  
`ftp://;mailto;;customtype1://;customtype2://`

Puede agregar tipos de URL solo para clientes Windows. Los clientes que faltan en la configuración del registro anterior rechazan el redireccionamiento de vuelta a la sesión de Citrix. El cliente debe tener instalada y configurada una aplicación para gestionar los tipos de URL especificados.

Para quitar tipos de URL de la lista de redirección predeterminada, cree la siguiente clave de Registro y valores en el VDA del servidor.

- Clave: HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Nombre del valor: DisableServerFTA
- Tipo de valor: DWORD
- Información del valor: 1
- Nombre del valor: NoRedirectClasses
- Tipo de valor: REG\_MULTI\_SZ
- Información del valor: Especifique cualquier combinación de los valores: `http`, `https`, `rtsp`, `rtspu`, `pnm` o `mms`. Si especifica varios valores, debe ser en líneas independientes. Por ejemplo:

http

https

rtsp

Para habilitar la redirección del host al cliente para un conjunto específico de sitios web, cree una clave de Registro y valores en el VDA de servidor.

- Clave: HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Nombre del valor: ValidSites
- Tipo de valor: REG\_MULTI\_SZ
- Información del valor: Especifique una combinación de nombres de dominio completo (FQDN). Si especifica varios nombres de dominio completos, debe ser en líneas independientes. Incluya solo el nombre de dominio completo, sin protocolos ([http://](#) o [https://](#)). Un nombre de dominio completo puede incluir un asterisco (\*) como carácter comodín solo a la izquierda. Ese comodín coincide con un único nivel de dominio, lo que es coherente con las reglas de RFC 6125. Por ejemplo:

[www.exmaple.com](#)

\*.[example.com](#)

**Nota:**

No se puede utilizar la clave **ValidSites** en combinación con las claves **DisableServerFTA** y **NoRedirectClasses**.

## Configuración predeterminada del explorador del VDA del servidor

Al habilitar la redirección del host al cliente, tal como se hace referencia en esta sección, sustituye cualquier configuración predeterminada anterior del explorador en el VDA del servidor. Si no se redirige una URL web, Citrix Launcher transmite la URL al explorador configurado en la clave de Registro [command\\_backup](#). La clave apunta a Internet Explorer de forma predeterminada, pero puede modificarla para incluir la ruta de acceso a otro explorador. Para obtener más información, consulte [Configuración predeterminada del explorador del VDA del servidor](#) en la lista de funciones administradas a través del Registro.

## Redirección bidireccional de contenido

April 19, 2024

La redirección bidireccional de contenido permite que las URL HTTP o HTTPS de los exploradores web, o integradas en aplicaciones, se reenvíen entre la sesión de Citrix VDA y el dispositivo de punto final del cliente en ambas direcciones. Una dirección URL introducida en un explorador que se ejecuta en la sesión de Citrix se puede abrir con el explorador predeterminado del cliente. A la inversa, una URL introducida en un explorador que se ejecuta en el cliente se puede abrir en una sesión de Citrix, ya sea con una aplicación o un escritorio publicados. Algunos casos de uso comunes para la redirección bidireccional de contenido incluyen:

- Redirección de URL web en los casos en que el explorador de inicio no tiene acceso de red al origen.
- Redirección de URL web por motivos de compatibilidad y seguridad del explorador.
- La redirección de URL web incrustadas en aplicaciones cuando se ejecuta un explorador web en la sesión de Citrix o no se quiere el cliente.

### Requisitos del sistema

- VDA para SO de sesión única o multisesión
- Aplicación Citrix Workspace para Windows
- Internet Explorer 11

### Configuración

La redirección bidireccional de contenido debe habilitarse mediante la directiva de Citrix tanto en el VDA como en el cliente para que funcione. La redirección bidireccional de contenido está inhabilitada de forma predeterminada.

Para la configuración del VDA, consulte [Redirección bidireccional de contenido](#) en Configuraciones de directiva de ICA.

Para la configuración del cliente, consulte [Redirección bidireccional de contenido](#) en la documentación de la aplicación Citrix Workspace para Windows.

La extensión del explorador deben registrarse con los comandos que se muestran. Ejecute los comandos según sea necesario en el VDA y el cliente.

Para registrar la extensión del explorador en el VDA, abra un símbolo del sistema. A continuación, ejecute `%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe` con la opción de explorador requerida, como se indica en este ejemplo:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regIE
```

Para cancelar el registro de la extensión del explorador, use la opción `/unregIE`, como en este ejemplo:

`%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /unregIE`

Para registrar la extensión de explorador en el cliente, abra un símbolo del sistema y ejecute `%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe` con las mismas opciones que en los ejemplos mostrados.

## Otras consideraciones

- Los requisitos y configuraciones de explorador solo se aplican al explorador que inicia la redirección. El explorador de destino, en el que se abre la URL una vez que ha tenido lugar la redirección, no se tiene en cuenta. Al redirigir las URL desde el VDA a un cliente, solo se requiere una configuración de explorador compatible en el VDA. A la inversa, al redirigir las URL desde el cliente a un VDA, solo se requiere una configuración de explorador compatible en el cliente. Las URL redirigidas se transfieren al explorador predeterminado configurado en la máquina de destino, ya sea el cliente o el VDA, según la dirección. NO es necesario usar el mismo tipo de explorador en el VDA y en el cliente.
- Compruebe que las reglas de redirección no resultan en un bucle. Por ejemplo, si se establece una directiva de VDA para redirigir <https://www.citrix.com> y la directiva de cliente está establecida para redirigir esa misma URL, se produce un bucle infinito.
- Solo se admiten las URL con protocolo HTTP/HTTPS. No se admiten acortadores de URL.
- La redirección de cliente a VDA requiere que el cliente Windows se instale con derechos de administrador.
- Si el explorador de destino ya está abierto, la URL redirigida se abre en una nueva ficha. De lo contrario, la URL se abre en una nueva ventana de explorador.
- La redirección bidireccional de contenido no funciona cuando el acceso a aplicaciones locales (LAA) está habilitado.

## Acceso a aplicaciones locales y redirección de URL

November 4, 2022

### Introducción

La función Acceso a aplicaciones locales integra perfectamente las aplicaciones Windows instaladas localmente en un entorno de escritorio alojado sin cambiar de un escritorio a otro. Con la función Acceso a aplicaciones locales, puede:

- Acceder a las aplicaciones instaladas localmente en un equipo portátil, un PC u otro dispositivo físico, directamente desde el escritorio virtual.
- Proporcionar una solución flexible para la entrega de aplicaciones. Si los usuarios disponen de aplicaciones locales que no se pueden virtualizar o que el departamento de TI no mantiene, dichas aplicaciones se comportan como si estuvieran instaladas en un escritorio virtual.
- Eliminar la latencia de doble salto que se produce cuando las aplicaciones no están alojadas en el escritorio virtual. Para ello, ponga un acceso directo a la aplicación publicada en el dispositivo Windows del usuario.
- Usar aplicaciones como:
  - Videoconferencia; por ejemplo, GoToMeeting.
  - Aplicaciones nicho o especializadas que aún no están virtualizadas.
  - Aplicaciones y periféricos que de otro modo transferirían grandes cantidades de datos desde un dispositivo de usuario a un servidor y de vuelta al dispositivo del usuario. Por ejemplo, grabadoras de DVD y sintonizadores de TV.

En Citrix Virtual Apps and Desktops, las sesiones de escritorio alojado usan la redirección de URL para iniciar aplicaciones de acceso local. La función Redirección de URL permite que la aplicación esté disponible en más de una URL. Inicia un explorador local (basado en la lista de direcciones URL bloqueadas de su explorador) mediante la selección de enlaces insertados en un explorador en una sesión de escritorio. Si se dirige a una URL que no está en la lista de bloqueados, esa URL se vuelve a abrir en la sesión de escritorio.

La función Redirección de URL solo funciona en sesiones de escritorio, no las sesiones de aplicación. La única función de redirección que puede usar para sesiones de aplicación es la redirección de contenido de host a cliente, que es un tipo de redirección FTA (asociación de tipos de archivo) para servidor. Esta FTA dirige ciertos protocolos al cliente, como HTTP, HTTPS, RTSP o MMS. Por ejemplo, si abre enlaces insertados solo con HTTP, estos se abren directamente con la aplicación cliente. No se admiten ni la lista de direcciones URL bloqueadas ni la lista de direcciones URL permitidas.

Cuando el acceso a aplicaciones locales está habilitado, las direcciones URL que se muestran a los usuarios como enlaces desde aplicaciones ejecutadas localmente, desde aplicaciones alojadas por el usuario o como accesos directos en el escritorio se redirigen de una de las siguientes maneras:

- Desde el equipo del usuario al escritorio alojado
- Desde el servidor de Citrix Virtual Apps and Desktops al equipo del usuario
- Generadas en el entorno donde se abren (no redirigidas)

Para especificar la ruta de redirección de contenido desde sitios web específicos, configure la lista de direcciones URL permitidas y la lista de direcciones URL bloqueadas en el Virtual Delivery Agent. Estas listas contienen claves de Registro de cadena múltiple que especifican la configuración de la directiva Redirección de URL. Para obtener más información, consulte las [configuraciones de directiva de Acceso a aplicaciones locales](#).

Las direcciones URL pueden generarse en el VDA, con las siguientes excepciones:

- Configuración regional y geográfica. Los sitios web que requieren configuración regional, como msn.com o news.google.com (abre la página de un país concreto, basada en la ubicación geográfica). Por ejemplo: si el VDA se aprovisionó desde un centro de datos en el Reino Unido y el cliente se conecta desde la India, el usuario espera ver in.msn.com. Sin embargo, el usuario ve uk.msn.com.
- Contenido multimedia. Los sitios web con contenido multimedia que, cuando se generan en el dispositivo cliente, ofrecen una experiencia nativa a los usuarios finales y ahorran ancho de banda incluso en redes de latencia alta. Esta función redirige sitios con otros tipos de contenido multimedia, como Silverlight. Este proceso se realiza en un entorno seguro. Es decir, las direcciones URL que el administrador haya aprobado se ejecutan en el cliente, mientras que el resto de las direcciones URL se redirigen al VDA.

Además de la redirección de URL, también puede utilizar la redirección de asociación de tipos de archivo (FTA). FTA inicia aplicaciones locales cuando se encuentra un archivo en la sesión. Si se inicia la aplicación local, esta debe tener acceso al archivo para abrirlo. Por lo tanto, solo puede abrir archivos que residen en recursos compartidos de red o en las unidades del cliente (mediante la asignación de unidades del cliente) con aplicaciones locales. Por ejemplo, cuando se abre un archivo PDF, si un lector de PDF es una aplicación local, el archivo se abre con ese lector de PDF. Debido a que la aplicación local puede acceder al archivo directamente, este no se transfiere por la red a través de ICA para abrirse.

## **Requisitos, consideraciones y limitaciones**

Acceso a aplicaciones locales recibe soporte en los sistemas operativos válidos para los VDA de SO multisesión Windows y los VDA de SO de sesión única Windows. Acceso a aplicaciones locales requiere la aplicación Citrix Workspace para Windows 4.1 (versión mínima). Se admiten los siguientes exploradores web:

- Internet Explorer 11 Puede usar Internet Explorer 8, 9 o 10, pero Microsoft admite (y Citrix recomienda usar) la versión 11.
- Firefox 3.5 a 21.0
- Chrome 10

Citrix Viewer también debe estar habilitado en el VDA.

Tenga en cuenta las siguientes consideraciones y limitaciones al usar las funciones Acceso a aplicaciones locales y Redirección de URL.

- La función Acceso a aplicaciones locales está diseñada para escritorios virtuales en pantalla completa expandida a todos los monitores:

- Si la función Acceso a aplicaciones locales se usa con un escritorio virtual que se ejecuta en modo de ventana o no se expande por todos los monitores, la experiencia de usuario puede ser confusa.
- Varios monitores: Si uno de ellos está maximizado, se convierte en el escritorio predeterminado de todas las aplicaciones que se inician en esa sesión. Este comportamiento predeterminado se da aunque las aplicaciones posteriores se iniciaran habitualmente en otro monitor.
- Esta función admite un solo VDA. No hay integración con varios VDA simultáneos.
- Algunas aplicaciones pueden funcionar de manera inesperada, afectando a los usuarios:
  - Las letras de unidad pueden resultar confusas; por ejemplo, C: local, en lugar de C: del escritorio virtual.
  - Las impresoras disponibles en el escritorio virtual no están disponibles para las aplicaciones locales.
  - Las aplicaciones que requieren permisos elevados no se pueden iniciar como aplicaciones alojadas en el cliente.
  - No hay tratamiento especial para aplicaciones de una sola instancia (como el Reproductor de Windows Media).
  - Las aplicaciones locales aparecen con el tema de Windows de la máquina local.
  - No se admiten las aplicaciones de pantalla completa. Estas aplicaciones pueden ser aquellas que se abren en el modo de pantalla completa, como las presentaciones con diapositivas de PowerPoint o los visores de fotos que ocupan todo el escritorio.
  - La función Acceso a aplicaciones locales copia al VDA las propiedades de la aplicación local (como los accesos directos en el escritorio del cliente y el menú Inicio). No obstante, no copia otras propiedades, como las teclas de acceso directo y los atributos de solo lectura.
  - Las aplicaciones que personalizan cómo se trata el orden de las ventanas superpuestas pueden mostrar resultados impredecibles. Por ejemplo, es posible que algunas ventanas estén ocultas.
  - No se admiten los accesos directos, incluidos los de Mi PC, Papelera de reciclaje, Panel de control, Unidad de red y carpetas.
  - Los siguientes archivos y tipos de archivo no se admiten: tipos de archivo personalizados, archivos que no están asociados a ningún programa, archivos ZIP y archivos ocultos.
  - La agrupación de la barra de tareas no recibe soporte en caso de aplicaciones alojadas en el cliente o aplicaciones del VDA que combinan 32 bits y 64 bits. Es decir, la agrupación de aplicaciones locales de 32 bits con aplicaciones de VDA de 64 bits.
  - Las aplicaciones no se pueden iniciar con COM. Por ejemplo: si hace clic en un documento de Office incrustado desde una aplicación de Office, el inicio del proceso no se puede detectar y falla la integración de la aplicación local.
- Los escenarios de doble salto, en los que un usuario inicia un escritorio virtual desde otra sesión

de escritorio virtual, no se admiten.

- La función Redirección de URL solo admite direcciones URL explícitas (es decir, aquellas que aparecen en la barra de direcciones del explorador o las que se encuentran navegando dentro del explorador, según el explorador que se esté utilizando).
- Redirección de URL solo funciona con sesiones de escritorio, no con sesiones de aplicación.
- La carpeta de escritorio local en una sesión de VDA no permite que los usuarios creen archivos.
- Varias instancias de una aplicación que se ejecuta localmente se comportan de acuerdo con la configuración de barras de tareas establecida para el escritorio virtual. Sin embargo, los accesos directos de aplicaciones ejecutadas localmente no se agrupan con las instancias en ejecución de esas aplicaciones. Tampoco se agrupan con instancias en ejecución de aplicaciones alojadas ni con los accesos directos anclados a aplicaciones alojadas. Los usuarios solo pueden cerrar las ventanas de las aplicaciones que se ejecutan localmente desde la barra de tareas. Si bien los usuarios pueden anclar las ventanas de las aplicaciones locales a la barra de tareas del escritorio y al menú Inicio, es posible que las aplicaciones no se inicien de forma consistente cuando se usen estos accesos directos.
- Si **habilita** la configuración de directiva **Permitir acceso a aplicaciones locales**, no se admite la redirección de contenido del explorador web.

## Interacción con Windows

La interacción de la función Acceso a aplicaciones locales con Windows incluye los siguientes comportamientos.

- Comportamiento de los accesos directos en Windows 8 y Windows Server 2012
  - Las aplicaciones de la Tienda Windows instaladas en el cliente no se indican en la lista de accesos directos de la función Acceso a aplicaciones locales.
  - Los archivos de imagen y vídeo se abren de forma predeterminada con las aplicaciones de la Tienda Windows. Sin embargo, la función Acceso a aplicaciones locales enumera las aplicaciones de la Tienda Windows y abre los accesos directos con aplicaciones de escritorio.
- Programas locales
  - Para Windows 7, la carpeta está disponible en el menú Inicio.
  - Para Windows 8, Programas locales solo está disponible si el usuario selecciona **Todas las aplicaciones** como una categoría desde la pantalla de Inicio. No se muestran todas las subcarpetas en Programas locales.
- Funciones de elementos gráficos de Windows 8 para aplicaciones
  - Las aplicaciones de escritorio están limitadas al área del escritorio y las cubren la pantalla Inicio y las aplicaciones de estilo de Windows 8.

- Las aplicaciones de acceso local no se comportan como aplicaciones de escritorio cuando se tienen varios monitores. En el modo de varios monitores, la pantalla de Inicio y el escritorio se muestran en monitores diferentes.
- Windows 8 y redirección de URL de acceso a aplicaciones locales
  - Como el Internet Explorer de Windows 8 no tiene complementos habilitados, use el Internet Explorer de escritorio para habilitar la redirección de URL.
  - En Windows Server 2012, Internet Explorer inhabilita los complementos de forma predefinida. Para implementar la redirección de URL, inhabilite la configuración mejorada de Internet Explorer. A continuación, restablezca las opciones de Internet Explorer y reinicie el programa para asegurarse de que los complementos están habilitados para los usuarios estándar.

## Configurar el acceso a aplicaciones locales y la redirección de URL

Para usar las funciones Acceso a aplicaciones locales y Redirección de URL con la aplicación Citrix Workspace:

- Instale la aplicación Citrix Workspace en la máquina cliente local. Puede habilitar ambas funciones durante la instalación de la aplicación Citrix Workspace, o bien, puede habilitar la plantilla de Acceso a aplicaciones locales mediante el Editor de directivas de grupo.
- Establezca la configuración de directiva **Permitir acceso a aplicaciones locales** como **Habilitada**. También puede configurar la lista de direcciones URL permitidas y la lista de direcciones URL bloqueadas para la redirección de URL. Para obtener más información, consulte [Configuraciones de directiva de Acceso a aplicaciones locales](#).

## Habilitar el acceso a aplicaciones locales y la redirección de URL

Para habilitar el acceso a aplicaciones locales para todas las aplicaciones locales, siga estos pasos:

1. Inicie Citrix Studio.
  - Para implementaciones locales, abra **Citrix Studio** desde el **menú Inicio**.
  - Para las implementaciones de servicios de Cloud, vaya a **Citrix Cloud > Virtual Apps and Desktops Service > ficha Administrar**.
2. En el panel de navegación de Studio, haga clic en **Directivas**.
3. En el panel Acciones, haga clic en **Crear directiva**.
4. En la ventana Crear directiva, escriba “Permitir acceso a aplicaciones locales” en el cuadro de búsqueda y, a continuación, haga clic en **Seleccionar**.

5. En la ventana Modificar parámetros, seleccione **Permitido**. De forma predeterminada, la directiva **Permitir acceso a aplicaciones locales** está prohibida. Con esta configuración habilitada, el VDA permite que el cliente decida si se habilitan los accesos directos de acceso a aplicaciones locales y aplicaciones publicadas por el administrador de cara a la sesión (si esta configuración está prohibida, no funcionan en el VDA ni los accesos directos de Acceso a aplicaciones locales ni las aplicaciones publicadas). Esta configuración de directiva se aplica a toda la máquina y a la directiva Redirección de URL.
6. En la ventana Crear directiva, escriba “Lista de redirección de direcciones URL permitidas” en el cuadro de búsqueda y, a continuación, haga clic en **Seleccionar**. La lista de redirección de direcciones URL permitidas especifica las URL que se pueden abrir en el explorador predeterminado de la sesión remota.
7. En la ventana Modificar configuración, haga clic en **Agregar** para agregar las URL y, a continuación, haga clic en **Aceptar**.
8. En la ventana Crear directiva, escriba “Lista de redirección de direcciones URL bloqueadas” en el cuadro de búsqueda y, a continuación, haga clic en **Seleccionar**. La lista de redirección de direcciones URL bloqueadas especifica las URL que se redirigen al explorador predeterminado que se ejecuta en el dispositivo de punto final.
9. En la ventana Modificar configuración, haga clic en **Agregar** para agregar las URL y, a continuación, haga clic en **Aceptar**.
10. En la página Parámetros, haga clic en **Siguiente**.
11. En la página Usuarios y máquinas, asigne la directiva a los grupos de entrega correspondientes y, a continuación, haga clic en **Siguiente**.
12. En la página Resumen, revise los parámetros y, a continuación, haga clic en **Finalizar**.

Para habilitar la redirección de URL en todas las aplicaciones locales durante la instalación de la aplicación Citrix Workspace, siga estos pasos:

1. Habilite y la redirección de URL durante la instalación de la aplicación Citrix Workspace para todos los usuarios de una máquina. Al hacerlo, también se registran los complementos del explorador necesarios para la redirección de URL.
2. En el símbolo del sistema, ejecute el comando apropiado para instalar la aplicación Citrix Workspace con una de las opciones siguientes:
  - Para CitrixReceiver.exe, utilice `/ALLOW_CLIENHOSTEDAPPSURL=1`.
  - Para CitrixReceiverWeb.exe, utilice `/ALLOW_CLIENHOSTEDAPPSURL=1`.

## Habilitar la plantilla de acceso a aplicaciones locales mediante el Editor de directivas de grupo

### Nota:

- Antes de habilitar la plantilla de acceso a aplicaciones locales mediante el Editor de direc-

- tivas de grupo, agregue los archivos de plantilla receiver.admx/adml al GPO local.
- Los archivos de plantilla de la aplicación Citrix Workspace para Windows están disponibles en el GPO local, en la carpeta **Plantillas administrativas > Componentes de Citrix > Citrix Workspace** solamente al agregar los archivos CitrixBase.admx o CitrixBase.adml a la carpeta %systemroot%\policyDefinitions.

Para habilitar la plantilla de acceso a aplicaciones locales mediante el Editor de directivas de grupo, siga estos pasos:

1. Ejecute **gpedit.msc**.
2. Vaya a **Configuración del equipo > Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Componentes de Citrix > Citrix Workspace > Experiencia de usuario**.
3. Haga clic en **Configuración del acceso a aplicaciones locales**.
4. Seleccione **Habilitada** y, a continuación, seleccione **Permitir redirección de URL**. Para la redirección de URL, registre los complementos del explorador web desde la línea de comandos, como se describe en la sección *Registro de complementos del explorador web* que aparece más abajo en este artículo.

### Proporcionar acceso solo a las aplicaciones publicadas

Puede proporcionar acceso a aplicaciones publicadas de una de estas dos formas:

Utilice el Editor del Registro.

1. En el servidor donde está instalado Citrix Studio, ejecute regedit.exe.
2. Vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\DesktopStudio`.
3. Agregue la entrada REG\_DWORD `ClientHostedAppsEnabled` y un valor de 1 (un valor 0 inhabilita el acceso a aplicaciones locales).

Use el SDK de PowerShell.

1. Abra PowerShell en la máquina donde se ejecuta el Delivery Controller.
2. Escriba el siguiente comando: `set-configsitemetadata -name "studio_clientHostedApps" -value "true"`.

Para tener acceso a **Agregar aplicación de acceso local** en una implementación de servicio de Cloud, use el SDK de PowerShell remoto de Citrix Virtual Apps and Desktops. Para obtener más información, consulte [SDK de PowerShell remoto de Citrix Virtual Apps and Desktops](#).

1. Descargue el instalador:

<https://download.apps.cloud.com/CitrixPoshSdk.exe>

2. Ejecute estos comandos:

- a) `asnp citrix.*`
  - b) `Get-XdAuthentication`
3. Escriba el siguiente comando: `set-configsite metadata -name "studio_clientHostedApps" -value "true"`.

Después de completar los pasos correspondientes anteriores, siga estos pasos para continuar.

1. Abra **Citrix Studio** desde el menú **Inicio**.
2. En el panel de navegación de Studio, haga clic en **Aplicaciones**.
3. En el panel central superior, haga clic con el botón secundario en el área vacía y seleccione **Agregar aplicación de acceso local** en el menú contextual. También puede hacer clic en **Agregar aplicación de acceso local** en el panel Acciones. Para mostrar la opción Agregar aplicación de acceso local en el panel Acciones, haga clic en **Actualizar**.
4. Publique aplicaciones de acceso local.
  - El asistente de acceso a aplicaciones locales se inicia con una página introductoria, la cual se puede eliminar de futuros inicios de este asistente.
  - El asistente le guiará a través de las páginas Grupos, Ubicación, Identificación, Entrega y Resumen que se describen a continuación. Cuando haya terminado con cada página, haga clic en **Siguiente** para ir a la página Resumen.
  - En la página Grupos, seleccione uno o varios grupos de entrega donde se agregarán las nuevas aplicaciones y, a continuación, haga clic en **Siguiente**.
  - En la página Ubicación, escriba toda la ruta ejecutable de la aplicación que hay en la máquina local del usuario y, también, la ruta a la carpeta donde se encuentra la aplicación. Citrix recomienda utilizar la ruta con variables de entorno del sistema; por ejemplo, `%ProgramFiles(x86)%\Internet Explorer\iexplore.exe`.
  - En la página Identificación, acepte los valores predeterminados o escriba la información que quiera y, a continuación, haga clic en **Siguiente**.
  - En la página Entrega, configure cómo se entregará esta aplicación a los usuarios y, a continuación, haga clic en **Siguiente**. Puede especificar el icono de la aplicación seleccionada. También puede indicar si el acceso directo a la aplicación local en el escritorio virtual estará visible en el menú Inicio, en el escritorio o en ambos.
  - En la página Resumen, revise los parámetros y, a continuación, haga clic en **Finalizar** para salir del asistente de acceso a aplicaciones locales.

## Registrar complementos del explorador web

### Nota

Los complementos del explorador web necesarios para la redirección de URL se registran automáticamente al instalar la aplicación Citrix Workspace desde la línea de comandos con la opción `/ALLOW_CLIENTHOSTEDAPPSURL=1`.

Puede usar los siguientes comandos para registrar y cancelar el registro de uno o todos los complementos:

- Para registrar complementos en un dispositivo cliente: `<carpeta de instalación del cliente>\redirector.exe /reg<explorador>`
- Para cancelar el registro de complementos en un dispositivo cliente: `<carpeta de instalación del cliente>\redirector.exe /unreg<explorador>`
- Para registrar complementos en un VDA: `<carpeta de instalación del VDA>\VDARedirector.exe /reg<explorador>`
- Para cancelar el registro de complementos en un VDA: `<carpeta de instalación del VDA>\VDARedirector.exe /unreg<explorador>`

Donde `<explorador>` es Internet Explorer, Firefox, Chrome o Todo.

Por ejemplo, el siguiente comando registra complementos de Internet Explorer en un dispositivo que ejecuta la aplicación Citrix Workspace.

```
C:\Archivos de programa\Citrix\ICA Client\redirector.exe/regIE
```

El siguiente comando registra todos los complementos en un VDA para sistemas operativos multi-sesión Windows.

```
C:\Archivos de programa (x86)\Citrix\System32\VDARedirector.exe /regAll
```

### Interceptación de URL entre exploradores web

- De manera predeterminada, Internet Explorer redirige la dirección URL que se haya introducido. Si la URL no está en la lista de bloqueados, pero el explorador o el sitio web la redirigen a otra URL, la URL final no se redirige. No se redirige incluso aunque esté en la lista de bloqueados.

Para que la redirección de URL funcione correctamente, habilite el complemento cuando lo solicite el explorador web. Si se inhabilitan los complementos que usan las opciones de Internet o los que pide el sistema, la redirección de URL no funciona correctamente.

- Los complementos de Firefox siempre redirigen las direcciones URL.

Cuando se instala un complemento, Firefox pide confirmación para permitir o impedir la instalación del complemento en una página de nueva pestaña. Permita el complemento para poder usar esta función.

- El complemento de Chrome siempre redirige la URL final de navegación y no las direcciones URL introducidas.

Las extensiones han sido instaladas externamente. Al inhabilitar la extensión, la función Redirección de URL no funciona en Chrome. Si se necesita la redirección de URL en modo de incógnito, permita que la extensión se ejecute en ese modo en la Configuración del explorador.

## Configurar el comportamiento de la aplicación local al cerrar sesión y al desconectar

### Nota:

Si no sigue estos pasos para configurar los parámetros, de forma predeterminada las aplicaciones locales siguen ejecutándose cuando un usuario cierra la sesión o se desconecta del escritorio virtual. Tras la reconexión, las aplicaciones locales vuelven a integrarse si están disponibles en el escritorio virtual.

1. En el escritorio alojado, ejecute **regedit.msc**.
2. Vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Client Hosted Apps\Policies\Session State`.

En un sistema de 64 bits, desplácese hasta `HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies\Session State`.

3. Agregue la entrada REG\_DWORD **Terminate** y uno de estos valores:
  - 1 - Las aplicaciones locales siguen ejecutándose cuando un usuario cierra sesión o se desconecta del escritorio virtual. Tras la reconexión, las aplicaciones locales vuelven a integrarse si están disponibles en el escritorio virtual.
  - 3 - Las aplicaciones locales se cierran cuando el usuario cierra la sesión o se desconecta del escritorio virtual.

## Consideraciones sobre unidades del cliente y redirección de USB genérico

April 19, 2024

La tecnología HDX ofrece **optimización** con los dispositivos USB más comunes. La optimización ofrece una experiencia de usuario mejorada, con mejor rendimiento y eficiencia del ancho de banda en una conexión por red WAN. La optimización suele ser la mejor opción, sobre todo en entornos de alta latencia o cuando se requiera confidencialidad.

La tecnología HDX ofrece la **redirección de USB genérico** para dispositivos específicos sin optimización o cuando esta no es adecuada; por ejemplo:

- El dispositivo USB tiene otras funciones avanzadas que no forman parte de la optimización, como mouse o cámaras web con botones adicionales.
- Los usuarios necesitan funciones que no forman parte de la optimización.
- Los dispositivos USB es un dispositivo especializado, como un equipo de pruebas o mediciones, o bien un automatismo industrial.
- Una aplicación requiere acceso directo al dispositivo como dispositivo USB.
- El dispositivo USB solo tiene disponible un controlador Windows. Por ejemplo, un lector de tarjetas inteligentes puede no tener disponible un controlador para la aplicación Citrix Workspace para Android.
- La versión de la aplicación Citrix Workspace no ofrece ninguna optimización para este tipo de dispositivo USB.

Con la redirección de USB genérico:

- Los usuarios no necesitan instalar controladores de dispositivos en el dispositivo de usuario.
- Los controladores de cliente de USB se instalan en la máquina del VDA.

#### **Importante:**

- La redirección de USB genérico puede utilizarse junto con la optimización. Si habilita la redirección USB genérica, configure las [directivas de dispositivos USB](#) de Citrix tanto para la redirección USB genérica como para la funcionalidad optimizada.
- La configuración de directiva [Reglas de optimización de dispositivos USB del cliente](#) de Citrix es una configuración específica para la redirección USB genérica, para un determinado de dispositivo USB. No se aplica a la optimización que se describe aquí.
- Al hacer de intermediario de una sesión mediante el software de Citrix con una máquina virtual de Azure, Citrix proporciona el máximo soporte para la redirección USB a la máquina virtual de Azure. Ofrecemos soporte para la solución de problemas del software de Citrix, pero no para la máquina virtual de Azure subyacente.

## **Consideraciones de rendimiento para dispositivos USB**

Con la redirección de USB genérico, para algunos tipos de dispositivos USB, la latencia de red y el ancho de banda pueden afectar a la experiencia de usuario y al funcionamiento del dispositivo USB. Por ejemplo, es posible que los dispositivos que tengan en cuenta el tiempo no funcionen correctamente en conexiones con enlaces de alta latencia y poco ancho de banda. En su lugar, se usa la optimización, si es posible.

Algunos dispositivos USB requieren mucho ancho de banda para poderse usar, por ejemplo, un mouse 3D (se usa con aplicaciones 3D que también suelen requerir una gran cantidad de ancho de banda).

Si no se puede aumentar el ancho de banda, es posible que pueda mitigar el problema ajustando el uso del ancho de banda de otros componentes mediante las configuraciones de directiva de ancho de banda. Para obtener más información, consulte [Configuraciones de directiva de Ancho de banda](#) para la redirección de dispositivos USB del cliente y [Configuraciones de directiva de Conexiones de multisección](#).

## Consideraciones de seguridad para dispositivos USB

Algunos dispositivos USB implican el uso de información confidencial por naturaleza; por ejemplo, los lectores de tarjetas inteligentes, los lectores de huellas digitales y los paneles táctiles de firma electrónica. Otros dispositivos USB, como los dispositivos de almacenamiento USB, se pueden usar para la transmisión de datos confidenciales.

Los dispositivos USB se utilizan con frecuencia para distribuir software malicioso (malware). Configurar la aplicación Citrix Workspace y Citrix Virtual Apps and Desktops puede reducir (pero no eliminar) el riesgo proveniente de esos dispositivos USB. Esta situación se aplica cuando se utiliza la optimización o la redirección de USB genérico.

### Importante:

En caso de dispositivos y datos confidenciales, proteja siempre la conexión HDX mediante [TLS](#) o [IPsec](#).

Habilite solo los dispositivos USB que necesite. Configure la redirección de USB genérico y la optimización para ello.

Proporcione instrucciones a los usuarios para el uso seguro de dispositivos USB:

- Usar solo dispositivos USB que se hayan obtenido de una fuente fiable.
- No dejar los dispositivos USB desatendidos en entornos abiertos (por ejemplo, una unidad flash en un cibercafé).
- Explique los riesgos de usar un dispositivo USB en más de un equipo.

## Compatibilidad con la redirección de USB genérico

La redirección de USB genérico se admite en dispositivos USB 2.0 y versiones anteriores. También se admite la redirección de USB genérico en dispositivos USB 3.0 conectados a puertos USB 2.0 o USB 3.0. En cambio, la redirección de USB genérico no admite las funciones de USB introducidas en USB 3.0 tales como la velocidad extra.

Estas aplicaciones Citrix Workspace admiten la redirección de USB genérico:

- Aplicación Citrix Workspace para Windows; consulte [Configurar la entrega de aplicaciones](#)
- Aplicación Citrix Workspace para Mac; consulte [Aplicación Citrix Workspace para Mac](#).

- Aplicación Citrix Workspace para Linux; consulte [Optimizar](#)
- Aplicación Citrix Workspace para Chrome OS; consulte [Aplicación Citrix Workspace para Chrome](#)

Para ver las versiones de la aplicación Citrix Workspace, consulte [Tabla de funciones de la aplicación Citrix Workspace](#).

Si usa versiones anteriores de la aplicación Citrix Workspace, consulte la documentación de la aplicación Citrix Workspace para ver si se admite la redirección de USB genérico. Consulte la documentación de la aplicación Citrix Workspace para ver las limitaciones de los tipos de dispositivos USB que se admiten.

La redirección de USB genérico se admite en sesiones de escritorio a partir de la versión 7.6 del VDA para SO de sesión única hasta la versión actual.

La redirección de USB genérico se admite en sesiones de escritorio a partir de la versión 7.6 del VDA para SO multisesión hasta la versión actual con las siguientes restricciones:

- El VDA debe estar ejecutándose en Windows Server 2012 R2 o Windows Server 2016.
- Los controladores del dispositivo USB deben ser compatibles con el host de sesión de Escritorio remoto (RDSH) para el SO del VDA (Windows 2012 R2), incluida la virtualización al completo.

A continuación, se ofrecen algunos tipos de dispositivos USB que no se admiten para la redirección de USB genérico porque no sería útil redirigirlos:

- Módems USB.
- Adaptadores de red USB.
- Concentradores USB. Los dispositivos USB conectados a los concentradores USB se administran de forma individual.
- Puertos USB COM virtuales. Use la redirección de puertos COM en lugar de la redirección de USB genérico.

Para obtener información acerca de los dispositivos USB que se han probado con la redirección de USB genérico, consulte [Citrix Ready Marketplace](#). Algunos dispositivos USB no funcionan correctamente con la redirección de USB genérico.

## **Configurar la redirección de USB genérico**

Puede decidir los tipos de dispositivos USB que usarán la redirección de USB genérico y configurar cada uno por separado.

- En el VDA, mediante configuraciones de directivas de Citrix. Para obtener más información, consulte [Redirección de dispositivos del cliente y dispositivos del usuario](#) y [Configuraciones de directiva de Dispositivos USB](#) en la Referencia para configuraciones de directivas.

- En la aplicación Citrix Workspace, mediante los mecanismos que dependen de la aplicación Citrix Workspace. Por ejemplo, una plantilla administrativa controla los parámetros de Registro que configuran la aplicación Citrix Workspace para Windows. De manera predeterminada, se permite la redirección USB para ciertas clases de dispositivos USB, y se rechaza para otras. Para obtener más información, consulte [Configurar](#) en la documentación de la aplicación Citrix Workspace para Windows.

Esta configuración independiente tiene la ventaja de ofrecer flexibilidad. Por ejemplo:

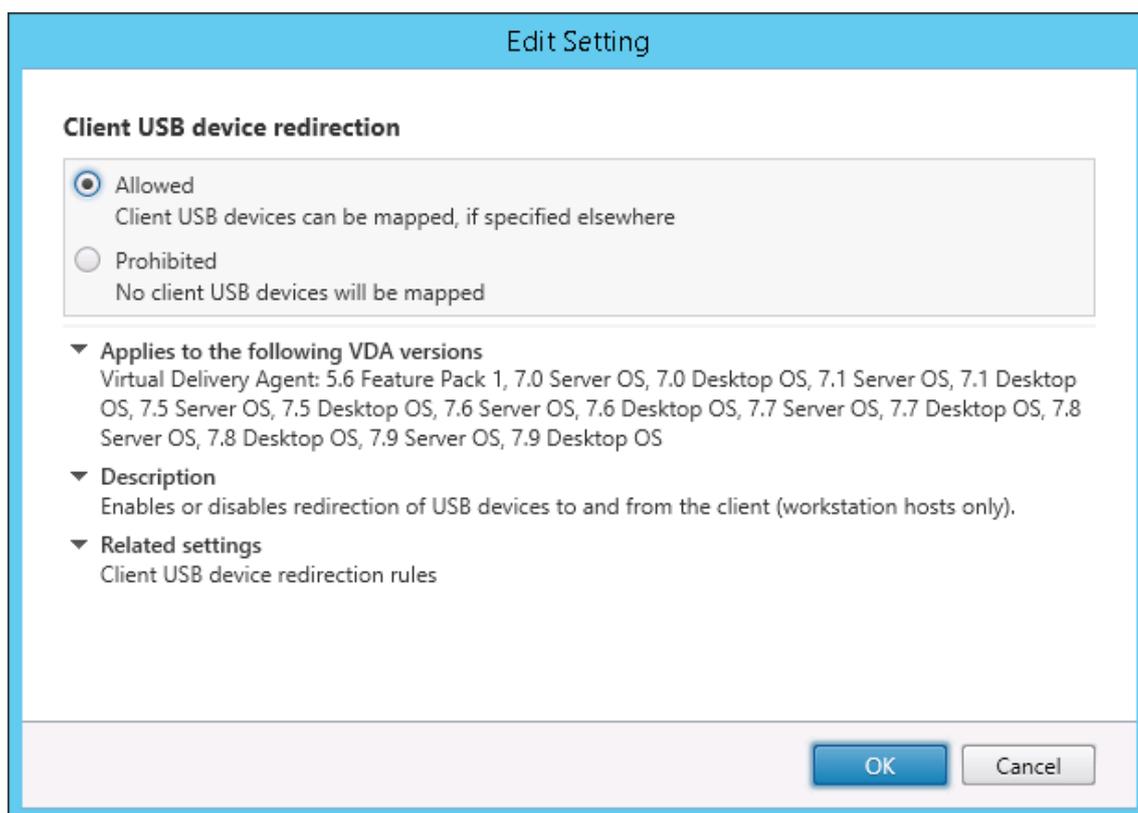
- Si dos departamentos o empresas diferentes se encargan de la aplicación Citrix Workspace y del VDA, pueden aplicar medidas de control por separado. Esta configuración se aplica cuando un usuario, ubicado en una empresa, acceda a una aplicación ubicada en otra empresa.
- Las configuraciones de directivas de Citrix sirven para controlar si se permiten dispositivos USB a ciertos usuarios o solo a aquellos usuarios que se conecten por medio de una red de área local (en lugar de hacerlo con Citrix Gateway).

### **Habilitar la redirección de USB genérico**

Para habilitar la redirección de USB genérico y no requerir una redirección manual por parte del usuario, defina las configuraciones de directivas Citrix y las preferencias de conexión de la aplicación Citrix Workspace.

En configuraciones de directiva de Citrix:

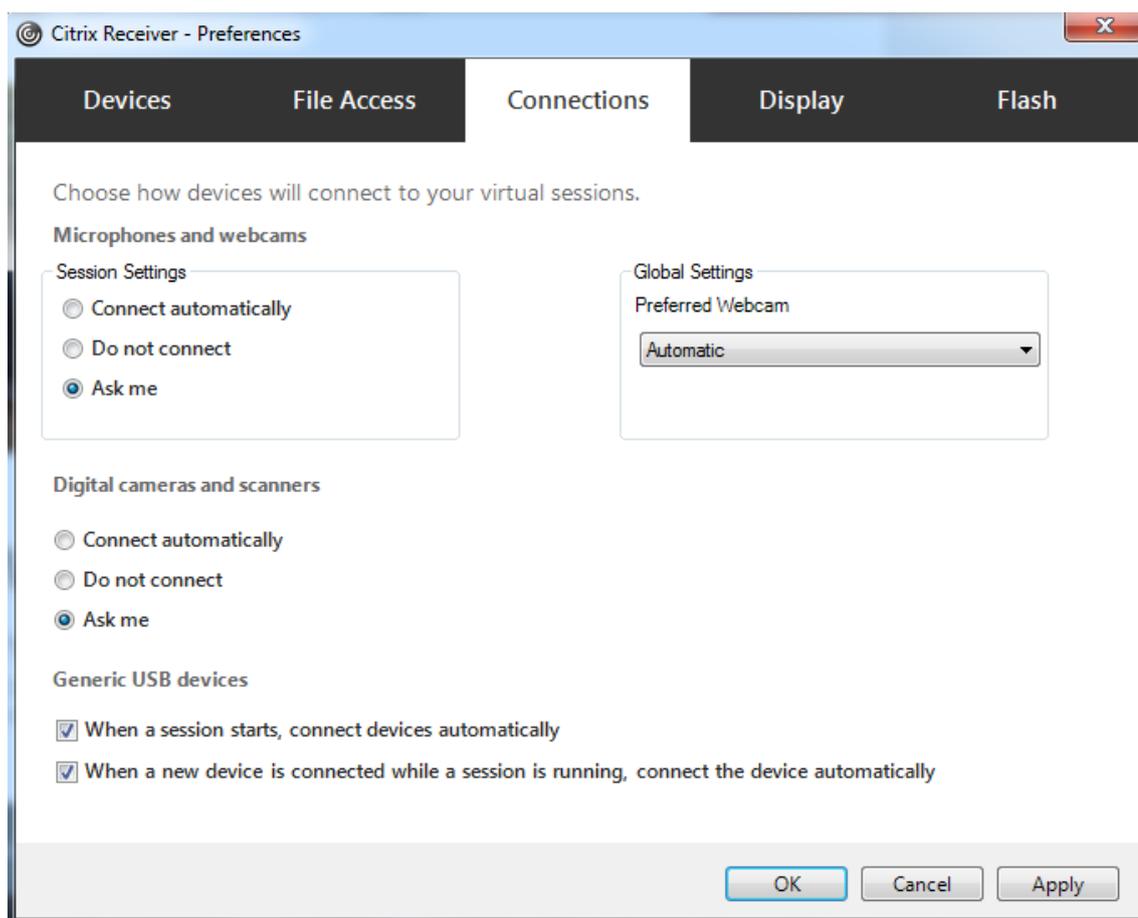
1. Agregue [Redirección de dispositivos USB del cliente](#) a una directiva y establezca su valor en **Permitida**.



2. (Optativo.) Para actualizar la lista de dispositivos USB disponibles para la redirección, agregue la configuración [Reglas de redirección de dispositivos USB del cliente](#) a una directiva y especifique las reglas de la directiva USB.

En la aplicación Citrix Workspace:

3. Especifique que los dispositivos se conecten automáticamente, sin redirección manual. Puede hacerlo mediante una plantilla administrativa, o bien en la aplicación Citrix Workspace para Windows > Preferencias > Conexiones.



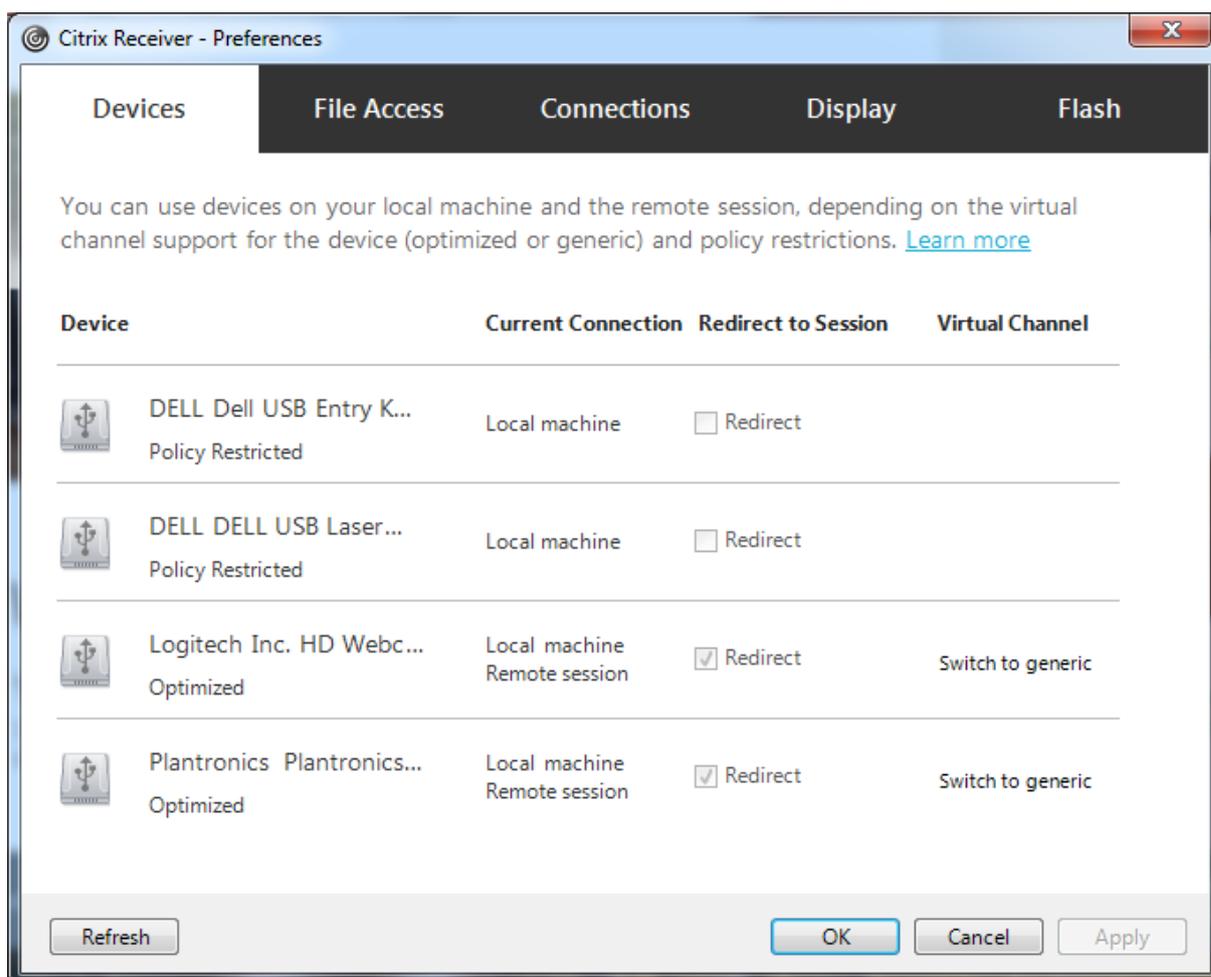
Si especificó reglas de directiva USB para el VDA en el paso anterior, especifique las mismas reglas de directiva para la aplicación Citrix Workspace.

Para los clientes ligeros, consulte al fabricante para obtener detalles sobre la compatibilidad con USB y cualquier configuración requerida.

### **Configurar los tipos de dispositivos USB disponibles para la redirección de USB genérico**

Los dispositivos USB se redirigen automáticamente cuando la compatibilidad con USB está habilitada y la configuración de las preferencias de usuario para USB está definida para conectar automáticamente los dispositivos USB. Los dispositivos USB también se redirigen automáticamente cuando la barra de conexión no está presente.

Los usuarios pueden redirigir explícitamente dispositivos que no se redirigen automáticamente. Para ello, deberán seleccionarlos en la lista de dispositivos USB. Para obtener más información, consulte el artículo [Mostrar los dispositivos en Desktop Viewer](#) en la ayuda de la aplicación Citrix Workspace para Windows.



Para usar la redirección de USB genérico en lugar de la optimización, puede:

- En la aplicación Citrix Workspace, seleccione manualmente el dispositivo USB con que se va a usar la redirección de USB genérico, elija **Cambiar a genérico** en la ficha “Dispositivos” del cuadro de diálogo “Preferencias”.
- Seleccione automáticamente el dispositivo USB con que se va a usar la redirección de USB genérico. Para ello, configure la redirección automática para el tipo de dispositivo USB (por ejemplo, `AutoRedirectStorage=1`) y establezca las preferencias de usuario para USB en la conexión automática de los dispositivos USB. Para obtener más información, consulte [Configure automatic redirection of USB devices](#).

**Nota:**

Configure la redirección de USB genérico para cámara web solo si esta no resulta compatible con la redirección multimedia HDX.

Para evitar que los dispositivos USB se redirijan o se enumeren, puede especificar reglas de dispositivo para la aplicación Citrix Workspace y el VDA.

Para la redirección de USB genérico, debe conocer al menos la clase y la subclase del dispositivo USB. No todos los dispositivos USB utilizan una clase y una subclase obvias. Por ejemplo:

- Las llaves de memoria o datos utilizan la clase de dispositivo del mouse.
- Los lectores de tarjeta inteligente pueden usar la clase de dispositivo HID o la que defina el proveedor.

Para un control más preciso, necesitará saber el ID de proveedor, el ID de producto y el ID de versión. Puede obtener esa información del proveedor del dispositivo.

**Importante:**

Los dispositivos USB dañinos pueden presentar funciones de dispositivo USB que no coincidan con el uso previsto para ellos. Las reglas de dispositivos no se han diseñado para evitar este comportamiento.

Puede definir qué dispositivos USB están disponibles para la redirección de USB genérico especificando reglas de redirección de dispositivos USB tanto para el VDA como para la aplicación Citrix Workspace. De esta manera, se anularán las reglas predeterminadas de la directiva USB.

Para el VDA:

- Modifique las reglas de invalidación del administrador para las máquinas con sistema operativo multisección mediante las reglas de directiva de grupo. La Consola de administración de directivas de grupo se incluye en los medios de instalación:
  - Para x64: `dvd root \os\lang\x64\Citrix Policy\CitrixGroupPolicyManagement_x64.msi`
  - Para x86: `dvd root \os\lang\x86\Citrix Policy\CitrixGroupPolicyManagement_x86.msi`

En la aplicación Citrix Workspace para Windows:

- Modifique el Registro en el dispositivo del usuario. En los medios de instalación, se incluye una plantilla administrativa (archivo ADM) que permite cambiar el dispositivo cliente mediante la Directiva de grupo de Active Directory:  
`dvd root \os\lang\Support\Configuration\icaclient_usb.adm.`

**Advertencia:**

Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Las reglas predeterminadas del producto se almacenan en `HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRu`. No modifique las reglas predeterminadas del producto. En su lugar, úselas como una guía para

la creación de reglas de suplantación del administrador, según se explica a continuación en este artículo. Las suplantaciones del objeto de directiva de grupo (GPO) se evalúan antes que las reglas predeterminadas del producto.

Las reglas de suplantación del administrador se almacenan en HKLM\SOFTWARE\Policies\Citrix\PortICA\GenericU. Las reglas de directivas de GPO toman el formato **{Allow: |Deny:}** seguidas de un conjunto de expresiones *etiqueta=valor* separadas por un espacio en blanco.

Se admiten las siguientes etiquetas:

Etiqueta	Descripción
VID	Identificador del proveedor tomado del descriptor del dispositivo
PID	Identificador del producto tomado del descriptor del dispositivo
REL	Identificador de la versión tomado del descriptor del dispositivo
Class	Clase tomada del descriptor del dispositivo o de un descriptor de interfaz; consulte el sitio web de USB <a href="http://www.usb.org/">http://www.usb.org/</a> para ver los códigos de clase USB disponibles.
SubClass	Subclase, tomada del descriptor del dispositivo o de un descriptor de la interfaz
Prot	Protocolo tomado del descriptor del dispositivo o de un descriptor de la interfaz

Al crear reglas de directivas, tenga en cuenta lo siguiente:

- Las reglas no distinguen entre mayúsculas y minúsculas.
- Las reglas pueden tener un comentario optativo al final que se introduce #. No es obligatorio utilizar un delimitador y el comentario se ignora para la comparación.
- Se ignoran las líneas en blanco y las que son exclusivamente de comentario.
- El espacio en blanco se usa como separador pero no puede aparecer en el medio de un número o de un identificador. Por ejemplo: Deny: Class = 08 SubClass=05 es una regla válida, pero Deny: Class=0 Sub Class=05 no lo es.
- Las etiquetas deben utilizar el operador de coincidencia =. Por ejemplo: VID=1230.
- Cada regla debe comenzar en una línea nueva o formar parte de una lista de reglas, separadas por punto y coma.

**Nota:**

Si utiliza el archivo de plantilla ADM, debe crear reglas en una única línea, como una lista separada por punto y coma.

**Ejemplos:**

- Este ejemplo muestra una regla de directiva de USB definida por un administrador para identificadores de producto y proveedor:

```
Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse  
Deny: VID=046D # Deny all Logitech products
```

- Este ejemplo muestra una regla de directiva de USB definida por un administrador para una clase, una subclase y un protocolo definidos:

```
Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices  
Allow: Class=EF SubClass=01 # Allow Sync devices  
Allow: Class=EF # Allow all USB-Miscellaneous devices
```

## Usar y quitar dispositivos USB

Los usuarios pueden conectar un dispositivo USB antes o después de iniciar una sesión virtual.

Cuando se usa la aplicación Citrix Workspace para Windows, ocurre lo siguiente:

- Los dispositivos que se conectan después haber iniciado la sesión aparecen inmediatamente en el menú USB de Desktop Viewer.
- Si un dispositivo USB no se redirige correctamente, puede intentar resolver el problema esperando para conectar el dispositivo hasta después de que la sesión virtual se haya iniciado.
- Para evitar la pérdida de datos, use el icono de “Extracción segura” de Windows antes de quitar el dispositivo USB.

## Controles de seguridad para dispositivos de almacenamiento USB

Se ofrece optimización para dispositivos de almacenamiento USB. Esta funcionalidad forma parte de la asignación de unidades del cliente que ofrecen Citrix Virtual Apps and Desktops. En el momento en que los usuarios inician sesión, las unidades del dispositivo del usuario se asignan automáticamente a las letras de las unidades del escritorio virtual. Las unidades se muestran como carpetas compartidas que tienen letras de unidades asignadas. Para configurar la asignación de unidades del cliente, use la configuración **Unidades extraíbles del cliente**. Esta configuración se encuentra en la sección [Configuraciones de directiva de Redirección de archivos](#) en la configuración de la directiva ICA.

Con dispositivos de almacenamiento USB, puede utilizar la asignación de unidades del cliente, la redirección de USB genérico o ambas. Contrólelas mediante directivas de Citrix. Las principales diferencias son:

Función	Asignación de unidades del cliente	Redirección de USB genérico
Habilitada de forma predeterminada	Sí	No
Configuración para acceso de solo lectura	Sí	No
Acceso a dispositivo cifrado	Sí, si el cifrado se desbloquea antes de acceder al dispositivo	Sí
Dispositivos BitLocker To Go	No	No
Dispositivo que eliminar con seguridad durante una sesión	No	Sí, si se siguen las recomendaciones del sistema operativo para quitar con seguridad el dispositivo

Si la directiva de redirección de USB genérico y la directiva de asignación de unidades del cliente están ambas habilitadas y se inserta un dispositivo de almacenamiento masivo antes o después de iniciar una sesión, el dispositivo se redirige mediante la asignación de unidades del cliente. Cuando la directiva de redirección de USB genérico y la directiva de asignación de unidades del cliente están ambas habilitadas y se configura un dispositivo para la redirección automática, y se introduce un dispositivo de almacenamiento masivo antes o después de iniciar una sesión, el dispositivo se redirige mediante la redirección de USB genérico. Para obtener más información, consulte el artículo [CTX123015](#) de Knowledge Center.

**Nota:**

Se admite la redirección USB en conexiones de poco ancho de banda: por ejemplo, conexiones de 50 kbps. Sin embargo, no se admite copiar archivos de gran tamaño.

## Controlar el acceso a archivos con la asignación de unidades del cliente

Puede controlar si los usuarios pueden copiar archivos desde sus entornos virtuales a sus dispositivos de usuario. De manera predeterminada, los archivos y carpetas de las unidades asignadas del cliente están disponibles en modo de lectura/escritura dentro de la sesión.

Si quiere impedir que los usuarios agreguen o modifiquen archivos y carpetas de los dispositivos de cliente asignados, habilite la configuración de directiva **Acceso de lectura solamente a unidades del**

**cliente.** Al agregar esta configuración a una directiva, compruebe que la configuración “Redirección de unidades del cliente” está establecida en **Permitida** y también se ha agregado a la directiva.

## Imprimir

March 10, 2022

La administración de impresoras en el entorno es un proceso compuesto por varias fases:

1. Familiarización con los conceptos de impresión, en el caso de que no se haya hecho ya.
2. Planificación de la arquitectura de impresión. Esto incluye analizar las necesidades del negocio, la infraestructura existente de impresión, la interacción entre usuarios y aplicaciones con la impresión hoy día y el modelo de administración de impresión que mejor se ajusta al entorno.
3. Configuración del entorno de impresión al seleccionar un método de aprovisionamiento de impresoras y, a continuación, crear directivas para implementar el diseño de impresión. Actualización de directivas cuando se agreguen empleados o servidores nuevos.
4. Prueba de una instalación de configuración piloto de impresión antes de implementarla a los usuarios.
5. Mantenimiento del entorno de impresión Citrix mediante la administración de controladores de impresora y la optimización del rendimiento de impresión.
6. Solución de los problemas que puedan surgir.

### Conceptos de impresión

Antes de empezar a planificar el entorno, conviene comprender los conceptos principales relacionados con la impresión:

- Tipos disponibles de aprovisionamiento de impresoras
- Cómo se enrutan los trabajos de impresión
- Conceptos básicos de administración de controladores de impresora

Los conceptos de impresión se basan en los conceptos de impresión de Windows. Para configurar y administrar correctamente la impresión en su entorno es necesario conocer cómo funciona la impresión de red y de clientes en Windows y cómo se traduce esto en el funcionamiento de la impresión en este entorno.

### Proceso de impresión

En este entorno, toda impresión se inicia (por un usuario) en las máquinas que alojan las aplicaciones. Los trabajos de impresión se redirigen a través del servidor de impresión de red o un dispositivo del

usuario hacia el dispositivo de impresión.

No hay ningún espacio de trabajo persistente para los usuarios de aplicaciones y escritorios virtuales. Cuando una sesión finaliza, se elimina el área de trabajo del usuario, por lo que todos los parámetros se deben volver a generar al comienzo de cada sesión. Por lo tanto, cada vez que un usuario inicia sesión, el sistema debe volver a generar el área de trabajo del usuario.

Cuando un usuario imprime:

- Determina las impresoras que se proporcionarán al usuario. Esto es lo que se conoce como aprovisionamiento de impresoras.
- Restaura las preferencias de impresión del usuario.
- Determina la impresora predeterminada de la sesión.

Puede personalizar el modo en que se realizan estas tareas si configura las opciones de aprovisionamiento de impresoras, enrutamiento de trabajos de impresión, retención de propiedades de impresora y administración de controladores. Asegúrese de conocer el modo en que los cambios en los diferentes parámetros de las opciones pueden afectar la experiencia de usuario y el rendimiento de la impresión en el entorno.

## Aprovisionar impresoras

El proceso mediante el cual se ponen impresoras a disposición de una sesión se conoce como aprovisionamiento. El aprovisionamiento de impresoras se suele administrar de forma dinámica. Es decir, las impresoras que aparecen en una sesión no están predeterminadas ni almacenadas. En vez de eso, las impresoras se agrupan en función de las directivas a medida que se genera la sesión durante el inicio de sesión y la reconexión. Por consiguiente, las impresoras pueden cambiar según la directiva, la ubicación del usuario y los cambios de red, siempre que estén recogidos en directivas. De esta manera, los usuarios que se muevan a una ubicación diferente pueden ver los cambios realizados en su área de trabajo.

El sistema también supervisa las impresoras del cliente y ajusta de forma dinámica las impresoras creadas automáticamente durante la sesión en función de las adiciones, las eliminaciones y los cambios que se hagan en las impresoras del cliente. La detección dinámica de impresoras beneficia a los usuarios móviles, ya que se conectan desde varios dispositivos.

A continuación, se ofrecen los métodos más comunes de aprovisionamiento de impresoras:

- **Universal Print Server:** El servidor de impresión universal de Citrix, [Universal Print Server](#), ofrece impresión universal para las impresoras de red. Universal Print Server usa el controlador de impresora universal. Esta solución le permite usar un solo controlador en una máquina con sistema operativo multisesión para la impresión en red desde cualquier dispositivo.

Citrix recomienda usar Citrix Universal Print Server para situaciones en las que intervienen servidores de impresión remotos. Universal Print Server transfiere el trabajo de impresión a través de la red en un formato optimizado y comprimido, lo que minimiza el uso de red y mejora la experiencia del usuario.

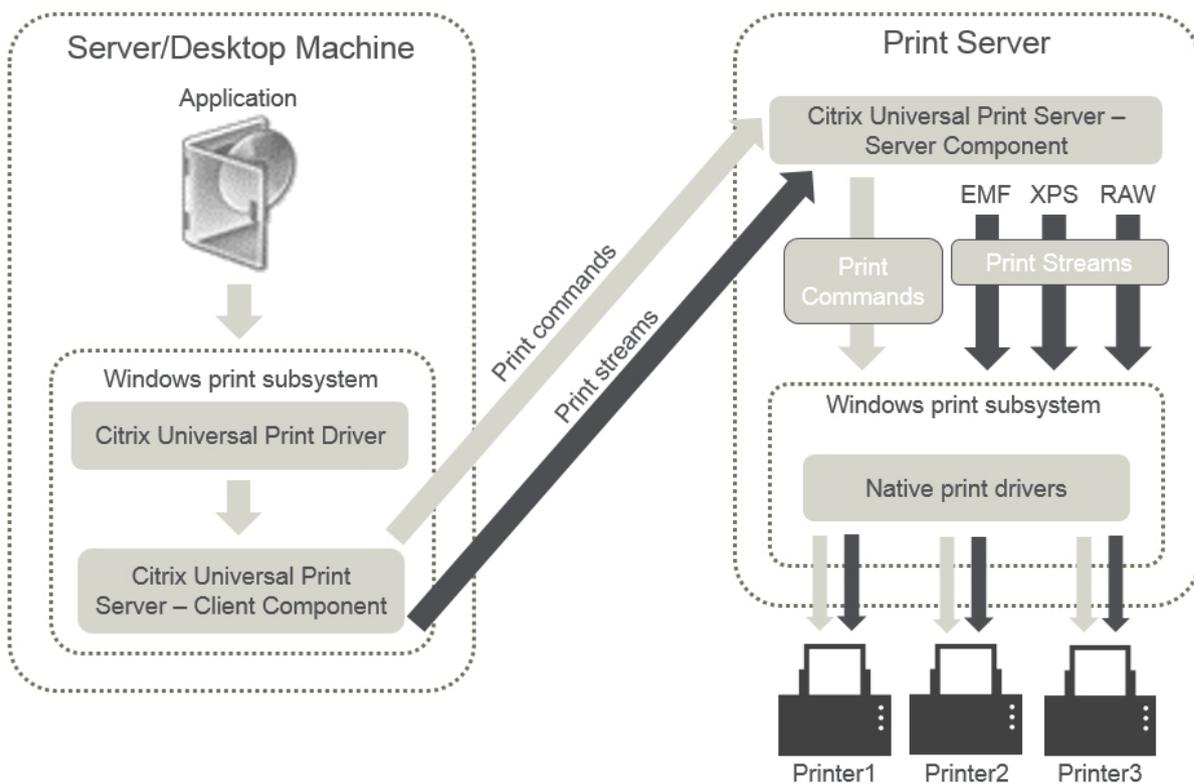
La función de Universal Print Server consta de:

Un componente de cliente, **UPClient**: Habilite UPClient en cada máquina con sistema operativo multi-sesión que aprovisione las impresoras de red de sesión y use el controlador de impresión universal.

Un componente de servidor, **UPServer**: Instale UPServer en cada servidor de impresión que aprovisiona las impresoras de red de sesión y utiliza el controlador de impresión universal para las impresoras de sesión (independientemente de si las impresoras de sesión están o no aprovisionadas centralmente).

Para obtener información acerca de la instalación y los requisitos de Universal Print Server, consulte los artículos [Requisitos del sistema](#) e [Instalar](#).

La siguiente ilustración muestra el flujo de trabajo típico que tiene una impresora de red en un entorno con Universal Print Server.



Al habilitar Citrix Universal Print Server, se aprovechan automáticamente todas las impresoras de red que están conectadas gracias a la detección automática.

**Nota:**

Universal Print Server también se admite en VDI-in-a-Box 5.3. Para obtener más información acerca de la instalación de Universal Print Server con VDI-in-a-Box, consulte la documentación de VDI-in-a-Box.

- **Creación automática:** La *Creación automática* hace referencia a las impresoras que se crean automáticamente al comienzo de cada sesión. Se pueden actualizar automáticamente tanto las impresoras de red remotas como las impresoras de cliente conectadas localmente. Considere la posibilidad de crear automáticamente solo la impresora predeterminada del cliente para entornos con un gran número de impresoras por usuario. La creación automática de un número menor de impresoras produce una sobrecarga menor (consume menos memoria y CPU) en máquinas con sistema operativo multisesión. Minimizar el número de impresoras creadas automáticamente también puede reducir el tiempo de inicio de sesión del usuario.

Las impresoras de creación automática se basan en:

- Impresoras instaladas en el dispositivo del usuario.
- Directivas que se aplican a la sesión.

Las configuraciones de directiva referentes a la creación automática le permiten limitar el número o el tipo de impresoras que se crean automáticamente. De forma predeterminada, las impresoras están disponibles en las sesiones cuando se configuran todas las impresoras en el dispositivo cliente automáticamente, incluidas las conectadas localmente a él y las impresoras de red.

Cuando el usuario finaliza la sesión, las impresoras de esa sesión se eliminan.

La creación automática de impresoras del cliente y de red va asociada a un mantenimiento. Por ejemplo, agregar una impresora requiere:

- Actualizar la configuración de directiva Impresoras de la sesión.
- Agregar el controlador a todas las máquinas con sistema operativo multisesión mediante la configuración de directiva Asignación y compatibilidad de controladores de impresora.

## Enrutamiento de trabajos de impresión

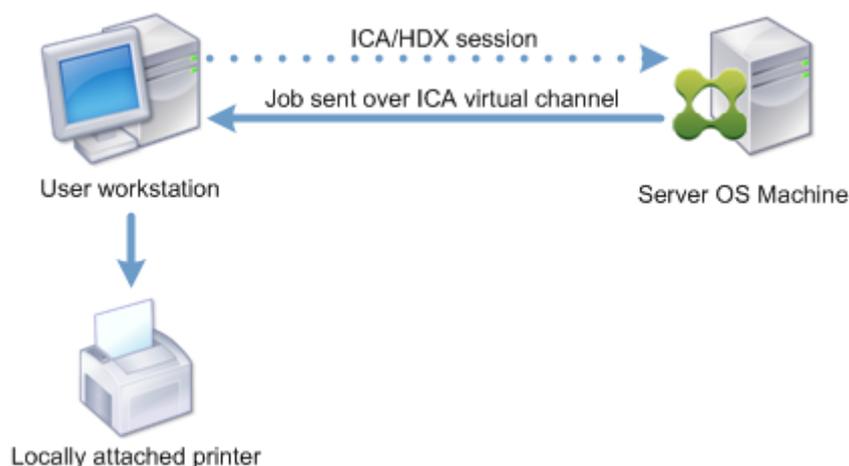
El término ruta de impresión incluye la ruta por la que se enrutan los trabajos de impresión y la ubicación donde se administran dichos trabajos en cola. Ambos aspectos de este concepto son importantes. El enrutamiento afecta al tráfico de red. La administración de la cola de impresión afecta a la utilización de recursos locales del dispositivo que procesa el trabajo de impresión.

En este entorno, los trabajos de impresión pueden tomar dos rutas para llegar a un dispositivo de impresión: a través del cliente o a través de un servidor de impresión de red. Estas rutas se conocen

como la ruta de impresión de cliente y la ruta de impresión de red. La ruta de acceso seleccionada de forma predeterminada depende del tipo de impresora utilizada.

### Impresoras conectadas localmente

El sistema redirige los trabajos a impresoras conectadas localmente desde la máquina de SO multi-sesión, a través del cliente y luego al dispositivo de impresión. El protocolo ICA optimiza y comprime el tráfico de los trabajos de impresión. Cuando un dispositivo de impresión está conectado localmente al dispositivo de usuario, los trabajos de impresión se enrutan a través del canal virtual ICA.



### Impresoras de red

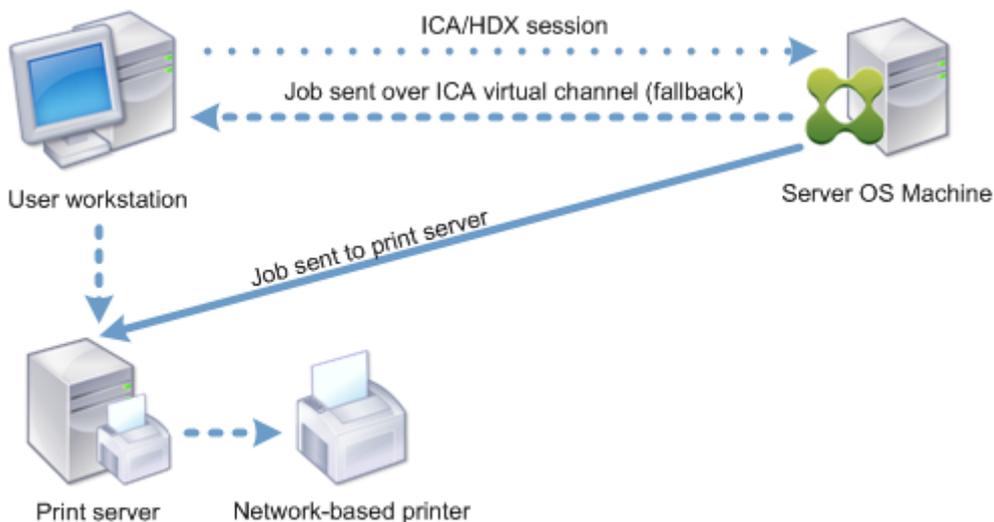
De forma predeterminada, todos los trabajos de impresión destinados a impresoras de red se enrutan desde la máquina con sistema operativo multisesión, pasan por la red y terminan directamente en el servidor de impresión. No obstante, los trabajos de impresión se enrutan automáticamente sobre la conexión ICA en las siguientes situaciones:

- Si el escritorio virtual o la aplicación no pueden establecer contacto con el servidor de impresión.
- Si el controlador nativo de impresora no está disponible en la máquina con sistema operativo multisesión.

Si Universal Print Server no está habilitado, configurar la ruta de impresión de cliente para la impresión de trabajos en red resulta útil para conexiones con poco ancho de banda, tales como las redes de área extensa (WAN). Este tipo de redes puede beneficiarse de la optimización y compresión del tráfico que se produce cuando se envían los trabajos a través de la conexión ICA.

La ruta de impresión de cliente también permite limitar el tráfico o restringir el ancho de banda asignado a los trabajos de impresión. Si no es posible enrutar trabajos a través del dispositivo del usuario,

como es el caso de clientes ligeros sin funciones de impresión, configure Calidad de servicio para priorizar el tráfico ICA/HDX y garantizar una buena experiencia de usuario durante la sesión.



### Administración de controladores de impresión

El controlador de impresora universal (UPD) de Citrix es un controlador de impresión independiente que se ha diseñado para funcionar con la mayoría de las impresoras. El controlador de impresora universal de Citrix consta de dos componentes:

**Componente del servidor.** El controlador de impresora universal de Citrix se instala como parte de la instalación de Citrix Virtual Apps and Desktops. El VDA instala los siguientes controladores con el controlador de impresora universal de Citrix: Citrix Universal Printer (controlador de EMF) y Citrix XPS Universal Printer (controlador de XPS).

Name	Processor	Type
Citrix Universal Printer	x64	Type 3 - User Mode
Citrix XPS Universal Printer	x64	Type 3 - User Mode

Los instaladores de VDA ya no ofrecen opciones para controlar la instalación del controlador de impresora PDF de Universal Print Server. El controlador de impresora PDF ahora siempre se instala automáticamente. Cuando actualiza la versión de VDA a 7.17 (o una versión posterior compatible), cualquier controlador de impresora PDF Citrix instalado previamente se elimina automáticamente y se reemplaza por la versión más reciente.

Cuando se inicia un trabajo de impresión, el controlador registra el resultado de la aplicación y lo envía, sin ninguna modificación en el dispositivo de punto final.

**Componente del cliente.** El controlador de impresora universal de Citrix se instala como parte de la instalación de la aplicación Citrix Workspace. Obtiene el flujo de impresión entrante de la sesión de

Citrix Virtual Apps and Desktops. A continuación, lo reenvía al subsistema de impresión local, donde el trabajo de impresión se genera con los controladores específicos de impresora.

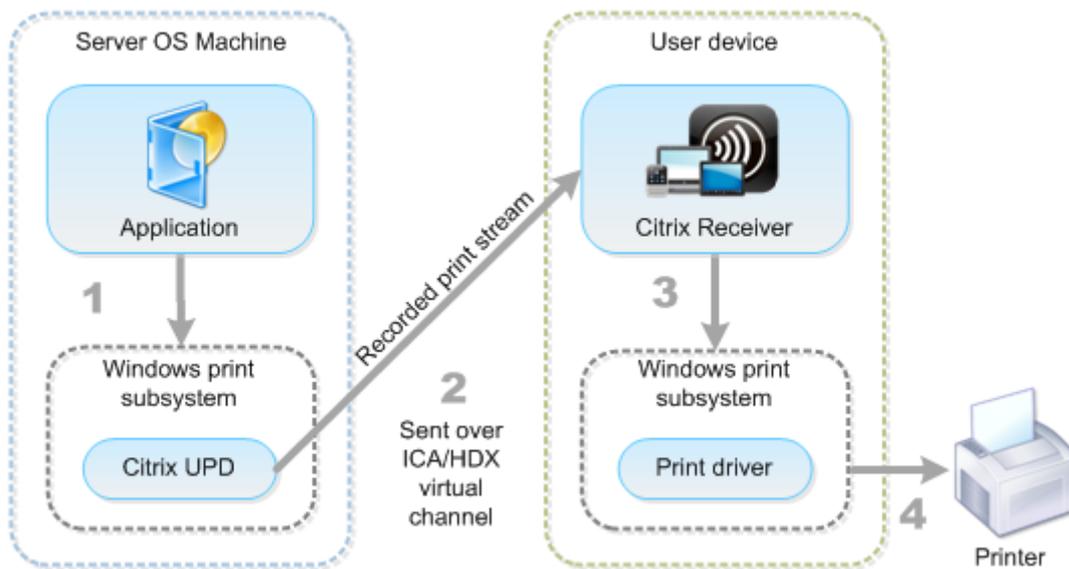
El controlador de impresora universal de Citrix admite los siguientes formatos de impresión:

- Formato **EMF**, predeterminado. EMF es la versión de 32 bits de Windows Metafile (WMF). Solo los clientes Windows pueden usar el controlador de EMF.
- XML Paper Specification (**XPS**). El controlador XPS utiliza XML para crear un “documento electrónico” independiente de la plataforma y similar al formato PDF de Adobe.
- Printer Command Language (**PCL5c** y **PCL4**). PCL es un protocolo de impresión desarrollado originalmente por Hewlett-Packard para impresoras de inyección de tinta. Se utiliza para imprimir gráficos y texto básicos, y se admite ampliamente en los periféricos multifunción y LaserJet de HP.
- PostScript (**PS**). PostScript es un lenguaje de computación que se puede usar para la impresión de texto y de gráficos vectoriales. El controlador se utiliza extensamente en impresoras de bajo coste y periféricos multifunción.

Los controladores PCL y PS son los más adecuados para dispositivos que no sean Windows (por ejemplo, un cliente Mac o UNIX). El orden en que el controlador de impresora universal de Citrix intenta usar los controladores puede cambiarse desde la configuración de directiva [Preferencia de controlador universal](#).

El controlador de impresora universal de Citrix (controladores EMF y XPS) admite funciones avanzadas de impresión, tales como el grapado y la selección del origen del papel. Estas funciones están disponibles si el controlador nativo las habilita mediante la tecnología de capacidad de impresión de Microsoft. El controlador nativo debe usar las palabras clave estándar de esquema de impresión en el XML de capacidades de impresión (Print Capabilities). Si utiliza palabras clave no estándar, las funciones de impresión avanzadas no estarán disponibles cuando se use el controlador de impresora universal de Citrix.

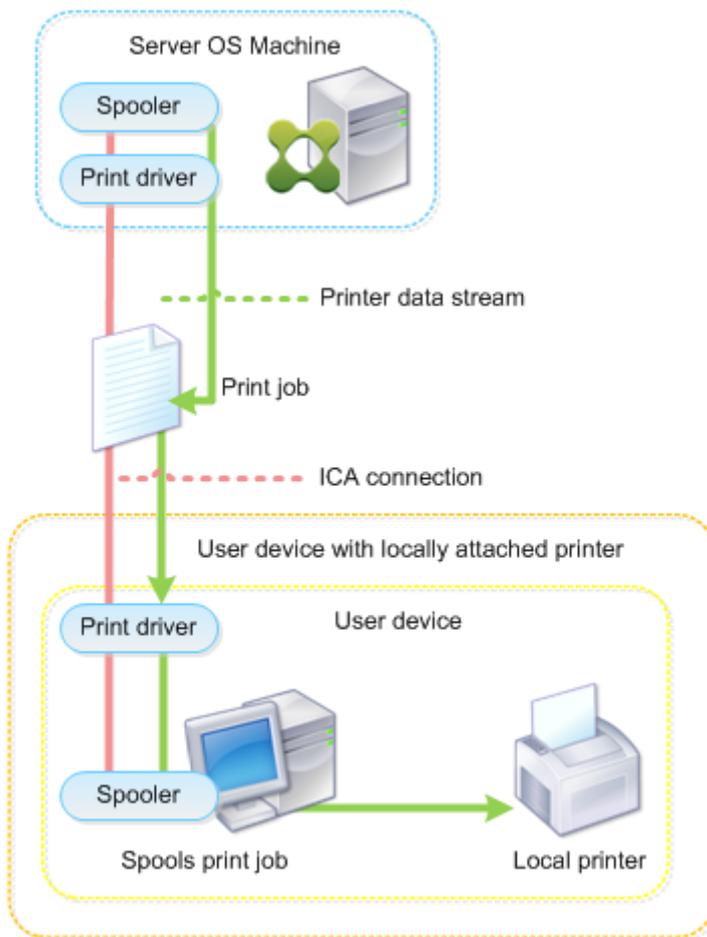
La siguiente ilustración muestra los componentes del controlador de impresión universal y el flujo de trabajo típico de una impresora conectada localmente a un dispositivo.



A la hora de planificar su estrategia de administración de controladores, decida si va a admitir controladores específicos del dispositivo, el controlador de impresión universal o ambos. Si decide admitir controladores estándar, también debe decidir:

Durante la creación automática de impresoras, si el sistema detecta una nueva impresora local conectada a un dispositivo del usuario, buscará el controlador de esa impresora en la máquina con sistema operativo multisesión. De forma predeterminada, si un controlador nativo de Windows no está disponible, el sistema usa el controlador de impresión universal.

El controlador de impresora de la máquina con sistema operativo multisesión y el controlador del dispositivo del usuario deben coincidir para que la impresión se lleve a cabo. La siguiente ilustración muestra el uso del controlador de impresora en dos sitios para la impresión del cliente.



- El tipo de controladores que admitirá.
- Si instalará o no los controladores de impresora automáticamente cuando no se encuentren en las máquinas con sistema operativo multisesión.
- Si creará o no listas de compatibilidad de controladores.

## Contenido relacionado

- [Ejemplo de configuración de la impresión](#)
- [Prácticas recomendadas, consideraciones de seguridad y operaciones predeterminadas](#)
- [Directivas y preferencias de impresión](#)
- [Aprovisionar impresoras](#)
- [Mantener el entorno de impresión](#)

## Ejemplo de configuración de la impresión

March 10, 2022

Con el fin de simplificar la administración de la impresión, elija las opciones de configuración más adecuadas a sus necesidades y su entorno. Aunque la configuración de impresión predeterminada permite a los usuarios imprimir en la mayoría de los entornos, es posible que los valores predeterminados no proporcionen ni la experiencia de usuario esperada ni el uso de red y administración de sobrecarga óptimos para el entorno.

La configuración de la impresión depende de estos factores:

- Las necesidades de su negocio y la infraestructura de impresión existente.

Diseñe la configuración de impresión teniendo en cuenta las necesidades de su organización. Estudie la implementación actual (capacidad de los usuarios para agregar impresoras, qué usuarios tienen acceso a qué impresora, etcétera) con el fin de que le sirva de guía a la hora de definir la configuración de la impresión.

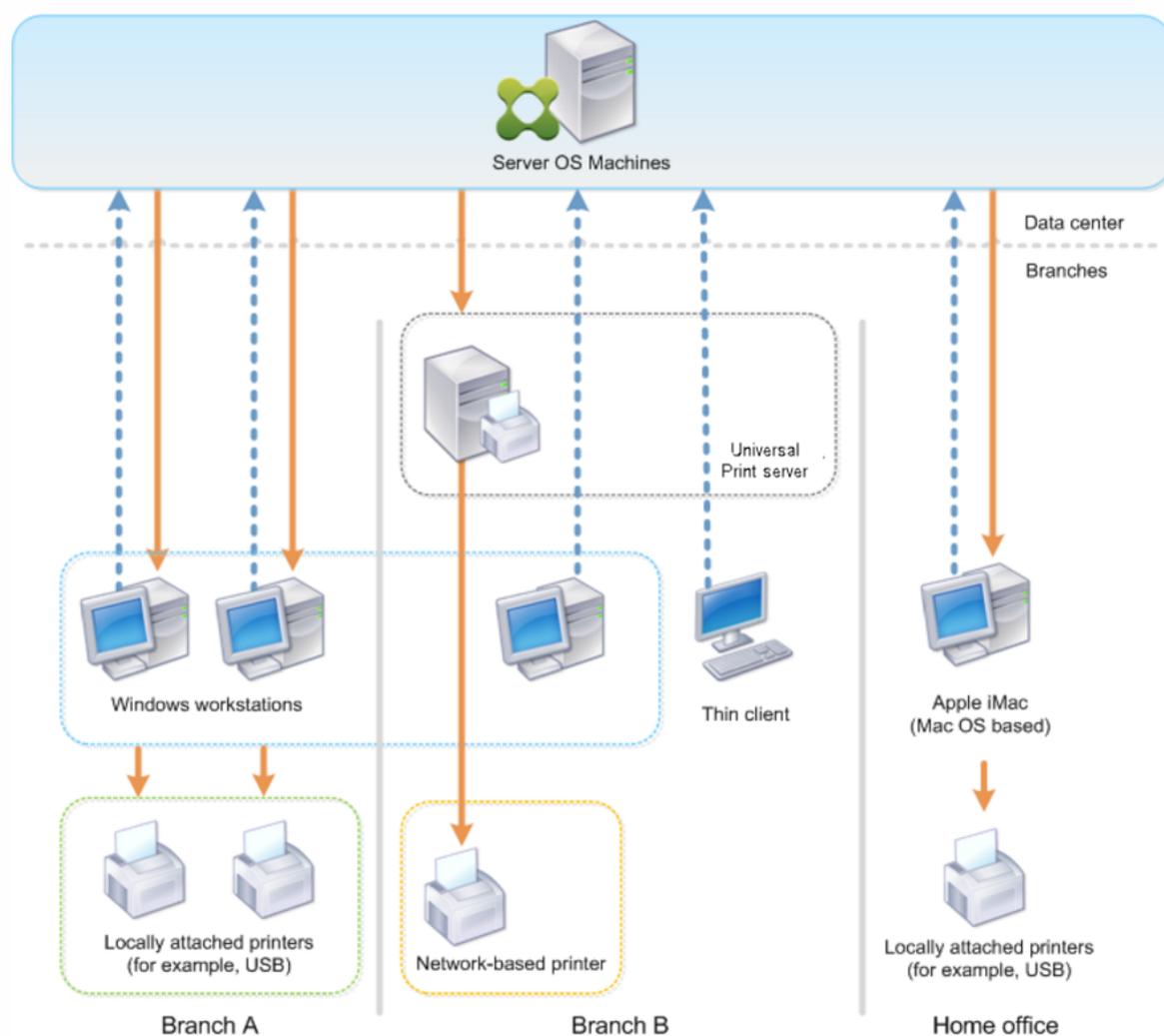
- Si la organización tiene unas directivas de seguridad que reservan impresoras a determinados usuarios (por ejemplo, impresoras solo para empleados de Recursos Humanos o los encargados de las nóminas).
- Si los usuarios necesitan imprimir desde lugares distintos de su ubicación de trabajo principal: por ejemplo, empleados que usan varias estaciones de trabajo o realizan frecuentes viajes de negocios.

Al diseñar la configuración de impresión, intente proporcionar a los usuarios la misma experiencia de sesión que tendrían si imprimieran desde dispositivos locales de usuario.

## Ejemplo de implementación de impresión

La siguiente ilustración muestra la implementación de impresión para estos casos de uso:

- **Oficina A:** Una pequeña sucursal exterior con algunas estaciones de trabajo Windows. La estación de trabajo de cada usuario tiene una impresora conectada localmente, privada.
- **Oficina B:** Una gran sucursal con clientes ligeros y estaciones de trabajo Windows. Para una mayor eficiencia, los usuarios de esta oficina comparten impresoras de red (una por planta). Unos servidores de impresión Windows ubicados dentro de la oficina se encargan de administrar las colas de impresión.
- **Oficina en casa:** Una oficina en el domicilio de un usuario, con un dispositivo de usuario Mac OS, que accede a la infraestructura Citrix de la empresa. El dispositivo del usuario tiene una impresora conectada localmente.



Las secciones siguientes describen las configuraciones que minimizan la complejidad del entorno y simplifican la administración.

### **Impresoras del cliente creadas automáticamente y controlador de impresión universal de Citrix**

En la Oficina A, todos los usuarios trabajan en estaciones de trabajo Windows; por lo tanto, se utilizan las impresoras cliente creadas automáticamente y el controlador de impresora universal. Estas tecnologías proporcionan las ventajas siguientes:

- **Rendimiento:** Los trabajos de impresión se entregan a través del canal ICA de impresión, por lo que los datos se pueden comprimir para ahorrar ancho de banda.

Con el fin de garantizar que el documento de un solo usuario (que imprima un documento de gran tamaño) no pueda degradar el rendimiento de las sesiones de otros usuarios, se configura

una directiva de Citrix para especificar el valor máximo de ancho de banda permitido para la impresión.

Una solución alternativa es aprovechar una conexión ICA de multisequencia. Se trata de una conexión en la que el tráfico de impresión se transfiere a través de otra conexión TCP de baja prioridad. La conexión ICA de multisequencia es una opción posible cuando no se implementa Calidad de servicio (QoS) en la conexión WAN.

- **Flexibilidad:** El controlador de impresora universal de Citrix garantiza que todas las impresoras conectadas a un cliente también se puedan usar desde la sesión de un escritorio virtual o una aplicación, sin integrar un nuevo controlador de impresora en el centro de datos.

## **Citrix Universal Print Server**

En la Oficina B, todas las impresoras están en red y sus colas de impresión se administran en un servidor de impresión Windows, por lo que Citrix Universal Print Server es la configuración más eficaz.

Los administradores locales instalan y administran todos los controladores de impresora obligatorios en el servidor de impresión. La asignación de impresoras en la sesión del escritorio virtual o de la aplicación funciona del siguiente modo:

- **Para estaciones de trabajo Windows:** El equipo de TI local ayuda a los usuarios a conectarse a la impresora de red correspondiente a sus estaciones de trabajo Windows. Esto permite a los usuarios imprimir desde las aplicaciones instaladas localmente.

Durante la sesión de una aplicación o un escritorio virtual, las impresoras configuradas de forma local se enumeran a través de la creación automática. A continuación, el escritorio virtual o la aplicación se conectan al servidor de impresión como una conexión de red directa, si es posible.

Los componentes de Citrix Universal Print Server están instalados y habilitados, por lo que no se requieren los controladores nativos de impresora. La actualización de un controlador o la modificación de una cola de impresión no requieren configuración adicional en el centro de datos.

- **Para clientes ligeros:** En caso de usuarios de clientes ligeros, las impresoras deben estar conectadas en la sesión del escritorio virtual o de la aplicación. Con el fin de proporcionar a los usuarios la experiencia de impresión más sencilla posible, los administradores configuran una sola directiva de Impresoras de la sesión de Citrix por planta para establecer la impresora de la planta como impresora predeterminada.

Para asegurarse de que esté conectada la impresora correcta incluso si los usuarios se desplazan entre las distintas plantas, las directivas se filtran según la subred o el nombre del cliente ligero. Esa configuración, conocida como impresión de proximidad, permite el mantenimiento del controlador de impresora local (de acuerdo con el modelo de administración delegada).

En caso de agregar o modificar una cola de impresión, los administradores Citrix deben modificar la correspondiente directiva de Impresoras de la sesión en el entorno.

Debido a que el tráfico de impresión de red se envía fuera del canal virtual ICA, se implementa QoS. El tráfico de red entrante y saliente de los puertos usados para el tráfico de ICA/HDX tiene prioridad sobre el tráfico de red restante. Esta configuración garantiza que las sesiones de usuario no se vean afectadas por trabajos de impresión de gran envergadura.

## **Impresoras del cliente creadas automáticamente y controlador de impresión universal de Citrix**

En caso de oficinas en casa, donde los usuarios trabajan con estaciones de trabajo no estandarizadas y utilizan dispositivos de impresión no administrados, lo más simple es usar las impresoras del cliente creadas automáticamente y el controlador de impresión universal.

### **Resumen de la implementación**

En definitiva, el ejemplo de implementación está configurado como se muestra a continuación:

- No se instalan controladores de impresora en máquinas con sistema operativo multisesión. Solo se utiliza el controlador de impresión universal de Citrix. Las opciones de recurrir a la impresión con controladores nativos y la instalación automática de controladores de impresora están inhabilitadas.
- Se configura una directiva con el fin de crear automáticamente todas las impresoras del cliente para todos los usuarios. De forma predeterminada, las máquinas con sistema operativo multisesión podrán conectarse directamente a los servidores de impresión. La única configuración obligatoria es habilitar los componentes de Universal Print Server.
- Se configura una directiva de impresora de sesión para cada planta de la Oficina B. Después, se aplica a todos los clientes ligeros de las plantas respectivas.
- Se implementa QoS para la Oficina B con el fin de garantizar una excelente experiencia de usuario.

## **Prácticas recomendadas, consideraciones de seguridad y operaciones predeterminadas**

September 22, 2021

## Prácticas recomendadas

Hay muchos factores que determinan la mejor solución de impresión para un entorno específico. Es posible que algunos de los procedimientos que se recomiendan no sean aplicables en su sitio.

- Use Citrix Universal Print Server.
- Use los controladores nativos de Windows o el controlador de impresora universal.
- Reduzca el número de controladores de impresora instalados en las máquinas con sistema operativo multisesión.
- Use la asignación de controladores con los controladores nativos.
- Nunca instale controladores de impresora sin haberlos probado en un sitio de producción.
- Evite actualizar los controladores. Siempre que pueda, intente primero desinstalar un controlador, reiniciar el servidor de impresión para, a continuación, instalar el controlador de sustitución.
- Desinstale los controladores que no utilice o use la directiva Asignación y compatibilidad de controladores de impresora para evitar que se creen impresoras con esos controladores.
- Intente evitar el uso de controladores modo kernel de versión 2.
- Para determinar si un modelo de impresora es compatible, póngase en contacto con el fabricante o consulte la guía de productos en Citrix Ready en [www.citrix.com/ready](http://www.citrix.com/ready).

En general, todos los controladores de impresora ofrecidos por Microsoft se han probado con Terminal Services y aseguran su funcionamiento con Citrix. Sin embargo, antes de utilizar controladores de impresora externos, consulte a su proveedor de controladores de impresora para comprobar si los controladores llevan la certificación para Terminal Services del programa Windows Hardware Quality Labs (WHQL). Citrix no certifica controladores de impresora.

## Consideraciones sobre seguridad

Las soluciones de impresión de Citrix se han diseñado para ofrecer seguridad.

- El servicio Citrix Print Manager Service lleva a cabo una supervisión constante y responde a sucesos de sesión tales como el inicio y cierre de sesión, la desconexión y reconexión, y la terminación de la sesión. Se encarga de las solicitudes de servicio mediante la suplantación de la sesión real del usuario.
- La impresión de Citrix asigna a cada impresora un único espacio de nombres en una sesión.
- La impresión de Citrix establece el descriptor de seguridad predeterminado para impresoras de creación automática para asegurarse de que las impresoras del cliente creadas automáticamente en una sesión no sean accesibles para usuarios de otras sesiones. De forma predeterminada, los usuarios administrativos no pueden imprimir por error en la impresora del cliente de

otra sesión, aunque sí pueden ver y ajustar manualmente los permisos de cualquier impresora del cliente.

## **Operaciones predeterminadas de impresión**

De forma predeterminada, si no se configuran reglas de directiva, la impresión funciona de este modo:

- La función Universal Print Server está inhabilitada.
- Todas las impresoras configuradas en el dispositivo del usuario se crean automáticamente al comienzo de cada sesión.

Este comportamiento equivale a usar la configuración de directiva de Citrix Crear automáticamente las impresoras del cliente con la opción Crear automáticamente todas las impresoras del cliente.

- El sistema redirige todos los trabajos de impresión enviados a la cola de las impresoras conectadas localmente a los dispositivos del usuario como trabajos de impresión de cliente (es decir, los redirige sobre el canal ICA y a través del dispositivo del usuario).
- El sistema redirige todos los trabajos de impresión enviados a la cola de impresoras de red directamente desde máquinas con sistema operativo multisesión. Si el sistema no puede enrutar los trabajos a través de la red, los redirige a través del dispositivo del usuario como trabajos de impresión de cliente redirigidos.

Este comportamiento equivale a inhabilitar la configuración de directiva de Citrix Conexiones directas con servidores de impresión.

- El sistema intenta almacenar en el dispositivo del usuario las propiedades de impresión, una combinación de las preferencias de impresión del usuario y la configuración de impresión del dispositivo. Si el cliente no admite esta operación, el sistema almacena las propiedades de impresión en el perfil de usuario de la máquina con sistema operativo multisesión.

Este comportamiento equivale a usar la configuración de directiva de Citrix Retención de las propiedades de impresora con la opción Guardado en perfil solo si no se guarda en el cliente.

- En la versión 7.16 de VDA y versiones posteriores, la configuración de directiva de Citrix “Instalación automática de controladores de impresora integrados” no surte efecto en Windows 8 y versiones posteriores de los sistemas operativos de Windows porque los controladores de impresora integrados V3 no se incluyen en el sistema operativo.
- En versiones de VDA anteriores a 7.16, el sistema emplea la versión de Windows del controlador de impresora si está disponible en la máquina con sistema operativo multisesión. Si el controlador de impresora no está disponible, el sistema intenta instalarlo desde el sistema operativo

Windows. Si el controlador no está disponible en Windows, usa el controlador de impresión universal de Citrix.

Este comportamiento equivale a habilitar la configuración de directiva de Citrix “Instalación automática de controladores de impresora” y definir la configuración Impresión universal con la opción “Usar impresión universal solo si el controlador solicitado no está disponible”.

Si se habilita “Instalación automática de controladores de impresora”, es posible que se instale una gran cantidad de controladores nativos.

**Nota:**

Si no sabe cuáles son los parámetros de impresión de fábrica, puede verlos creando una directiva y definiendo todas las reglas de directiva de impresión en Habilitada. La opción que aparece es la opción predeterminada.

## Registros Always-On

Una función de registro de Always-On está disponible para el servidor de impresión y el subsistema de impresión en el VDA.

Para intercalar los registros como archivo comprimido y enviarlo por correo o para cargar automáticamente los registros en Citrix Insight Services, use el cmdlet **Start-TelemetryUpload** de PowerShell.

## Directivas y preferencias de impresión

September 22, 2021

Cuando los usuarios acceden a impresoras desde las aplicaciones publicadas, puede configurar directivas de Citrix para especificar:

- Cómo se aprovisionan las impresoras (es decir, cómo se agregan a las sesiones)
- Cómo se enrutan los trabajos de impresión
- Cómo se administran los controladores de impresora

Puede tener configuraciones de impresión diferentes para distintos dispositivos del usuario, usuarios o cualquier otro objeto sobre los que se puedan aplicar filtros de directiva.

La mayoría de las funcionalidades de impresión se configuran mediante las [directivas de impresión](#) de Citrix. Las configuraciones de impresión siguen el comportamiento de las directivas estándar de Citrix.

El sistema puede escribir las configuraciones de impresora en el objeto de impresora al final de la sesión o en un dispositivo de impresión del cliente, con tal de que la cuenta de red del usuario tenga

los permisos necesarios. De forma predeterminada, la aplicación Citrix Workspace usa las configuraciones almacenadas en el objeto de impresora de la sesión, antes de buscar configuraciones y preferencias en otras ubicaciones.

De forma predeterminada, el sistema almacena o conserva las propiedades de la impresora en el dispositivo del usuario (si es compatible con el dispositivo) o en el perfil del usuario de la máquina con sistema operativo multisesión. Cuando un usuario cambia las propiedades de la impresora durante una sesión, los cambios se actualizan en el perfil de usuario de la máquina. La próxima vez que el usuario inicie sesión o se reconecte, el dispositivo del usuario hereda la configuración conservada. Es decir, los cambios en las propiedades de la impresora en el dispositivo del usuario no afectan a la sesión actual hasta que el usuario cierra la sesión e inicia sesión de nuevo.

## Ubicaciones de preferencias de impresión

En los entornos de impresión de Windows, los cambios realizados en las preferencias de impresión se pueden guardar en el equipo local o en un documento. En este entorno, cuando los usuarios modifican los parámetros de impresión, los parámetros se guardan en estas ubicaciones:

- **En el dispositivo del usuario en sí:** Los usuarios de Windows pueden cambiar la configuración del dispositivo en su dispositivo. Para ello, deben hacer clic con el botón secundario en la impresora del Panel de control y seleccionar Preferencias de impresión. Por ejemplo, si se selecciona una orientación de página Horizontal, se guarda la orientación horizontal como preferencia predeterminada para esa impresora.
- **Dentro de un documento:** En programas de procesamiento de texto y creación de publicaciones, los parámetros del documento (por ejemplo, la orientación de la página) suelen almacenarse dentro de los documentos. Por ejemplo, cuando envía un documento a la cola para imprimir, Microsoft Word normalmente almacena las preferencias de impresión especificadas como, por ejemplo, la orientación de la página y el nombre de la impresora, dentro del documento. Estos parámetros aparecen de manera predeterminada la siguiente vez que imprime ese documento.
- **En los cambios realizados por un usuario durante una sesión:** El sistema mantiene solamente los cambios en la configuración de impresión de una impresora creada de forma automática si los cambios se realizaron en el Panel de control de la sesión, es decir, en la máquina con sistema operativo multisesión.
- **En la máquina con sistema operativo multisesión:** Esta es la configuración predeterminada asociada a un controlador de impresora concreto de la máquina.

Las configuraciones conservadas en los entornos basados en Windows varían según el lugar en el que el usuario realice los cambios. Esto también significa que la configuración de impresión que aparece en un lugar como, por ejemplo, un programa de hojas de cálculo, puede ser distinta a la que aparece

en otro (por ejemplo, en documentos). Como resultado, la configuración de impresión aplicada a una impresora específica puede cambiar durante la misma sesión.

### **Jerarquía de preferencias de impresión de los usuarios**

Las preferencias de impresión pueden almacenarse en varios sitios, por lo que el sistema las procesa por orden de prioridad. Es importante tener en cuenta que las configuraciones de los dispositivos se tratan de manera distinta a las configuraciones de los documentos, y normalmente las primeras tienen preferencia sobre estas segundas.

De forma predeterminada, el sistema siempre aplica la configuración de impresión que el usuario haya modificado durante una sesión, es decir, la configuración conservada, antes de tener en cuenta otra configuración. Cuando el usuario imprime, el sistema combina y aplica la configuración de impresora predeterminada almacenada en la máquina con sistema operativo multisesión con cualquier otra configuración de impresora conservada o del cliente.

### **Guardar las preferencias de impresión del usuario**

Citrix recomienda no modificar el lugar donde se almacenan las propiedades de impresora. El parámetro predeterminado, que guarda las propiedades de la impresora en el dispositivo del usuario, es la forma más sencilla de asegurar que las propiedades de impresión son consistentes. Si el sistema no puede guardar las propiedades en el dispositivo del usuario, recurre automáticamente al perfil del usuario de la máquina con sistema operativo multisesión.

Compruebe la configuración de directiva de la Retención de las propiedades de impresora si se da uno de los siguientes casos:

- Si utiliza plug-ins antiguos que no permiten a los usuarios almacenar las propiedades de la impresora en un dispositivo de usuario.
- Si utiliza perfiles obligatorios en la red de Windows y quiere conservar las propiedades de impresora del usuario.

## **Aprovisionar impresoras**

March 10, 2022

### **Citrix Universal Print Server**

Para determinar la mejor solución de impresión para el entorno, tenga en cuenta lo siguiente:

- Universal Print Server ofrece funciones no disponibles para el proveedor de impresión de Windows: almacenamiento en caché de imágenes y fuentes, compresión avanzada, optimización y compatibilidad con QoS.
- El controlador de impresión universal admite los parámetros públicos independientes del dispositivo definidos por Microsoft. Si los usuarios necesitan acceder a la configuración de un dispositivo específica del fabricante del controlador de impresora, Universal Print Server y el controlador nativo de Windows podrían ser la mejor solución. Con esa configuración, conserva las ventajas de Universal Print Server a la vez que proporciona a los usuarios acceso a funciones específicas de impresora. Por otro lado, hay un factor no tan ventajoso que, no obstante, se debe tener en cuenta: los controladores nativos de Windows requieren mantenimiento.
- Citrix Universal Print Server ofrece la funcionalidad de impresión universal para impresoras de red. Universal Print Server usa el controlador de impresión universal, un único controlador en la máquina con sistema operativo multisesión, que permite la impresión local o de red desde cualquier dispositivo, incluidos los clientes ligeros y las tabletas.

Para usar Universal Print Server con un controlador nativo de Windows, habilite Universal Print Server. De forma predeterminada, se utiliza el controlador nativo de Windows, si está disponible. Si no lo está, se utiliza el controlador de impresión universal. Para especificar cambios de este comportamiento tales como, por ejemplo, utilizar solo el controlador nativo de Windows o solo el controlador de impresión universal, actualice la configuración de directiva Uso de controladores de impresión universal.

### Instalar Universal Print Server

Para usar Universal Print Server, instale el componente UpsServer en los servidores de impresión siguiendo los pasos descritos en los documentos de instalación y, a continuación, configúrelo. Para obtener más información, consulte [Instalar componentes principales](#) e [Instalación desde la línea de comandos](#).

Para entornos donde se quiere implementar el componente UPClient por separado, por ejemplo, con **XenApp 6.5**:

1. Descargue el paquete independiente del Virtual Delivery Agent (VDA) de Citrix Virtual Apps and Desktops para SO de sesión única Windows o SO multisesión Windows.
2. Extraiga el VDA siguiendo las instrucciones de línea de comandos descritas en [Instalación desde la línea de comandos](#).
3. Instale los requisitos previos desde `\Image-Full\Support\VcRedist_2013_RTM`
  - `Vcredist_x64 / vcredist_x86`
    - Ejecute x86 solo para sistemas de 32 bits, y ejecute ambos para implementaciones de 64 bits

4. Instale el requisito previo de cdf desde \Image-Full\x64\Virtual Desktop Components o \Image-Full\x86\Virtual Desktop Components.
  - Cdf\_x64 / Cdf\_x86
    - x86 para 32 bits, x64 para 64 bits
5. Ejecute el componente UPClient en \Image-Full\x64\Virtual Desktop Components o \Image-Full\x86\Virtual Desktop Components.
6. Instale el componente UPClient extrayendo y ejecutando el archivo MSI del componente.
7. Se necesita reiniciar el sistema después de instalar el componente UPClient.

### Dejar de participar en el programa CEIP para Universal Print Server

Cuando instala Universal Print Server, usted queda inscrito automáticamente en el programa CEIP de mejora de la experiencia del cliente (Citrix Customer Experience Improvement Program). La primera carga de datos tiene lugar aproximadamente transcurridos siete días desde la fecha y la hora de la instalación.

Si quiere dejar de participar en el programa CEIP, modifique la clave de Registro **HKLM\Software\Citrix\Universal Print Server\CEIPEnabled** para establecer el valor **DWORD** en **0**.

Si decide reanudar su participación, establezca **DWORD** con el valor **1**.

**Precaución:** Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Para obtener más información, consulte [Citrix Insight Services](#).

### Configurar Universal Print Server

Utilice las siguientes configuraciones de directiva de Citrix para definir Universal Print Server. Para obtener más información, consulte la ayuda en pantalla de las configuraciones de directiva.

- **Habilitar Universal Print Server.** De forma predeterminada, Universal Print Server está inhabilitado. Al habilitar Universal Print Server, puede elegir si desea usar el proveedor de impresión de Windows en caso de que Universal Print Server no esté disponible. Después de habilitar Universal Print Server, los usuarios pueden agregar y enumerar las impresoras de red a través de las interfaces del proveedor de impresión de Windows y del proveedor de Citrix.
- **Puerto del flujo de datos de impresión de Universal Print Server (CGP).** Especifica el número de puerto TCP utilizado por el proceso de escucha del protocolo CGP del flujo de datos de impresión de Universal Print Server. El valor predeterminado es **7229**.

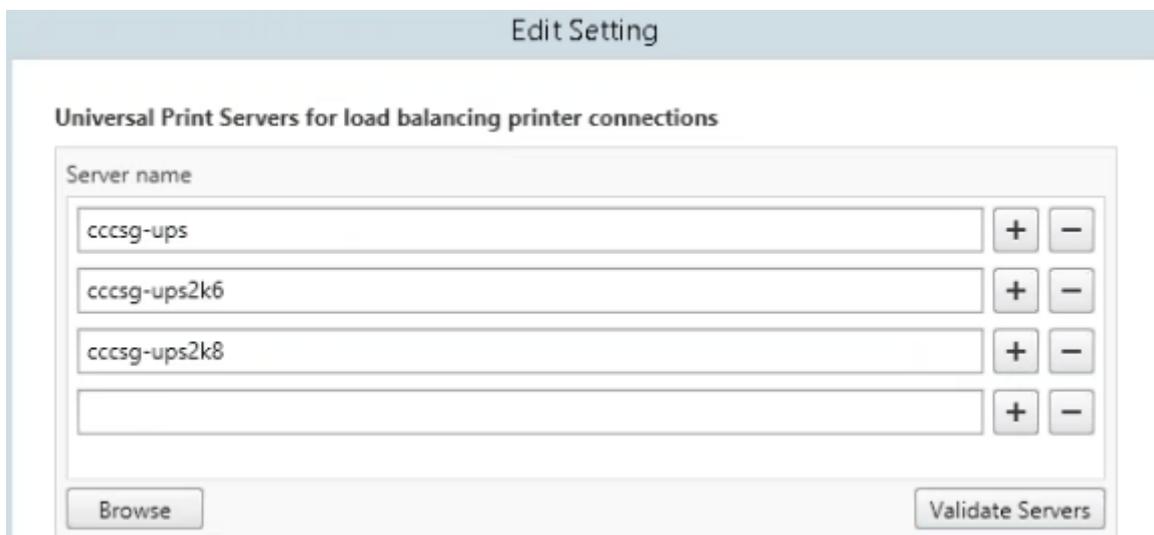
- **Puerto del servicio web de Universal Print Server (HTTP/SOAP).** Especifica el número de puerto TCP utilizado por el proceso de escucha de Universal Print Server para solicitudes HTTP/SOAP entrantes. El valor predeterminado es **8080**.

Para cambiar el puerto predeterminado de HTTP 8080 para la comunicación entre Universal Print Server y los agentes VDA de Citrix Virtual Apps and Desktops, también debe crearse la siguiente clave de Registro y modificarse el valor del número de puerto en los equipos de Universal Print Server:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PrintingPolicies  
"UpsHttpPort"=DWORD:<número de puerto>
```

Este número de puerto debe coincidir con el puerto del servicio web de Universal Print Server (HTTP/SOAP) de la directiva HDX, en Studio.

- **Límite de ancho de banda del flujo de entrada de impresión de Universal Print Server (kbps).** Especifica el límite superior (en kilobits por segundo) de la velocidad de transferencia de datos de impresión entregada desde cada trabajo de impresión a Universal Print Server mediante CGP. El valor predeterminado es 0 (no hay límite).
- **Universal Print Servers para equilibrio de carga.** Esta configuración enumera los servidores de impresión universal que se usarán para equilibrar la carga de las conexiones de impresora establecidas al comienzo de las sesiones, después de evaluar otras configuraciones de impresión de Citrix. Para optimizar la creación de impresoras, Citrix recomienda que todos los servidores de impresión tengan el mismo conjunto de impresoras compartidas.



- **Umbral para servidores Universal Print Server fuera de servicio.** Especifica cuánto tiempo debe esperar el equilibrador de carga a que se recupere un servidor de impresión no disponible antes de determinar que ese servidor está fuera de línea permanentemente y redistribuir su carga en otros servidores de impresión disponibles. El valor predeterminado es 180 segundos.

Una vez que las directivas de impresión se modifican en el Delivery Controller, los cambios de la directiva pueden tardar unos minutos en aplicarse en los VDA.

**Interacciones con otras configuraciones de directiva** Universal Print Server acepta otras configuraciones de directiva de impresión Citrix e interactúa con ellas como se indica en la siguiente tabla. En la tabla siguiente se presupone que la directiva de Universal Print Server está habilitada, que sus componentes están instalados y que se están aplicando las configuraciones de la directiva.

---

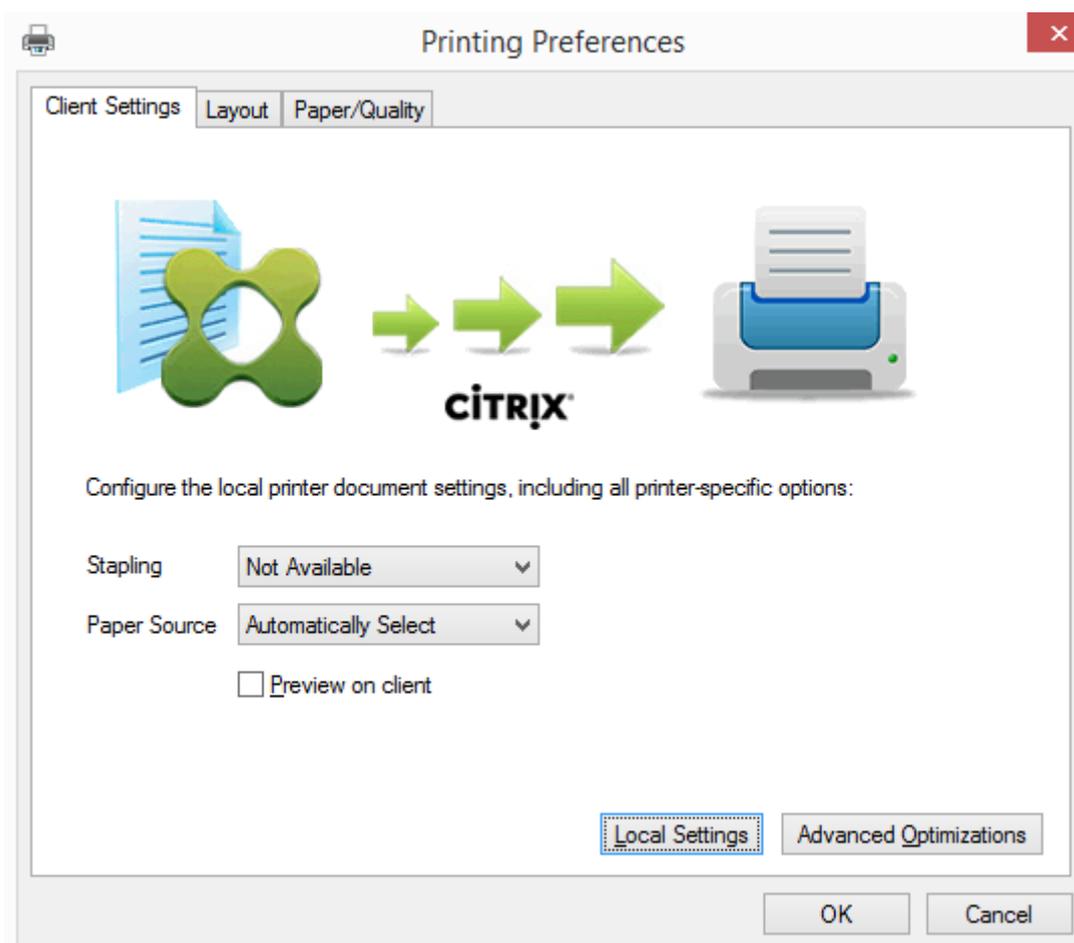
Configuración de directiva	Interacción
Redirección de impresoras del cliente, Crear automáticamente las impresoras del cliente	Después de habilitar Universal Print Server, las impresoras de red del cliente se crean mediante el controlador de impresión universal en lugar de los controladores nativos. Los usuarios verán el mismo nombre de impresora que antes.
Impresoras de la sesión	Cuando se utiliza la solución Citrix Universal Print Server, se respetan las configuraciones de directiva del controlador de impresión universal.
Conexiones directas con servidores de impresión	Cuando Universal Print Server está habilitado y la configuración de directiva sobre el uso del controlador de impresión universal está configurada para usar solo la impresión universal, se puede crear una conexión directa entre la impresora de red y el servidor de impresión mediante el controlador de impresión universal.
Preferencia de UPD	Admite controladores XPS y EMF.

---

**Efectos en las interfaces de usuario:** El controlador de impresora universal de Citrix que usa el servidor Universal Print Server inhabilita los siguientes controles de interfaz de usuario:

- En el cuadro de diálogo Propiedades de impresora, el botón Parámetros de impresora local
- En el cuadro de diálogo Propiedades del documento, los botones de cliente Parámetros de impresora local y Vista previa

El controlador de impresora universal de Citrix (controladores EMF y XPS) admite funciones avanzadas de impresión, tales como el grapado y el origen del papel. El usuario puede seleccionar opciones de Grapado o de Origen del papel en el cuadro de diálogo personalizado de UPD si las impresoras del cliente o de red que están asignadas al controlador UPD en la sesión admiten dichas funciones.



Para configurar parámetros de impresora no estándar (como el grapado y un PIN seguro), seleccione **Parámetros locales** en el diálogo de impresión de UPD del cliente para cualquier impresora cliente asignada que utilice los controladores de impresora universal EMF o XPS de Citrix. El diálogo **Preferencias de impresión** de la impresora asignada se muestra fuera de sesión en el cliente, lo que permite al usuario cambiar cualquier opción de impresora; los parámetros modificados de impresora se utilizan en la sesión activa para imprimir el documento en sí.

Estas funciones están disponibles si el controlador nativo las habilita mediante la tecnología de capacidad de impresión de Microsoft. El controlador nativo debe usar las palabras clave estándar de esquema de impresión en el XML de capacidades de impresión (Print Capabilities). Si utiliza palabras clave no estándar, las funciones de impresión avanzadas no estarán disponibles cuando se use el controlador de impresora universal de Citrix.

Cuando se usa Universal Print Server, el asistente Agregar impresora para el proveedor de impresión de Citrix es el mismo que el asistente Agregar impresora del proveedor de impresión de Windows, con las siguientes excepciones:

- Cuando se agrega una impresora por su nombre o su dirección, puede proporcionar un número de puerto HTTP/SOAP para el servidor de impresión. Ese número de puerto formará parte del

nombre de la impresora y es el que se muestra en pantalla.

- Si en la configuración de directiva sobre el uso del controlador de impresión universal de Citrix se especifica que se debe usar la impresión universal, cuando se seleccione una impresora aparecerá el nombre del controlador de impresión universal. El proveedor de impresión de Windows no puede usar el controlador de impresión universal.

El proveedor de impresión de Citrix no admite la generación en el lado del cliente.

Para obtener más información acerca de Universal Print Server, consulte [CTX200328](#).

## Impresoras del cliente creadas automáticamente

Se suministran estas soluciones de impresión universal para las impresoras cliente:

- **Impresora universal de Citrix:** Una impresora genérica, creada al comienzo de las sesiones, que no está vinculada a ningún dispositivo de impresión. La Impresora universal de Citrix no es necesaria para enumerar las impresoras del cliente disponibles durante el inicio de sesión, lo que puede reducir notablemente el uso de los recursos y el tiempo que tarda en iniciarse la sesión del usuario. La Impresora universal puede imprimir en cualquier dispositivo de impresión del cliente.

Es posible que la Impresora universal de Citrix no funcione en todos los dispositivos de usuario ni todas las aplicaciones Citrix Workspace de su entorno. La Impresora universal de Citrix requiere un entorno de Windows y no es compatible con Citrix Offline Plug-in o las aplicaciones que se entregan por streaming al cliente. Considere la posibilidad de usar impresoras de cliente creadas automáticamente y el controlador de impresión universal para esos entornos.

Si quiere usar una solución de impresión universal para las aplicaciones Citrix Workspace que no sean de Windows, use uno de los demás controladores de impresión universal que están basados en PostScript/PCL y se instalan automáticamente.

- **Controladores de impresora universal de Citrix:** Un controlador de impresora universal que es independiente del dispositivo. Si configura el controlador de impresión universal de Citrix, el sistema usa el controlador de impresión universal EMF de forma predeterminada.

El controlador de impresión universal de Citrix también puede crear trabajos de impresión más pequeños que controladores de impresora anteriores o menos avanzados. No obstante, puede que sea necesario usar el controlador específico del dispositivo para optimizar los trabajos de impresión para la impresora especializada.

**Configurar la impresión universal:** Utilice las siguientes configuraciones de directiva Citrix para configurar la impresión universal. Para obtener más información, consulte la ayuda en pantalla de las configuraciones de directiva.

- Uso de controladores de impresión universal. Especifica cuándo se usa la impresión universal.

- Crear automáticamente una impresora universal genérica. Habilita o inhabilita la creación automática del objeto genérico de Citrix Universal Printer para las sesiones en las que se utiliza un dispositivo de usuario compatible con la impresión universal. De forma predeterminada, el objeto genérico de impresora universal no se crea automáticamente.
- Preferencia de controlador universal. Especifica el orden en que el sistema intenta usar los controladores de impresión universal, a partir del primer elemento de la lista. Es posible agregar, modificar o eliminar controladores, y cambiar el orden de los controladores en la lista.
- Preferencia de vista previa en impresión universal. Especifica si se usará la función de vista previa de impresión para las impresoras universales genéricas o creadas automáticamente.
- Modo de procesamiento EMF de la impresión universal. Controla el método de procesamiento del archivo EMF de la cola de impresión en el dispositivo Windows del usuario. De forma predeterminada, los registros EMF se envían directamente a la impresora. Esto permite al administrador de trabajos de impresión procesar los registros más rápido y usa menos recursos de la CPU.

Para conocer más directivas, consulte [Optimizar el rendimiento de la impresión](#). Para cambiar los valores predeterminados de parámetros como el tamaño del papel, la calidad de impresión, el color, la impresión a doble cara y el número de copias, consulte [CTX113148](#).

**Crear impresoras automáticamente desde el dispositivo de usuario:** Al principio de una sesión, el sistema crea automáticamente todas las impresoras en el dispositivo de usuario de forma predeterminada. Es posible controlar qué tipo de impresoras se proporcionan a los usuarios y evitar la creación automática de estas.

Use la configuración de directiva de Citrix

Crear automáticamente las impresoras del cliente para controlar la creación automática. Puede especificar que:

- Todas las impresoras visibles en el dispositivo del usuario, incluidas las impresoras de red y las conectadas localmente al equipo, se creen automáticamente al comienzo de cada sesión (opción predeterminada)
- Todas las impresoras conectadas físicamente al dispositivo del usuario se creen automáticamente
- Solo se cree automáticamente la impresora predeterminada del dispositivo del usuario
- La función de creación automática esté inhabilitada para todas las impresoras del cliente

La configuración Crear automáticamente las impresoras del cliente requiere que la configuración Redirección de impresoras del cliente tenga el valor Permitida (valor predeterminado).

## Asignar impresoras de red a los usuarios

De forma predeterminada, las impresoras de red del dispositivo del usuario se crean automáticamente al comienzo de las sesiones. El sistema permite reducir el número de impresoras de red que se enumeran y se asignan al especificar las impresoras de red que se crearán en cada sesión. Estas impresoras se denominan impresoras de sesión.

Puede filtrar las directivas de impresora de sesión por dirección IP para proporcionar la impresión de proximidad. Con la impresión de proximidad los usuarios que se encuentran dentro de un intervalo de direcciones IP especificado acceden automáticamente a los dispositivos de impresión en red que existen dentro de ese intervalo. Citrix Universal Print Server ofrece la impresión de proximidad, que no requiere la configuración que se describe en esta sección.

La impresión de proximidad puede utilizarse en estas circunstancias:

- La red interna de la empresa opera con un servidor DHCP que designa automáticamente direcciones IP a los usuarios.
- Todos los departamentos de la organización tienen intervalos de direcciones IP designados de manera exclusiva.
- Existen impresoras de red para cada uno de los intervalos de direcciones IP de departamento.

Cuando se configura la impresión de proximidad y un empleado se desplaza de un departamento a otro, no se requiere la configuración adicional de un dispositivo de impresión. Después de reconocer el dispositivo del usuario en el nuevo intervalo de direcciones IP del departamento, este dispositivo tendrá acceso a todas las impresoras de red pertenecientes a ese intervalo.

**Configurar impresoras específicas para redirigirlas durante las sesiones:** Para crear impresoras asignadas por un administrador, configure el parámetro de directiva de Citrix Impresoras de la sesión. Agregue una impresora de red a esa directiva mediante uno de los siguientes métodos:

- Especifique la ruta UNC de la impresora con el formato `\\nombre_servidor\nombre_impresora`.
- Busque una ubicación para la impresora en la red.
- Busque impresoras en un servidor específico. Introduzca el nombre del servidor con el formato `\\nombre_servidor` y haga clic en Examinar.

**Importante:** El servidor combina todas las configuraciones de parámetros de impresoras de sesión que estén habilitadas en todas las directivas aplicadas, empezando por las de mayor prioridad. Cuando una impresora está configurada en varios objetos de directiva, se toman los parámetros predeterminados únicamente del objeto de directiva de mayor prioridad en el cual se haya configurado la impresora.

Las impresoras de red creadas con la configuración Impresoras de la sesión pueden variar según las condiciones en donde se inició la sesión al aplicar un filtro en objetos, como, por ejemplo, las subredes.

**Especificar una impresora de red predeterminada para una sesión:** De manera predeterminada, se usa la impresora principal del usuario como la impresora predeterminada de la sesión. Use la configuración de directiva de Citrix Impresora predeterminada para cambiar la forma en que la impresora predeterminada del dispositivo del usuario se establece en una sesión.

1. En la página de configuración Impresora predeterminada, seleccione un parámetro para Elegir impresora predeterminada del cliente:
  - Nombre de impresora de red. Las impresoras agregadas con la configuración de directiva Impresoras de la sesión aparecen en este menú. Seleccione la impresora de red que desee usar como predeterminada para esta directiva.
  - No ajustar la impresora predeterminada del usuario. Usa el parámetro de impresora predeterminada existente en el perfil de usuario actual de Terminal Services o de Windows. Para obtener más información, consulte la ayuda en pantalla de las configuraciones de directiva.
2. Aplique la directiva al grupo de usuarios (u otros objetos filtrados) donde quiera que tenga efecto.

**Configurar la impresión de proximidad:** Citrix Universal Print Server también ofrece la impresión de proximidad, que no requiere la configuración que se describe aquí.

1. Cree una directiva para cada subred (o para que corresponda con la ubicación de la impresora).
2. En cada directiva, agregue las impresoras que se encuentran en la ubicación geográfica de esa subred a la configuración Impresoras de la sesión.
3. Establezca el parámetro Impresora predeterminada en No ajustar la impresora predeterminada del usuario.
4. Filtre las directivas por dirección IP del cliente. Asegúrese de actualizar estas directivas para reflejar los cambios en los intervalos de direcciones IP DHCP.

## Mantener el entorno de impresión

September 22, 2021

Mantener el entorno de impresión incluye:

- Administrar controladores de impresora
- Optimizar el rendimiento de la impresión
- Mostrar la impresora y administrar las colas de impresión

## Administrar controladores de impresora

Para minimizar la carga de administración y los problemas potenciales de los controladores de impresión, Citrix recomienda el uso del controlador de impresión universal de Citrix.

Si se produce un error en el proceso de creación automática, de forma predeterminada, el sistema instala un controlador de impresora nativo de Windows, proporcionado con Windows. Si el controlador no está disponible, el sistema recurre al controlador de impresión universal. Para obtener más información acerca de los valores predeterminados del controlador de impresora, consulte [Procedimientos recomendados, aspectos a tener en cuenta sobre la seguridad y operaciones predeterminadas](#).

Si el controlador de impresión universal de Citrix no es una opción válida en todas las situaciones, asigne controladores de impresora para reducir la cantidad de controladores instalados en las máquinas con sistema operativo multisesión. Además, asignando controladores de impresora puede:

- Permitir que las impresoras especificadas usen solo el controlador de impresión universal de Citrix
- Permitir o impedir la creación de impresoras con un controlador especificado
- Sustituir controladores de impresora dañados u obsoletos por controladores que funcionan
- Sustituir un controlador disponible en el servidor Windows por un nombre de controlador del cliente

**Impedir la instalación automática de controladores de impresora:** La instalación automática de controladores de impresora debe estar inhabilitada para garantizar la coherencia entre máquinas con sistema operativo multisesión. Esto se logra a través de las directivas de Citrix, las de Microsoft o ambas. Para impedir la instalación automática de controladores de impresora nativos de Windows, inhabilite la configuración de directiva de Citrix Instalación automática de controladores de impresora.

**Asignar controladores de impresora del cliente:** Cada cliente proporciona información acerca de las impresoras del cliente durante el inicio de sesión, incluido el nombre del controlador de la impresora. Durante la creación automática de las impresoras del cliente, se seleccionan los nombres de controladores de impresora del servidor de Windows que correspondan a los nombres de modelo de impresora que proporciona el cliente. A continuación, el proceso de creación automática emplea los controladores de impresora disponibles que se identificaron para crear las colas de impresión de cliente redirigidas.

A continuación se describe el proceso general para definir las reglas de sustitución de controladores y modificar los parámetros de impresión de los controladores de impresoras del cliente asignadas:

1. Para especificar reglas de sustitución de controladores destinados a impresoras del cliente creadas automáticamente, use la configuración de directiva de Citrix Asignación y compatibilidad de controladores de impresora. Para ello, agregue el nombre del controlador de la

impresora del cliente y seleccione el controlador de servidor con el que desea sustituir el controlador de la impresora del cliente desde el menú Buscar controlador de impresora. Esta configuración admite caracteres comodín. Por ejemplo, para forzar a todas las impresoras HP a usar un controlador específico, establezca HP\* en la configuración de directiva.

2. Para prohibir un controlador de impresora, seleccione el nombre del controlador y elija el parámetro No crear.
3. Si fuera necesario, modifique una asignación existente de controladores, elimínela o cambie el orden de los controladores en la lista.
4. Si quiere modificar los parámetros de impresión para los controladores de impresoras del cliente asignadas, seleccione el controlador de impresora, haga clic en Configuración y especifique parámetros tales como la calidad de impresión, la orientación y el color. Si especifica una opción de impresión que no admite el controlador, la opción no tendrá ningún efecto. Esta configuración sobrescribe los parámetros de impresora que se conservaron después de que el usuario los definiera durante una sesión anterior.
5. Citrix recomienda hacer pruebas exhaustivas para comprobar el comportamiento de las impresoras después de la asignación de controladores de impresora, puesto que algunas funciones pueden estar disponibles solo con un controlador específico.

Cuando los usuarios inician sesión, el sistema comprueba la lista de compatibilidad de controladores de impresora del cliente antes de configurar las impresoras del cliente.

## **Optimizar el rendimiento de la impresión**

Para optimizar el rendimiento de la impresión, use Universal Print Server y el controlador de impresión universal. Las siguientes directivas rigen la optimización y la compresión de la impresión:

- Valores predeterminados de optimización de la impresión universal. Especifica los parámetros predeterminados al crear una impresora universal para la sesión:
  - Calidad de imagen deseada especifica el límite predeterminado de compresión de imagen aplicable a la impresión universal. De forma predeterminada, la Calidad estándar está habilitada, de manera que los usuarios solo pueden imprimir imágenes con la compresión de calidad estándar o reducida.
  - Habilitar la compresión intensa habilita o inhabilita la reducción de ancho de banda más allá del nivel de compresión definido por Calidad de imagen deseada, sin pérdida de calidad de imagen. La compresión intensa está inhabilitada de forma predeterminada.
  - La configuración de Almacenamiento en caché de imágenes y fuentes especifica si las imágenes y fuentes que aparecen varias veces en el flujo de impresión se almacenan en caché, para que cada imagen individual se envíe solo una vez a la impresora. De forma predeterminada, las fuentes e imágenes incrustadas se almacenan en caché.

- Permitir a los no administradores modificar estos parámetros especifica si los usuarios pueden cambiar los parámetros predeterminados de optimización de la impresión en una sesión. De forma predeterminada, los usuarios no pueden cambiar los parámetros predeterminados de la optimización de impresión.
- Límite de compresión de imagen para la impresión universal. Define la calidad máxima y el nivel de compresión mínimo disponibles para las imágenes impresas con el controlador de impresión universal. De forma predeterminada, el límite de compresión de imagen está definido en Mejor calidad (compresión sin pérdida).
- Límite de calidad de la impresión universal. Especifica la cantidad máxima de puntos por pulgada (PPP) disponibles para generar una salida impresa en la sesión. De forma predeterminada, no existe ningún límite.

De forma predeterminada, todos los trabajos de impresión destinados a impresoras de red se enrutan desde la máquina con sistema operativo multisesión, pasan por la red y terminan directamente en el servidor de impresión. Considere la posibilidad de dirigir trabajos de impresión a través de la conexión ICA si la red tiene una latencia sustancial o un ancho de banda limitado. Para ello, inhabilite la configuración de directiva de Citrix Conexiones directas con servidores de impresión. Los datos enviados al cliente a través de conexiones ICA se comprimen, por lo que se consume menos ancho de banda en la transmisión de datos a través de la WAN.

**Mejorar el rendimiento de las sesiones al limitar el ancho de banda de impresión:** Al imprimir archivos provenientes de máquinas con sistema operativo multisesión en las impresoras de los usuarios, otros canales virtuales (como el de vídeo) pueden sufrir una disminución del rendimiento debido a la competencia por el ancho de banda, especialmente si los usuarios acceden a los servidores a través de redes lentas. Para evitar esa degradación, puede limitar el ancho de banda utilizado para la impresión del cliente. Al limitar la velocidad de las transmisiones de la impresión, se amplía el ancho de banda disponible para las secuencias de datos HDX para transmisiones de vídeo, señales de teclado y datos del puntero.

**Importante:**

El límite de ancho de banda para la impresora se aplica siempre, incluso cuando no se están utilizando otros canales.

Utilice las configuraciones de directiva de Citrix de Ancho de banda descritas a continuación para configurar los límites de ancho de banda para la impresión. Para configurar los límites del sitio, realice esta tarea con Studio. Para configurar los límites de servidores individuales, realice esta tarea con la Consola de administración de directivas de grupo en Windows localmente y en cada máquina con sistema operativo multisesión.

- La configuración Límite de ancho de banda de redirección de impresoras especifica el ancho de banda disponible de la impresión en kilobits por segundo (kbps).

- La configuración Porcentaje límite de ancho de banda de redirección de impresoras limita el ancho de banda disponible para la impresión como porcentaje del ancho de banda total disponible.

Nota: Para especificar el ancho de banda como un porcentaje con la configuración Porcentaje límite de ancho de banda de redirección de impresoras, habilite también la configuración Límite de ancho de banda global de la sesión.

Si introduce valores para ambas configuraciones, se aplicará el valor más restrictivo (el valor más bajo).

Para obtener información en tiempo real acerca del ancho de banda de impresión, use Citrix Director.

## **Equilibrar la carga de los servidores Universal Print Server**

La solución de servidores de impresión universal (Universal Print Server) puede ampliarse agregando servidores de impresión adicionales para el equilibrio de carga. No hay ningún punto de fallo único, ya que cada VDA tiene su propio equilibrador de carga para distribuir la carga de impresión entre todos los servidores de impresión.

Use las configuraciones de directiva [Universal Print Servers para equilibrio de carga](#) y [Umbral para servidores Universal Print Server fuera de servicio](#) para distribuir la carga de impresión entre todos los servidores de impresión en la solución de equilibrio de carga.

Si un servidor de impresión falla de forma imprevista, el mecanismo de conmutación por error del equilibrador de carga en cada VDA redistribuye automáticamente las conexiones de impresora asignadas al servidor fallido entre los otros servidores de impresión disponibles, de forma que todas las sesiones existentes y entrantes funcionen normalmente sin que el fallo afecte a la experiencia de los usuarios y sin necesitar de la intervención inmediata de un administrador.

Los administradores pueden supervisar la actividad de equilibrio de carga de servidores de impresión mediante un conjunto de contadores de rendimiento para realizar un rastreo de lo siguiente en el VDA:

- Lista de servidores de impresión con equilibrio de carga en el VDA y su estado (disponible, no disponible)
- Cantidad de conexiones de impresora aceptadas por cada servidor de impresión
- Cantidad de conexiones de impresora fallidas en cada servidor de impresión
- Cantidad de conexiones de impresora activas en cada servidor de impresión
- Cantidad de conexiones de impresora pendientes en cada servidor de impresión

## Ver y administrar colas de impresión

La siguiente tabla resume los sitios donde se pueden administrar colas de impresión y mostrar las impresoras existentes en el entorno.

		Ruta de impresión
Impresoras del cliente (Impresoras conectadas al dispositivo del usuario)	Ruta de impresión de cliente	Control de cuentas de usuario habilitado en: Complemento Administración de impresión de la consola Microsoft Management Console; Control de cuentas de usuario inhabilitado: Antes de Windows 8: Panel de control, Windows 8: Complemento Administración de impresión
Impresoras de red (Impresoras de un servidor de impresión en red)	Ruta de impresión en red	Control de cuentas de usuario habilitado en: Servidor de impresión > Complemento Administración de impresión de la consola Microsoft Management Console; Control de cuentas de usuario inhabilitado: Servidor de impresión > Panel de control
Impresoras de red (Impresoras de un servidor de impresión en red)	Ruta de impresión de cliente	Control de cuentas de usuario habilitado en: Servidor de impresión > Complemento Administración de impresión de la consola Microsoft Management Console; Control de cuentas de usuario inhabilitado: Antes de Windows 8: Panel de control, Windows 8: Complemento Administración de impresión

		Ruta de impresión
Impresoras de servidor de red local (impresoras de un servidor de impresión en red que se agregan a una máquina con sistema operativo multisesión)	Ruta de impresión en red	Control de cuentas de usuario habilitado: Servidor de impresión > Panel de control; Control de cuentas de usuario inhabilitado: Servidor de impresión > Panel de control

**Nota:**

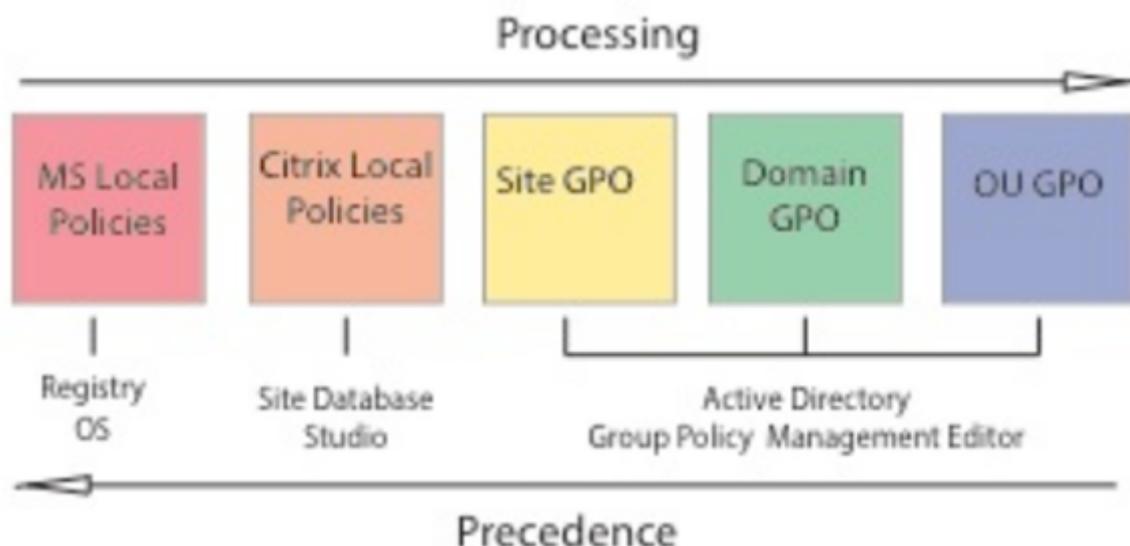
Las colas de impresión de las impresoras de red que usan la ruta de impresión en red son privadas y no se pueden administrar en el sistema.

## Directivas

September 22, 2021

Las directivas son un conjunto de configuraciones que definen la forma en que se administran las sesiones, el ancho de banda y la seguridad para un grupo de usuarios, dispositivos o tipos de conexión.

Puede aplicar configuraciones de directiva a las máquinas físicas y virtuales o a los usuarios. Puede aplicar configuraciones a usuarios individuales a un nivel local, o a grupos de seguridad en Active Directory. Las configuraciones definen criterios y reglas específicos. A menos que se asignen directivas específicamente, las configuraciones se aplican a todas las conexiones.



Puede aplicar las directivas en diferentes niveles de la red. Las configuraciones de directiva colocadas en el nivel de objeto de directiva de grupo (GPO) de unidad organizativa (OU) tienen precedencia en la red. Las directivas a nivel de grupo GPO del dominio anulan las directivas de GPO del sitio que, a su vez, anulan las directivas en conflicto que haya en los niveles de directivas locales de Citrix y de Microsoft.

Todas las directivas locales de Citrix se crean y administran desde la consola de Citrix Studio y se almacenan en la base de datos de configuración del sitio. Las directivas de grupo se crean y administran mediante la consola Microsoft Management Console (GPMC) y se almacenan en Active Directory. Las Directivas locales de Microsoft se crean en el sistema operativo y se guardan en el Registro de Windows.

Studio usa un asistente de Modelado para ayudar a los administradores a comparar los parámetros de configuración incluidos en las plantillas y las directivas, de modo que puedan eliminar parámetros redundantes o conflictivos. Los administradores pueden configurar objetos de directiva de grupo (GPO) mediante la Consola de administración de directivas de grupo y aplicarlos a un conjunto de usuarios de destino en diferentes niveles de la red.

Estos GPO se guardan en Active Directory, y el acceso a la administración de estas configuraciones, por lo general, está restringido para la mayoría del equipo de TI por motivos de seguridad.

Las configuraciones se fusionan según su condición y prioridad. Una configuración inhabilitada anula una configuración habilitada de menor prioridad. Las configuraciones de directiva sin definir se omiten y no supeditan las configuraciones de menor rango.

Las directivas locales también pueden tener conflictos con directivas de grupo en Active Directory, lo que podría invalidarlas mutuamente, dependiendo de la situación.

Todas las directivas se procesan en el orden siguiente:

1. El usuario inicia sesión en una máquina con credenciales de dominio.
2. Las credenciales se envían al controlador de dominio.
3. Active Directory aplica todas las directivas (usuario final, punto final, unidad organizativa y dominio).
4. El usuario inicia una sesión en la aplicación Citrix Workspace y accede a una aplicación o un escritorio.
5. Las directivas de Citrix y Microsoft se procesan para el usuario final y la máquina que aloja el recurso.
6. Active Directory determina el orden de prioridad de las configuraciones de directivas. A continuación, las aplica a los Registros de los dispositivos de punto final y a la máquina que aloja el recurso.
7. El usuario cierra la sesión en el recurso. Las directivas de Citrix para el usuario final y el dispositivo de punto final ya no están activas.
8. El usuario cierra la sesión en el dispositivo de usuario, lo que libera las directivas del GPO de usuario.
9. El usuario final apaga el dispositivo, lo que libera las directivas del GPO de máquina.

Al crear directivas para grupos de usuarios, dispositivos y máquinas, algunos miembros pueden tener diferentes requisitos y necesitan excepciones en algunas configuraciones de directiva. Las excepciones se realizan mediante filtros en Studio y la consola GPMC, que determinan a quién o a qué afecta la directiva.

**Nota:**

No se admite la combinación de directivas de Windows y Citrix en el mismo objeto de directiva de grupo.

## Trabajar con directivas

March 15, 2022

Configure directivas de Citrix para controlar el acceso de los usuarios y los entornos de sesión. Las directivas de Citrix son el método más eficaz para controlar los parámetros de conexión, seguridad y ancho de banda. Puede crear directivas para grupos de usuarios, dispositivos o tipos de conexión específicos. Cada directiva puede contener varias configuraciones.

### Herramientas para trabajar con las directivas de Citrix

Puede utilizar las siguientes herramientas para trabajar con directivas de Citrix.

- **Studio:** Si usted es un administrador Citrix y no tiene permisos para administrar directivas de grupo, utilice Studio para crear directivas para su sitio. Las directivas creadas con Studio se almacenan en la base de datos del sitio y las actualizaciones se envían al escritorio virtual cuando el escritorio virtual se registra con el broker o cuando un usuario se conecta a ese escritorio virtual.
- **Editor de directivas de grupo local** (complemento de Microsoft Management Console): Si su entorno de red utiliza Active Directory y usted tiene permisos para administrar las directivas de grupo, puede usar el Editor de directivas de grupo local para crear directivas para un sitio. Las configuraciones que defina afectarán a los objetos de directiva de grupo (GPO) que especifique en la Consola de administración de directivas de grupo.

### Importante

Debe usar el Editor de directivas de grupo local para definir algunas configuraciones de directiva, incluidas las relacionadas con el registro de los VDA en el Controller, y las relacionadas con servidores de Microsoft App-V.

## Procesamiento de directivas y precedencia

Las configuraciones de directiva de grupo se procesan en el orden siguiente:

1. GPO locales
2. GPO del sitio de XenDesktop o XenApp (almacenados en la base de datos del sitio)
3. GPO de sitio
4. GPO de dominio
5. Unidades organizativas

No obstante, en caso de un conflicto, las configuraciones de directiva que se procesan las últimas pueden anular a las procesadas con anterioridad. Esto significa que las configuraciones de directiva toman precedencia en el orden siguiente:

1. Unidades organizativas
2. GPO de dominio
3. GPO de sitio
4. GPO del sitio de XenDesktop o XenApp (almacenados en la base de datos del sitio)
5. GPO locales

Por ejemplo, un administrador de Citrix usa Studio para crear una directiva (directiva A) que habilita la redirección de archivos del cliente para los empleados de ventas de la empresa. Al mismo tiempo, otro administrador usa el Editor de directivas de grupo para crear una directiva (directiva B) que inhabilita la redirección de archivos del cliente para los empleados de ventas. Cuando los empleados de ventas inician sesión en los escritorios virtuales, se aplica la directiva B y la directiva A se omite porque la

directiva B se procesó a nivel del dominio y la directiva A se procesa en el nivel de objeto de directiva de grupo de sitio de XenApp o XenDesktop.

No obstante, cuando un usuario inicia una sesión ICA o RDP, la configuración de sesión de Citrix anula la misma configuración definida en una directiva de Active Directory o mediante la Configuración de host de sesión de Escritorio remoto. Esto incluye los parámetros relacionados con la configuración típica de conexión del cliente RDP, como Tapiz del escritorio, Animación de menús y Ver contenido de las ventanas al arrastrar.

Cuando se utilizan varias directivas, puede priorizar las que contienen configuraciones conflictivas; consulte [Comparar, priorizar, modelar y solucionar problemas de directivas](#) para obtener más información.

## Flujo de trabajo para las directivas de Citrix

El proceso para la configuración de directivas es el siguiente:

1. Cree la directiva.
2. Configure los parámetros de la configuración de directiva.
3. Asigne la directiva a los objetos de usuario y máquina.
4. Dé una prioridad a la directiva.
5. Compruebe que la directiva funciona ejecutando el asistente de Modelado de Directivas de grupo de Citrix.

## Explorar las directivas y las configuraciones de Citrix

En el Editor de directivas de grupo local, las directivas y las configuraciones aparecen en dos categorías: Configuración de equipo y Configuración de usuario. Cada categoría tiene un nodo de Directivas de Citrix. Consulte la documentación de Microsoft para obtener más detalles sobre cómo explorar y usar este complemento.

En Studio, las configuraciones de directiva se ordenan en categorías según la funcionalidad o la característica a la que afectan. Por ejemplo, la sección Profile Management contiene las configuraciones de directiva de Profile Management.

- Las configuraciones de equipo (configuraciones de directiva que se aplican a las máquinas) definen el comportamiento de los escritorios virtuales y se aplican cuando se inicia un escritorio virtual. Estas configuraciones se aplican incluso cuando no hay sesiones de usuario activas en el escritorio virtual. Las configuraciones de usuario definen la experiencia del usuario al conectarse mediante ICA. Las directivas de usuario se aplican cada vez que un usuario se conecta o reconecta mediante ICA. Las directivas de usuario no se aplican cuando un usuario se conecta a través de RDP o inicia sesión directamente en la consola.

Para acceder a las directivas, sus configuraciones y plantillas, seleccione Directivas en el panel de navegación de Studio.

- La ficha **Directivas** muestra todas las directivas. Cuando se selecciona una directiva, las etiquetas a la derecha muestran: Información general (el nombre, la prioridad, su estado habilitado o inhabilitado y una descripción), Configuraciones (lista de configuraciones definidas) y Asignada a (objetos de usuario y máquina a los que la directiva esté asignada en ese momento). Para obtener más información, consulte [Creación de directivas](#).
- La ficha **Plantillas** enumera las plantillas suministradas por Citrix y las plantillas que usted haya creado. Cuando se selecciona una plantilla, las fichas a la derecha muestran: Descripción (para qué se puede usar la plantilla) y Configuraciones (lista de configuraciones definidas). Para obtener más información, consulte [Plantillas de directiva](#).
- La ficha **Comparación** permite comparar las configuraciones de una directiva o de una plantilla con las de otras directivas o plantillas. Por ejemplo, puede que quiera verificar los valores de configuración para asegurar que se cumplen las directrices recomendadas. Para obtener más información, consulte [Comparación, prioridad, modelado y solución de problemas de directivas](#).
- En la ficha **Modelado**, puede simular escenarios de conexión con directivas de Citrix. Para obtener más información, consulte [Comparación, prioridad, modelado y solución de problemas de directivas](#).

Para buscar una configuración dentro de una directiva o una plantilla:

1. Seleccione la directiva o la plantilla.
2. Seleccione Modificar directiva o Modificar plantilla en el panel Acciones.
3. En la página Configuraciones, comience a escribir el nombre de la configuración.

Puede limitar la búsqueda si selecciona una versión específica del producto, seleccionando una categoría (por ejemplo, el Ancho de banda) o marcando la casilla Ver solo seleccionadas o eligiendo buscar solo entre las configuraciones que se han agregado a la directiva seleccionada. Para realizar una búsqueda sin filtro, seleccione Todas las configuraciones.

- Para buscar una configuración dentro de una directiva:
  1. Seleccione la directiva.
  2. Seleccione la ficha Configuraciones y comience a escribir el nombre de la configuración.

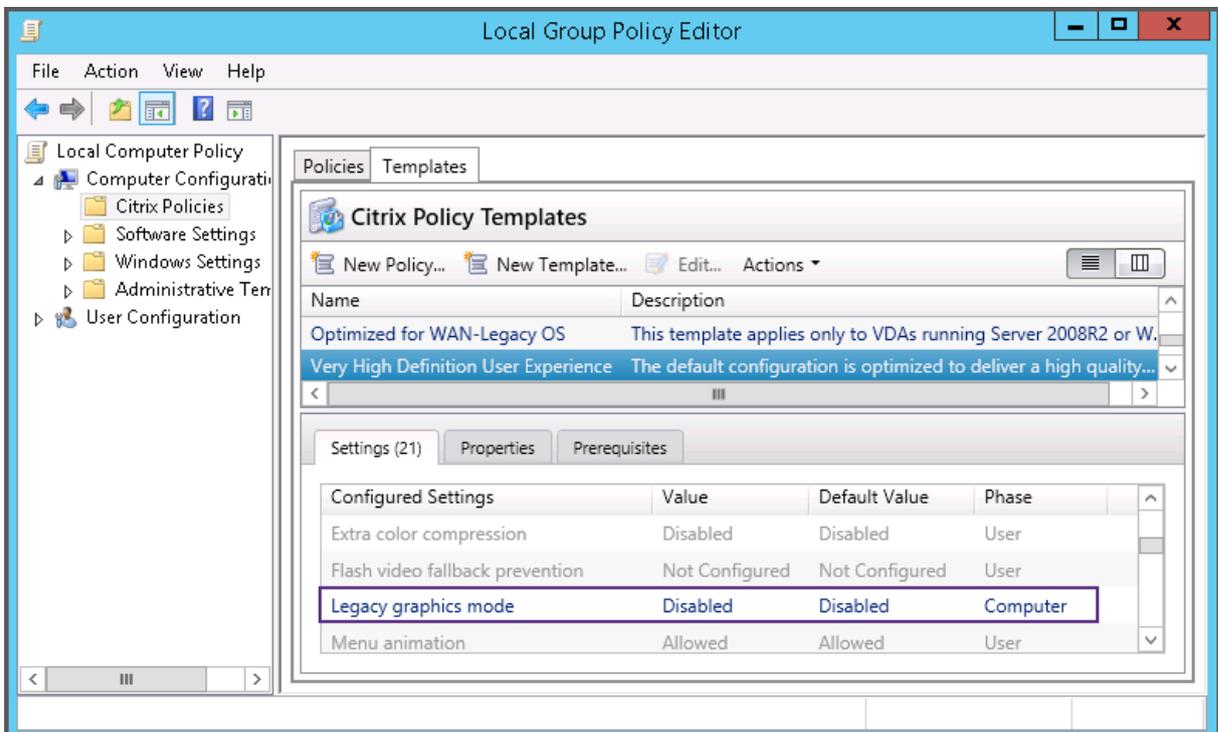
Puede limitar la búsqueda mediante la selección de una versión específica del producto o al seleccionar una categoría. Para realizar una búsqueda sin filtro, seleccione Todas las configuraciones.

Una vez creada, una directiva es completamente independiente de la plantilla utilizada. Puede usar el campo de descripción de una nueva directiva para realizar un rastreo de la plantilla de origen utilizada.

En Studio, las directivas y las plantillas se muestran en una única lista, independientemente de si contienen configuraciones de usuario, equipo o ambos, y se pueden aplicar tanto con filtros de usuario como con filtros de equipo.

En el Editor de directivas de grupo, las configuraciones de equipo y de usuario se deben aplicar de forma independiente incluso aunque se hayan creado a partir de una plantilla con los dos tipos de configuración. En este ejemplo, se ha optado por usar una plantilla de experiencia de usuario de definición muy alta en la configuración de equipo:

- El modo de gráficos antiguo es una configuración de equipo que se usará en una directiva creada a partir de esta plantilla.
- Las configuraciones de usuario, en gris, no se usarán en una directiva creada a partir de esta plantilla.



## Plantillas de directiva

April 19, 2024

Las plantillas son un punto de partida para la creación de directivas a partir de opciones iniciales predefinidas. Las plantillas integradas de Citrix, optimizadas para condiciones de red o entornos específicos, se pueden utilizar como:

- Un borrador para crear unas directivas y plantillas propias que se compartirán entre diferentes sitios.
- Una referencia para una comparación más fácil de los resultados entre las implementaciones, ya que puede citar los resultados; por ejemplo, “[...] cuando se usa la plantilla X o Y de Citrix [...]”.
- Un método para comunicar directivas a Citrix Support o a terceros de confianza mediante la importación o exportación de plantillas.

Las plantillas de directivas se pueden importar y exportar.

Para conocer los aspectos a tener en cuenta cuando se utilicen plantillas para crear directivas, consulte el artículo [CTX202330](#) de Knowledge Center. Para descargar el PDF, inicie sesión con sus credenciales.

## Plantillas integradas de Citrix

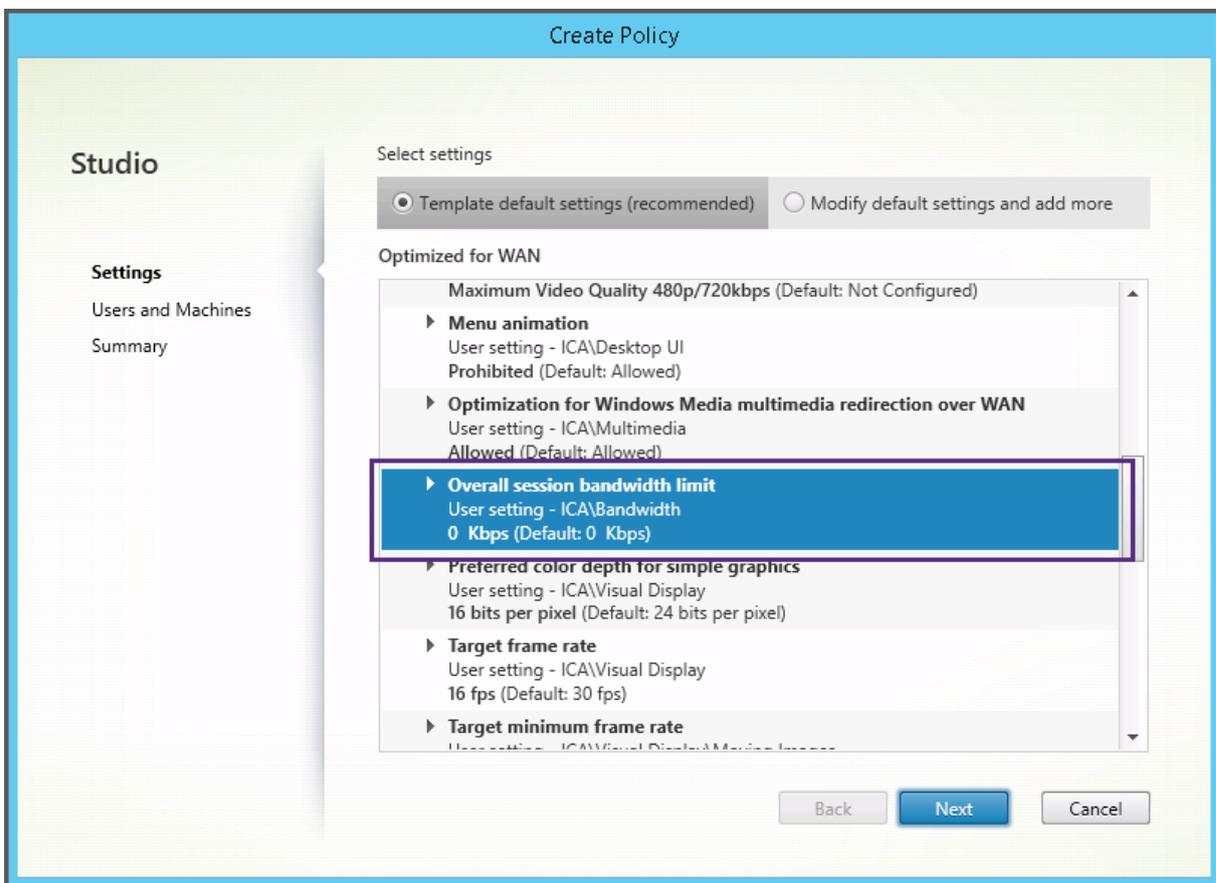
Están disponibles las siguientes plantillas de directiva:

- **Experiencia de usuario de muy alta definición.** Con esta plantilla, se aplica la configuración predeterminada que optimiza la experiencia de usuario. Use esta plantilla en situaciones donde se procesan varias directivas por orden de prioridad.
- **Alta escalabilidad de servidores.** Aplique esta plantilla para ahorrar recursos de servidor. Esta plantilla equilibra la experiencia del usuario y la capacidad de escalabilidad del servidor. Ofrece una buena experiencia de usuario al mismo tiempo que aumenta la cantidad de usuarios que se pueden alojar en un solo servidor. Esta plantilla no usa ningún códec de vídeo para la compresión de gráficos e impide la generación multimedia de contenido en el lado del servidor.
- **Alta escalabilidad de servidores - SO antiguos.** Esta plantilla de alta escalabilidad de servidores se aplica solo a los agentes VDA con Windows Server 2008 R2 o Windows 7 y versiones anteriores. Esta plantilla se basa en el modo de gráficos antiguo, que es más eficaz para esos sistemas operativos.
- **Optimizado para NetScaler SD-WAN.** Aplique esta plantilla para optimizar la entrega de Citrix Virtual Desktops a los usuarios que trabajan en sucursales con NetScaler SD-WAN implementado. (NetScaler SD-WAN es el nuevo nombre de CloudBridge.)
- **Optimizado para WAN.** Esta plantilla es para trabajadores de tareas situados en sucursales que utilizan una conexión de red WAN compartida, o bien utilizan ubicaciones remotas con conexiones de poco ancho de banda que acceden a aplicaciones con sencillas interfaces gráficas de usuario y poco contenido multimedia. Esta plantilla intercambia la experiencia de reproducción de vídeos y parte de la escalabilidad de los servidores por una eficiencia optimizada del ancho de banda.
- **Optimizado para WAN - SO antiguos.** Esta plantilla de *optimización para redes WAN* se aplica solo a los agentes VDA con Windows Server 2008 R2 o Windows 7 y versiones anteriores. Esta

plantilla se basa en el modo de gráficos antiguo, que es más eficaz para esos sistemas operativos.

- **Seguridad y control.** Use esta plantilla en entornos con poca tolerancia a fallos para minimizar las funciones habilitadas de forma predeterminada en Citrix Virtual Apps and Desktops. Esta plantilla incluye opciones de configuración que inhabilitan el acceso a la impresora, el portapapeles, los dispositivos periféricos, la asignación de unidades, la redirección de puertos y la aceleración de Flash en los dispositivos de usuario. Aplicar esta plantilla puede usar más ancho de banda y reducir la densidad de usuarios por servidor.

Aunque se recomienda usar las plantillas integradas de Citrix con la configuración predeterminada, hay opciones que no tienen ningún valor concreto recomendado. Por ejemplo: el **límite de ancho de banda global de la sesión**, incluido en las plantillas de optimización de redes WAN. En este caso, en la plantilla se ofrece la opción de configuración para que el administrador entienda que esta opción se puede aplicar.



Si trabaja con una implementación (administración de directivas y agentes VDA) anterior a XenApp y XenDesktop 7.6 FP3, y necesita plantillas de alta escalabilidad de servidores y optimización de WAN, use las versiones para SO antiguos de esas plantillas cuando corresponda.

**Nota:**

Citrix crea y actualiza las plantillas integradas. No se puede modificar ni eliminar estas plantillas.

## Crear y administrar plantillas mediante Studio

Para crear una plantilla basada, a su vez, en una plantilla:

1. Seleccione **Directivas** en el panel de navegación de Studio.
2. Haga clic en la ficha **Plantillas** y seleccione la plantilla a partir de la cual creará otra.
3. Seleccione **Crear plantilla** en el panel Acciones.
4. Seleccione y configure las configuraciones de directiva que desea incluir en la plantilla. Quite cualquier parámetro existente que no sea pertinente. Introduzca un nombre para la plantilla.

Después de hacer clic en **Finalizar**, la nueva plantilla aparecerá en la ficha **Plantillas**.

Para crear una plantilla basada en una directiva:

1. Seleccione **Directivas** en el panel de navegación de Studio.
2. Haga clic en la ficha **Directivas** y seleccione la directiva a partir de la cual creará otra.
3. Seleccione **Guardar como plantilla** en el panel Acciones.
4. Seleccione y defina las configuraciones de directiva que desea incluir en la plantilla. Quite cualquier parámetro existente que no sea pertinente. Introduzca un nombre y una descripción para la nueva plantilla y haga clic en **Finalizar**.

Para importar una plantilla:

1. Seleccione **Directivas** en el panel de navegación de Studio.
2. Seleccione la ficha **Plantillas** y seleccione **Importar plantilla**.
3. Seleccione el archivo de plantilla a importar y, a continuación, haga clic en **Abrir**. Si importa una plantilla que se llama igual que otra plantilla existente, puede elegir entre sobrescribir esta última o guardar la plantilla importada con otro nombre generado automáticamente.

Para exportar una plantilla:

1. Seleccione **Directivas** en el panel de navegación de Studio.
2. Seleccione la ficha **Plantillas** y seleccione **Exportar plantilla**.
3. Seleccione la ubicación donde desea guardar la plantilla y haga clic en **Guardar**.

Se creará un archivo `.gpt` en la ubicación especificada.

## Crear y administrar plantillas mediante el Editor de directivas de grupo

En el Editor de directivas de grupo, expanda Configuración del equipo o Configuración de usuario. Expanda el nodo **Directivas** y seleccione **Directivas de Citrix**. Elija la acción adecuada.

Tarea	Instrucción
Crear una plantilla a partir de una directiva existente	En la ficha <b>Directivas</b> , seleccione la directiva y, a continuación, seleccione <b>Acciones &gt; Guardar como plantilla</b> .
Crear una directiva a partir de una plantilla existente	En la ficha <b>Plantillas</b> , seleccione la plantilla y, a continuación, haga clic en <b>Nueva directiva</b> .
Crear una plantilla a partir de una plantilla existente	En la ficha <b>Plantillas</b> , seleccione la plantilla y, a continuación, haga clic en <b>Nueva plantilla</b> .
Importar una plantilla	En la ficha <b>Plantillas</b> , seleccione <b>Acciones &gt; Importar</b> .
Exportar una plantilla	En la ficha <b>Plantillas</b> , seleccione <b>Acciones &gt; Exportar</b> .
Ver la configuración de la plantilla	En la ficha <b>Plantillas</b> , seleccione la plantilla y, a continuación, haga clic en la ficha <b>Parámetros</b> .
Ver un resumen de las propiedades de la plantilla	En la ficha <b>Plantillas</b> , seleccione la plantilla y, a continuación, haga clic en la ficha <b>Propiedades</b> .
Ver requisitos previos de la plantilla	En la ficha <b>Plantillas</b> , seleccione la plantilla y, a continuación, haga clic en la ficha <b>Requisitos previos</b> .

## Plantillas y administración delegada

Las plantillas de directiva se almacenan en la máquina donde se ha instalado el paquete de administración de directivas. Esta máquina es la máquina del Delivery Controller o la máquina de administración de objetos de directiva de grupo, no la base de datos del sitio de Citrix Virtual Apps and Desktops. Esto significa que los permisos administrativos de Windows controlan los archivos de plantilla de directiva en lugar de los roles y los ámbitos de la administración delegada del sitio.

Como resultado, un administrador con permisos de solo lectura en el sitio puede, por ejemplo, crear plantillas. Sin embargo, como las plantillas son archivos locales, no se realiza ningún cambio en el entorno.

Las plantillas personalizadas solo están visibles para la cuenta de usuario que las crea y se guardan en el perfil de usuario de Windows. Para dar mayor visibilidad a una plantilla personalizada, cree una directiva a partir de ella o expórtela a una ubicación compartida.

## Crear directivas

September 22, 2021

Antes de crear una directiva, decida a qué grupo de usuarios o dispositivos debe afectar. Puede crear una directiva según las funciones laborales del usuario, el tipo de conexión, el dispositivo de usuario o la ubicación geográfica. De forma alternativa, puede utilizar los mismos criterios que utiliza para las directivas de grupo de Active Directory de Windows.

Si ya creó una directiva aplicable a un grupo, considere la posibilidad de modificar dicha directiva para agregarle las configuraciones apropiadas, en lugar de crear otra directiva nueva. Evite la creación de una directiva nueva exclusivamente para habilitar una configuración específica o para excluir la aplicación de la directiva a determinados usuarios.

Al crear una nueva directiva, puede basarla en las configuraciones de una plantilla de directiva y personalizarlas según sea necesario, o puede crearla sin usar plantilla y agregar las configuraciones que necesite.

En Citrix Studio, las nuevas directivas creadas se establecen como inhabilitadas a menos que se marque explícitamente la casilla Habilitar directiva.

## Configuraciones de directivas

Las configuraciones de directiva pueden estar habilitadas, inhabilitadas o sin configurar. De forma predeterminada, las configuraciones de directiva no están definidas; es decir, que no están agregadas a una directiva. La configuración solamente puede aplicarse cuando se agrega a una directiva.

Algunas configuraciones de directiva pueden tener uno de los siguientes estados:

- Permitida o Prohibida, permite o impide la acción controlada por la configuración. En algunos casos, se permite o se impide que los usuarios administren la acción de la configuración en la sesión. Por ejemplo, si se define la configuración Animación de menús como Permitida, los usuarios pueden controlar las animaciones de los menús en su entorno de cliente.
- Habilitada o Inhabilitada, habilita o inhabilita la configuración. Si se inhabilita una configuración, no se habilita en ninguna directiva de menor prioridad.

Asimismo, algunas configuraciones controlan la eficacia de otras configuraciones dependientes. Por ejemplo, la configuración Redirección de unidades del cliente controla si los usuarios pueden acceder a las unidades de sus dispositivos. Para permitir que los usuarios accedan a sus unidades de red, es necesario agregar tanto esta configuración como la configuración Unidades de red del cliente a la directiva. Si la configuración Redirección de unidades del cliente está inhabilitada, los usuarios no pueden acceder a sus unidades de red aunque la configuración Unidades de red del cliente esté habilitada.

En general, los cambios de configuraciones de directiva que afectan a máquinas surten efecto cuando se reinicia el escritorio virtual o cuando un usuario inicia una sesión. Los cambios de configuraciones de directiva que afectan a usuarios surten efecto la próxima vez que el usuario inicia una sesión. Si se utiliza Active Directory, las configuraciones de directiva se actualizan cuando Active Directory vuelve a evaluar las directivas en intervalos regulares de 90 minutos y se aplican cuando se reinicia el escritorio virtual o cuando un usuario inicia sesión.

Para algunas configuraciones de directiva, puede especificar o seleccionar un valor cuando se las agrega a una directiva. Puede limitar la configuración del parámetro si selecciona Usar el valor predeterminado. Esto impide configurar el parámetro y permite usar solo el valor predeterminado al aplicar la configuración de directiva, independientemente del valor que se hubiera introducido antes de seleccionar Usar el valor predeterminado.

Recomendaciones:

- Asigne las directivas a grupos y no a usuarios individuales. Si asigna directivas a un grupo, las asignaciones se actualizan automáticamente cuando se agregan o se quitan usuarios.
- No habilite configuraciones que puedan entrar en conflicto o que se superpongan en Configuración de host de sesión de Escritorio remoto. En algunos casos, Configuración de host de sesión de Escritorio remoto ofrece funciones similares a las configuraciones de directiva de Citrix. Siempre que sea posible, mantenga la consistencia entre todas las configuraciones (habilitadas o inhabilitadas) para facilitar la solución de problemas.
- Inhabilite las directivas que no use. Las directivas sin configuración generan una actividad de procesamiento innecesaria.

## **Asignaciones de directiva**

Al crear una directiva, hay que asignarla a ciertos objetos de usuario y máquina; dicha directiva se aplica a las conexiones según criterios o reglas específicos. Por lo general, es posible agregar tantas asignaciones como se desee a una directiva, según una combinación de criterios. Si no se especifica ninguna asignación, la directiva se aplica a todas las conexiones.

En la siguiente tabla se muestran las asignaciones disponibles:

Nombre de asignación	Aplica una directiva según
Control de acceso	Condiciones de control de acceso del cliente. <i>Tipo de conexión:</i> Si se debe aplicar la directiva a las conexiones realizadas con o sin NetScaler Gateway. <i>Nombre de la comunidad de NetScaler Gateway:</i> Nombre del servidor virtual de NetScaler Gateway. <i>Condición de acceso:</i> Nombre de la directiva de análisis o de la directiva de sesión que se va a usar en el dispositivo de punto final.
NetScaler SD-WAN	Si se inicia o no una sesión de usuario a través de NetScaler SD-WAN. Nota: Puede agregar solo una asignación de NetScaler SD-WAN a una directiva.
Dirección IP del cliente	Dirección IP del dispositivo del usuario, utilizado para conectarse a la sesión. Ejemplos de IPv4: 12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24. Ejemplos de IPv6: 2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54
Nombre del cliente	Nombre del dispositivo de usuario. Coincidencia exacta: ClientABCName. Uso de comodines: Client*Name.
Grupo de entrega	Pertenencia a un grupo de entrega.
Tipo de grupo de entrega	Tipo de escritorio o aplicación: escritorio privado, escritorio compartido, aplicación privada o aplicación compartida. <b>Nota:</b> Las opciones de filtro de escritorio privado y escritorio compartido solo están disponibles para Citrix Virtual Apps and Desktops 7.x. Para obtener más información, consulte <a href="#">CTX219153</a> .
Unidad organizativa (UO)	Unidad organizativa.
Etiqueta	Etiquetas. <b>Nota:</b> Aplique esta directiva a todas las máquinas etiquetadas. Tenga en cuenta que las etiquetas de aplicación no están incluidas.
Usuario o grupo	Nombre de usuario o grupo.

Cuando un usuario inicia sesión, se identifican todas las directivas que coinciden con las asignaciones para la conexión. Las directivas se ordenan por prioridad y se comparan varias instancias de cualquier configuración. Cada configuración se aplica según la clasificación de prioridades de la directiva. Toda configuración de directiva que esté inhabilitada prevalece sobre las configuraciones habilitadas de menor prioridad. Las configuraciones de directiva que no están configuradas se ignoran.

**Importante:**

Si configura las directivas de Active Directory y Citrix mediante la Consola de administración de directivas de grupo, es posible que las asignaciones y las configuraciones no se apliquen de la forma esperada. Para obtener más información, consulte [CTX127461](#).

De forma predeterminada se proporciona una directiva “Sin filtro”.

- Si utiliza Studio para administrar las directivas de Citrix, las configuraciones que agregue a la directiva sin filtro se aplican a todos los servidores, escritorios y conexiones de un sitio.
- Si utiliza el Editor de directivas de grupo local para administrar las directivas de Citrix, las configuraciones que se agreguen a la directiva sin filtro se aplican a todos los sitios y conexiones que abarquen los objetos de directiva de grupo (GPO) que contienen la directiva. Por ejemplo, la unidad organizativa Ventas contiene un GPO denominado Ventas-EE. UU. que incluye a todos los miembros del equipo de ventas de los Estados Unidos. El GPO Ventas-EE. UU. tiene configurada una directiva sin filtro que incluye varias configuraciones de directiva de usuario. Cuando el administrador de Ventas-EE. UU. inicia sesión en el sitio, la configuración de la directiva sin filtro se aplica automáticamente a la sesión, ya que el usuario es miembro del GPO Ventas-EE. UU.

El modo de una asignación determina si la directiva se aplica exclusivamente a las conexiones que coinciden con todos los criterios de la asignación. Si el modo está establecido en Permitir (Allow) (valor predeterminado), la directiva se aplica solamente a las conexiones que coinciden con los criterios de la asignación. Si el modo está establecido en Denegar (Deny), la directiva se aplica si la conexión no coincide con las asignaciones del filtro. Los siguientes ejemplos ilustran cómo los modos de las asignaciones afectan a las directivas de Citrix cuando hay varias asignaciones.

- **Ejemplo: Asignaciones del mismo tipo en modos distintos:** En las directivas con dos asignaciones del mismo tipo, donde una está establecida en Permitir y la otra en Denegar, la asignación establecida en Denegar tiene precedencia, siempre que la conexión satisfaga ambas asignaciones. Por ejemplo:

La directiva 1 incluye las siguientes asignaciones:

- La asignación A especifica el grupo Ventas, con el modo Permitir
- La asignación B especifica la cuenta del jefe de Ventas, con el modo Denegar

Como el modo de la asignación B es Denegar, no se aplica la directiva cuando el jefe de Ventas inicia sesión en el sitio, aunque este usuario sea miembro del grupo Ventas.

- **Ejemplo: Asignaciones de diferentes tipos con modos iguales:** En las directivas con dos o más asignaciones de diferentes tipos, establecidas en Permitir, la conexión debe satisfacer al menos una asignación de cada tipo para que se aplique la directiva. Por ejemplo:

La directiva 2 incluye las siguientes asignaciones:

- La asignación C es una asignación de usuario que especifica el grupo Ventas con el modo Permitir
- La asignación D es una asignación de dirección IP del cliente que especifica 10.8.169.\* (la red de la empresa) con el modo Permitir

Cuando el jefe de Ventas inicia sesión en el sitio desde la oficina, se aplica la directiva, ya que la conexión satisface ambas asignaciones.

La directiva 3 incluye las siguientes asignaciones:

- La asignación E es una asignación de usuario que especifica el grupo Ventas con el modo Permitir
- La asignación F es una asignación de control de acceso que especifica condiciones de conexión de NetScaler Gateway con el modo Permitir

Cuando el jefe de Ventas inicia sesión en el sitio desde la oficina, no se aplica la directiva, ya que la conexión no satisface la asignación F.

## Crear una directiva basada en una plantilla mediante Studio

1. Seleccione Directivas en el panel de navegación de Studio.
2. Seleccione la ficha Plantillas y seleccione la plantilla.
3. Seleccione Crear directiva con una plantilla en el panel Acciones.
4. De forma predeterminada, la nueva directiva utiliza todos los valores de configuración predeterminados en la plantilla (el botón Usar configuraciones de plantilla está seleccionado). Si quiere cambiar configuraciones, seleccione Modificar y agregar más configuraciones predeterminadas y, a continuación, agregue o quite configuraciones.
5. Especifique cómo se aplica la directiva, seleccionando una de las siguientes opciones:
  - Asignar a objetos de usuario y máquina seleccionados; a continuación, elija los objetos de usuario y máquina a los que aplicar la directiva.
  - Asignar a Todos los objetos del sitio, para aplicar la directiva a todos los objetos de usuario y máquina en el sitio.
6. Introduzca un nombre para la directiva (o acepte el predeterminado). Conviene que el nombre dado a la directiva esté basado en a quién o a qué afecta; por ejemplo, “Departamento de Contabilidad” o “Usuarios remotos”. Si lo desea, puede proporcionar una descripción.

La directiva está habilitada de forma predeterminada; se puede inhabilitar. Si la directiva está habilitada, se aplica de inmediato a los usuarios que inician sesión en el sitio. Si se inhabilita, la directiva no se aplica. Si necesita establecer la prioridad de una directiva o agregar configuraciones en otro momento, puede inhabilitar la directiva hasta que esté listo para aplicarla.

### **Crear una directiva basada en una plantilla mediante Studio**

1. Seleccione Directivas en el panel de navegación de Studio.
2. Seleccione la ficha Plantillas y seleccione la plantilla.
3. Seleccione Crear directiva con una plantilla en el panel Acciones.
4. De forma predeterminada, la nueva directiva utiliza todos los valores de configuración predeterminados en la plantilla (el botón Usar configuraciones de plantilla está seleccionado). Si quiere cambiar configuraciones, seleccione Modificar y agregar más configuraciones predeterminadas y, a continuación, agregue o quite configuraciones.
5. Especifique cómo se aplica la directiva, seleccionando una de las siguientes opciones:
  - Asignar a objetos de usuario y máquina seleccionados; a continuación, elija los objetos de usuario y máquina a los que aplicar la directiva.
  - Asignar a Todos los objetos del sitio, para aplicar la directiva a todos los objetos de usuario y máquina en el sitio.
6. Introduzca un nombre para la directiva (o acepte el predeterminado). Conviene que el nombre dado a la directiva esté basado en a quién o a qué afecta; por ejemplo, “Departamento de Contabilidad” o “Usuarios remotos”. Si lo desea, puede proporcionar una descripción.

La directiva está habilitada de forma predeterminada; se puede inhabilitar. Si la directiva está habilitada, se aplica de inmediato a los usuarios que inician sesión en el sitio. Si se inhabilita, la directiva no se aplica. Si necesita establecer la prioridad de una directiva o agregar configuraciones en otro momento, puede inhabilitar la directiva hasta que esté listo para aplicarla.

### **Crear una directiva mediante Studio**

1. Seleccione Directivas en el panel de navegación de Studio.
2. Seleccione la ficha Directivas.
3. Seleccione Crear directiva en el panel Acciones.
4. Agregue y defina configuraciones de directiva.
5. Especifique cómo quiere aplicar la directiva, seleccionando una de las siguientes opciones:

- Asignar a objetos de usuario y máquina seleccionados; a continuación, elija los objetos de usuario y máquina a los que aplicar la directiva.
  - Asignar a Todos los objetos del sitio, para aplicar la directiva a todos los objetos de usuario y máquina en el sitio.
6. Introduzca un nombre para la directiva (o acepte el predeterminado). Conviene que el nombre dado a la directiva esté basado en a quién o a qué afecta; por ejemplo, “Departamento de Contabilidad” o “Usuarios remotos”. Si lo desea, puede proporcionar una descripción.

La directiva está habilitada de forma predeterminada; se puede inhabilitar. Si la directiva está habilitada, se aplica de inmediato a los usuarios que inician sesión en el sitio. Si se inhabilita, la directiva no se aplica. Si necesita establecer la prioridad de una directiva o agregar configuraciones en otro momento, puede inhabilitar la directiva hasta que esté listo para aplicarla.

### Crear y administrar directivas con el Editor de directivas de grupo

En el Editor de directivas de grupo, expanda Configuración del equipo o Configuración de usuario. Expanda el nodo Directivas y seleccione Directivas de Citrix. Elija la acción adecuada.

Tarea	Instrucción
Crear una directiva	En la ficha Directivas, haga clic en Nueva.
Modificar una directiva existente	En la ficha Directivas, seleccione la directiva y, a continuación, haga clic en Modificar.
Cambiar la prioridad de una directiva existente	En la ficha Directivas, seleccione la directiva y, a continuación, haga clic en Superior o Inferior.
Ver información de resumen acerca de una directiva	En la ficha Directivas, seleccione la directiva y, a continuación, haga clic en la ficha Resumen.
Ver y corregir configuraciones de directiva	En la ficha Directivas, seleccione la directiva y, a continuación, haga clic en la ficha Configuraciones.
Ver y corregir filtros de directiva	En la ficha Directivas, seleccione la directiva y, a continuación, haga clic en la ficha Filtros. Cuando se agrega más de un filtro a una directiva, se deben cumplir todas las condiciones de filtro para que se aplique la directiva.
Habilitar o inhabilitar una directiva	En la ficha Directivas, seleccione la directiva y, a continuación, seleccione Acciones > Habilitar o Acciones > Inhabilitar.

---

Tarea	Instrucción
Crear una directiva a partir de una plantilla existente	En la ficha Plantillas, seleccione la plantilla y, a continuación, haga clic en Nueva directiva.

---

## Comparar, priorizar, modelar y solucionar problemas de directivas

January 4, 2021

Puede utilizar varias directivas para personalizar el entorno y responder a las necesidades de los usuarios según su función laboral, su ubicación geográfica o su tipo de conexión. Por ejemplo, es posible que, por motivos de seguridad, deba establecer restricciones en los grupos de usuarios que trabajan regularmente con datos confidenciales. Puede crear una directiva para evitar que los usuarios guarden archivos con información confidencial en sus unidades de cliente locales. No obstante, si algunos de los miembros del grupo de usuarios necesitan acceder a las unidades locales, puede crear otra directiva para permitirles el acceso a esos usuarios en particular. A continuación, puede clasificar y dar prioridad a las dos directivas para establecer cuál de ellas tiene preferencia.

Cuando se utilizan varias directivas, debe determinar cuál es su prioridad, cómo crear las excepciones y cómo ver la directiva vigente cuando hay un conflicto de directivas.

En general, las directivas anulan configuraciones similares definidas para todo el sitio, para Delivery Controllers específicos o en el dispositivo del usuario. La excepción a este principio es la seguridad. La configuración de cifrado más exigente en su entorno, incluidos el sistema operativo y la configuración de remedo más restrictiva, siempre anulan otras configuraciones y directivas.

Las directivas de Citrix interactúan con directivas configuradas en su sistema operativo. En un entorno de Citrix, los parámetros de Citrix sobrescriben los parámetros similares configurados en una directiva de Active Directory o mediante Configuración de host de sesión de Escritorio remoto. Esto incluye las configuraciones relacionadas con la configuración típica de conexión del cliente del Protocolo de escritorio remoto (RDP), como Tapiz del escritorio, Animación de menú y Ver contenido de las ventanas al arrastrar. En el caso de algunas configuraciones de directiva, como Secure ICA, la configuración de las directivas debe coincidir con la configuración del sistema operativo. Si se configura un nivel de cifrado de mayor prioridad en otro lugar, la configuración de directiva de Secure ICA que especifique en la directiva o al entregar una aplicación o un escritorio puede anularse.

Por ejemplo, los parámetros de cifrado especificados al crear grupos de entrega deben estar al mismo nivel que los parámetros de cifrado especificados en todo el entorno.

Nota: En el segundo salto de los casos de doble salto, cuando un VDA de SO de sesión única se conecta a un VDA de SO multisesión, las directivas de Citrix actúan en el VDA de SO de sesión única como si

fuera el dispositivo del usuario. Por ejemplo, si las directivas están configuradas para guardar imágenes en caché en el dispositivo del usuario, las imágenes guardadas en el segundo salto del caso de doble salto se guardan en caché en la máquina VDA de SO de sesión única.

## Comparar directivas y plantillas

Puede comparar las configuraciones de una directiva o de una plantilla con las de otras directivas o plantillas. Por ejemplo, puede que necesite verificar los valores de configuración para asegurar que se cumplen las directrices recomendadas. También puede comparar las configuraciones de una directiva o plantilla con las configuraciones predeterminadas proporcionadas por Citrix.

1. Seleccione Directivas en el panel de navegación de Studio.
2. Haga clic en la ficha Comparación y, a continuación, haga clic en Seleccionar.
3. Seleccione las directivas o plantillas que desea comparar. Para incluir los valores predeterminados en la comparación, marque la casilla Comparar con la configuración predeterminada.
4. Haga clic en Comparar, las configuraciones definidas se mostrarán en columnas.
5. Para ver todas las configuraciones, seleccione Mostrar todas las configuraciones. Para volver a la vista predeterminada, seleccione Mostrar configuraciones en común.

## Priorizar directivas

La asignación de prioridades en las directivas le permite definir la prioridad de las directivas cuando contienen configuraciones conflictivas. Cuando un usuario inicia sesión, se identifican todas las directivas que coinciden con las asignaciones para la conexión. Las directivas se ordenan por prioridad y se comparan varias instancias de cualquier configuración. Cada configuración se aplica según la clasificación de prioridades de la directiva.

Usted asigna la prioridad de las directivas asignándoles diferentes números de prioridad en Studio. De forma predeterminada, las nuevas directivas tienen la prioridad más baja. Si hay conflictos en la configuración de las directivas, las directivas de mayor prioridad (el número de prioridad 1 es el máximo) anulan las de menor prioridad. Las configuraciones se combinan según su prioridad y su condición (por ejemplo, si la configuración está habilitada o inhabilitada). Una configuración inhabilitada anula otra configuración de menor prioridad que esté habilitada. Las configuraciones de directiva que no estén configuradas se omiten y no anulan ninguna configuración de menor prioridad.

1. Seleccione Directivas en el panel de navegación de Studio. Asegúrese de que la ficha Directivas está seleccionada.
2. Seleccione una directiva.
3. Seleccione Prioridad baja o Prioridad alta en el panel Acciones.

## Excepciones

Al crear directivas para grupos de usuarios, dispositivos de usuario o máquinas, es posible que deba crear excepciones en alguna configuración de directiva para determinados miembros del grupo. Para crear excepciones, debe:

- Crear una directiva exclusiva para los miembros del grupo que necesitan las excepciones y luego dar mayor prioridad a esta directiva que a la directiva de la totalidad del grupo.
- Usar el modo Denegar para una asignación agregada a la directiva

Una asignación con el modo Denegar aplica una directiva solo a las conexiones que no coinciden con los criterios de asignación. Por ejemplo, una directiva contiene las siguientes asignaciones:

- La asignación A es una asignación de dirección IP del cliente que especifica el intervalo 208.77.88.\* con el modo Permitir
- La asignación B es una asignación de usuario que especifica una cuenta de usuario determinada con el modo Denegar

La directiva se aplica a todos los usuarios que inician sesión en el sitio con las direcciones IP incluidas en el intervalo indicado en la asignación A. Sin embargo, la directiva no se aplica al usuario que inicia sesión en el sitio con la cuenta especificada en la asignación B, aunque al equipo del usuario tenga una dirección IP que se encuentre en el intervalo especificado en la asignación A.

## Determinar las directivas que se aplican a una conexión

En ocasiones, una conexión no responde según lo previsto debido a que se aplican varias directivas. Si se aplica una directiva de mayor prioridad a una conexión, esta puede anular la configuración definida en la directiva original. Es posible determinar cómo se combinan las configuraciones de directiva finales para una conexión mediante el cálculo del Conjunto resultante de directivas o RSOP (Resultant Set of Policies).

El Conjunto resultante de directivas se puede calcular de diversas maneras:

- Usando el asistente de Modelado de Directivas de grupo Citrix para simular un caso de conexión y observar la forma en que se aplicarían las directivas de Citrix. Puede especificar condiciones para un caso de conexión, por ejemplo, un controlador de dominio, usuarios, valores de evidencia de asignaciones de directiva de Citrix y parámetros de entorno simulados, como una conexión de red lenta. El informe generado por el asistente incluye una lista de las directivas de Citrix que se aplicarían en el caso especificado. Si está conectado a Controller como un usuario del dominio, el asistente calcula el conjunto resultante de directivas mediante tanto la configuración de directivas del sitio como los objetos de directiva de grupo (GPO) de Active Directory.
- Use los Resultados de directivas de grupo para obtener un informe donde se describen las directivas de Citrix vigentes para un usuario o un Controller específico. La herramienta Resultados

de directivas de grupo ayuda a evaluar el estado actual de los GPO en el entorno y genera un informe donde se describe la forma en que se aplican estos objetos, incluidas las directivas de Citrix, a un usuario y un Controller específicos.

Puede iniciar el asistente de Modelado de Directivas de grupo Citrix desde el panel Acciones de Studio. Puede ejecutar cualquiera de las dos herramientas desde la Consola de administración de directivas de grupo de Windows.

Si ejecuta el asistente de Modelado de Directivas de grupo Citrix o la herramienta Resultados de directivas de grupo desde la Consola de administración de directivas de grupo, no se incluyen las configuraciones de directiva del sitio creadas con Studio en el grupo de directivas resultante.

Para asegurarse de obtener el grupo de directivas resultante más completo, Citrix recomienda iniciar el asistente de Modelado de Directivas de grupo Citrix desde Studio, a menos que cree las directivas mediante solo la Consola de administración de directivas de grupo.

## **Usar el Asistente de modelado de directivas de grupo Citrix**

Abra el Asistente de modelado de directivas de grupo Citrix mediante uno de los procedimientos siguientes:

- Seleccione Directivas en el panel de navegación de Studio, seleccione la ficha Modelado y, a continuación, seleccione Iniciar asistente de modelado en el panel Acciones.
- Abra la Consola de administración de directivas de grupo (gpmc.msc), haga clic con el botón secundario en el nodo Modelado de Directivas de grupo Citrix del panel del árbol y seleccione Asistente de modelado de Directivas de grupo Citrix.

Siga las instrucciones del asistente para seleccionar el controlador de dominio, los usuarios, los equipos, los parámetros del entorno y los criterios de asignación de Citrix que desee usar en la simulación. Al hacer clic en Finalizar, el asistente presenta un informe de los resultados del modelado. En Studio, el informe aparece en el panel central, en la ficha Modelado.

Para ver el informe, seleccione Ver informe de modelado.

## **Solucionar problemas de directivas**

Los usuarios, las direcciones IP y otros objetos asignados pueden tener varias directivas que se aplican de forma simultánea. Esto puede ocasionar conflictos en los que puede que una directiva no se comporte como se espera. Cuando ejecuta el asistente de Modelado de Directivas de grupo Citrix o la herramienta Resultados de directivas de grupo, es posible que detecte que no se aplican directivas a las conexiones de usuario. Cuando esto ocurre, los usuarios que se conectan a sus aplicaciones y escritorios en condiciones que coinciden con los criterios de evaluación de directivas no se ven afectados por ninguna configuración de directiva. Esta situación ocurre cuando:

- Ninguna de las directivas tiene asignaciones que coinciden con los criterios de evaluación de la directiva.
- Las directivas que coinciden con la asignación no tienen ninguna configuración definida.
- Las directivas que coinciden con la asignación están inhabilitadas.

Si desea aplicar configuraciones de directiva a las conexiones que cumplen un criterio determinado, asegúrese de lo siguiente:

- Las directivas que desea aplicar a esas conexiones están habilitadas.
- Las directivas que desea aplicar tienen definidas las configuraciones adecuadas.

## Configuraciones predeterminadas de directivas

September 22, 2021

Las tablas siguientes enumeran configuraciones de directiva, sus valores predeterminados y las versiones de Virtual Delivery Agent (VDA) a las que se pueden aplicar.

### ICA

Nombre	Configuración predeterminada	VDA
Transporte adaptable	No; Usar si se prefiere	Desde VDA 7.13 hasta 7.15; desde VDA 7.16 hasta la actual
Redirección del portapapeles del cliente	Se permite	Todas las versiones de VDA
Inicios de escritorio	Prohibida	VDA para SO multisesión, desde la versión 7 hasta la actual
Número de puerto de escucha ICA	1494	Todas las versiones de VDA
Inicio de programas no publicados durante la conexión del cliente	Prohibida	VDA para SO multisesión, desde la versión 7 hasta la actual
Formatos permitidos de escritura en el portapapeles del cliente	No se han especificado formatos	Desde VDA 7.6 hasta la actual
Protocolo Rendezvous	Inhabilitada	Se aplica solo a las sesiones HDX establecidas a través de Citrix Cloud.

Nombre	Configuración predeterminada	VDA
Restringir escritura en el portapapeles del cliente	Prohibida	Desde VDA 7.6 hasta la actual
Restringir escritura en el portapapeles de la sesión	Prohibida	Desde VDA 7.6 hasta la actual
Formatos permitidos de escritura en el portapapeles de la sesión	No se han especificado formatos	Desde VDA 7.6 hasta la actual
Cambiar modo tableta	Habilitado	Las versiones de VDA desde 7.16 hasta la actual; para VDA 7.14 y LTSR 7.15, configure este parámetro mediante el Registro.
Lista de canales virtuales permitidos	Inhabilitada	VDA 1912

### ICA/Entrega de Adobe Flash/Redirección de Flash

Nombre	Configuración predeterminada	VDA
Impedimento para recurrir al vídeo Flash	No configurado	Desde VDA 7.6 FP3 hasta la actual
Error de impedimento para recurrir al vídeo Flash (*.swf)		Desde VDA 7.6 FP3 hasta la actual

### ICA/Sonido

Nombre	Configuración predeterminada	VDA
Sonido Plug and Play	Se permite	VDA para SO multisesión, desde la versión 7 hasta la actual
Calidad de sonido	Alta: sonido de alta definición	Todas las versiones de VDA
Redirección de sonido del cliente	Se permite	Todas las versiones de VDA
Redirección de micrófonos del cliente	Se permite	Todas las versiones de VDA

**ICA/Reconexión automática de clientes**

Nombre	Configuración predeterminada	VDA
Transporte de sonido en tiempo real sobre UDP	Se permite	Todas las versiones de VDA
Reconexión automática de clientes	Se permite	Todas las versiones de VDA
Autenticación para reconexión automática de clientes	No requerir autenticación	Todas las versiones de VDA
Registro de reconexión automática de clientes	No registrar sucesos de reconexión automática	Todas las versiones de VDA
Tiempo de espera de la Reconexión automática de clientes	120 segundos	Desde VDA 7.13 hasta la actual
Nivel de transparencia de la interfaz de usuario durante la reconexión	80 %	Desde VDA 7.13 hasta la actual

**ICA\Ancho de banda**

Nombre	Configuración predeterminada	VDA
Límite de ancho de banda de redirección de sonido	0 Kbps	Todas las versiones de VDA
Porcentaje límite de ancho de banda de redirección de sonido	0	Todas las versiones de VDA
Límite de ancho de banda de redirección de dispositivos USB del cliente	0 Kbps	VDA 5.5, 5.6 FP1, VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual
Porcentaje límite de ancho de banda de redirección de dispositivos USB del cliente	0	VDA 5.5, 5.6 FP1, VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual
Límite de ancho de banda de redirección del portapapeles	0 Kbps	Todas las versiones de VDA

Nombre	Configuración predeterminada	VDA
Porcentaje límite de ancho de banda de redirección del portapapeles	0	Todas las versiones de VDA
Límite de ancho de banda de redirección de puertos COM	0 Kbps	Todas las versiones de VDA; para las versiones desde VDA 7.0 hasta la versión 7.8, configure este parámetro mediante el Registro.
Porcentaje límite de ancho de banda de redirección de puertos COM	0	Todas las versiones de VDA; para las versiones desde VDA 7.0 hasta la versión 7.8, configure este parámetro mediante el Registro.
Límite de ancho de banda de redirección de archivos	0 Kbps	Todas las versiones de VDA
Porcentaje límite de ancho de banda de redirección de archivos	0	Todas las versiones de VDA
Límite de ancho de banda de aceleración multimedia HDX MediaStream	0 Kbps	VDA 5.5, 5.6 FP1, VDA para SO multisesión 7 y VDA para SO de sesión única 7 hasta la versión actual de VDA para SO multisesión y VDA para SO de sesión única
Porcentaje límite de ancho de banda de aceleración multimedia HDX MediaStream	0	VDA 5.5, 5.6 FP1, VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual
Límite de ancho de banda de redirección de puertos LPT	0 Kbps	Todas las versiones de VDA; para las versiones desde VDA 7.0 hasta la versión 7.8, configure este parámetro mediante el Registro.

Nombre	Configuración predeterminada	VDA
Porcentaje límite de ancho de banda de redirección de puertos LPT	0	Todas las versiones de VDA; para las versiones desde VDA 7.0 hasta la versión 7.8, configure este parámetro mediante el Registro.
Límite de ancho de banda global de la sesión	0 Kbps	Todas las versiones de VDA
Límite de ancho de banda de redirección de impresoras	0 Kbps	Todas las versiones de VDA
Porcentaje límite de ancho de banda de redirección de impresoras	0	Todas las versiones de VDA
Límite de ancho de banda de redirección de dispositivos TWAIN	0 Kbps	VDA 5.5, 5.6 FP1, VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual
Porcentaje límite de ancho de banda de redirección de dispositivos TWAIN	0	VDA 5.5, 5.6 FP1, VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual

### ICA/Redirección de contenido bidireccional

Nombre	Configuración predeterminada	VDA
Permitir redirección de contenido bidireccional	Prohibida	Desde VDA 7.13 hasta la actual
Direcciones URL permitidas para redirigir al cliente	vacío	Desde VDA 7.13 hasta la actual
Direcciones URL permitidas para redirigir al VDA	vacío	Desde VDA 7.13 hasta la actual
Redirección de cliente a host (VDA) y redirección de contenido de cliente a cliente		Utilice la plantilla administrativa de GPO de la aplicación Citrix Workspace.

**ICA/Redirección de contenido de explorador web**

Nombre	Configuración predeterminada	VDA
Redirección de contenido de explorador web	Se permite	Desde VDA 7.16 hasta la actual
Configuración de lista ACL para redirección de contenido del explorador web	<a href="https://www.youtube.com/">https://www.youtube.com/</a> *	Desde VDA 7.16 hasta la actual
Configuración de proxy para redirección de contenido del explorador web	vacío	Desde VDA 7.16 hasta la actual

**ICA/Sensores del cliente**

Nombre	Configuración predeterminada	VDA
Permitir que las aplicaciones usen la ubicación física del dispositivo cliente	Prohibida	VDA 5.6 FP1, VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual

**ICA/Interfaz de usuario de escritorio**

Nombre	Configuración predeterminada	VDA
Redirección de composición del escritorio	Inhabilitado (desde 7.6 FP3 hasta la actual); Habilitado (desde 5.6 hasta 7.6 FP2)	VDA 5.6, VDA para SO de sesión única, desde la versión 7 hasta 7.15
Calidad de gráficos de composición del escritorio	Medio	VDA 5.6, VDA para SO de sesión única, desde la versión 7 hasta 7.15
Tapiz del escritorio	Se permite	Todas las versiones de VDA
Animación de menús	Se permite	Todas las versiones de VDA
Ver contenido de las ventanas al arrastrar	Se permite	Todas las versiones de VDA

**ICA/Supervisión de usuario final**

Nombre	Configuración predeterminada	VDA
Cálculo del tiempo de retorno ICA	Habilitado	Todas las versiones de VDA
Intervalo de cálculo del tiempo de retorno ICA	15 segundos	Todas las versiones de VDA
Cálculo del tiempo de retorno ICA para conexiones inactivas	Inhabilitada	Todas las versiones de VDA

**ICA/Enhanced Desktop Experience**

Nombre	Configuración predeterminada	VDA
Enhanced Desktop Experience	Se permite	VDA para SO multisesión, desde la versión 7 hasta la actual

**ICA/Redirección de archivos**

Nombre	Configuración predeterminada	VDA
Conectar automáticamente las unidades del cliente	Se permite	Todas las versiones de VDA
Redirección de unidades del cliente	Se permite	Todas las versiones de VDA
Unidades fijas del cliente	Se permite	Todas las versiones de VDA
Unidades de disco flexible del cliente	Se permite	Todas las versiones de VDA
Unidades de red del cliente	Se permite	Todas las versiones de VDA
Unidades ópticas del cliente	Se permite	Todas las versiones de VDA
Unidades extraíbles del cliente	Se permite	Todas las versiones de VDA
Redirección del host al cliente	Inhabilitada	VDA para SO multisesión, desde la versión 7 hasta la actual
Conservar las letras de unidad del cliente	Inhabilitada	VDA 5, 5.5, 5.6 FP1, VDA para SO de sesión única, desde la versión 7 hasta la actual

Nombre	Configuración predeterminada	VDA
Acceso de lectura solamente a unidades del cliente	Inhabilitada	VDA 5.5, 5.6 FP1, VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual
Redirección de carpetas especiales	Se permite	Solo implementaciones de Interfaz Web; VDA para SO multisesión, desde la versión 7 hasta la versión actual
Usar escrituras asíncronas	Inhabilitada	Todas las versiones de VDA

## ICA/Gráficos

Nombre	Configuración predeterminada	VDA
Permitir compresión sin pérdida visual	Inhabilitada	Desde VDA 7.6 hasta la actual
Límite de memoria de presentación	65536 KB	VDA 5, 5.5, 5.6 FP1, VDA para SO de sesión única, desde la versión 7 hasta la actual
Preferencia de degradación de presentación	Degradar primero la profundidad de color	Todas las versiones de VDA
Vista previa de ventanas dinámicas	Habilitado	VDA 5.5, 5.6 FP1, VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual
Caché de imágenes	Habilitado	VDA 5.5, 5.6 FP1, VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual
Modo de gráficos antiguo	Inhabilitada	VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual

Nombre	Configuración predeterminada	VDA
Profundidad de color máxima permitida	32 bits por píxel	Todas las versiones de VDA
Notificar al usuario cuando se degrada la presentación	Inhabilitada	VDA para SO multisesión, desde la versión 7 hasta la actual
Optimizar para cargas de trabajo de gráficos 3D	Inhabilitada	Desde VDA 7.17 hasta la actual
Cola y descarte	Habilitado	Todas las versiones de VDA
Usar códec de vídeo para compresión	Usar códec de vídeo si se prefiere	Desde VDA 7.6 FP3 hasta la actual
Usar codificación por hardware para códec de vídeo	Habilitado	Desde VDA 7.11 hasta la actual

### ICA/Gráficos/Almacenamiento en caché

Nombre	Configuración predeterminada	VDA
Umbral de caché persistente	3 000 000 Kbps	VDA para SO multisesión, desde la versión 7 hasta la actual

### ICA/Gráficos/Framehawk

Nombre	Configuración predeterminada	VDA
Canal de presentación Framehawk	Inhabilitada	Desde VDA 7.6 FP2 hasta la actual
Intervalo de puertos del canal de presentación Framehawk	3224, 3324	Desde VDA 7.6 FP2 hasta la actual

### ICA/Keep Alive

Nombre	Configuración predeterminada	VDA
Tiempo de espera de ICA Keep Alive	60 segundos	Todas las versiones de VDA

Nombre	Configuración predeterminada	VDA
ICA Keep Alive	No enviar mensajes de ICA Keep Alive	Todas las versiones de VDA

### ICA/Acceso a aplicaciones locales

Nombre	Configuración predeterminada	VDA
Permitir acceso a aplicaciones locales	Prohibida	VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual
Lista de direcciones URL de redirección bloqueadas	No se especifica ningún sitio	VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual
Lista de direcciones URL de redirección permitidas	No se especifica ningún sitio	VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual

### ICA/Experiencia móvil

Nombre	Configuración predeterminada	VDA
Presentación automática del teclado	Prohibida	VDA 5.6 FP1, VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual

Nombre	Configuración predeterminada	VDA
Iniciar escritorio con optimización táctil	Se permite	VDA 5.6 FP1, VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual. Esta configuración está inhabilitada y no está disponible para máquinas Windows 10 y Windows Server 2016.
Control remoto de cuadros combinados	Prohibida	VDA 5.6 FP1, VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual

## ICA/Multimedia

Nombre	Configuración predeterminada	VDA
Redirección de vídeo HTML5	Prohibida	Desde VDA 7.12 hasta la actual
Límite de calidad de vídeo	No configurado	VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual
Redirección de Microsoft Teams	Se permite	VDA para SO multisesión, desde la versión 1906 hasta la actual, VDA para SO de sesión única, desde la versión 1906 hasta la actual
Conferencia multimedia	Se permite	Todas las versiones de VDA
Optimización de la redirección de medios de Windows Media sobre WAN	Se permite	VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual

Nombre	Configuración predeterminada	VDA
Usar GPU para optimizar redirección de medios de Windows Media sobre WAN	Prohibida	VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual
Prevención de reserva de Windows Media	No configurado	Desde VDA 7.6 FP3 hasta la actual
Obtención de contenido de Windows Media en el lado del cliente	Se permite	VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual
Redirección de Windows Media	Se permite	Todas las versiones de VDA
Tamaño del búfer para la redirección de Windows Media	5 segundos	Desde VDA 5, 5.5, 5.6 FP1 hasta la actual
Uso del tamaño de búfer para redirección de Windows Media	Inhabilitada	Desde VDA 5, 5.5, 5.6 FP1 hasta la actual

### ICA/Conexiones de multisequencia

Nombre	Configuración predeterminada	VDA
Sonido sobre UDP	Se permite	VDA para SO multisesión, desde la versión 7 hasta la actual
Intervalo de puertos UDP de sonido	16500, 16509	VDA 5.5, 5.6 FP1, VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual
Directiva Puertos múltiples	El puerto principal (2598) tiene prioridad alta	VDA 5.5, 5.6 FP1, VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual
Configuración de equipo para multisequencia	Inhabilitada	VDA 5.5, 5.6 FP1, VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual

Nombre	Configuración predeterminada	VDA
Configuración de usuario para multisequencia	Inhabilitada	VDA 5.5, 5.6 FP1, VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual
Configuración de asignación del flujo de canales virtuales multisequencia	Consulte <a href="#">Parámetros de asignación de canales virtuales multisequencia</a> para conocer las asignaciones de secuencias predeterminadas	VDA 1912

### ICA/Redirección de puertos

Nombre	Configuración predeterminada	VDA
Conectar automáticamente puertos COM del cliente	Inhabilitada	Todas las versiones de VDA; para las versiones desde VDA 7.0 hasta la versión 7.8, configure este parámetro mediante el Registro.
Conectar automáticamente puertos LPT del cliente	Inhabilitada	Todas las versiones de VDA; para las versiones desde VDA 7.0 hasta la versión 7.8, configure este parámetro mediante el Registro.
Redirección de puertos COM del cliente	Prohibida	Todas las versiones de VDA; para las versiones desde VDA 7.0 hasta la versión 7.8, configure este parámetro mediante el Registro.
Redirección de puertos LPT del cliente	Prohibida	Todas las versiones de VDA; para las versiones desde VDA 7.0 hasta la versión 7.8, configure este parámetro mediante el Registro.

**ICA/Impresión**

Nombre	Configuración predeterminada	VDA
Redirección de impresoras del cliente	Se permite	Todas las versiones de VDA
Impresora predeterminada	Definir la impresora principal del cliente como la impresora predeterminada	Todas las versiones de VDA
Asignaciones de impresora	La impresora actual del usuario se usa como predeterminada durante la sesión	Todas las versiones de VDA
Preferencia de registro de sucesos de creación automática de impresoras	Registrar errores y advertencias	Todas las versiones de VDA
Impresoras de la sesión	No se especifica ninguna impresora	Todas las versiones de VDA
Esperar a que se creen las impresoras (escritorio)	Inhabilitada	Todas las versiones de VDA

**ICA/Impresión/Impresoras del cliente**

Nombre	Configuración predeterminada	VDA
Crear automáticamente las impresoras del cliente	Crear automáticamente todas las impresoras cliente	Todas las versiones de VDA
Crear automáticamente una impresora universal genérica	Inhabilitada	Todas las versiones de VDA
Nombres de impresora del cliente	Nombres de impresora estándar	VDA 5.6
Conexiones directas con servidores de impresión	Habilitado	Todas las versiones de VDA
Asignación y compatibilidad de controladores de impresora	No se especifica ninguna regla	Todas las versiones de VDA
Retención de las propiedades de impresora	Mantener en el perfil del usuario si no se guardan en el cliente	Todas las versiones de VDA
Impresoras del cliente retenidas o restauradas	Se permite	VDA 5, 5.5, 5.6 FP1

**ICA/Impresión/Controladores**

Nombre	Configuración predeterminada	VDA
Instalación automática de controladores de impresora	Habilitado	Todas las versiones de VDA
Preferencia de controlador universal	EMF; XPS; PCL5c; PCL4; PS	Todas las versiones de VDA
Uso de controladores de impresión universal	Usar impresión universal solo si el controlador solicitado no está disponible	Todas las versiones de VDA

**ICA/Impresión/Universal Print Server**

Nombre	Configuración predeterminada	VDA
Habilitar Universal Print Server	Inhabilitada	Todas las versiones de VDA
Puerto del flujo de datos de impresión de Universal Print Server (CGP)	7229	Todas las versiones de VDA
Límite de ancho de banda del flujo de entrada de impresión de Universal Print Server (kbps)	0	Todas las versiones de VDA
Puerto del servicio web de Universal Print Server (HTTP/SOAP)	8080	Todas las versiones de VDA
Universal Print Servers para equilibrio de carga		Versiones de VDA 7.9 hasta la actual
Umbral de Universal Print Server fuera de servicio	180 (segundos)	Versiones de VDA 7.9 hasta la actual

**ICA/Impresión/Impresión universal**

Nombre	Configuración predeterminada	VDA
Modo de procesamiento EMF de la impresión universal	Enviar directamente a la cola de impresión	Todas las versiones de VDA

Nombre	Configuración predeterminada	VDA
Límite de compresión de imagen para la impresión universal	Mejor calidad (compresión sin pérdida)	Todas las versiones de VDA
Valores predeterminados de optimización de impresión universal	Compresión de imagen: Calidad de imagen deseada = Calidad estándar, Habilitar la compresión intensa = Falso; Almacenamiento en caché de imágenes y fuentes: Permitir el almacenamiento en caché de imágenes incrustadas = Verdadero; Permitir a los no administradores modificar estos parámetros = Falso;	Todas las versiones de VDA
Preferencia de vista previa en impresión universal	No usar vista previa en las impresoras de creación automática o universales genéricas	Todas las versiones de VDA
Límite de calidad de la impresión universal	Sin límite	Todas las versiones de VDA

## ICA/Seguridad

Nombre	Configuración predeterminada	VDA
Nivel de cifrado mínimo de SecureICA	Básica	VDA para SO multisesión, desde la versión 7 hasta la actual

## ICA/Límites de servidor

Nombre	Configuración predeterminada	VDA
Intervalo de temporizador de servidor inactivo	0 milésimas de segundo	VDA para SO multisesión, desde la versión 7 hasta la actual

**ICA/Límites de sesión**

Nombre	Configuración predeterminada	VDA
Temporizador de sesión desconectada	Inhabilitada	VDA 5, 5.5, 5.6 FP1, VDA para SO de sesión única, desde la versión 7 hasta la actual
Intervalo de temporizador de sesiones desconectadas	1440 minutos	VDA 5, 5.5, 5.6 FP1, VDA para SO de sesión única, desde la versión 7 hasta la actual
Temporizador de conexión de sesión	Inhabilitada	VDA 5, 5.5, 5.6 FP1, VDA para SO de sesión única, desde la versión 7 hasta la actual
Intervalo de temporizador de conexión de sesiones	1440 minutos	VDA 5, 5.5, 5.6 FP1, VDA para SO de sesión única, desde la versión 7 hasta la actual
Temporizador de sesión inactiva	Habilitado	VDA 5, 5.5, 5.6 FP1, VDA para SO de sesión única, desde la versión 7 hasta la actual
Intervalo de temporizador de sesiones inactivas	1440 minutos	VDA 5, 5.5, 5.6 FP1, VDA para SO de sesión única, desde la versión 7 hasta la actual

**ICA/Fiabilidad de la sesión**

Nombre	Configuración predeterminada	VDA
Conexiones de fiabilidad de la sesión	Se permite	Todas las versiones de VDA
Número de puerto para fiabilidad de la sesión	2598	Todas las versiones de VDA
Tiempo de espera de fiabilidad de la sesión	180 segundos	Todas las versiones de VDA

**ICA/Control de zona horaria**

Nombre	Configuración predeterminada	VDA
Calcular hora local para clientes antiguos	Habilitado	VDA para SO multisesión, desde la versión 7 hasta la actual
Restaurar la zona horaria del SO de sesión única al desconectar o al cerrar la sesión	Habilitado	Versión actual de VDA
Usar la hora local del cliente	Usar zona horaria del servidor	Todas las versiones de VDA

### ICA/Dispositivos TWAIN

Nombre	Configuración predeterminada	VDA
Redirección de dispositivos TWAIN del cliente	Se permite	VDA 5.5, 5.6 FP1, VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual
Nivel de compresión TWAIN	Medio	VDA 5.5, 5.6 FP1, VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual

### ICA/Dispositivos USB

Nombre	Configuración predeterminada	VDA
Reglas de optimización de dispositivos USB del cliente	Habilitadas (desde VDA 7.6 FP3 hasta la actual). Inhabilitadas (desde VDA 7.11 hasta la actual). De manera predeterminada, no se especifican reglas	Desde VDA 7.6 FP3 hasta la actual
Redirección de dispositivos USB del cliente	Prohibida	Todas las versiones de VDA

Nombre	Configuración predeterminada	VDA
Reglas de redirección de dispositivos USB del cliente	No se especifica ninguna regla	Todas las versiones de VDA
Redirección de dispositivos USB Plug and Play del cliente	Se permite	VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual

### ICA/Presentación visual

Nombre	Configuración predeterminada	VDA
Profundidad de color preferida para gráficos simples	24 bits por píxel	Desde VDA 7.6 FP3 hasta la actual
Velocidad de fotogramas de destino	30 fps	Todas las versiones de VDA
Calidad visual	Medio	VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual

### ICA/Presentación visual/Imágenes en movimiento

Nombre	Configuración predeterminada	VDA
Calidad de imagen mínima	Normal	VDA 5.5, 5.6 FP1, VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual
Compresión de imágenes en movimiento	Habilitado	VDA 5.5, 5.6 FP1, VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual

Nombre	Configuración predeterminada	VDA
Nivel de compresión progresiva	Ninguno	VDA 5.5, 5.6 FP1, VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual
Valor de umbral de compresión progresiva	2 147 483 647 Kbps	VDA 5.5, 5.6 FP1, VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual
Velocidad de fotogramas mínima de destino	10 fps	VDA 5.5, 5.6 FP1, VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual

### ICA/Presentación visual/Imágenes fijas

Nombre	Configuración predeterminada	VDA
Compresión de color adicional	Inhabilitada	Todas las versiones de VDA
Umbral de compresión de color adicional	8192 Kbps	Todas las versiones de VDA
Compresión intensa	Inhabilitada	Todas las versiones de VDA
Nivel de compresión con pérdida	Medio	Todas las versiones de VDA
Valor de umbral de compresión con pérdida	2 147 483 647 Kbps	Todas las versiones de VDA

### ICA/WebSockets

Nombre	Configuración predeterminada	VDA
Conexiones con WebSockets	Prohibida	VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual
Número de puerto de WebSockets	8008	VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual
Lista de servidores de origen de WebSockets de confianza	Se utiliza el carácter comodín * para confiar en todas las URL de Receiver para Web.	VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual

### Administración de carga

Nombre	Configuración predeterminada	VDA
Tolerancia de inicios de sesión simultáneos	2	VDA para SO multisesión, desde la versión 7 hasta la actual
Uso de CPU	Inhabilitada	VDA para SO multisesión, desde la versión 7 hasta la actual
Prioridad de procesos excluidos para el uso de CPU	Por debajo de lo normal o baja	VDA para SO multisesión, desde la versión 7 hasta la actual
Uso del disco	Inhabilitada	VDA para SO multisesión, desde la versión 7 hasta la actual
Número máximo de sesiones	250	VDA para SO multisesión, desde la versión 7 hasta la actual
Uso de memoria	Inhabilitada	VDA para SO multisesión, desde la versión 7 hasta la actual
Carga base de uso de memoria	Carga cero: 768 MB	VDA para SO multisesión, desde la versión 7 hasta la actual

### Profile Management/Parámetros avanzados

Nombre	Configuración predeterminada	VDA
Inhabilitar configuración automática	Inhabilitada	Todas las versiones de VDA
Cerrar la sesión del usuario si hay algún problema	Inhabilitada	Todas las versiones de VDA
Reintentos de acceso a archivos bloqueados	5	Todas las versiones de VDA
Procesar cookies de Internet al cerrar la sesión	Inhabilitada	Todas las versiones de VDA

### Profile Management/Parámetros básicos

Nombre	Configuración predeterminada	VDA
Reescritura activa	Inhabilitada	Todas las versiones de VDA
Habilitar Profile Management	Inhabilitada	Todas las versiones de VDA
Grupos excluidos	Inhabilitado. Se procesan los miembros de todos los grupos de usuarios.	Todas las versiones de VDA
Compatibilidad con perfiles sin conexión	Inhabilitada	Todas las versiones de VDA
Ruta al almacén de usuarios	Windows	Todas las versiones de VDA
Procesar inicios de sesión de administradores locales	Inhabilitada	Todas las versiones de VDA
Grupos procesados	Inhabilitado. Se procesan los miembros de todos los grupos de usuarios.	Todas las versiones de VDA

### Profile Management/Configuración multiplataforma

Nombre	Configuración predeterminada	VDA
Grupos de usuarios de configuración multiplataforma	Inhabilitado. Se procesan todos los grupos de usuarios especificados en Grupos procesados.	Todas las versiones de VDA

Nombre	Configuración predeterminada	VDA
Habilitar configuración multiplataforma	Inhabilitada	Todas las versiones de VDA
Ruta de definiciones multiplataforma	Inhabilitado. No se especifica ninguna ruta.	Todas las versiones de VDA
Ruta del almacén de configuración multiplataforma	Inhabilitado. Se usa Windows\PM_CM.	Todas las versiones de VDA
Origen para crear configuración multiplataforma	Inhabilitada	Todas las versiones de VDA

### Profile Management/Sistema de archivos/Exclusiones

Nombre	Configuración predeterminada	VDA
Lista de exclusión de directorios	Inhabilitado. Se sincronizan todas las carpetas del perfil de usuario.	Todas las versiones de VDA
Lista de exclusión de archivos	Inhabilitado. Se sincronizan todos los archivos del perfil de usuario.	Todas las versiones de VDA

### Profile Management/Sistema de archivos/Sincronización

Nombre	Configuración predeterminada	VDA
Directorios que sincronizar	Inhabilitado. Solo se sincronizan las carpetas no excluidas.	Todas las versiones de VDA
Archivos que sincronizar	Inhabilitado. Solo se sincronizan los archivos no excluidos.	Todas las versiones de VDA
Carpetas para reflejar	Inhabilitado. No se refleja ninguna carpeta.	Todas las versiones de VDA

### Profile Management/Redirección de carpetas

Nombre	Configuración predeterminada	VDA
Conceder acceso a administradores	Inhabilitada	Todas las versiones de VDA
Incluir nombre de dominio	Inhabilitada	Todas las versiones de VDA

### **Profile Management/Redirección de carpetas/AppData(Roaming)**

Nombre	Configuración predeterminada	VDA
Ruta de AppData(Roaming)	Inhabilitado. No se especifica ninguna ubicación.	Todas las versiones de VDA
Parámetros de redirección para AppData(Roaming)	El contenido se redirige a la ruta UNC especificada en la configuración de la directiva Ruta de AppData(Roaming)	Todas las versiones de VDA

### **Profile Management/Redirección de carpetas/Contactos**

Nombre	Configuración predeterminada	VDA
Ruta de Contactos	Inhabilitado. No se especifica ninguna ubicación.	Todas las versiones de VDA
Parámetros de redirección para Contactos	El contenido se redirige a la ruta UNC especificada en la configuración de la directiva Ruta de Contactos	Todas las versiones de VDA

### **Profile Management/Redirección de carpetas/Escritorio**

Nombre	Configuración predeterminada	VDA
Ruta de Escritorio	Inhabilitado. No se especifica ninguna ubicación.	Todas las versiones de VDA

Nombre	Configuración predeterminada	VDA
Parámetros de redirección para Escritorio	El contenido se redirige a la ruta UNC especificada en la configuración de la directiva Ruta de Escritorio	Todas las versiones de VDA

### Profile Management/Redirección de carpetas/Documentos

Nombre	Configuración predeterminada	VDA
Ruta de Documentos	Inhabilitado. No se especifica ninguna ubicación.	Todas las versiones de VDA
Parámetros de redirección para Documentos	El contenido se redirige a la ruta UNC especificada en la configuración de la directiva Ruta de Documentos	Todas las versiones de VDA

### Profile Management/Redirección de carpetas/Descargas

Nombre	Configuración predeterminada	VDA
Ruta de Descargas	Inhabilitado. No se especifica ninguna ubicación.	Todas las versiones de VDA
Parámetros de redirección para Descargas	El contenido se redirige a la ruta UNC especificada en la configuración de la directiva Ruta de Descargas	Todas las versiones de VDA

### Profile Management/Redirección de carpetas/Favoritos

Nombre	Configuración predeterminada	VDA
Ruta de Favoritos	Inhabilitado. No se especifica ninguna ubicación.	Todas las versiones de VDA

Nombre	Configuración predeterminada	VDA
Parámetros de redirección para Favoritos	El contenido se redirige a la ruta UNC especificada en la configuración de la directiva Ruta de Favoritos	Todas las versiones de VDA

### Profile Management/Redirección de carpetas/Vínculos

Nombre	Configuración predeterminada	VDA
Ruta de Vínculos	Inhabilitado. No se especifica ninguna ubicación.	Todas las versiones de VDA
Parámetros de redirección para Vínculos	El contenido se redirige a la ruta UNC especificada en la configuración de la directiva Ruta de Enlaces	Todas las versiones de VDA

### Profile Management/Redirección de carpetas/Música

Nombre	Configuración predeterminada	VDA
Ruta de Música	Inhabilitado. No se especifica ninguna ubicación.	Todas las versiones de VDA
Configuraciones de redirección para Música	El contenido se redirige a la ruta UNC especificada en la configuración de la directiva Ruta de Música	Todas las versiones de VDA

### Profile Management/Redirección de carpetas/Imágenes

Nombre	Configuración predeterminada	VDA
Ruta de Imágenes	Inhabilitado. No se especifica ninguna ubicación.	Todas las versiones de VDA

Nombre	Configuración predeterminada	VDA
Parámetros de redirección para Imágenes	El contenido se redirige a la ruta UNC especificada en la configuración de la directiva Ruta de Imágenes	Todas las versiones de VDA

### Profile Management/Redirección de carpetas/Juegos guardados

Nombre	Configuración predeterminada	VDA
Ruta de Juegos guardados	Inhabilitado. No se especifica ninguna ubicación.	Todas las versiones de VDA
Parámetros de redirección para Juegos guardados	El contenido se redirige a la ruta UNC especificada en la configuración de la directiva Ruta de Juegos guardados	Todas las versiones de VDA

### Profile Management/Redirección de carpetas/Búsquedas

Nombre	Configuración predeterminada	VDA
Ruta de Búsquedas	Inhabilitado. No se especifica ninguna ubicación.	Todas las versiones de VDA
Parámetros de redirección para Búsquedas	El contenido se redirige a la ruta UNC especificada en la configuración de la directiva Ruta de Búsquedas	Todas las versiones de VDA

### Profile Management/Redirección de carpetas/Menú Inicio

Nombre	Configuración predeterminada	VDA
Ruta de Menú Inicio	Inhabilitado. No se especifica ninguna ubicación.	Todas las versiones de VDA

Nombre	Configuración predeterminada	VDA
Parámetros de redirección para Menú Inicio	El contenido se redirige a la ruta UNC especificada en la configuración de la directiva Ruta de Menú Inicio	Todas las versiones de VDA

### Profile Management/Redirección de carpetas/Vídeos

Nombre	Configuración predeterminada	VDA
Ruta de Vídeos	Inhabilitado. No se especifica ninguna ubicación.	Todas las versiones de VDA
Parámetros de redirección para Vídeos	El contenido se redirige a la ruta UNC especificada en la configuración de la directiva Ruta de Vídeos	Todas las versiones de VDA

### Profile Management/Parámetros de registro

Nombre	Configuración predeterminada	VDA
Acciones de Active Directory	Inhabilitada	Todas las versiones de VDA
Información común	Inhabilitada	Todas las versiones de VDA
Advertencias comunes	Inhabilitada	Todas las versiones de VDA
Habilitar registro	Inhabilitada	Todas las versiones de VDA
Acciones del sistema de archivos	Inhabilitada	Todas las versiones de VDA
Notificaciones del sistema de archivos	Inhabilitada	Todas las versiones de VDA
Cierre de sesión	Inhabilitada	Todas las versiones de VDA
Inicio de sesión	Inhabilitada	Todas las versiones de VDA
Tamaño máximo del archivo de registro	1 048 576	Todas las versiones de VDA

Nombre	Configuración predeterminada	VDA
Ruta al archivo de registro	Inhabilitado. Los archivos de registro se guardan en la ubicación predeterminada: %SystemRoot%\System32\Logfiles\UserProfileManager.	Todas las versiones de VDA
Información de usuario personalizada	Inhabilitada	Todas las versiones de VDA
Valores de directivas al iniciar y cerrar la sesión	Inhabilitada	Todas las versiones de VDA
Acciones del Registro del sistema	Inhabilitada	Todas las versiones de VDA
Diferencias en el Registro del sistema al cerrar la sesión	Inhabilitada	Todas las versiones de VDA

### Management/Profile Management/Gestión de perfiles

Nombre	Configuración predeterminada	VDA
Demora antes de eliminar perfiles en caché	0	Todas las versiones de VDA
Eliminar perfiles guardados en caché local al cerrar la sesión	Inhabilitada	Todas las versiones de VDA
Gestión de conflictos de perfiles locales	Usar el perfil local	Todas las versiones de VDA
Migración de perfiles existentes	Locales y móviles	Todas las versiones de VDA
Ruta al perfil de plantilla	Inhabilitado. Los perfiles de usuario nuevos se crean a partir del perfil de usuario predeterminado en el equipo en el que el usuario inicia una sesión por primera vez.	Todas las versiones de VDA
El perfil de plantilla anula el perfil local	Inhabilitada	Todas las versiones de VDA
El perfil de plantilla sobrescribe el perfil móvil	Inhabilitada	Todas las versiones de VDA

Nombre	Configuración predeterminada	VDA
Perfil de plantilla utilizado como perfil de Citrix obligatorio para todos los inicios de sesión	Inhabilitada	Todas las versiones de VDA

### Profile Management/Registro del sistema

Nombre	Configuración predeterminada	VDA
Lista de exclusión	Inhabilitado. Todas las claves del Registro en el subárbol HKCU se procesan cuando un usuario cierra la sesión.	Todas las versiones de VDA
Lista de inclusión	Inhabilitado. Todas las claves del Registro en el subárbol HKCU se procesan cuando un usuario cierra la sesión.	Todas las versiones de VDA

### Profile Management/Perfiles de usuario de streaming

Nombre	Configuración predeterminada	VDA
Guardar siempre en caché	Inhabilitada	Todas las versiones de VDA
Tamaño de caché	0 MB	Todas las versiones de VDA
Streaming de perfiles	Inhabilitada	Todas las versiones de VDA
Grupos de perfiles de usuarios de streaming	Inhabilitado. Todos los perfiles de usuario dentro de una unidad organizativa se procesan con normalidad.	Todas las versiones de VDA
Tiempo de espera (en días) para bloqueo del área de archivos pendientes	1 día	Todas las versiones de VDA

### Receiver

Nombre	Configuración predeterminada	VDA
Lista de cuentas de StoreFront	No se han especificado almacenes	VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual

### Capa de personalización de usuarios

Nombre	Configuración predeterminada	VDA
Ruta del repositorio de capas de usuarios	Inhabilitado. No se especifica ninguna ruta.	VDA 19.12 y versiones posteriores
Tamaño de las capas de usuarios en GB	0 GB (el valor predeterminado es el tamaño mínimo de capa de 10 GB)	VDA 19.12 o versiones posteriores

### Virtual Delivery Agent

Nombre	Configuración predeterminada	VDA
Máscara de red IPv6 para el registro de Controller	No se especifica ninguna máscara de red.	VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual
Puerto de registro de Controller	80	Todas las versiones de VDA
SID de Controller	No se especifica ningún SID	Todas las versiones de VDA
Controllers	No se especifica ningún Controller	Todas las versiones de VDA
Habilitar actualización automática de Controller	Habilitado	VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual
Usar solo el registro de Controller con IPv6	Inhabilitada	VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual

Nombre	Configuración predeterminada	VDA
GUID del sitio	No se especifica ningún GUID	Todas las versiones de VDA

### Virtual Delivery Agent/HDX 3D Pro

Nombre	Configuración predeterminada	VDA
Habilitar sin pérdida	Habilitado	VDA 5.5, 5.6 Feature Pack 1
Parámetros de calidad de HDX 3D Pro		VDA 5.5, 5.6 Feature Pack 1

### Virtual Delivery Agent/Monitoring

Nombre	Configuración predeterminada	VDA
Habilitar supervisión de procesos	Inhabilitada	Desde VDA 7.11 hasta la actual
Habilitar supervisión de recursos	Habilitado	Desde VDA 7.11 hasta la actual

### IP virtual

Nombre	Configuración predeterminada	VDA
Funcionalidad de bucle invertido de IP virtual	Inhabilitada	Desde VDA 7.6 hasta la actual
Lista de programas para bucle invertido de IP virtual	Ninguno	Desde VDA 7.6 hasta la actual

## Referencia para configuraciones de directivas

September 22, 2021

Las directivas contienen configuraciones que se aplican cuando éstas se implementan. Las descripciones de esta sección también indican si se requieren configuraciones adicionales para habilitar una función y si hay configuraciones similares.

## Referencia rápida

Las siguientes tablas muestran las configuraciones que se pueden definir en una directiva. Busque la tarea que quiere realizar en la columna de la izquierda y, a continuación, localice la configuración correspondiente en la columna de la derecha.

Dispone de una lista completa de todas las configuraciones de directiva en formato CHM (HTML compilado) y formato CSV. Estos archivos están disponibles en la carpeta `\program files\citrix\grouppolicy`, presente en el servidor donde está instalado el broker (Delivery Controller). También puede descargar la versión más reciente de las configuraciones de directivas haciendo clic [aquí](#).

## Sonido

---

Para esta tarea	Use esta configuración de directiva
Controlar si se permite el uso de varios dispositivos de sonido	Sonido Plug and Play
Controlar si se permite la entrada de sonido desde los micrófonos del dispositivo del usuario	Redirección de micrófonos del cliente
Controlar la calidad de sonido en el dispositivo de usuario	Calidad de sonido
Controlar la asignación de sonido a los altavoces del dispositivo de usuario	Redirección de sonido del cliente

---

## Ancho de banda para dispositivos de usuario

---

Para limitar el ancho de banda utilizado para	Use esta configuración de directiva
Asignación de sonido del cliente	Límite de ancho de banda de redirección de sonido o Porcentaje límite de ancho de banda de redirección de sonido
Cortar y pegar mediante el portapapeles local	Límite de ancho de banda de redirección del portapapeles o Porcentaje límite de ancho de banda de redirección del portapapeles

---

Para limitar el ancho de banda utilizado para	Use esta configuración de directiva
Acceso a las unidades del cliente locales durante una sesión	Límite de ancho de banda de redirección de archivos o Porcentaje límite de ancho de banda de redirección de archivos
Aceleración multimedia HDX MediaStream	Límite de ancho de banda de aceleración multimedia HDX MediaStream o Porcentaje límite de ancho de banda de aceleración multimedia HDX MediaStream
Sesión del cliente	Límite de ancho de banda global de la sesión
Impresión	Límite de ancho de banda de redirección de impresoras o Porcentaje límite de ancho de banda de redirección de impresoras
Dispositivos TWAIN (como cámaras o escáneres)	Límite de ancho de banda de redirección de dispositivos TWAIN o Porcentaje límite de ancho de banda de redirección de dispositivos TWAIN
Dispositivos USB	Límite de ancho de banda de redirección de dispositivos USB del cliente o Porcentaje límite de ancho de banda de redirección de dispositivos USB del cliente

## Redirección de dispositivos del cliente y dispositivos del usuario

Para esta tarea	Use esta configuración de directiva
Controlar si se conectan las unidades del dispositivo del usuario cuando los usuarios inician sesión en el servidor	Conectar automáticamente las unidades del cliente
Controlar la transferencia de datos mediante cortar y pegar entre el servidor y el portapapeles local	Redirección del portapapeles del cliente
Controlar la forma en que se deben asignar las unidades del dispositivo del usuario	Redirección de unidades del cliente
Controlar si los discos duros local de los usuarios están disponibles en una sesión	Unidades fijas del cliente y Redirección de unidades del cliente
Controlar si las unidades de disco flexible locales de los usuarios están disponibles en una sesión	Unidades de disco flexible del cliente y Redirección de unidades del cliente

Para esta tarea	Use esta configuración de directiva
Controlar si las unidades de red de los usuarios están disponibles en una sesión	Unidades de red del cliente y Redirección de unidades del cliente
Controlar si las unidades de CD, DVD o Blu-ray locales de los usuarios están disponibles en una sesión	Unidades ópticas del cliente y Redirección de unidades del cliente
Controlar si las unidades extraíbles locales de los usuarios están disponibles en una sesión	Unidades extraíbles del cliente y Redirección de unidades del cliente
Controlar si los dispositivos TWAIN de los usuarios, como escáneres y cámaras, están disponibles en una sesión y controlar la compresión de transferencias de datos de imágenes	Redirección de dispositivos TWAIN del cliente; Redirección de compresión TWAIN
Controlar si los dispositivos USB están disponibles en una sesión	Redirección de dispositivos USB del cliente y Reglas de redirección de dispositivos USB del cliente
Mejorar la velocidad de escritura y copia de archivos en los discos del cliente en redes WAN	Usar escrituras asíncronas

## Redirección de contenido

Para esta tarea	Use esta configuración de directiva
Controlar si se utiliza la redirección de contenido desde el servidor al dispositivo del usuario	Redirección del host al cliente

## Interfaz de usuario de escritorio

Para esta tarea	Use esta configuración de directiva
Controlar si se usa el papel tapiz del escritorio en las sesiones de los usuarios	Tapiz del escritorio
Ver el contenido de las ventanas al arrastrarlas	Ver contenido de las ventanas al arrastrar

## Gráficos y multimedia

**Importante:**

La directiva de Flash solo permanece para permitir que los clientes con agentes VDA antiguos utilicen controladores más nuevos (por ejemplo, controladores de versión 1912) y sigan mediante Flash. Esta versión de VDA no es compatible con Flash.

Para esta tarea	Use esta configuración de directiva
Controlar la cantidad máxima de fotogramas por segundo enviados a los dispositivos de los usuarios desde escritorios virtuales	Velocidad de fotogramas de destino
Controlar la calidad visual de las imágenes que se muestran en el dispositivo del usuario	Calidad visual
Controlar si los sitios web pueden mostrar contenido Flash cuando se accede a ellos desde una sesión	Lista de URL para obtener contenido Flash del lado del servidor; Lista de compatibilidad de URL de Flash; Configuración de la directiva Prevención de reserva de vídeo de Flash; Error de impedimento para recurrir al vídeo Flash (*.swf)
Controlar la compresión de vídeos generados en el servidor	Usar códec de vídeo para compresión; Usar codificación por hardware para códec de vídeo
Controlar la entrega de contenido multimedia web en HTML5 a los usuarios	Redirección de vídeo HTML5

**Establecer prioridades para el tráfico de red de multisequencia**

Para esta tarea	Use esta configuración de directiva
Especificar puertos para el tráfico ICA a través de varias conexiones y establecer prioridades de red	Directiva Puertos múltiples
Habilitar la compatibilidad con conexiones de multisequencia entre servidores y dispositivos de usuario	Multisequencia (configuración de equipo y usuario)

**Imprimir**

Para esta tarea	Use esta configuración de directiva
Controlar la creación de impresoras del cliente en el dispositivo del usuario	Crear automáticamente las impresoras del cliente y Redirección de impresoras del cliente
Controlar la ubicación donde se guardan las propiedades de la impresora	Retención de las propiedades de impresora
Controlar si las solicitudes de impresión se procesan en el cliente o en el servidor	Conexiones directas con servidores de impresión
Controlar si los usuarios pueden acceder a las impresoras conectadas a sus dispositivos	Redirección de impresoras del cliente
Controlar la instalación de controladores nativos de Windows al crear automáticamente impresoras de cliente y de red	Instalación automática de controladores de impresora
Decidir cuándo utilizar el controlador de impresora universal	Uso de controladores de impresión universal
Elegir una impresora en función de la información de sesión de un usuario itinerante	Impresora predeterminada
Equilibrar la carga y definir el umbral de conmutación por error para servidores Universal Print Server	Universal Print Servers para equilibrio de carga; Umbral para servidores Universal Print Server fuera de servicio

**Nota:**

Las directivas no pueden usarse para habilitar un salvapantallas en una sesión de escritorio o aplicación. Para los usuarios que necesiten un salvapantallas, éste se puede implementar en el dispositivo del usuario.

## Configuraciones de la directiva ICA

June 19, 2023

### Transporte adaptable

Esta configuración permite o impide el transporte de datos sobre EDT como opción principal u opción de recurrir a TCP (como método secundario).

De forma predeterminada, el transporte adaptable está habilitado (**Preferido**), y se usa EDT cuando sea posible (cuando no sea posible, se recurre a TCP). Si se ha inhabilitado y la quiere habilitar, siga este procedimiento.

1. En Studio, habilite la configuración de directiva “Transporte adaptable HDX”. Asimismo, se recomienda no habilitar esta funcionalidad como una directiva universal para todos los objetos del sitio.
2. Para habilitar esta configuración de directiva, establézcala en **Preferido** y, a continuación, haga clic en **Aceptar**.

**Preferido.** Se utiliza el transporte adaptable por EDT cuando sea posible; cuando no lo sea, se recurre a TCP.

**Modo de diagnóstico.** Se obliga el uso de EDT y la opción de recurrir a TCP está inhabilitada. Esta configuración se recomienda solamente para la solución de problemas.

**Desactivado.** Se obliga el uso de TCP y EDT está inhabilitado.

Para obtener más información, consulte [Transporte adaptable](#).

## Tiempo de espera de inicio de la aplicación

Esta configuración especifica el tiempo (en milisegundos) que una sesión debe esperar para que se inicie la primera aplicación. Si el inicio de la aplicación supera este período de tiempo, la sesión se termina.

Puede elegir el tiempo predeterminado (10 000 milisegundos) o puede especificar una cantidad de tiempo en milisegundos.

## Redirección del portapapeles del cliente

Esta configuración permite o impide la asignación del portapapeles del dispositivo del usuario al portapapeles del servidor.

La redirección del portapapeles está permitida de forma predeterminada.

Para impedir la transferencia de datos mediante cortar y pegar entre una sesión y el portapapeles local, seleccione **Prohibida**. Los usuarios podrán seguir copiando y pegando datos entre aplicaciones ejecutadas en sesiones.

Después de permitir esta configuración, configure el ancho de banda máximo permitido que el portapapeles puede consumir en una conexión de cliente. Utilice los parámetros **Límite de ancho de banda de redirección del portapapeles** o **Porcentaje límite de ancho de banda de redirección del portapapeles**.

## Formatos permitidos de escritura en el portapapeles del cliente

Cuando el parámetro **Restringir escritura en el portapapeles del cliente** está **habilitado**, los datos del portapapeles del host no se pueden compartir con el punto final cliente. Puede usar esta configu-

ración para permitir que formatos específicos de datos se puedan compartir con el portapapeles del dispositivo final cliente. Para usar esta configuración, habilítela y agregue los formatos específicos que quiere permitir.

Los siguientes formatos de portapapeles están definidos por el sistema:

- CF\_TEXT
- CF\_BITMAP
- CF\_METAFILEPICT
- CF\_SYLK
- CF\_DIF
- CF\_TIFF
- CF\_OEMTEXT
- CF\_DIB
- CF\_PALETTE
- CF\_PENDATA
- CF\_RIFF
- CF\_WAVE
- CF\_UNICODETEXT
- CF\_ENHMETAFILE
- CF\_HDROP
- CF\_LOCALE
- CF\_DIBV5
- CF\_OWNERDISPLAY
- CF\_DSPTEXT
- CF\_DSPBITMAP
- CF\_DSPMETAFILEPICT
- CF\_DISPENHMETAFILE
- CF\_HTML

Los siguientes formatos personalizados están predefinidos en XenApp y XenDesktop y Citrix Virtual Apps and Desktops:

- CFX\_RICHTEXT
- CFX\_OfficeDrawingShape
- CFX\_BIFF8
- CFX\_FILE

El formato HTML está inhabilitado de forma predeterminada. Para habilitar esta funcionalidad:

- Compruebe que la configuración **Redirección del portapapeles del cliente** está **permitida**.
- Compruebe que la configuración **Restringir escritura en el portapapeles del cliente** está **habilitada**.

- Agregue una entrada para **CF\_HTML** (y otros formatos que quiera admitir) en la opción **Formatos permitidos de escritura en el portapapeles del cliente**.

Puede agregar más formatos personalizados. El nombre del formato personalizado debe coincidir con los formatos para registrar con el sistema. Los nombres de formato distinguen entre mayúsculas y minúsculas.

Esta configuración no se aplicará si **Redirección del portapapeles del cliente** o **Restringir escritura en el portapapeles del cliente** están configuradas como **Prohibidas**.

#### Nota

Si se permite copiar contenido en formato HTML al portapapeles (en otras palabras, si se habilita el formato CF\_HTML), se copian los scripts del origen del contenido al destino. Antes de proceder a copiar contenido, compruebe el origen de datos para saber si confiar en él. Si copia contenido que contiene scripts, solo se activarán si guarda el archivo de destino como HTML y lo ejecuta.

### Restringir escritura en el portapapeles del cliente

Si esta configuración está **permitida**, los datos del portapapeles del host no se pueden compartir con el punto final cliente. Puede permitir algunos formatos específicos, habilitando la configuración **Formatos permitidos de escritura en el portapapeles del cliente**.

De forma predeterminada, esta configuración está prohibida.

### Restringir escritura en el portapapeles de la sesión

Cuando esta configuración está **permitida**, los datos del portapapeles del cliente no se pueden compartir con la sesión del usuario. Puede permitir algunos formatos específicos, habilitando el parámetro **Formatos permitidos de escritura en el portapapeles de la sesión**.

De forma predeterminada, esta configuración está prohibida.

### Formatos permitidos de escritura en el portapapeles de la sesión

Cuando la configuración **Restringir escritura en el portapapeles de la sesión** está **permitida**, los datos de portapapeles del cliente no se pueden compartir con las aplicaciones de la sesión. Puede usar esta configuración para permitir que formatos específicos de datos se puedan compartir con el portapapeles de la sesión.

Los siguientes formatos de portapapeles están definidos por el sistema:

- CF\_TEXT

- CF\_BITMAP
- CF\_METAFILEPICT
- CF\_SYLK
- CF\_DIF
- CF\_TIFF
- CF\_OEMTEXT
- CF\_DIB
- CF\_PALETTE
- CF\_PENDATA
- CF\_RIFF
- CF\_WAVE
- CF\_UNICODETEXT
- CF\_ENHMETAFILE
- CF\_HDROP
- CF\_LOCALE
- CF\_DIBV5
- CF\_OWNERDISPLAY
- CF\_DSPTEXT
- CF\_DSPBITMAP
- CF\_DSPMETAFILEPICT
- CF\_DISPENHMETAFILE
- CF\_HTML

Los siguientes formatos personalizados están predefinidos en XenApp y XenDesktop y Citrix Virtual Apps and Desktops:

- CFX\_RICHTEXT
- CFX\_OfficeDrawingShape
- CFX\_BIFF8

El formato HTML está inhabilitado de forma predeterminada. Para habilitar esta funcionalidad:

- Compruebe que la configuración **Redirección del portapapeles del cliente** está **permitida**.
- Compruebe que la configuración **Restringir escritura en el portapapeles de la sesión** está **habilitada**.
- Agregue una entrada para **CF\_HTML** (y otros formatos que quiera admitir) en la opción **Formatos permitidos de escritura en el portapapeles de la sesión**.

Puede agregar más formatos personalizados. El nombre del formato personalizado debe coincidir con los formatos para registrar con el sistema. Los nombres de formato distinguen entre mayúsculas y minúsculas.

Esta configuración no se aplicará si Redirección del portapapeles del cliente o Restringir escritura en el portapapeles de la sesión están configuradas como prohibidas.

#### **Nota**

Si se permite copiar contenido en formato HTML al portapapeles (en otras palabras, si se habilita el formato CF\_HTML), se copian los scripts del origen del contenido al destino. Antes de proceder a copiar contenido, compruebe el origen de datos para saber si confiar en él. Si copia contenido que contiene scripts, solo se activarán si guarda el archivo de destino como HTML y lo ejecuta.

### **Inicios de escritorio**

Esta configuración permite o impide que usuarios no administrativos que formen parte del grupo de usuarios con acceso directo en un VDA se conecten a ese VDA mediante conexiones ICA.

De forma predeterminada, los usuarios no administradores no pueden conectarse a estas sesiones.

Esta configuración no afecta a usuarios no administrativos que formen parte del grupo de usuarios de acceso directo en un VDA y que usen una conexión RDP. Estos usuarios pueden conectarse al VDA tanto si esta configuración está habilitada como si no. Esta configuración no afecta a usuarios no administrativos que no formen parte del grupo de usuarios con acceso directo en un VDA. Estos usuarios no pueden conectarse al VDA tanto si esta configuración está habilitada como si no.

### **Tiempo de espera de la conexión de escucha ICA**

Esta configuración permite especificar el tiempo de espera máximo para establecer conexiones que usan el protocolo ICA.

El tiempo de espera predeterminado es de 120000 milésimas de segundo, es decir, dos minutos.

### **Número de puerto de escucha ICA**

Esta configuración permite especificar el número de puerto TCP/IP que usará el protocolo ICA en el servidor.

De forma predeterminada, el número de puerto es el 1494.

Los números de puerto válidos deben estar entre 0 y 65 535, y no deben coincidir con otros números de puerto conocidos. Si cambia el número de puerto, vuelva a iniciar el servidor para que se aplique el nuevo valor. Si cambia el número de puerto en el servidor, también deberá cambiarlo en cada aplicación Citrix Workspace o plug-in que se conecte a ese servidor.

## Editor de métodos de entrada (IME) y teclado

### Nota:

Esta directiva se aplica solo a 1912 LTSR CU2 y versiones posteriores.

Esta configuración habilita o inhabilita la sincronización dinámica de la distribución del teclado, el Editor de métodos de entrada (IME) y la asignación de la distribución del teclado Unicode, y oculta o muestra el mensaje de diálogo de la notificación del cambio de distribución del teclado.

1. En Studio, seleccione **Teclado e IME**.
2. Seleccione **Sincronización de la distribución del teclado del cliente y mejora de IME** para controlar la sincronización dinámica de la distribución del teclado y las funciones genéricas del Editor de métodos de entrada (IME) del cliente en el VDA. Puede configurar:

**Inhabilitado:** Sincronización dinámica de la distribución del teclado y Editor genérico de métodos de entrada (IME) del cliente.

**Compatibilidad con sincronización dinámica de la distribución del teclado del cliente:** Permite la sincronización dinámica de la distribución del teclado.

**Sincronización de la distribución del teclado del cliente y mejora de IME.** Permite controlar la sincronización dinámica de la distribución del teclado y las funciones genéricas del Editor de métodos de entrada (IME).

3. Seleccione **Habilitar la asignación de distribución de teclado Unicode** para habilitar o inhabilitar la asignación de teclado Unicode.
4. Seleccione **Ocultar cuadro de mensaje emergente del botón de distribución del teclado** para permitir o prohibir que un mensaje muestre que la distribución del teclado se sincroniza cuando el usuario cambia la distribución del teclado del cliente.

Parámetros predeterminados:

- **Sincronización de la distribución del teclado del cliente y mejora de IME**
  - Sincronización inhabilitada en Windows Server 2016 y Windows Server 2019.
  - Está disponible la sincronización dinámica de la distribución del teclado del cliente y mejora de IME en Windows Server 2012 y Windows 2010.
- **Inhabilitar la asignación de distribución de teclado Unicode**
- **Mostrar cuadro de mensaje emergente del botón de distribución del teclado**

Esta directiva reemplaza los parámetros del Registro que se indican en la sección **Descripción** de las configuraciones de la directiva.

## Demora en inicio de comprobador de cierre de sesión

Esta configuración especifica la duración que tendrá la demora antes de iniciar el comprobador del cierre de sesión. Utilice esta directiva para establecer el tiempo (en segundos) que espera una sesión de cliente antes de desconectar la sesión.

Esta configuración también aumenta el tiempo necesario para que un usuario cierre la sesión en el servidor.

## Protocolo Rendezvous

Esta configuración cambia la forma en que las sesiones HDX se envían por proxy cuando se utiliza Citrix Gateway Service. Cuando está habilitado, el tráfico HDX ya no pasa por Citrix Cloud Connector. En vez de ello, el VDA establece una conexión saliente directamente con Citrix Gateway Service (con lo que mejora la escalabilidad de Cloud Connector).

### Importante:

Esta función se puede activar y desactivar en Citrix Cloud, así como una configuración en la directiva HDX. La opción para activar o desactivar la función de Citrix Cloud está habilitada de forma predeterminada, mientras que el parámetro HDX está inhabilitado de forma predeterminada. El parámetro de HDX solo afecta a las sesiones HDX establecidas a través de Citrix Gateway Service. Las sesiones establecidas directamente entre el cliente y el VDA o a través de un dispositivo Citrix Gateway local no se ven afectadas por este parámetro.

Para obtener información, consulte [Protocolo Rendezvous](#).

## Iniciar programas no publicados durante la conexión del cliente

Esta configuración especifica si se permite iniciar aplicaciones iniciales a través de RDP en el servidor.

De manera predeterminada, no se permite iniciar aplicaciones iniciales a través de RDP en el servidor.

## Configuraciones de la directiva Cambiar modo tableta

El modo tableta optimiza la apariencia y el comportamiento de los almacenes de aplicaciones, las aplicaciones Win32 y el shell de Windows en el VDA. El escritorio virtual cambia automáticamente al modo tableta cuando un usuario se conecta a él desde dispositivos de formato pequeño (como teléfonos, tabletas o cualquier dispositivo táctil).

Si esta directiva está inhabilitada, el VDA permanecerá en todo momento en el modo en que lo defina el usuario, sin importar el tipo de cliente.

## Configuraciones de la directiva Reconexión automática de clientes

September 22, 2021

La sección “Reconexión automática de clientes” contiene configuraciones para controlar la reconexión automática de las sesiones.

### Reconexión automática de clientes

Esta configuración permite o impide la reconexión automática de un cliente tras la interrupción de la conexión.

A partir de Citrix Receiver para Windows 4.7 y la aplicación Citrix Workspace 1808, la Reconexión automática de clientes solo usa las configuraciones de directiva de Citrix Studio. Las actualizaciones de estas directivas en Studio sincronizan la Reconexión automática de clientes desde el servidor hasta el cliente. En caso de versiones anteriores de Citrix Receiver para Windows, para configurar la Reconexión automática de clientes, use una directiva de Studio y modifique el Registro o el archivo default.ica.

La Reconexión automática de clientes permite a los usuarios reanudar el trabajo en el punto en que se interrumpió su conexión. La reconexión automática detecta las conexiones interrumpidas y luego vuelve a conectar a los usuarios a sus sesiones.

Si no usa la cookie de la aplicación Citrix Workspace que contiene la clave del ID de sesión y las credenciales, la reconexión automática puede derivar en el inicio de una nueva sesión. Es decir, se inicia una nueva sesión en vez de reconectarse a una sesión existente. La cookie no se utiliza si está caducada, por ejemplo, por retrasos en la reconexión o si las credenciales tienen que volver a introducirse. No hay reconexión automática de clientes si los usuarios se desconectan voluntariamente.

La ventana de la sesión se oscurece mientras tiene lugar una reconexión. Aparece un temporizador que muestra el tiempo restante antes de volver a conectarse a la sesión. Cuando se supera el tiempo de espera, la sesión se desconecta.

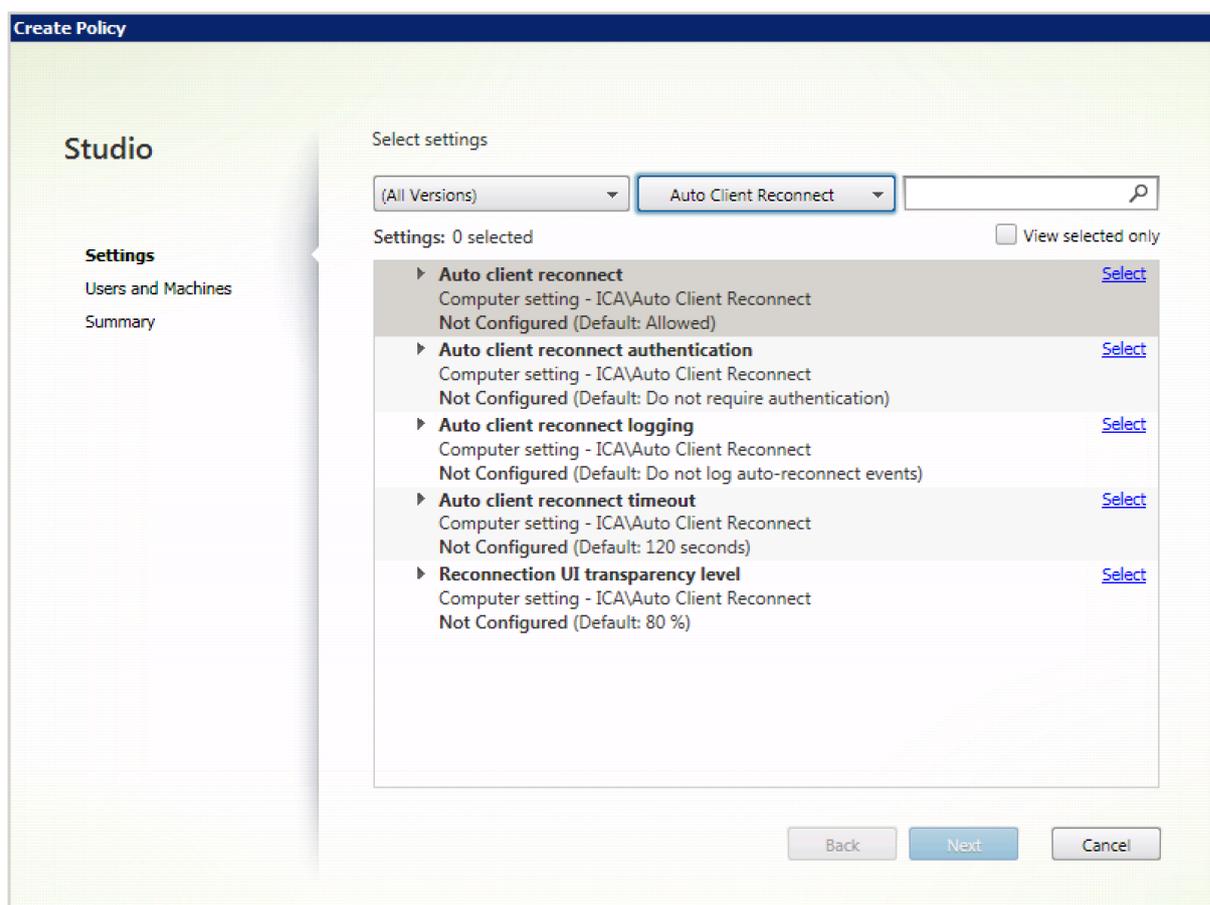
En las sesiones de aplicaciones, cuando la Reconexión automática está permitida, en el área de notificaciones aparece un temporizador que indica el tiempo restante antes de volver a conectarse a la sesión. La aplicación Citrix Workspace intenta reconectarse a la sesión hasta que lo logra o hasta que el usuario cancela los intentos de reconexión.

Para las sesiones de usuario, cuando la Reconexión automática está permitida, la aplicación Citrix Workspace intenta volver a conectarse a la sesión durante un período de tiempo especificado, a menos que se produzca una reconexión o el usuario cancele el intento de reconexión. De forma predeterminada, este período es de dos minutos. Para cambiar este período, modifique la directiva.

De forma predeterminada, la Reconexión automática de clientes está permitida.

Para inhabilitar la Reconexión automática de clientes:

1. Inicie Citrix Studio.
2. Abra la directiva **Reconexión automática de clientes**.
3. Establezca la directiva en **Prohibida**.



## Autenticación para reconexión automática de clientes

Esta configuración hace necesaria la autenticación para las reconexiones automáticas de clientes.

Cuando un usuario inicia sesión por primera vez, sus credenciales se cifran y se almacenan en la memoria. Además, se crea una cookie con la clave de cifrado. La cookie se envía a la aplicación Citrix

Workspace. Cuando esta configuración está definida, las cookies no se utilizan. En su lugar, aparece un cuadro de diálogo que solicita que los usuarios introduzcan sus credenciales cuando la aplicación Citrix Workspace intenta volver a conectarse automáticamente.

De forma predeterminada, la autenticación no es necesaria.

Para cambiar la autenticación de la Reconexión automática de clientes:

1. Inicie Citrix Studio.
2. Abra la directiva **Autenticación para reconexión automática de clientes**.
3. Habilite o inhabilite la autenticación.
4. Elija **Aceptar**.

### **Registro de reconexión automática de clientes**

Esta configuración habilita o inhabilita el registro de las reconexiones automáticas de clientes en el registro de sucesos.

Cuando se habilita la captura de registros, el Registro del sistema del servidor recopila información sobre los sucesos de reconexión automática correctos y fallidos. Un sitio no proporciona los registros combinados de sucesos de reconexión que han tenido lugar en todos los servidores.

De forma predeterminada, el registro está inhabilitado.

Para cambiar la captura de registros de Reconexión automática de clientes:

1. Inicie Citrix Studio.
2. Abra la directiva **Registro de reconexión automática de clientes**.
3. Habilite o inhabilite la captura de registros.
4. Elija **Aceptar**.

### **Tiempo de espera de la Reconexión automática de clientes**

De forma predeterminada, el tiempo de espera de la Reconexión automática de clientes está establecido en 120 segundos. El valor máximo configurable de tiempo de espera para la Reconexión automática de clientes es de 300 segundos.

Para cambiar el tiempo de espera de la Reconexión automática de clientes:

1. Inicie Citrix Studio.
2. Abra la directiva **Tiempo de espera de la reconexión automática de clientes**.
3. Cambie el valor del tiempo de espera.
4. Elija **Aceptar**.

## Nivel de transparencia de la interfaz de usuario durante la reconexión

Puede usar la directiva de Studio para configurar el nivel de opacidad que se aplica a la ventana de sesión de XenApp o XenDesktop durante el tiempo de reconexión de la fiabilidad de la sesión.

De manera predeterminada, el nivel de transparencia de la interfaz de usuario es del 80%.

Para modificar el nivel de opacidad de la interfaz de usuario durante una reconexión:

1. Inicie Citrix Studio.
2. Abra la directiva **Nivel de transparencia de la interfaz de usuario durante la reconexión**.
3. Cambie el valor.
4. Elija **Aceptar**.

## Configuraciones de directiva de Sonido

January 4, 2021

La sección “Sonido” contiene las configuraciones que permiten que los dispositivos de usuario reciban y envíen sonido en las sesiones, sin disminuir su rendimiento.

### Transporte de sonido en tiempo real sobre UDP

Esta configuración permite o impide la transmisión y la recepción de sonido entre el VDA y el dispositivo del usuario a través de RTP mediante el protocolo UDP. Cuando esta configuración está inhabilitada, el sonido se envía y recibe sobre TCP.

De forma predeterminada, el sonido sobre UDP está permitido.

### Sonido Plug and Play

Esta configuración permite o impide el uso de varios dispositivos de sonido para grabar y reproducir sonido.

De forma predeterminada, el uso de varios dispositivos de sonido está permitido.

Esta configuración solo se aplica a máquinas de SO multisesión Windows.

### Calidad de sonido

Esta configuración especifica el nivel de calidad de sonido recibido en las sesiones de usuario.

De forma predeterminada, la calidad de sonido está establecida en Alta: sonido de alta definición.

Para controlar la calidad del sonido, seleccione una de las siguientes opciones:

- **Seleccione Baja:** para conexiones de baja velocidad, para las conexiones con ancho de banda reducido. Los sonidos enviados al dispositivo del usuario se comprimen hasta 16 Kbps. Esta compresión resulta en una disminución importante de la calidad del sonido pero permite un rendimiento razonable en conexiones con poco ancho de banda.
- **Seleccione Media:** optimizado para voz para entregar aplicaciones VoIP o para entregar aplicaciones multimedia en conexiones de red difíciles, con líneas de menos de 512 Kbps o que presentan una congestión y pérdida de paquetes significativas. Este códec ofrece una mayor rapidez de codificación, por lo que es ideal para usarlo con programas softphone y aplicaciones de comunicaciones unificadas, cuando se necesita un procesamiento de medios en el lado del servidor.

El sonido enviado al dispositivo del usuario se comprime hasta 64 Kbps. Esta compresión provoca un ligero descenso en la calidad del sonido que se reproduce en el dispositivo del usuario, pero la latencia es menor y se consume poco ancho de banda. Si la calidad VoIP no es satisfactoria, compruebe que la configuración de directiva “Transporte de sonido en tiempo real sobre UDP” esté establecida en “Permitida”.

Actualmente, RTP (transporte en tiempo real) sobre UDP solo se admite cuando se selecciona esta calidad de sonido. Use esta calidad de sonido incluso para la entrega de aplicaciones multimedia en conexiones de red con poco ancho de banda (inferior a 512 Kbps), y cuando hay congestión de tráfico y pérdida de datos en la red.

- **Elija Alta:** sonido de alta definición para las conexiones en las cuales no hay problemas de ancho de banda y la calidad del sonido es importante. Los clientes pueden ejecutar el sonido sin compresión adicional. Los sonidos se comprimen con un nivel alto de calidad manteniendo una calidad de nivel CD, y mediante hasta 112 Kbps de ancho de banda. La transmisión de tal cantidad de datos puede ocasionar un incremento en la utilización de la CPU y congestionar la red.

El ancho de banda solo se utiliza cuando el sonido se graba o reproduce. Si se graba y se reproduce al mismo tiempo, el consumo de ancho de banda se duplica.

Para especificar el ancho de banda máximo, configure las configuraciones de directiva Límite de ancho de banda de redirección de sonido o Porcentaje límite de ancho de banda de redirección de sonido.

## **Redirección de sonido del cliente**

Esta configuración especifica si las aplicaciones alojadas en el servidor pueden reproducir sonidos mediante un dispositivo de sonido instalado en el dispositivo del usuario. Esta configuración también

especifica si los usuarios pueden grabar una entrada de sonido.

La redirección del sonido está permitida de forma predeterminada.

Una vez habilitada esta configuración, es posible limitar el ancho de banda utilizado para la reproducción o la grabación de sonido. Limitar el ancho de banda utilizado para el sonido permite mejorar el rendimiento de las aplicaciones, pero también reduce la calidad de sonido. El ancho de banda solo se utiliza cuando el sonido se graba o reproduce. Si se graba y se reproduce al mismo tiempo, el consumo de ancho de banda se duplica. Para especificar el ancho de banda máximo, configure las configuraciones de directiva Límite de ancho de banda de redirección de sonido o Porcentaje límite de ancho de banda de redirección de sonido.

En las máquinas con SO multisesión Windows, compruebe también que la configuración Sonido Plug and Play está habilitada para admitir varios dispositivos de sonido.

Importante: Cuando la Redirección de sonido del cliente está Prohibida, toda la función de sonido de HDX queda inhabilitada.

## **Redirección de micrófonos del cliente**

Esta configuración habilita o inhabilita la redirección de micrófonos del cliente. Cuando está habilitada, los usuarios pueden usar un micrófono para grabar entradas de sonido en una sesión.

De forma predeterminada, se permite la redirección de micrófonos.

Por motivos de seguridad, se alerta a los usuarios cuando haya servidores sin relación de confianza con el dispositivo intentando acceder a sus micrófonos. Los usuarios podrán aceptar o no el acceso. Los usuarios pueden inhabilitar la alerta en la aplicación Citrix Workspace.

En las máquinas con SO multisesión Windows, compruebe también que la configuración Sonido Plug and Play está habilitada para admitir varios dispositivos de sonido.

Si se inhabilita la configuración Redirección de sonido del cliente en el dispositivo del usuario, esta regla no tiene ningún efecto.

## **Configuraciones de directiva de Ancho de banda**

September 22, 2021

La sección “Ancho de banda” contiene configuraciones que se pueden definir para evitar problemas de rendimiento relacionados con el uso del ancho de banda de las sesiones de cliente.

Importante: Tenga en cuenta que se pueden producir resultados inesperados si se usan estas configuraciones de directiva con las configuraciones de directiva Multisequencia. Si se usan las configuraciones de multisequencia en una directiva, asegúrese de que la configuración de directivas de límite de ancho de banda no esté incluida.

### **Límite de ancho de banda de redirección de sonido**

Esta configuración permite especificar el valor máximo permitido de ancho de banda, en kilobits por segundo, para la reproducción o la grabación de sonido en una sesión de usuario.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Porcentaje límite de ancho de banda de redirección de sonido, se aplicará el más restrictivo (el de valor más bajo).

### **Porcentaje límite de ancho de banda de redirección de sonido**

Esta configuración permite especificar el límite máximo permitido de ancho de banda para la reproducción y la grabación de sonido, como porcentaje del ancho de banda total de la sesión.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Límite de ancho de banda de redirección de sonido, se aplicará el más restrictivo (el de valor más bajo).

Si usa esta configuración, también debe definir la configuración Límite de ancho de banda global de la sesión, que indica el ancho de banda total disponible para las sesiones de cliente.

### **Límite de ancho de banda de redirección de dispositivos USB del cliente**

Esta configuración especifica el ancho de banda máximo permitido, en kilobits por segundo, para la redirección de dispositivos USB hacia y desde el cliente.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Porcentaje límite de ancho de banda de redirección de dispositivos USB del cliente, se aplicará el más restrictivo (el de valor más bajo).

### **Porcentaje límite de ancho de banda de redirección de dispositivos USB del cliente**

Esta configuración especifica el ancho de banda máximo permitido para la redirección de dispositivos USB hacia y desde el cliente como un porcentaje del ancho de banda total de la sesión.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Límite de ancho de banda de redirección de dispositivos USB del cliente, se aplicará el más restrictivo (el de valor más bajo).

Si usa esta configuración, también debe definir la configuración Límite de ancho de banda global de la sesión, que indica el ancho de banda total disponible para las sesiones de cliente.

### **Límite de ancho de banda de redirección del portapapeles**

Esta configuración permite especificar el valor máximo permitido de ancho de banda, en kilobits por segundo, para la transferencia de datos entre una sesión y el portapapeles local.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Porcentaje límite de ancho de banda de redirección del portapapeles, se aplicará el más restrictivo (el de valor más bajo).

### **Porcentaje límite de ancho de banda de redirección del portapapeles**

Esta configuración permite especificar el valor máximo permitido de ancho de banda para la transferencia de datos entre una sesión y el portapapeles local como porcentaje del ancho de banda total de la sesión.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Límite de ancho de banda de redirección del portapapeles, se aplicará el más restrictivo (el de valor más bajo).

Si usa esta configuración, también debe definir la configuración Límite de ancho de banda global de la sesión, que indica el ancho de banda total disponible para las sesiones de cliente.

### **Límite de ancho de banda de redirección de puertos COM**

Nota: Para los agentes Virtual Delivery Agent 7.0 a 7.8, configure esta configuración con el Registro; consulte [Configurar la redirección de puertos COM y puertos LPT mediante el Registro](#).

Esta configuración permite especificar el valor máximo permitido de ancho de banda, en kilobits por segundo, para el acceso a un puerto COM en una conexión de cliente. Si introduce un valor para esta configuración y otro para la configuración Porcentaje límite de ancho de banda de redirección de puertos COM, se aplicará el más restrictivo (el de valor más bajo).

## **Porcentaje límite de ancho de banda de redirección de puertos COM**

Nota: Para los agentes Virtual Delivery Agent 7.0 a 7.8, configure esta configuración con el Registro; consulte [Configurar la redirección de puertos COM y puertos LPT mediante el Registro](#).

Esta configuración permite especificar el valor máximo permitido de ancho de banda para el acceso a puertos COM en una conexión de cliente, como porcentaje del ancho de banda total de la sesión.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Límite de ancho de banda de redirección de puertos COM, se aplicará el más restrictivo (el de valor más bajo).

Si define esta configuración, también debe definir la configuración Límite de ancho de banda global de la sesión, que indica el ancho de banda total disponible para las sesiones de cliente.

## **Límite de ancho de banda de redirección de archivos**

Esta configuración permite especificar el valor máximo permitido de ancho de banda, en kilobits por segundo, para el acceso a una unidad del cliente en una sesión de usuario.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Porcentaje límite de ancho de banda de redirección de archivos, se aplicará el más restrictivo (el de valor más bajo).

## **Porcentaje límite de ancho de banda de redirección de archivos**

Esta configuración permite especificar el límite máximo permitido de ancho de banda para el acceso a unidades del cliente como porcentaje del ancho de banda total de la sesión.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Límite de ancho de banda de redirección de archivos, se aplicará el más restrictivo (el de valor más bajo).

Si usa esta configuración, también debe definir la configuración Límite de ancho de banda global de la sesión, que indica el ancho de banda total disponible para las sesiones de cliente.

## **Límite de ancho de banda de aceleración multimedia HDX MediaStream**

Esta configuración especifica el límite de ancho de banda máximo permitido, en kilobits por segundo, para entregar por streaming sonido y vídeo mediante la aceleración multimedia HDX MediaStream.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Porcentaje límite de ancho de banda de aceleración multimedia HDX MediaStream, se aplicará el más restrictivo (el de valor más bajo).

### **Porcentaje límite de ancho de banda de aceleración multimedia HDX MediaStream**

Esta configuración especifica el ancho de banda máximo permitido para entregar por streaming sonido y vídeo mediante la aceleración multimedia HDX MediaStream como porcentaje del ancho de banda total de la sesión.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración “Límite de ancho de banda de aceleración multimedia HDX MediaStream”, se aplicará el más restrictivo (el de valor más bajo).

Si usa esta configuración, también debe definir la configuración Límite de ancho de banda global de la sesión, que indica el ancho de banda total disponible para las sesiones de cliente.

### **Límite de ancho de banda de redirección de puertos LPT**

Nota: Para los agentes Virtual Delivery Agent 7.0 a 7.8, configure esta configuración con el Registro; consulte [Configurar la redirección de puertos COM y puertos LPT mediante el Registro](#).

Esta configuración permite especificar el valor máximo permitido de ancho de banda, en kilobits por segundo, para trabajos de impresión mediante un puerto LPT en una sesión de usuario individual.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Porcentaje límite de ancho de banda de redirección de puertos LPT, se aplicará el más restrictivo (el de valor más bajo).

### **Porcentaje límite de ancho de banda de redirección de puertos LPT**

Nota: Para los agentes Virtual Delivery Agent 7.0 a 7.8, configure esta configuración con el Registro; consulte [Configurar la redirección de puertos COM y puertos LPT mediante el Registro](#).

Esta configuración permite especificar el límite de ancho de banda para los trabajos de impresión mediante un puerto LPT en una sesión de cliente individual como porcentaje del ancho de banda total de la sesión.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Límite de ancho de banda de redirección de puertos LPT, se aplicará el más restrictivo (el de valor más bajo).

Si usa esta configuración, también debe definir la configuración Límite de ancho de banda global de la sesión, que indica el ancho de banda total disponible para las sesiones de cliente.

### **Límite de ancho de banda global de la sesión**

Esta configuración permite especificar el total de ancho de banda disponible, en kilobits por segundo, para las sesiones de usuario.

El límite de ancho de banda máximo que puede imponerse es de 10 Mbps (10000 Kbps). De forma predeterminada, no se especifica ningún valor máximo (cero).

Al limitar el ancho de banda de las conexiones de cliente, se puede mejorar el rendimiento cuando otras aplicaciones fuera de la conexión de cliente compiten por un ancho de banda limitado.

### **Límite de ancho de banda de redirección de impresoras**

Esta configuración permite especificar el valor máximo permitido de ancho de banda, en kilobits por segundo, para el acceso a impresoras del cliente en una sesión de usuario.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Porcentaje límite de ancho de banda de redirección de impresoras, se aplicará el más restrictivo (el de valor más bajo).

### **Porcentaje límite de ancho de banda de redirección de impresoras**

Esta configuración permite especificar el valor máximo permitido de ancho de banda para el acceso a impresoras del cliente como porcentaje del ancho de banda total de la sesión.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Límite de ancho de banda de redirección de impresoras, se aplicará el más restrictivo (el de valor más bajo).

Si usa esta configuración, también debe definir la configuración Límite de ancho de banda global de la sesión, que indica el ancho de banda total disponible para las sesiones de cliente.

### **Límite de ancho de banda de redirección de dispositivos TWAIN**

Esta configuración permite especificar el valor máximo permitido ancho de banda, en kilobits por segundo, para el control de dispositivos de imágenes TWAIN desde aplicaciones publicadas.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Porcentaje límite de ancho de banda de redirección de dispositivos TWAIN, se aplicará el más restrictivo (el de valor más bajo).

### **Porcentaje límite de ancho de banda de redirección de dispositivos TWAIN**

Esta configuración permite especificar el valor máximo permitido de ancho de banda para el control de dispositivos de imágenes TWAIN desde aplicaciones publicadas como porcentaje del ancho de banda total de la sesión.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Límite de ancho de banda de redirección de dispositivos TWAIN, se aplicará el más restrictivo (el de valor más bajo).

Si usa esta configuración, también debe definir la configuración Límite de ancho de banda global de la sesión, que indica el ancho de banda total disponible para las sesiones de cliente.

## **Configuraciones de directiva de Redirección bidireccional de contenido**

April 19, 2024

### **Permitir redirección bidireccional de contenido**

Establezca esta directiva en **Permitida** para habilitar la redirección entre el servidor (VDA) y el cliente. La configuración predeterminada es **Prohibida**.

Para configurar la lista de direcciones URL para la redirección de VDA a cliente, utilice la directiva **Direcciones URL permitidas para redirigir al cliente**.

#### **Nota:**

Esta directiva debe establecerse con la directiva **Redirección bidireccional de contenido** en el cliente para permitir la redirección.

### **Direcciones URL permitidas para redirigir al cliente**

Especifica la lista de URL que se abrirán en el cliente cuando se permita la redirección bidireccional de contenido.

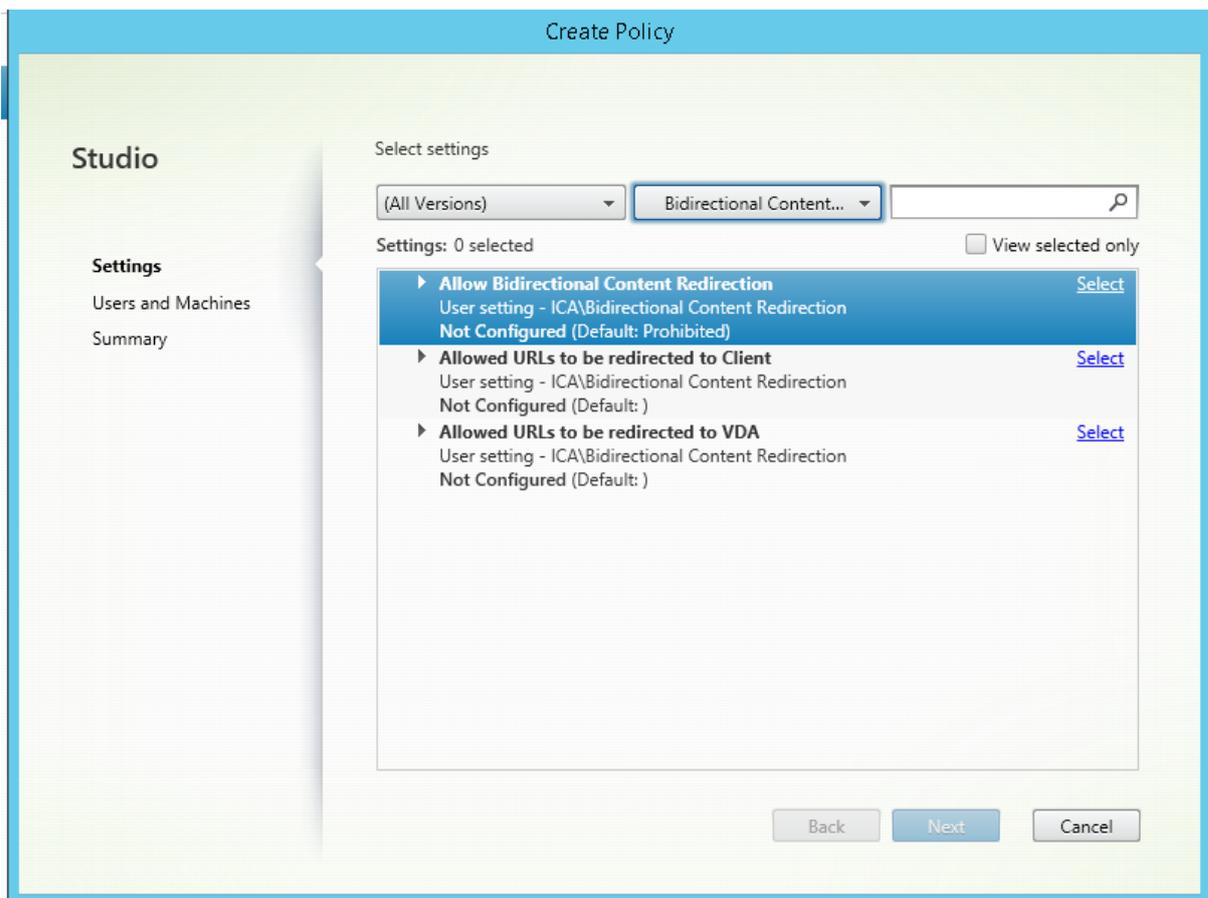
El delimitador es un punto y coma (;). Se puede usar un asterisco (\*) como comodín. Por ejemplo:

## Para habilitar la redirección bidireccional de contenido

Al incluir direcciones URL, puede especificar una sola dirección URL o una lista de direcciones URL, delimitadas por punto y coma. Puede utilizar un asterisco (\*) como comodín en el nombre de dominio. Por ejemplo:

[http://\\*.citrix.com](http://*.citrix.com); <http://www.google.com>

1. Inicie Citrix Studio.
2. Abra la directiva **Redirección bidireccional de contenido**.
3. Seleccione **Permitir redirección bidireccional de contenido**, elija **Permitida** y haga clic en **Aceptar**. Si no permite esta opción, no podrá completar este procedimiento.
4. Seleccione **Direcciones URL permitidas para redirigir al cliente** y especifique una dirección URL, una lista de direcciones URL, o bien, elija el valor predeterminado.
5. Seleccione **Direcciones URL permitidas para redirigir al VDA** y especifique una dirección URL, una lista de direcciones URL, o bien, elija el valor predeterminado.



Para obtener información sobre la configuración de la redirección bidireccional de contenido del lado del cliente en la aplicación Citrix Workspace, consulte [Redirección bidireccional de contenido](#) en la documentación de la aplicación Citrix Workspace para Windows.

## Copiar y pegar contenido entre sesiones y clientes

Para configurar la funcionalidad de copiar y pegar contenido de una sesión a un cliente, configure estas directivas de la siguiente manera:

- Redirección del portapapeles del cliente: Permitida.
- Restringir escritura en el portapapeles del cliente: Restrinja el pegado de todos los formatos del portapapeles al cliente.
- Formatos permitidos de escritura en el portapapeles del cliente: Cree una excepción para pegar archivos del portapapeles al cliente (utilice el formato CFX\_FILE para permitirlo).
- Restringir escritura en el portapapeles de la sesión: Restrinja la pegado de todos los formatos del portapapeles a la sesión de VDA.
- Formatos permitidos de escritura en el portapapeles de la sesión: Cree una excepción para pegar archivos del portapapeles al VDA (utilice el formato CFX\_FILE para permitirlo).

## Registrar complementos del explorador web

El complemento del explorador Internet Explorer es necesario para la redirección bidireccional de contenido.

Puede usar los siguientes comandos para registrar y cancelar el registro de un complemento de Internet Explorer:

- Para registrar el complemento de Internet Explorer en un dispositivo cliente: <carpeta de instalación del cliente>\redirector.exe /regIE
- Para cancelar el registro del complemento de Internet Explorer en un dispositivo cliente: <carpeta de instalación del cliente>\redirector.exe /unregIE
- Para registrar el complemento de Internet Explorer en un VDA: <carpeta de instalación del VDA>\VDARedirector.exe /regIE
- Para cancelar el registro del complemento de Internet Explorer en un VDA: <carpeta de instalación del VDA>\VDARedirector.exe /unregIE

Por ejemplo, el siguiente comando registra el complemento de Internet Explorer en un dispositivo que ejecuta la aplicación Citrix Workspace.

```
C:\Archivos de programa\Citrix\ICA Client\redirector.exe/regIE
```

El siguiente comando registra el complemento de Internet Explorer en un VDA para sistemas operativos multisesión Windows.

```
C:\Archivos de programa (x86)\Citrix\System32\VDARedirector.exe /regIE
```

## Configuraciones de la directiva Redirección de contenido de explorador web

March 10, 2022

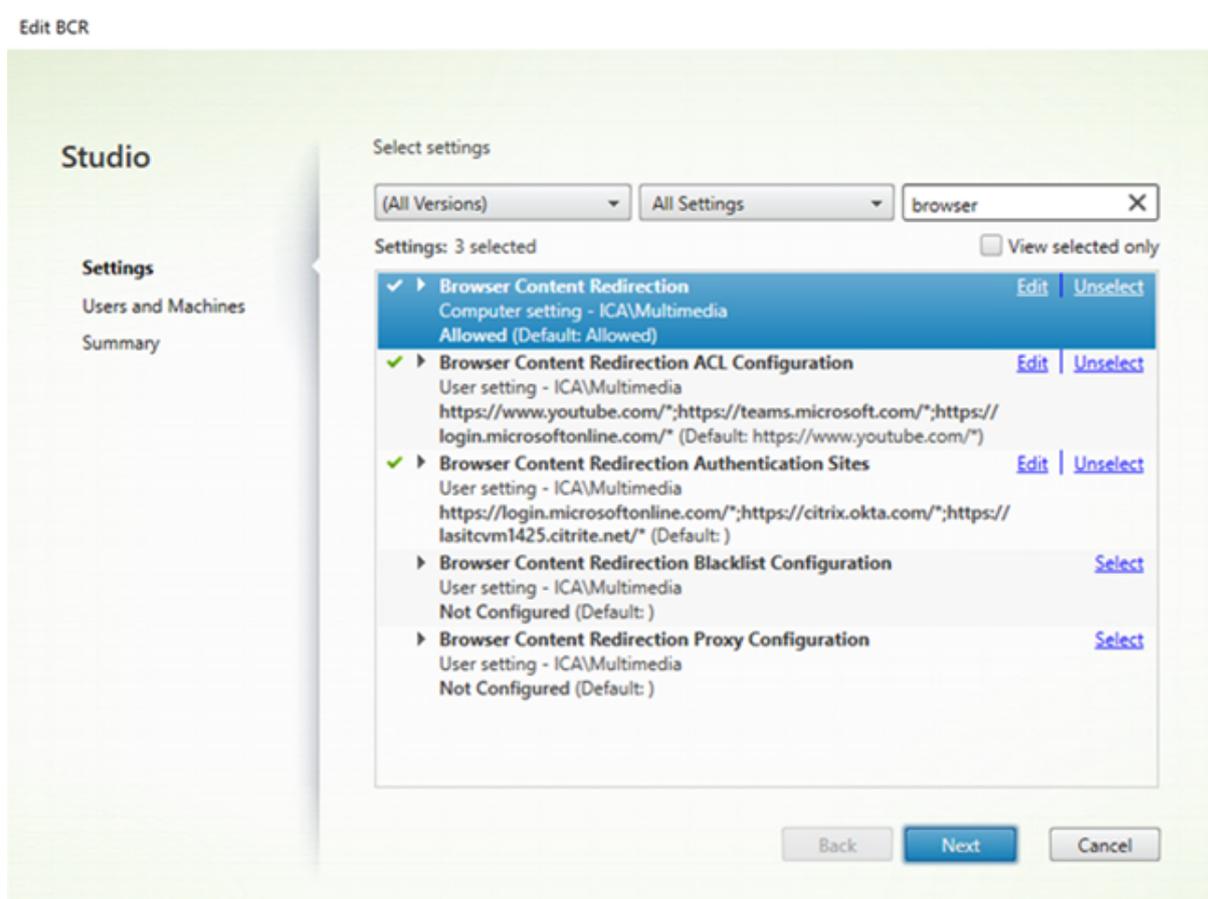
La sección “Redirección de contenido de explorador web” contiene configuraciones para definir esta función.

Con la redirección de contenido del explorador web, puede controlar y optimizar el modo en que Citrix Virtual Apps and Desktops entregan contenido de los exploradores web (por ejemplo, contenido HTML5) a los usuarios. Solo se redirige el área visible del explorador web donde se muestra el contenido.

La Redirección de vídeo HTML5 y la Redirección de contenido del explorador web son funciones independientes. Las directivas de redirección de vídeo HTML5 no son necesarias para que esta función funcione, pero se usa el servicio Citrix HDX HTML5 Video Redirection Service para la redirección de contenido del explorador web. Para obtener más información, consulte [Redirección de contenido de explorador web](#).

### Configuraciones de directivas:

En Citrix Studio, están disponibles las siguientes configuraciones de directiva para la función Redirección de contenido de explorador web. Estas directivas pueden anularse con claves de Registro en el VDA, aunque esas claves de Registro son opcionales.



## TLS y la redirección de contenido del explorador web

Puede usar la redirección contenido del explorador web para redirigir los sitios web HTTPS. El JavaScript insertado en esos sitios web debe establecer una conexión TLS al servicio Citrix HDX HTML5 Video Redirection Service (WebSocketService.exe) que se ejecuta en el VDA. Para conseguir esta redirección y mantener la integridad TLS de la página web, el servicio Citrix HDX HTML5 Video Redirection Service genera dos certificados personalizados en el almacén de certificados del VDA.

HdxVideo.js utiliza Secure WebSockets para comunicarse con WebSocketService.exe que se ejecuta en el VDA. Este proceso se ejecuta en el sistema local y realiza la terminación SSL y la asignación de sesiones de usuario.

WebSocketService.exe escucha en 127.0.0.1 en el puerto 9001.

## Redirección de contenido de explorador web

De forma predeterminada, la aplicación Citrix Workspace intenta obtener y generar el contenido en el cliente. Si falla la opción de obtener y generar el contenido en el cliente, se intenta generar contenido

en el lado del servidor. Si también habilita la directiva “Configuración de proxy para redirección de contenido de explorador web”, la aplicación Citrix Workspace solo intenta la opción de obtener contenido en el servidor y generar contenido en el cliente.

De forma predeterminada, esta configuración está permitida.

## **Configuración Autenticación de proxies web de la obtención del servidor de redirección de contenido del explorador**

### **Nota:**

Esta directiva solo está disponible en 1912 CU3 y versiones posteriores.

Este parámetro redirige el tráfico HTTP procedente de una superposición a través de un proxy web descendente. El proxy web que sigue en la cadena autoriza y autentica el tráfico HTTP mediante las credenciales de dominio del usuario del VDA a través del esquema de autenticación Negotiate.

Debe configurar la redirección de contenido del explorador para el modo de obtención del servidor en el archivo PAC mediante la directiva de configuración Proxy de redirección de contenido del explorador. En el script PAC, proporcione instrucciones para redirigir el tráfico de la superposición a través de un proxy web descendente. A continuación, configure el proxy web descendente para autenticar a los usuarios de los VDA mediante el esquema de autenticación Negotiate.

Cuando se establece en **Permitido**, el proxy web responde con un desafío 407 Negotiate, que contiene un encabezado **Proxy-Authenticate: Negotiate**. A continuación, la redirección de contenido del explorador obtiene un tíquet de servicio Kerberos mediante las credenciales de dominio del usuario del VDA e incluye el tíquet de servicio en solicitudes posteriores al proxy web.

Cuando se establece en **Prohibido**, la redirección de contenido del explorador hace de intermediaria de todo el tráfico TCP entre la superposición y el proxy web sin interferir. La superposición utiliza credenciales de autenticación básicas o cualquier otra credencial disponible para autenticarse en el proxy web.

De forma predeterminada, esta configuración está prohibida.

## **Configuraciones de directiva para la lista de control de acceso (ACL) en la redirección de contenido de explorador web**

Use esta configuración para definir una lista de control de acceso (ACL) con las direcciones URL que pueden utilizar la redirección de contenido del explorador web y las direcciones URL a las que se deniega el acceso a la redirección de contenido del explorador web.

Las direcciones URL autorizadas son aquellas URL cuyo contenido se redirige al cliente.

Se permite el carácter comodín \*, salvo en el protocolo o en la parte de dirección de dominio de la URL.

Permitido: <http://www.xyz.com/index.html>, [https://www.xyz.com/\\*](https://www.xyz.com/*), [http://www.xyz.com/\\*videos\\*](http://www.xyz.com/*videos*)

No permitido: [http://\\*.xyz.com/](http://*.xyz.com/)

Puede lograr una mayor granularidad si especifica rutas en la URL. Por ejemplo, si especifica <https://www.xyz.com/sports/index.html>, solo se redirige la página index.html.

De forma predeterminada, esta configuración está establecida en [https://www.youtube.com/\\*](https://www.youtube.com/*)

Para obtener más información, consulte el artículo [CTX238236](#) de Knowledge Center.

### **Sitios de autenticación para la Redirección de contenido de explorador web**

Use esta configuración para definir una lista de direcciones URL. Los sitios redirigidos mediante la Redirección de contenido de explorador web utilizan esa lista para autenticar usuarios. La configuración especifica las URL para las que la Redirección de contenido de explorador web permanece activa (se redirige el contenido) cuando se navega de una URL incluida en una lista de permitidos a otra que no lo está.

Un ejemplo típico es un sitio web que relega la autenticación a un proveedor de identidades (IdP). Por ejemplo, el sitio web [www.xyz.com](http://www.xyz.com) debe redirigirse al dispositivo de punto final, pero un IdP de terceros, como Okta ([www.xyz.okta.com](http://www.xyz.okta.com)), gestiona la parte de autenticación. El administrador utiliza la directiva Configuración de lista ACL para redirección de contenido del explorador web para incluir [www.xyz.com](http://www.xyz.com) en la lista de permitidos, y luego utiliza los sitios de autenticación de Redirección de contenido de explorador web para incluir [www.xyz.okta.com](http://www.xyz.okta.com) en la lista de permitidos.

Para obtener más información, consulte el artículo [CTX238236](#) de Knowledge Center.

### **Configuración de lista de prohibidos para la redirección de contenido del explorador web**

Esta configuración funciona junto con la configuración de la lista ACL de redirección de contenido del explorador web. Si las URL están presentes en la configuración de la ACL de redirección de contenido del explorador web y en la configuración de la lista de prohibidos, la configuración de la lista de prohibidos tiene prioridad y el contenido del explorador web de la URL no se redirige.

**Direcciones URL no autorizadas:** Especifica las URL incluidas en la lista de prohibidos cuyo contenido del explorador web no se redirige al cliente, sino que se genera en el servidor.

Se permite el carácter comodín \*, salvo en el protocolo o en la parte de dirección de dominio de la URL.

Permitido: `http://www.xyz.com/index.html`, `https://www.xyz.com/*`, `http://www.xyz.com/*videos*`

No permitido: `http://*.xyz.com/`

Puede lograr una mayor granularidad si especifica rutas en la URL. Por ejemplo, si especifica `https://www.xyz.com/sports/index.html`, solo `index.html` se incluye en la lista de prohibidos.

## Configuraciones de directiva de redirección de contenido de explorador web

### Importante:

Los parámetros siguientes solo se aplican a 1912 LTSR CU1 o a versiones posteriores.

Esta configuración ofrece opciones para definir un proxy en el VDA y redirigir el contenido del explorador web. Si está habilitada y tiene una dirección proxy y un número de puerto, una dirección URL PAC/WPAD o un parámetro Directo/transparente, la aplicación Citrix Workspace solo intenta obtener contenido en el servidor y generarlo en el cliente.

Si está inhabilitada o no configurada y se utiliza un valor predeterminado, la aplicación Citrix Workspace intenta obtener contenido en el cliente y generarlo en el cliente.

De forma predeterminada, esta configuración está prohibida.

### Patrón permitido para un proxy explícito:

`http://\<hostname/ip address\>:\<port\>`

### Ejemplo:

`http://proxy.example.citrix.com:80`

`http://10.10.10.10:8080`

### Patrones permitidos para archivos PAC/WPAD:

`http://<hostname/ip address>:<port>/<path>/<Proxy.pac>`

**Ejemplo:** `http://wpad.myproxy.com:30/configuration/pac/Proxy.pac`

`https://<hostname/ip address>:<port>/<path>/<wpad.dat>`

**Ejemplo:** `http://10.10.10.10/configuration/pac/wpad.dat`

### Patrones permitidos para proxies directos o transparentes:

Escriba la palabra **DIRECT** en el cuadro de texto de directiva.

## Anulaciones de claves de Registro para la redirección de contenido del explorador web

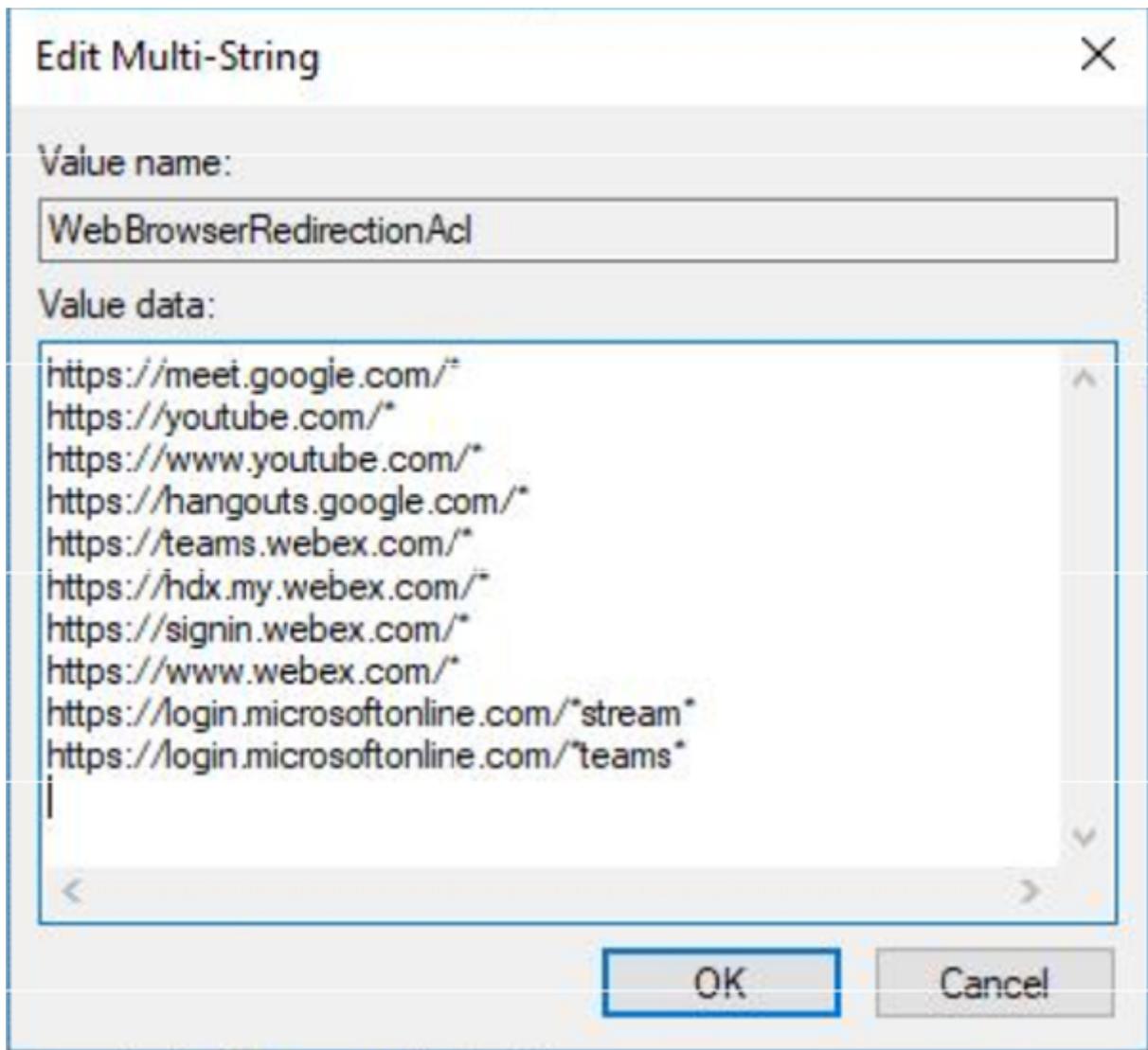
### Advertencia

Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

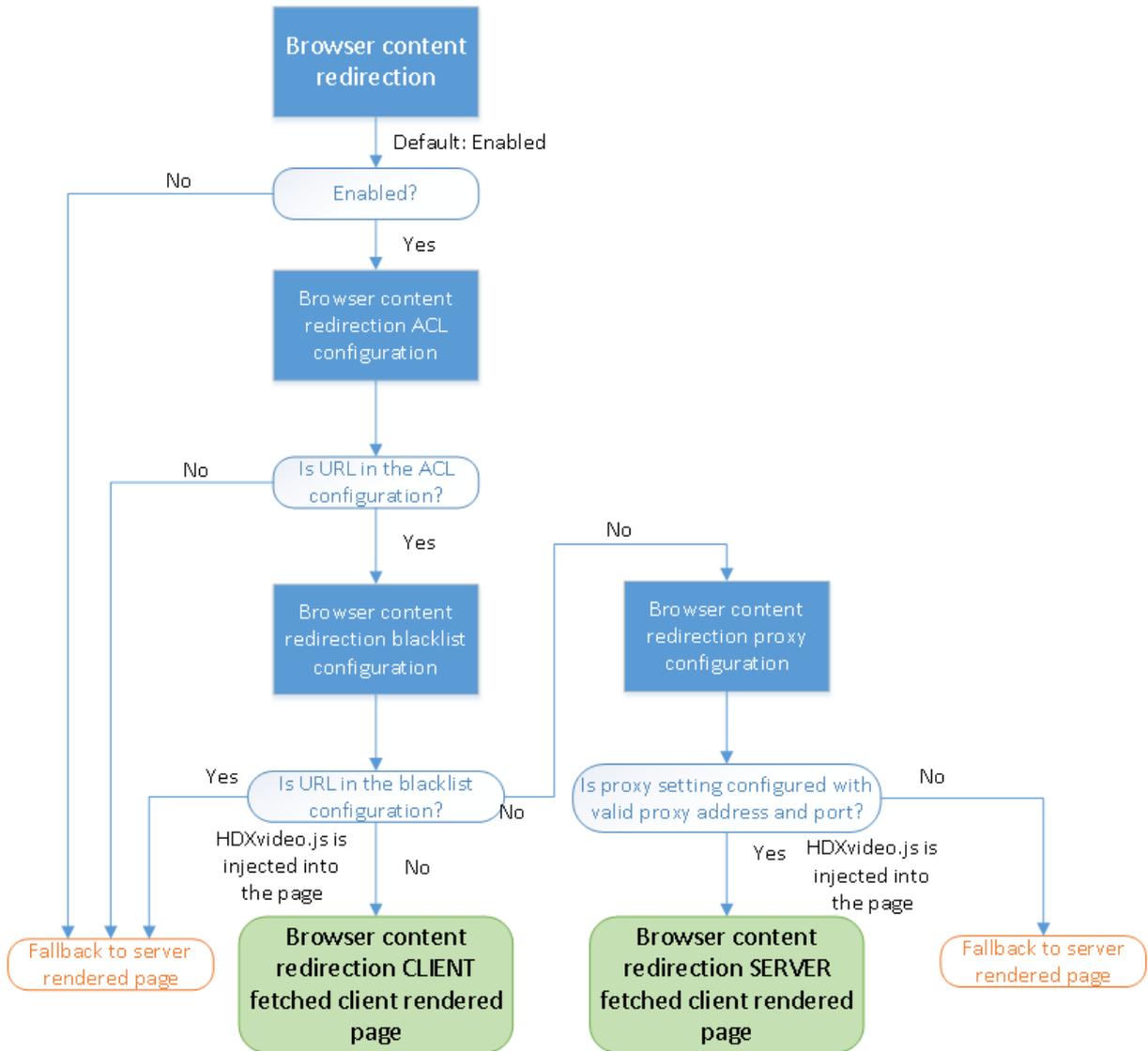
Opciones de anulación del Registro para configuraciones de directiva:

`\HKLM \SOFTWARE\Wow6432Node\Citrix\HdxMediastream`

Nombre	Tipo	Valor
WebBrowserRedirection	DWORD	1 = Permitido, 0 = Prohibido
WebBrowserRedirectionAcl	REG_MULTI_SZ	
WebBrowserRedirectionAuthenticationSites	REG_MULTI_SZ	
WebBrowserRedirectionProxyAddresses	REG_SZ	<code>http://myproxy.citrix.com:8080</code> <code>http://10.10.10.10:8888</code>
WebBrowserRedirectionBlacklist	REG_MULTI_SZ	



## Insertar HDXVideo.js para redirigir contenido del explorador web



HdxVideo.js se inserta en la página web mediante la redirección de contenido de la extensión de Chrome o el Objeto Auxiliar de Explorador (BHO) de Internet Explorer. El objeto BHO es un modelo de plug-in para Internet Explorer. Ofrece enlaces para las API de explorador web y permite que el plug-in acceda a Document Object Model (DOM) de la página para controlar la navegación.

El objeto BHO decide si insertar HdxVideo.js en una página determinada. La decisión se basa en directivas administrativas mostradas en el gráfico anterior.

Después de que se haya decidido insertar JavaScript y redirigir el contenido del explorador web al cliente, la página web del Internet Explorer presente en el VDA se queda vacía. Dejar vacío **document.body.innerHTML** elimina el cuerpo entero de la página web en el VDA. La página está lista para enviarse al cliente, donde se verá en el explorador superpuesto (Hdxbrowser.exe).

## Configuraciones de directiva de Sensores del cliente

February 6, 2020

La sección “Sensores del cliente” contiene configuraciones de directiva para controlar cómo se gestiona la información de sensor del dispositivo móvil en una sesión de usuario.

### Permitir que las aplicaciones usen la ubicación física del dispositivo cliente

Esta configuración determina si las aplicaciones que se ejecutan en la sesión de un dispositivo móvil pueden usar la ubicación física del dispositivo de usuario.

De forma predeterminada, no se permite el uso de la información de ubicación.

Cuando esta configuración está prohibida, los intentos de una aplicación por obtener información de ubicación tendrán como resultado “permiso denegado”.

Cuando esta configuración está permitida, el usuario puede prohibir el uso de la información de ubicación denegando la solicitud de la aplicación Citrix Workspace para acceder a la ubicación. Los dispositivos Android y iOS preguntan al usuario cuando solicitan información de ubicación por primera vez en cada sesión.

Al desarrollar aplicaciones alojadas que usan la configuración Permitir que las aplicaciones usen la ubicación física del dispositivo cliente, tenga en cuenta lo siguiente:

- Una aplicación que tenga información de ubicación habilitada no debe depender totalmente de la disponibilidad de dicha información porque:
  - Puede que un usuario no le permita acceder a la información de ubicación.
  - Es posible que la ubicación cambie o no esté disponible mientras se ejecuta la aplicación.
  - Un usuario puede conectarse a la sesión de la aplicación desde un dispositivo diferente que no ofrezca la información de ubicación.
- Una aplicación con información de ubicación habilitada debe:
  - Tener la función de ubicación inhabilitada de forma predeterminada.
  - Dar al usuario la opción de permitir o prohibir la función mientras se está ejecutando la aplicación.
  - Dar al usuario la opción de borrar la información de ubicación que almacena la aplicación en caché. (La aplicación Citrix Workspace no almacena en caché la información de ubicación.)
- Una aplicación con información de ubicación habilitada debe gestionar la complejidad de la información de ubicación, de manera que los datos obtenidos sean apropiados para los fines

de la aplicación en particular y cumplan con las normas aplicables en todas las jurisdicciones pertinentes.

- Aplicar una conexión segura (por ejemplo, con TLS o una red VPN) es imprescindible para usar los servicios de ubicación. Conecte la aplicación Citrix Workspace a servidores de confianza.
- Consulte la información legal referente al uso de servicios de ubicación.

## Configuraciones de directiva de Interfaz de usuario de escritorio

January 4, 2021

La sección “Interfaz de usuario de escritorio” contiene configuraciones que controlan los efectos visuales, como el papel tapiz del escritorio, las animaciones de menús y las imágenes de arrastrar y colocar, a fin de administrar el ancho de banda utilizado en las conexiones del cliente. Se puede mejorar el rendimiento sobre conexiones WAN limitando el uso de ancho de banda.

### Importante

En esta versión, no se admiten el modo de gráficos antiguos ni la redirección de composición del escritorio (DCR). Esa directiva se incluye solo para la compatibilidad con versiones anteriores cuando se usa XenApp 7.15 LTSR y XenDesktop 7.15 LTSR, así como las versiones anteriores de VDA con Windows 7 y Windows 2008 R2.

### Redirección de composición del escritorio

Esta configuración especifica si se debe usar la capacidad de procesamiento de la unidad de procesamiento de gráficos (GPU) o el procesador de gráficos integrado (IGP) en el dispositivo del usuario en la generación de gráficos locales de DirectX para proporcionar a los usuarios una experiencia de escritorio de Windows más fluida. Cuando está habilitada, Redirección de composición del escritorio proporciona una experiencia de Windows muy fluida y, al mismo tiempo, mantiene una alta escalabilidad en el servidor.

De forma predeterminada, Redirección de composición del escritorio está inhabilitada.

Para inhabilitar la redirección de composición del escritorio y reducir el ancho de banda necesario para las sesiones de usuario, seleccione Inhabilitada cuando agregue esta configuración a una directiva.

### Calidad de gráficos de composición del escritorio

Esta configuración especifica la calidad de los gráficos utilizados para la redirección de composición del escritorio.

El valor predeterminado es “Alta”.

Elija la calidad entre las opciones Alta, Media, Baja o Sin pérdida.

### **Tapiz del escritorio**

Esta configuración permite o evita que se muestre el tapiz del escritorio en las sesiones de los usuarios.

De forma predeterminada, las sesiones de usuario pueden mostrar el tapiz del escritorio.

Para inhabilitar el tapiz del escritorio y reducir el ancho de banda necesario para las sesiones de usuario, seleccione Prohibida cuando agregue esta configuración a una directiva.

### **Animación de menús**

Esta configuración permite o evita la animación de menús en las sesiones de los usuarios.

La animación de menús está permitida de forma predeterminada.

Animación de menús es una configuración de preferencia personal de Microsoft para facilitar el acceso. Cuando está habilitado, provoca que el menú aparezca tras una breve demora, ya sea con un desplazamiento o un fundido. Aparece un icono de flecha en la parte inferior del menú. El menú se muestra al apuntar a dicha flecha.

La animación de menús se habilita en un escritorio si esta configuración de directiva se define como Permitida y la configuración de preferencia personal de animación de menús de Microsoft está habilitada.

Nota: Los cambios en la configuración de preferencia personal de animación de menús de Microsoft son cambios hechos en el escritorio. Si el escritorio está configurado para descartar los cambios cuando finalice la sesión, un usuario que haya habilitado las animaciones de menú durante la sesión no verá animaciones de menú en sesiones subsiguientes en ese escritorio. Si los usuarios requieren animaciones de menú, habilite la configuración de Microsoft en la imagen maestra del escritorio para garantizar que el escritorio conserva los cambios del usuario.

### **Ver contenido de las ventanas al arrastrar**

Esta configuración permite o evita que se muestre el contenido de las ventanas al arrastrarlas por la pantalla.

La presentación del contenido de las ventanas está habilitada de forma predeterminada.

Si se establece en Permitida, parecerá que toda la ventana se mueve al arrastrarla. Si se establece en Prohibida, parecerá que solo los bordes se mueven hasta que se suelta la ventana.

## **Configuraciones de directiva de Supervisión de usuario final**

February 6, 2020

La sección Supervisión de usuario final contiene configuraciones de directiva para medir el tráfico de la sesión.

### **Cálculo del tiempo de retorno ICA**

Esta configuración determina si se realizan cálculos del tiempo de retorno ICA para las conexiones activas.

De forma predeterminada, los cálculos para las conexiones activas están habilitados.

De forma predeterminada, el inicio de cada medición de tiempo de retorno ICA espera hasta que se detecte tráfico que indique la interacción del usuario. La duración de esta espera puede ser indefinida y su función es evitar que se produzca tráfico ICA con el único fin de medir tiempos de retorno de ICA.

### **Intervalo de cálculo del tiempo de retorno ICA**

Esta configuración permite especificar la frecuencia, en segundos, para el cálculo del tiempo de retorno ICA.

De forma predeterminada, el tiempo de retorno ICA se calcula cada 15 segundos.

### **Cálculo del tiempo de retorno ICA para conexiones inactivas**

Esta configuración determina si se realizan cálculos del tiempo de retorno ICA para las conexiones inactivas.

De forma predeterminada, no se realizan cálculos para las conexiones inactivas.

De forma predeterminada, el inicio de cada medición de tiempo de retorno ICA espera hasta que se detecte tráfico que indique la interacción del usuario. La duración de esta espera puede ser indefinida y su función es evitar que se produzca tráfico ICA con el único fin de medir tiempos de retorno de ICA.

## **Configuración de directiva de Enhanced Desktop Experience**

February 6, 2020

Con la configuración de directiva Enhanced Desktop Experience, las sesiones que se ejecutan en sistemas operativos de servidor tienen el mismo aspecto que los escritorios locales con Windows 7, lo que proporciona a los usuarios una mejor experiencia de escritorio.

De forma predeterminada, esta configuración está permitida.

Si ya existe un perfil de usuario con el tema Windows clásico en el escritorio virtual, habilitar esta directiva no proporciona una mejor experiencia de escritorio para ese usuario. Si un usuario con un perfil con el tema Windows 7 inicia sesión en un escritorio virtual que ejecuta Windows Server 2012 para el que esta directiva esté sin configurar o inhabilitada, el usuario ve un mensaje de error que indica que no se pudo aplicar el tema.

En ambos casos, el problema se resuelve restableciendo el perfil de usuario.

Si la directiva cambia de habilitada a inhabilitada en un escritorio virtual con sesiones de usuario activas, la apariencia de las sesiones es inconsistente con la experiencia de escritorio de Windows 7 y Windows clásico. Para evitar este problema, debe reiniciar el escritorio virtual después de cambiar esta configuración de directiva. También debe eliminar los perfiles móviles del escritorio virtual. Citrix también recomienda eliminar otros perfiles de usuario del escritorio virtual a fin de evitar inconsistencias entre perfiles.

Si se utilizan perfiles de usuario móviles en el entorno, asegúrese de que la función Enhanced Desktop Experience está habilitada o inhabilitada para todos los escritorios virtuales que comparten un perfil.

Citrix no recomienda el uso compartido de los perfiles móviles entre los escritorios virtuales con sistemas operativos de servidor y de cliente. Los perfiles para sistemas operativos de cliente y sistemas operativos de servidor difieren y el uso compartido de perfiles móviles entre ambos tipos de SO puede dar lugar a incoherencias en las propiedades de los perfiles cuando el usuario pasa de uno a otro.

## **Configuraciones de directiva de Redirección de archivos**

February 6, 2020

La sección “Redirección de archivos” contiene configuraciones relacionadas con la asignación y la optimización de unidades del cliente.

### **Conectar automáticamente las unidades del cliente**

Esta configuración permite o impide la conexión automática de unidades del cliente cuando los usuarios inician sesión.

La conexión automática está permitida de forma predeterminada.

Cuando agregue esta configuración a una directiva, debe habilitar también las configuraciones correspondientes a los tipos de unidades que quiera que se conecten automáticamente. Por ejemplo, para permitir la conexión automática de las unidades de CD-ROM de los usuarios, use esta configuración y la configuración Unidades ópticas del cliente.

Configuraciones de directiva relacionadas:

- Redirección de unidades del cliente
- Unidades de disco flexible del cliente
- Unidades ópticas del cliente
- Unidades fijas del cliente
- Unidades de red del cliente
- Unidades extraíbles del cliente

## **Redirección de unidades del cliente**

Esta configuración habilita o inhabilita la redirección de archivos hacia el dispositivo del usuario y desde él.

De forma predeterminada, la redirección de archivos está habilitada.

### **Nota:**

La configuración de directiva de redirección de unidades del cliente no se aplica a las unidades asignadas a sesiones mediante redirección de USB genérico.

Si está habilitada, los usuarios pueden guardar archivos en todas las unidades del cliente. Si está inhabilitada, se impide cualquier redirección de archivos, independientemente del estado de las configuraciones individuales de redirección de archivos, como Unidades de disco flexible del cliente y Unidades de red del cliente.

Configuraciones de directiva relacionadas:

- Unidades de disco flexible del cliente
- Unidades ópticas del cliente
- Unidades fijas del cliente
- Unidades de red del cliente
- Unidades extraíbles del cliente

## **Unidades fijas del cliente**

Esta configuración permite o impide que los usuarios accedan a las unidades fijas del dispositivo del usuario o guarden archivos en ellas.

De forma predeterminada, el acceso a las unidades fijas del cliente está permitido.

Al agregar esta configuración a una directiva, compruebe que la configuración Redirección de unidades del cliente está presente y establecida en la opción Permitida. Si esta configuración está inhabilitada, no se asignan las unidades fijas del cliente y los usuarios no pueden acceder a ellas de forma manual, independientemente del estado de la configuración Unidades fijas del cliente.

Para garantizar que las unidades fijas se conecten automáticamente cuando los usuarios inician sesión, configure Conectar automáticamente las unidades del cliente.

### **Unidades de disco flexible del cliente**

Esta configuración permite o impide que los usuarios accedan a las unidades de disco flexible del dispositivo del usuario o guarden archivos en ellas.

De forma predeterminada, el acceso a las unidades de disco flexible del cliente está permitido.

Al agregar esta configuración a una directiva, compruebe que la configuración Redirección de unidades del cliente está presente y establecida en la opción Permitida. Si esta configuración está inhabilitada, no se asignan las unidades de disco flexible del cliente y los usuarios no pueden acceder a ellas de forma manual, independientemente del estado de la configuración Unidades de disco flexible del cliente.

Para garantizar que las unidades de disco flexible se conecten automáticamente cuando los usuarios inician sesión, configure Conectar automáticamente las unidades del cliente.

### **Unidades de red del cliente**

Esta configuración permite o impide que los usuarios accedan a las unidades de red (remotas) o guarden archivos en ellas mediante el dispositivo del usuario.

De forma predeterminada, el acceso a las unidades de red del cliente está permitido.

Al agregar esta configuración a una directiva, compruebe que la configuración Redirección de unidades del cliente está presente y establecida en la opción Permitida. Si esta configuración está inhabilitada, no se asignan las unidades de red del cliente y los usuarios no pueden acceder a ellas de forma manual, independientemente del estado de la configuración Unidades de red del cliente.

Para garantizar que las unidades de red se conecten automáticamente cuando los usuarios inician sesión, configure Conectar automáticamente las unidades del cliente.

### **Unidades ópticas del cliente**

Esta configuración permite o impide que los usuarios tengan acceso a las unidades de CD-ROM, DVD-ROM y BD-ROM en el dispositivo del usuario o guarden archivos en ellas.

De forma predeterminada, el acceso a las unidades ópticas del cliente está permitido.

Al agregar esta configuración a una directiva, compruebe que la configuración Redirección de unidades del cliente está presente y establecida en la opción Permitida. Si esta configuración está inhabilitada, no se asignan las unidades ópticas del cliente y los usuarios no pueden acceder a ellas de forma manual, independientemente del estado de la configuración Unidades ópticas del cliente.

Para garantizar que las unidades ópticas se conecten automáticamente cuando los usuarios inician sesión, configure Conectar automáticamente las unidades del cliente.

### **Unidades extraíbles del cliente**

Esta configuración permite o impide que los usuarios accedan a las unidades USB del dispositivo del usuario o guarden archivos en ellas.

De forma predeterminada, el acceso a las unidades extraíbles del cliente está permitido.

Al agregar esta configuración a una directiva, compruebe que la configuración Redirección de unidades del cliente está presente y establecida en la opción Permitida. Si esta configuración está inhabilitada, no se asignan las unidades extraíbles del cliente y los usuarios no pueden acceder a ellas de forma manual, independientemente del estado de la configuración Unidades extraíbles del cliente.

Para garantizar que las unidades extraíbles se conecten automáticamente cuando los usuarios inician sesión, configure Conectar automáticamente las unidades del cliente.

### **Redirección del host al cliente**

Esta configuración habilita o inhabilita las asociaciones de tipos de archivos para direcciones URL y contenido multimedia que se abren en el dispositivo del usuario. Si está inhabilitada, el contenido se abre en el servidor.

De forma predeterminada, la asociación de tipos de archivo está inhabilitada.

Cuando se habilita esta configuración, los siguientes tipos de direcciones URL se abren de forma local:

- Protocolo HTTP
- Protocolo HTTP seguro (HTTPS)
- Real Player y QuickTime (RTSP)
- Real Player y QuickTime (RTSPU)
- Real Player (PNM) antiguo
- Microsoft Media Server (MMS)

## **Conservar las letras de unidad del cliente**

Esta configuración habilita o inhabilita la asignación de unidades del cliente a la misma letra de unidad en la sesión.

De forma predeterminada, las letras de las unidades del cliente no se conservan.

Al agregar esta configuración a una directiva, compruebe que la configuración Redirección de unidades del cliente está presente y establecida en la opción Permitida.

## **Acceso de lectura solamente a unidades del cliente**

Esta configuración permite o impide que los usuarios y las aplicaciones creen o modifiquen archivos o carpetas en las unidades de cliente asignadas.

De forma predeterminada, los archivos y las carpetas en las unidades de cliente asignadas se pueden modificar.

Si se establece en Habilitada, se podrá acceder a los archivos y las carpetas con permisos de solo lectura.

Al agregar esta configuración a una directiva, compruebe que la configuración Redirección de unidades del cliente está presente y establecida en la opción Permitida.

## **Redirección de carpetas especiales**

Esta configuración permite o impide que los usuarios de la aplicación Citrix Workspace y de la Interfaz Web vean las carpetas especiales locales Documentos y Escritorio desde una sesión.

De forma predeterminada, la redirección de carpetas especiales está permitida.

Esta configuración impide la redirección de carpetas especiales para los objetos filtrados mediante una directiva, independientemente de las configuraciones de otras secciones. Cuando se prohíbe esta configuración, se omiten las configuraciones relacionadas especificadas para StoreFront, la Interfaz Web o la aplicación Citrix Workspace.

Para definir qué usuarios podrán usar la redirección de carpetas especiales, seleccione Permitida e incluya esta configuración en una directiva filtrada para los usuarios que desee. Esta configuración sobrescribe cualquier otra configuración de redirección de carpetas especiales.

Como la redirección de carpetas especiales interactúa con el dispositivo del usuario, las configuraciones de directiva que impiden que los usuarios accedan a sus discos duros locales o guarden archivos en ellos también impiden el funcionamiento de la redirección de carpetas especiales.

Al agregar esta configuración a una directiva, compruebe que la configuración “Unidades fijas del cliente” esté presente y establecida en Permitida.

## Usar escrituras asíncronas

Esta configuración habilita o inhabilita las escrituras asíncronas en los discos.

De forma predeterminada, las escrituras asíncronas están inhabilitadas.

En redes WAN, caracterizadas por mucho ancho de banda y latencia alta, las escrituras asíncronas pueden acelerar la transferencia de archivos y la escritura en los discos del cliente. Sin embargo, si hay un error de conexión o de disco, el archivo o los archivos del cliente que se vayan a escribir pueden terminar en un estado indefinido. Si esto sucede, aparecerá una ventana emergente con la lista de archivos afectados. El usuario puede entonces corregir el error, por ejemplo, puede reanudar la transferencia interrumpida de archivos al volver a conectarse o cuando se corrija el error en el disco.

Citrix recomienda habilitar la escritura asíncrona solamente para usuarios que necesiten conexiones remotas con buena velocidad de acceso a los archivos y en las que el usuario pueda recuperar fácilmente los archivos o datos perdidos cuando haya problemas de conexión o errores en el disco.

Al agregar esta configuración a una directiva, compruebe que la configuración Redirección de unidades del cliente está presente y establecida en la opción Permitida. Si esta configuración está inhabilitada, no se realizan escrituras asíncronas.

## Configuraciones de directiva de Gráficos

September 22, 2021

La sección Gráficos contiene configuraciones de directiva para controlar la gestión de imágenes en las sesiones de usuario.

### Permitir compresión sin pérdida visual

Esta configuración permite usar compresión sin pérdida visual en lugar de compresión sin pérdida verdadera para los gráficos. La compresión sin pérdida visual mejora el rendimiento en mayor medida que la compresión sin pérdida verdadera, con una pérdida menor que no se nota a la vista. Esta configuración cambia el modo en que se usan los valores de la configuración Calidad visual.

De forma predeterminada, esta configuración está inhabilitada.

### Indicador de estado de gráficos

Este parámetro definirá el indicador del estado de gráficos que se va a ejecutar en la sesión del usuario. Este indicador permite al usuario ver datos sobre el modo de gráficos que se está utilizando, incluido

el proveedor de gráficos, el codificador, la codificación por hardware, la calidad de imagen, el estado de pantalla progresiva y la compresión sin pérdida de texto.

De forma predeterminada, el indicador del modo de gráficos está inhabilitado. Esta configuración sustituye al indicador de compresión sin pérdida. En las versiones anteriores de Citrix Virtual Apps and Desktops, se habilita el indicador de compresión sin pérdida en lugar del indicador del modo de gráficos.

### **Limitación debido al tiempo de silencio de Microsoft:**

Después de habilitar el indicador de estado de los gráficos, puede producirse un problema la **primera vez** que un usuario inicia sesión en Citrix Virtual Apps and Desktops. Transcurren cuatro horas antes de que aparezca el icono del indicador de estado en el área de notificaciones.

### **Límite de memoria de presentación**

Esta configuración permite especificar el tamaño máximo de búfer para vídeo, en kilobytes, asignado a la sesión.

El límite de memoria de presentación predeterminado es de 65536 kilobytes.

Permite especificar el tamaño máximo de búfer para vídeo, en kilobytes, asignado a la sesión. Especifique una cifra en kilobytes de 128 a 4 194 303. El valor máximo (4,194,303) no limita la memoria de presentación. La memoria de presentación predeterminada es de 65536 kilobytes. Si se utiliza mayor profundidad de color y mayor resolución para las conexiones, se necesitará más memoria. En el modo de gráficos antiguos, si se alcanza el límite de memoria, la presentación se degrada según esté definida la configuración Preferencia de degradación de presentación.

Para las conexiones que requieran mayor profundidad de color y mayor resolución, aumente el límite. Puede calcular la memoria máxima necesaria con la siguiente ecuación:

Profundidad de memoria en bytes = (profundidad de color en bits por píxel) / 8 x (resolución vertical en píxeles) x (resolución horizontal en píxeles).

Por ejemplo, si la profundidad de color es 32, la resolución vertical es 600 y la resolución horizontal es 800, la memoria máxima necesaria es  $(32 / 8) \times (600) \times (800) = 1\,920\,000$  bytes, por lo que habría que establecer el límite de memoria de presentación en 1920 KB.

Las profundidades de color que no son de 32 bits solo están disponibles si la configuración de directiva Modo de gráficos antiguo está habilitada.

HDX asigna solo la cantidad de memoria de presentación necesaria para cada sesión. Por lo tanto, si tan solo algunos usuarios necesitan más memoria de la predeterminada, no hay ningún impacto negativo en la escalabilidad si se aumenta el límite de memoria de presentación.

## Preferencia de degradación de presentación

### Nota:

Para Virtual Delivery Agent 7.x, esta configuración de directiva solo se aplica cuando la configuración de directiva Modo de gráficos antiguo está habilitada.

Esta configuración permite especificar que la profundidad de color o la resolución sean las primeras funciones en degradarse cuando se alcance el límite de memoria para la presentación.

De forma predeterminada, se degrada primero la profundidad de color.

Cuando se alcanza el límite de memoria para presentación, se puede reducir la calidad de la imagen presentada e indicar si se degradará primero la profundidad de color o la resolución. Cuando se degrada primero la profundidad de color, se usan menos colores para las imágenes. Cuando se degrada primero la resolución, se muestran las imágenes con menos píxeles por pulgada.

Para notificar a los usuarios de la degradación de la profundidad de color o de la resolución, defina la configuración Notificar al usuario cuando se degrada la presentación.

## Vista previa de ventanas dinámicas

Esta configuración habilita o inhabilita la visualización de ventanas integradas en:

- Rotar (Flip)
- 3D rotado (Flip 3D)
- Vista previa de la barra de tareas
- Vistazo (Peek)

Opción de vista previa de Aero de Windows	Descripción
Vista previa de la barra de tareas	Cuando el usuario pasa el cursor sobre un icono de la barra de tareas de una ventana, se muestra una imagen de dicha ventana encima de la barra de tareas.
Vistazo (Peek)	Cuando el usuario pasa el cursor sobre una imagen de vista previa de la barra de tareas, se muestra una imagen en tamaño completo de dicha ventana en la pantalla.
Rotar (Flip)	Al presionar ALT+TAB, se muestran pequeños iconos de vista previa de cada ventana abierta.

Opción de vista previa de Aero de Windows	Descripción
3D rotado (Flip 3D)	Cuando el usuario presiona las teclas TAB+logotipo de Windows, se realiza una presentación en cascada de las ventanas abiertas en la pantalla.

De manera predeterminada, esta configuración está habilitada.

## Caché de imágenes

### Nota:

Para Virtual Delivery Agent 7.x, esta configuración de directiva solo se aplica cuando la configuración de directiva Modo de gráficos antiguo está habilitada.

Esta configuración habilita o inhabilita el almacenamiento en caché y la recuperación de secciones de imágenes en las sesiones. El almacenamiento en caché de secciones de imágenes y su recuperación a medida que se necesitan, permite que el desplazamiento por la imagen sea más suave, reduce la cantidad de datos transmitidos por la red y reduce el procesamiento necesario en el dispositivo del usuario.

De forma predeterminada, el almacenamiento en caché de imágenes está habilitado.

### Nota:

La configuración de almacenamiento en caché de imágenes controla el modo en que se almacenan y se obtienen las imágenes. La configuración no controla si las imágenes se almacenan en caché. Las imágenes se almacenan en caché si la configuración Modo de gráficos antiguo está habilitada.

## Modo de gráficos antiguo: no se admite. Solo para la compatibilidad con versiones anteriores

### Importante:

En esta versión, no se admiten el modo de gráficos antiguos ni la redirección de composición del escritorio (DCR). Esa directiva se incluye solo para la compatibilidad con versiones anteriores cuando se usa XenApp 7.15 LTSR y XenDesktop 7.15 LTSR, así como las versiones anteriores de VDA con Windows 7 y Windows 2008 R2.

Esta configuración inhabilita la experiencia de gráficos enriquecidos. Utilice esta opción para volver a la experiencia de gráficos antiguos, que reduce el consumo de ancho de banda por WAN o una conex-

ión móvil. Las reducciones de ancho de banda introducidas en XenApp y XenDesktop 7.13 hacen obsoleto este modo.

De forma predeterminada, esta configuración está inhabilitada y los usuarios reciben la experiencia gráfica completa.

El modo de gráficos antiguo se admite en los VDA con Windows 7 y Windows Server 2008 R2.

El modo de gráficos antiguo no se admite en Windows 8.x, 10 o Windows Server 2012, 2012 R2 y 2016.

Consulte [CTX202687](#) para ver más información sobre la optimización de los modos de gráficos y directivas en XenApp y XenDesktop 7.6 FP3 o versiones posteriores.

## Profundidad de color máxima permitida

### Nota:

Para Virtual Delivery Agent 7.x, esta configuración de directiva solo se aplica cuando la configuración de directiva Modo de gráficos antiguo está habilitada.

Esta configuración permite especificar la profundidad de color máxima permitida para una sesión.

De manera predeterminada, la profundidad de color máxima permitida es de 32 bits por píxel.

Esta configuración se aplica solo a conexiones y controladores Thinwire. No se aplica a agentes VDA que tienen un controlador de pantalla principal que no sea Thinwire, como los agentes VDA que usan un controlador Windows Display Driver Model (WDDM) en calidad de controlador de pantalla principal. Para agentes VDA con SO de sesión única que utilicen un controlador WDDM como controlador de pantalla principal (como Windows 8), esta configuración no tiene ningún efecto. Para agentes VDA con SO multisesión Windows que utilicen un controlador WDDM (como Windows Server 2012 R2), esta configuración puede impedir que los usuarios se conecten a los VDA.

Una mayor profundidad de color requerirá más memoria. Para que se degrade la profundidad de color cuando se alcanza el límite de memoria, configure el parámetro **Preferencia de degradación de presentación**. Cuando se degrada la profundidad de color, se usan menos colores para las imágenes.

## Notificar al usuario cuando se degrada la presentación

### Nota:

Para Virtual Delivery Agent 7.x, esta configuración de directiva solo se aplica cuando la configuración de directiva Modo de gráficos antiguo está habilitada.

Esta configuración muestra al usuario una breve explicación cuando se degrada la profundidad de color o la resolución.

De forma predeterminada, estas notificaciones están inhabilitadas.

### **Optimizar para cargas de trabajo de gráficos 3D**

Esta configuración define la configuración predeterminada que mejor se ajuste a cargas de trabajo con muchos gráficos. Habilite esta configuración para usuarios cuyas cargas de trabajo se centren en aplicaciones ricas en gráficos. Aplique esta directiva solo en situaciones donde haya una GPU disponible en la sesión. Tiene prioridad cualquier otra configuración que anule explícitamente la configuración predeterminada establecida por esta directiva.

De forma predeterminada, la configuración “Optimizar para cargas de trabajo de gráficos 3D” está inhabilitada.

### **Cola y descarte**

**Nota:**

Para Virtual Delivery Agent 7.x, esta configuración de directiva solo se aplica cuando la configuración de directiva Modo de gráficos antiguo está habilitada.

Esta configuración descarta las imágenes en cola que reemplaza otra imagen.

De manera predeterminada, la configuración “Cola y descarte” está habilitada.

Esta configuración mejora la respuesta cuando se envían elementos gráficos al dispositivo del usuario. Esta configuración puede hacer que las animaciones aparezcan entrecortadas debido a fotogramas descartados.

### **Usar códec de vídeo para compresión**

Permite el uso de un códec de vídeo para comprimir gráficos cuando la decodificación de vídeo está disponible en el punto final. Si selecciona **Para la pantalla entera**, el códec de vídeo se aplica como el códec predeterminado para todo. Si selecciona **Para áreas en cambio constante**, el códec de vídeo se usa para las áreas donde haya cambios constantes en pantalla, mientras que para los demás datos se usa la compresión de imágenes estáticas y la memoria caché de mapas de bits. Cuando la decodificación de vídeo no está disponible en el punto final, o bien cuando se especifica la opción **No usar códec de vídeo**, se utilizan la compresión de imágenes estáticas y la memoria caché de mapas de bits. Si se selecciona **Usar códec de vídeo si se prefiere**, el sistema elige en función de varios factores. Los resultados pueden variar entre las versiones, ya que se mejora el método de selección.

Seleccione **Usar códec de vídeo si se prefiere** para permitir que el sistema elija la configuración más apropiada para la situación actual.

Seleccione **Para la pantalla entera** para optimizar el ancho de banda y la experiencia del usuario, especialmente cuando haya un uso intensivo de vídeo y gráficos 3D generados en el servidor.

Seleccione **Para áreas en cambio constante** para optimizar el rendimiento del vídeo, especialmente en entornos con poco ancho de banda, mientras mantiene la posibilidad de escalabilidad para contenido estático y de cambio lento. Esta configuración se admite en implementaciones de varios monitores.

Seleccione **No usar códec de vídeo** para optimizar la carga de la CPU del servidor y para casos donde no haya muchos vídeos ni aplicaciones de gráficos generados en el servidor.

El valor predeterminado es **Usar si se prefiere**.

### Uso de codificación por hardware para vídeo

Esta configuración permite el uso de hardware de gráficos, si está disponible, para comprimir los elementos en pantalla con el códec de vídeo. Si no está disponible, el VDA recurre a la codificación basada en CPU con el códec de vídeo del software.

La opción predeterminada de esta configuración de directiva es **Habilitada**.

Se admiten varios monitores.

Con la codificación por hardware, se puede usar cualquier aplicación Citrix Workspace que admita la decodificación de vídeo.

### NVIDIA

Para las GPU de NVIDIA GRID, la codificación por hardware se admite en agentes VDA para SO de sesión única y SO multisesión.

Las GPU de NVIDIA deben admitir la codificación por hardware NVENC. Consulte [NVIDIA video codec SDK](#) para ver una lista de las GPU admitidas.

NVIDIA GRID requiere la versión 3.1 o posterior de controlador. NVIDIA Quadro requiere la versión 362.56 o posterior de controlador. Citrix recomienda usar los controladores de la rama R361 de NVIDIA.

La función “Sin pérdida de texto” no es compatible con la codificación por hardware NVENC. Si ha habilitado el texto sin pérdida, este tiene prioridad sobre la codificación por hardware de NVENC.

Se admite el uso selectivo del códec de hardware H.264 para áreas en cambio constante.

Se admite la compresión sin pérdida visual (4:4:4). La compresión sin pérdida visual (en la directiva de gráficos, la configuración [Permitir compresión sin pérdida visual](#)) requiere la aplicación Citrix Workspace 1808 o posterior, o Citrix Receiver para Windows 4.5 o versiones posteriores.

## Intel

Para procesadores de gráficos Intel Iris Pro, la codificación por hardware se admite en agentes VDA para SO de sesión única y para SO multisesión.

Se admiten los procesadores de gráficos Intel Iris Pro de la [familia de procesadores Intel Broadwell](#) y versiones posteriores. Se necesita la versión 1.0 del SDK de Intel Remote Displays, que se puede descargar del sitio web de Intel: [Remote Displays SDK](#).

Sin pérdida de texto solo se admite cuando la directiva “Código de vídeo” está configurada para toda la pantalla, y la directiva **Optimizar para cargas de trabajo de gráficos 3D** está inhabilitada.

No se admite la compresión sin pérdida visual (YUV 4:4:4).

El codificador Intel ofrece una buena experiencia de usuario para un máximo de ocho sesiones de codificación (por ejemplo, un usuario con ocho monitores u ocho usuarios con un monitor cada uno). Si se requieren más de ocho sesiones de codificación, consulte la cantidad de monitores a los que se conecta la máquina virtual. Para mantener una buena experiencia de usuario, el administrador puede definir esta configuración de directiva por usuario o por máquina.

## AMD

Para AMD, la codificación por hardware se admite en los VDA para SO de sesión única.

Las GPU de AMD deben admitir el SDK de RapidFire. Por ejemplo, las GPU Radeon Pro o FirePro de AMD.

Para que la codificación funcione, debe instalar los controladores de AMD más recientes. Puede descargarlos en <https://www.amd.com/en/support>.

La función “Sin pérdida de texto” no es compatible con la codificación por hardware de AMD. Si ha habilitado el texto sin pérdida, este tiene prioridad sobre la codificación por hardware de AMD.

Se admite el uso selectivo del códec de hardware H.264 para áreas en cambio constante.

## Configuraciones de directiva de Almacenamiento en caché

February 6, 2020

La sección Almacenamiento en caché contiene configuraciones de directiva que permiten el almacenamiento en caché de los datos de imágenes en los dispositivos de usuario cuando el ancho de banda es limitado en las conexiones con el cliente.

### **Umbral de caché persistente**

Nota: Para Virtual Delivery Agent 7.x, esta configuración de directiva solo se aplica cuando la configuración de directiva Modo de gráficos antiguo está habilitada.

Esta configuración almacena en caché los mapas de bits en las unidades de disco duro del dispositivo del usuario. Esto permite la reutilización de imágenes grandes de sesiones anteriores que se usan con frecuencia.

De manera predeterminada, el valor umbral es de 3000000 bits por segundo.

Este valor representa el umbral por debajo del cual tendrá efecto la función de caché persistente. Es decir, con el valor predeterminado, los mapas de bits se almacenan en caché en el disco duro del dispositivo del usuario cuando el ancho de banda está por debajo de 3000000 bps.

## **Configuraciones de directiva de Framehawk**

September 22, 2021

### **Importante:**

A partir de Citrix Virtual Apps and Desktops 7 1903, Framehawk ya no se admite. En su lugar, utilice [Thinwire](#) con el [transporte adaptable](#) habilitado.

La sección Framehawk contiene configuraciones de directiva para habilitar y configurar el canal de presentación Framehawk en el servidor.

### **Canal de presentación Framehawk**

Cuando se habilita, el servidor intenta usar el canal virtual Framehawk para la presentación remota de entradas y gráficos del usuario. Ese canal de presentación usará UDP para ofrecer una mejor experiencia de usuario en redes con grandes pérdidas de paquetes y latencia alta. Sin embargo, también puede utilizar más recursos y ancho de banda del servidor que otros modos gráficos.

De forma predeterminada, el canal de presentación Framehawk está inhabilitado.

## **Intervalo de puertos del canal de presentación Framehawk**

Esta configuración de directiva permite especificar el intervalo de números de puerto UDP (con el formato *número de puerto más bajo, número de puerto más alto*) que el VDA utiliza para intercambiar datos del canal de presentación Framehawk con el dispositivo de usuario. El agente VDA intenta utilizar todos los puertos, comenzando por el de número más bajo y subiendo en cada intento subsiguiente. El puerto gestiona el tráfico de entrada y salida.

De forma predeterminada, el intervalo de puertos es 3224,3324.

## **Configuraciones de directiva de Keep Alive**

February 6, 2020

La sección Keep Alive contiene configuraciones de directiva para gestionar los mensajes de ICA Keep Alive.

### **Tiempo de espera de ICA Keep Alive**

Esta configuración permite especificar cuántos segundos deben transcurrir entre los mensajes sucesivos de ICA Keep Alive.

El intervalo predeterminado para los mensajes de Keep Alive es de 60 segundos.

Especifique un intervalo entre 1 y 3600 segundos para el envío de mensajes de ICA Keep Alive. No configure esto si tiene un software de supervisión de red que se encarga de cerrar las conexiones inactivas.

### **ICA Keep Alive**

Esta configuración habilita o inhabilita el envío periódico de mensajes de ICA Keep Alive.

De manera predeterminada, no se envían mensajes de Keep Alive.

Si se habilita esta configuración, se evita la desconexión de las conexiones interrumpidas. Si el servidor no detecta ninguna actividad, esta configuración evita que los Servicios de Escritorio remoto (RDS) desconecten la sesión. El servidor envía mensajes de Keep Alive cada pocos segundos para detectar si la sesión está activa. Si la sesión ya no está activa, el servidor la marca como desconectada.

La función ICA Keep Alive no funciona si se usa Fiabilidad de la sesión. Configure ICA Keep Alive únicamente para conexiones que no usen Fiabilidad de la sesión.

Configuraciones de directiva relacionadas: Conexiones de fiabilidad de la sesión.

## Configuraciones de directiva de Acceso a aplicaciones locales

March 1, 2021

La sección “Acceso a aplicaciones locales” contiene configuraciones de directiva para gestionar la integración de las aplicaciones de los usuarios instaladas localmente con las aplicaciones alojadas en un entorno de escritorios alojados.

### Permitir acceso a aplicaciones locales

Esta configuración permite o impide la integración de las aplicaciones de usuarios instaladas localmente con las aplicaciones alojadas en un entorno de escritorios alojados.

Cuando un usuario inicia una aplicación instalada localmente, la aplicación parece ejecutarse en su escritorio virtual, aunque en realidad se está ejecutando de forma local.

Si **habilita** la configuración de directiva **Permitir acceso a aplicaciones locales**, no se admite la redirección de contenido del explorador web.

De forma predeterminada, el acceso a aplicaciones locales está prohibido.

### Lista de bloqueados de redirección de URL

Esta configuración especifica los sitios web que se redirigen y se inician en el explorador web local. Pueden incluirse los sitios web que requieren información regional (como msn.com o news-google.com), o bien, sitios web con contenido multimedia enriquecido que se genera mejor en el dispositivo del usuario.

De forma predeterminada, no hay ningún sitio especificado.

### Lista de permitidos de redirección de URL

Esta configuración especifica los sitios web que se generan en el entorno en que se inician.

De forma predeterminada, no hay ningún sitio especificado.

## Configuraciones de directiva de Experiencia móvil

February 6, 2020

La sección Experiencia móvil contiene configuraciones de directiva para la gestión de Citrix Mobility Pack.

### **Presentación automática del teclado**

Esta configuración habilita o inhabilita la presentación automática del teclado en las pantallas de los dispositivos móviles.

De manera predeterminada, la presentación automática del teclado está inhabilitada.

### **Iniciar escritorio con optimización táctil**

Esta configuración está inhabilitada y no está disponible para máquinas Windows 10 o Windows Server 2016.

Esta configuración determina el comportamiento general de la interfaz de la aplicación Citrix Workspace, ya que permite o prohíbe una interfaz táctil intuitiva, optimizada para dispositivos tipo tableta.

De forma predeterminada, se utiliza una interfaz táctil intuitiva.

Para usar solo la interfaz de Windows, defina esta configuración de directiva como Prohibida.

### **Control remoto de cuadros combinados**

Esta configuración determina los tipos de cuadros combinados que se pueden ver en sesiones de dispositivos móviles. Para mostrar el control de cuadros combinados nativo del dispositivo, defina esta configuración de directiva como Permitida. Cuando esta configuración está permitida, un usuario puede cambiar el parámetro en la sesión de la aplicación Citrix Workspace para iOS y utilizar el cuadro combinado de Windows.

De forma predeterminada, la función Control remoto de cuadros combinados está prohibida.

## **Configuraciones de directiva de Multimedia**

June 27, 2024

La sección Multimedia contiene configuraciones de directiva para gestionar la transmisión por streaming de audio y vídeo HTML5 y Windows a las sesiones de usuario.

### **Advertencia**

Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si usa el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

### **Directivas de Multimedia**

De forma predeterminada, todas las directivas de Multimedia establecidas en Delivery Controller se almacenan en estos registros:

Directivas de máquina:

```
HKEY_LOCAL_MACHINE\Software\Policies\Citrix\MultimediaPolicies
```

Directivas de usuario:

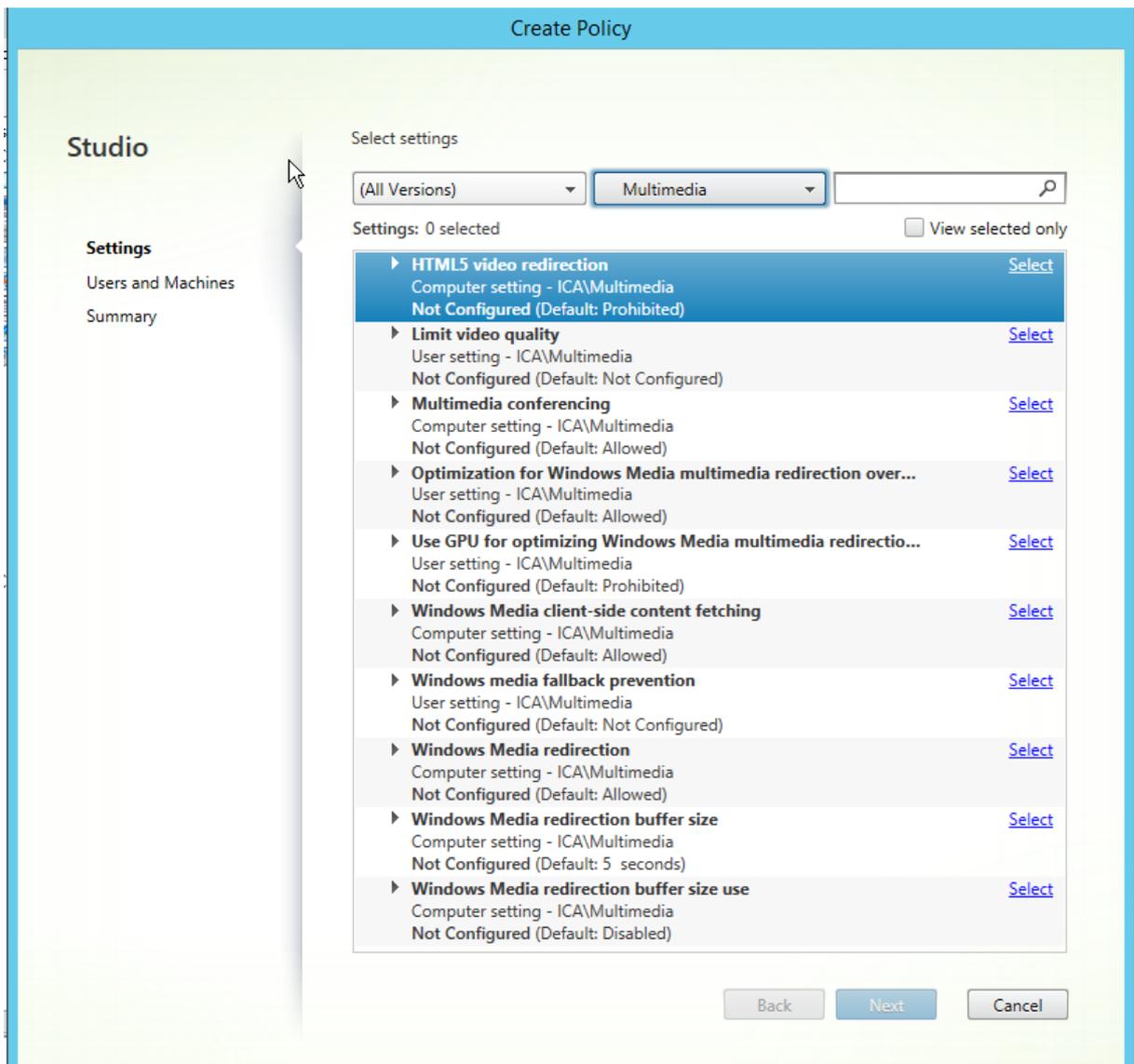
```
HKEY_LOCAL_MACHINE\Software\Policies\Citrix{ User Session ID } \User\MultimediaPolicies
```

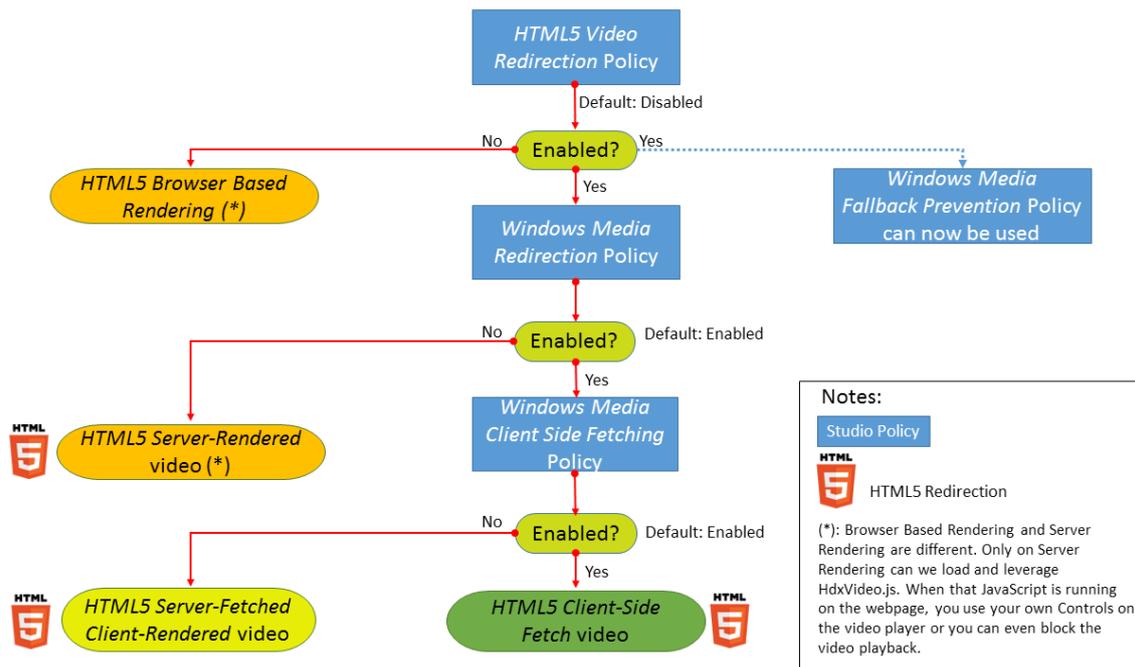
Para buscar el ID de sesión del usuario actual (User Session ID), emita el comando **qwinsta** desde la línea de comandos de Windows.

### **Redirección de vídeo HTML5**

Controla y optimiza el modo en que los servidores de Citrix Virtual Apps and Desktops entregan contenido multimedia web de HTML5 a los usuarios.

De forma predeterminada, esta configuración está inhabilitada.





En esta versión, esta funcionalidad está disponible solo para las páginas web controladas. Requiere agregar JavaScript a las páginas web que tengan contenido multimedia para HTML5 disponible; por ejemplo, vídeos en un sitio interno de formación.

Para configurar la redirección de vídeo HTML5:

1. Copie el archivo **HdxVideo.js** de %Archivos de programa%/Citrix/ICA Service/HTML5 Video Redirection en la instalación del VDA a la ubicación de la página web interna.
2. Inserte esta línea en la página web (si la página web tiene otros scripts, incluya **HdxVideo.js** antes de ellos):

```
<script src="HdxVideo.js" type="text/javascript"></script>
```

**Nota:** Si HdxVideo.js no está en la misma ubicación que la página web, utilice el atributo **src** para especificar la ruta completa a él.

Si no se agrega JavaScript a las páginas web controladas y el usuario reproduce un vídeo HTML5, Citrix Virtual Apps and Desktops recurrirán a la generación en el lado del servidor.

Debe estar permitida la **Redirección de Windows Media** para que la Redirección de vídeo HTML5 funcione correctamente. Esta directiva es obligatoria para Obtención en servidor, generación en cliente, y es necesaria para Obtención del lado del cliente (que a su vez requiere que *Obtención de contenido de Windows Media en el lado del cliente* esté permitida).

Microsoft Edge no admite esta función.

HdxVideo.js reemplaza los controles del reproductor HTML5 del explorador por los suyos propios. Para comprobar que la directiva Redirección de vídeo HTML5 está en vigor para un determinado sitio

web, compare los controles del reproductor con un caso en que la directiva **Redirección de vídeo HTML5** está prohibida:

(Controles personalizados de Citrix cuando la directiva está permitida)



(Controles nativos de la página web cuando la directiva está prohibida o no configurada)



Se pueden usar los siguientes controles de vídeo:

- reproducir
- pausa
- buscar
- repetir
- audio
- pantalla completa

Dispone de una página para pruebas de redirección de vídeo HTML5 en <https://www.citrix.com/solutions/html5-redirect.html>.

## **TLS, la redirección de vídeo HTML5 y la redirección de contenido del explorador web**

Puede utilizar la redirección de vídeo HTML5 para redirigir vídeos desde sitios web HTTPS o la redirección de contenido del explorador para redirigir todo el sitio web. El JavaScript insertado en esos sitios web debe establecer una conexión TLS al servicio Citrix HDX HTML5 Video Redirection Service (WebSocketService.exe) que se ejecuta en el VDA. Para conseguir esta redirección y mantener la integridad TLS de la página web, el servicio Citrix HDX HTML5 Video Redirection Service genera dos certificados personalizados en el almacén de certificados del VDA.

HdxVideo.js utiliza Secure WebSockets para comunicarse con WebSocketService.exe que se ejecuta en el VDA. Este proceso se ejecuta como una cuenta del sistema local y realiza la terminación SSL y la asignación de sesiones de usuario.

WebSocketService.exe escucha en 127.0.0.1 en el puerto 9001.

## **Límite de calidad de vídeo**

Esta configuración solo se aplica a Windows Media, no a HTML5. Requiere que habilite **Optimización de la redirección de medios de Windows Media sobre WAN**.

Esta configuración especifica el nivel máximo de calidad de vídeo permitido para una conexión HDX. Cuando está configurado, se limita la calidad de vídeo al valor especificado, por lo que se mantiene la Calidad de servicio (QoS) multimedia en un entorno.

De manera predeterminada, esta configuración no está definida.

Para limitar el nivel de calidad de vídeo permitido, elija una de las siguientes opciones:

- 1080p/8,5 Mbps
- 720p/4,0 Mbps
- 480p/720 kbps
- 380p/400 kbps
- 240p/200 kbps

La reproducción de varios vídeos simultáneamente en el mismo servidor consume muchos recursos y puede afectar a la escalabilidad del servidor.

### **Redirección de Microsoft Teams**

Este parámetro permite la optimización de Microsoft Teams, basada en la tecnología HDX.

**Edit Setting**

**Microsoft Teams redirection**

Allowed  
This setting will be allowed.

Prohibited  
This setting will be prohibited.

▼ **Applies to the following VDA versions**  
Virtual Delivery Agent: 1906 Server OS, 1906 Desktop OS

▼ **Description**  
Controls and optimizes the way Citrix Virtual Apps and Desktops servers deliver Microsoft Teams multimedia content to users.

Only multimedia content is redirected to the user's client machine, where it is decoded locally, effectively offloading all CPU, RAM, GPU, I/O, and bandwidth processing from the VDA to the endpoint.

In addition to this policy, the appropriate version of Citrix Workspace app is required for Microsoft Teams redirection to occur.

For more information and troubleshooting, see Knowledge Center article CTX253754.

**OK** **Cancel**

Si esta directiva está habilitada y está utilizando una versión compatible de la aplicación Citrix Workspace, esta clave del Registro se establece en **1** en el VDA. La aplicación Microsoft Teams lee la clave para cargar en modo VDI.

Tenga en cuenta que no es necesario establecer manualmente la clave de Registro.

HKEY\_CURRENT\_USER\Software\Citrix\HDXMediaStream

Nombre: MSTeamsRedirSupport

Valor: DWORD (1: activado, 0: desactivado)

**Nota:**

Si utiliza agentes VDA de la versión 1906.2 o posterior con versiones anteriores de Controller (por ejemplo, la versión 7.15), que no tienen la directiva disponible en Studio, la optimización HDX está habilitada de forma predeterminada en el VDA. Si la versión de la aplicación Workspace es 1907 o posterior, Teams se inicia en modo optimizado.

En este caso, para inhabilitar la función en usuarios específicos, puede anular el parámetro del Registro mediante una directiva de grupo para aplicar un script de inicio de sesión a la unidad organizativa del usuario.

De forma predeterminada, la redirección de Microsoft Teams está habilitada.

## Conferencia multimedia

Esta configuración permite o impide el uso de tecnología optimizada de redirección para cámara web mediante aplicaciones de conferencias de vídeo.

De forma predeterminada, se admiten las conferencias de vídeo.

Al agregar esta configuración a una directiva, compruebe que la configuración Redirección de Windows Media esté presente y establecida en Permitida (opción predeterminada).

Si usa conferencias multimedia, compruebe que se cumplen las siguientes condiciones:

- Los controladores del fabricante para la cámara web que se va a utilizar para las conferencias multimedia están instalados en el cliente.
- Conecte la cámara web al dispositivo del usuario antes de iniciar una sesión de conferencia de vídeo. El servidor utiliza solamente una cámara web instalada a la vez. Si hay varias cámaras web instaladas en el dispositivo del usuario, el servidor intenta usar una cámara tras otra hasta que logra crear una sesión de conferencia de vídeo.

Esta directiva no es necesaria cuando la cámara web se redirige mediante la redirección de USB genérico. En ese caso, instale los controladores de la cámara web en el VDA.

## Optimización de la redirección de medios de Windows Media sobre WAN

Esta configuración solo se aplica a Windows Media, no a HTML5. Este parámetro permite la transcodificación multimedia en tiempo real, lo que permite la transmisión por streaming de medios de audio y vídeo a dispositivos móviles en condiciones degradadas de red y mejora la experiencia del usuario al mejorar la entrega del contenido de Windows Media a través de redes WAN.

De forma predeterminada, la entrega de contenido de Windows Media a través de WAN está optimizada.

Al agregar este parámetro a una directiva, compruebe que el parámetro **Redirección de Windows Media** esté presente y establecido en **Permitido**.

Cuando este parámetro está habilitado, la transcodificación de multimedia en tiempo real se implementa automáticamente según sea necesario para la transmisión multimedia por streaming y proporciona una experiencia de usuario fluida incluso en condiciones de conexión extremas.

## Usar GPU para optimizar redirección de medios de Windows Media sobre WAN

Esta configuración solo se aplica a Windows Media y permite que la transcodificación multimedia en tiempo real se realice en la unidad de procesamiento de gráficos (GPU) en el Virtual Delivery Agent (VDA). Lo que mejora la escalabilidad del servidor. La transcodificación de GPU solo está disponible si el VDA tiene una GPU compatible para la aceleración por hardware. De lo contrario, la transcodificación recurre a la CPU.

**Nota:** La transcodificación de GPU solo se admite en las GPU de NVIDIA.

De forma predeterminada, el uso de la GPU en el VDA para optimizar la entrega de contenido de Windows Media a través de WAN está prohibido.

Al agregar esta configuración a una directiva, compruebe que las configuraciones Redirección de Windows Media y Optimización de la redirección de medios de Windows Media sobre WAN estén presentes y establecidas como Permitidas.

## Prevención de reserva de Windows Media

Esta configuración se aplica a la redirección de contenido del explorador, HTML5 y Windows Media. Para que funcione con HTML5, establezca la directiva **Redirección de vídeo HTML5** en **Permitida**.

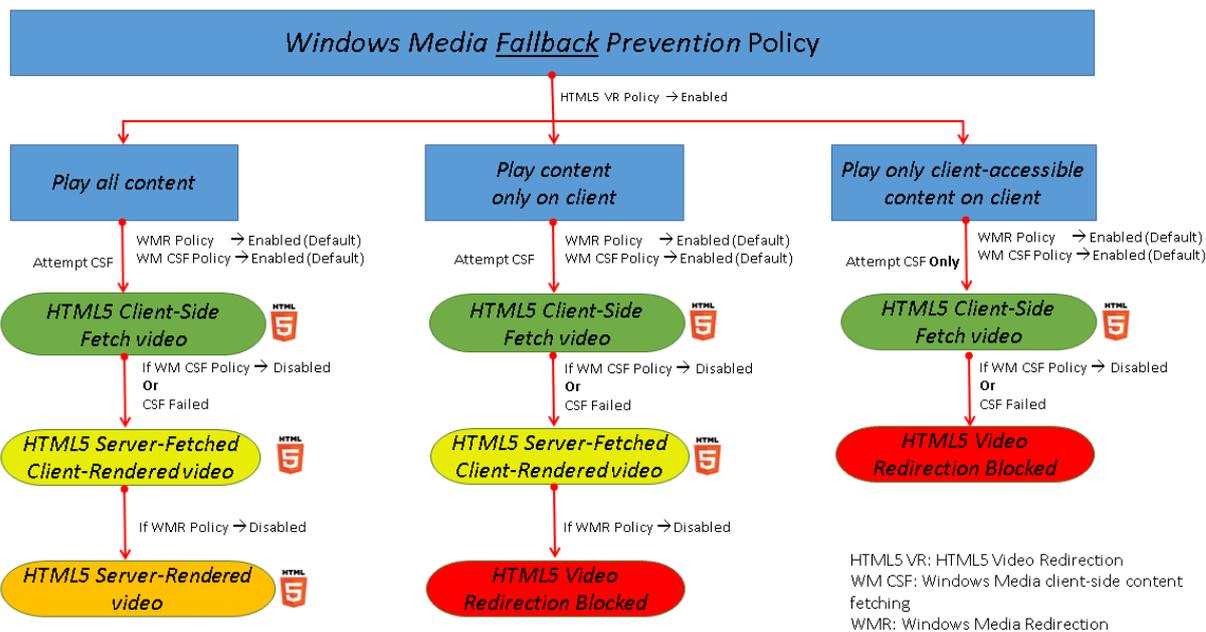
Los administradores pueden usar la directiva Prevención de reserva de Windows Media para especificar los métodos que se utilizarán para entregar contenido por streaming a los usuarios.

De manera predeterminada, esta configuración no está definida. Cuando la configuración está establecida en No configurada, el comportamiento es el mismo que **Reproducir todo el contenido**.

Para definir esta configuración, elija alguna de estas opciones:

- **Reproducir todo el contenido.** Intentar obtener contenido del lado del cliente; luego Redirección de Windows Media. Si no se realiza correctamente, reproducir contenido en el servidor.
- **Reproducir todo el contenido solo en el cliente.** Intentar obtener contenido del lado del cliente; luego Redirección de Windows Media. Si no se realiza correctamente, no se reproduce el contenido.
- **Reproducir solo el contenido accesible por el cliente.** Solo intentar la obtención de contenido del lado del cliente. Si no se realiza correctamente, no se reproduce el contenido.

Si el contenido no se reproduce, aparece el mensaje de error “La empresa ha bloqueado el vídeo debido a falta de recursos” en la ventana del reproductor (durante un período predeterminado de 5 segundos).



La duración de este mensaje de error puede ajustarse con la siguiente clave de Registro en el VDA. Si no existe la entrada del Registro, se usa la duración predeterminada (5 segundos).

La ruta del Registro varía en función de la arquitectura del VDA:

\HKLM\SOFTWARE\Wow6432Node\Citrix\HdxMediastream

o

\HKLM\SOFTWARE\Citrix\HdxMediastream

Clave del Registro:

Nombre: VideoLoadManagementErrDuration

Tipo: DWORD

Intervalo: 1 - hasta el límite DWORD (predeterminado = 5)

Unidad: segundos

### Obtención de contenido de Windows Media en el lado del cliente

Esta configuración se aplica a Windows Media y HTML5. Esta configuración permite a un dispositivo de usuario distribuir por streaming los archivos multimedia directamente desde su proveedor de origen en Internet o la intranet, en vez de hacerlo a través del servidor host de XenApp o XenDesktop.

De forma predeterminada, esta configuración está **permitida**. Cuando se habilita esta configuración, se mejora el uso de la red y la escalabilidad del servidor porque se transfiere el procesamiento del

medio desde el servidor host al dispositivo del usuario. También elimina la necesidad de tener instalado un software de infraestructura multimedia avanzado, como Microsoft DirectShow o Media Foundation, en el dispositivo del usuario; el dispositivo del usuario requiere solo la capacidad de reproducir un archivo a partir de una URL.

Al agregar este parámetro a una directiva, compruebe que el parámetro **Redirección de Windows Media** esté presente y establecido en **Permitido**. Si **Redirección de Windows Media** está inhabilitada, también está inhabilitada la distribución por streaming de archivos multimedia al dispositivo del usuario directamente desde el proveedor de origen.

### **Redirección de Windows Media**

Esta configuración se aplica a HTML5 y Windows Media. Controla y optimiza el modo en que los servidores entregan audio y vídeo por streaming a los usuarios.

De forma predeterminada, esta configuración está **permitida**. Para HTML5, esta configuración no se aplica si la directiva **Redirección de vídeo HTML5** está **prohibida**.

Cuando se habilita esta configuración, se aumenta la calidad de audio y vídeo que se genera desde el servidor a un nivel comparable al del audio y el vídeo ejecutados localmente en un dispositivo del usuario. El servidor transmite por streaming el material multimedia al cliente en el formato original comprimido y deja que el dispositivo del usuario lo descomprima y lo genere.

La función de redirección de Windows Media optimiza los archivos multimedia codificados con códecs que cumplen con las normas DirectShow de Microsoft, DirectX Media Objects (DMO) y Media Foundation. Para reproducir un archivo multimedia específico, el dispositivo del usuario debe tener un códec compatible con el formato de cifrado del archivo multimedia.

De forma predeterminada, el audio está inhabilitado en la aplicación Citrix Workspace. Para permitir que los usuarios ejecuten aplicaciones multimedia en sesiones ICA, habilite el audio u otorgue permisos a los usuarios para que lo habiliten en su interfaz de la aplicación Citrix Workspace.

Seleccione **Prohibida** solamente si la reproducción multimedia con la redirección de Windows Media resulta ser peor que cuando se genera mediante la compresión básica de ICA y el audio normal. Esta situación no es habitual, pero puede ocurrir en condiciones de ancho de banda bajo; por ejemplo, con medios que tengan una frecuencia de fotogramas clave muy baja.

### **Tamaño del búfer para la redirección de Windows Media**

Esta configuración es antigua y no se aplica a HTML5.

Esta configuración permite especificar un tamaño de búfer de entre 1 y 10 segundos para la aceleración multimedia.

El tamaño predeterminado es de 5 segundos.

## Uso del tamaño de búfer para redirección de Windows Media

Esta configuración es antigua y no se aplica a HTML5.

Esta configuración habilita o inhabilita el uso del tamaño del búfer especificado en **Tamaño del búfer para la redirección de Windows Media**.

De forma predeterminada, no se usa el tamaño de búfer especificado.

Si esta configuración está inhabilitada o el Tamaño del búfer para la redirección de Windows Media no se ha configurado, el servidor usa el valor de búfer predeterminado (5 segundos).

## Configuraciones de directiva de Conexiones de multisequencia

September 22, 2021

La sección “Conexiones de multisequencia” contiene configuraciones de directiva para gestionar las prioridades de Calidad de servicio (QoS) cuando hay varias conexiones ICA en una sesión.

### Sonido sobre UDP

Esta configuración permite o impide el sonido sobre UDP en el servidor.

De forma predeterminada, el sonido sobre UDP está inhabilitado en el servidor.

Cuando está habilitada, esta configuración abre un puerto UDP en el servidor para admitir todas las conexiones configuradas para usar el Transporte de sonido en tiempo real sobre UDP.

### Intervalo de puertos UDP de sonido

Esta configuración especifica el intervalo de números de puerto (con el formato “número de puerto más bajo, número de puerto más alto”) que Virtual Delivery Agent (VDA) utiliza para intercambiar datos de paquetes de audio con el dispositivo del usuario. VDA intenta utilizar cada par de puertos UDP para intercambiar datos con el dispositivo del usuario, comenzando por el número menor y aumentando en incrementos de 2 en cada intento subsiguiente. Cada puerto gestiona tanto el tráfico de entrada como el de salida.

De forma predeterminada, este valor está establecido en 16500,16509.

## Directiva Puertos múltiples

Esta configuración especifica los puertos TCP que deben usarse para el tráfico ICA y establece la prioridad de red para cada puerto.

De forma predeterminada, el puerto primario (2598) tiene prioridad Alta.

Cuando configure los puertos, puede asignarles las siguientes prioridades:

- **Muy alta:** Para las actividades en tiempo real, como conferencias con cámaras web.
- **Alta:** Para los elementos interactivos, como la pantalla, el teclado y el puntero.
- **Media:** Para procesos con gran cantidad de datos, como la asignación de unidades del cliente.
- **Baja:** Para las actividades en segundo plano, como la impresión.

Cada puerto debe tener una prioridad exclusiva. Por ejemplo, no puede asignar la prioridad Muy alta a dos puertos, como CGP puerto 1 y CGP puerto 3.

Para quitar un puerto del sistema de prioridades, defina el número de puerto como 0. El puerto primario no puede eliminarse y no se puede modificar su nivel de prioridad.

Después de definir esta configuración, reinicie el servidor. Esta configuración solo tiene efecto después de haber habilitado la configuración de directiva Configuración de equipo para multisequencia.

## Configuración de equipo para multisequencia

Esta configuración habilita o inhabilita la multisequencia en el servidor.

De forma predeterminada, la multisequencia está inhabilitada. Defina la directiva Configuración de equipo para multisequencia si utiliza Citrix SD-WAN o enrutadores de terceros para lograr la calidad de servicio pertinente.

Cuando defina esta configuración, reinicie el servidor para que los cambios tengan efecto.

### Importante:

El uso de esta configuración de directiva junto con otras configuraciones de límite de ancho de banda, como Límite de ancho de banda global de la sesión, puede producir resultados inesperados. Cuando incluya esta configuración en una directiva, asegúrese de que no haya configuraciones de límite de ancho de banda en la misma.

## Configuración de usuario para multisequencia

Esta configuración habilita o inhabilita la multisequencia en el dispositivo del usuario.

De forma predeterminada, la multisequencia está inhabilitada para todos los usuarios. Defina la directiva Configuración de usuario para multisequencia si utiliza Citrix SD-WAN o enrutadores de terceros para lograr la calidad de servicio pertinente.

Esta configuración solo tiene efecto en los hosts donde se ha habilitado la configuración de directiva Configuración de equipo para multisequencia.

**Importante:**

El uso de esta configuración de directiva junto con otras configuraciones de límite de ancho de banda, como Límite de ancho de banda global de la sesión, puede producir resultados inesperados. Cuando incluya esta configuración en una directiva, asegúrese de que no haya configuraciones de límite de ancho de banda en la misma.

## Parámetros de asignación de canales virtuales multisequencia

**Importante:**

Los parámetros siguientes solo se aplican a 1912 LTSR CU1 o a versiones posteriores.

Este parámetro especifica la secuencia ICA a la que se asignan los canales virtuales cuando se utiliza la multisequencia.

Si no configura estos parámetros, los canales virtuales se mantienen en su secuencia predeterminada. Para asignar un canal virtual a una secuencia ICA, seleccione el número de secuencia correspondiente (0, 1, 2, 3) en la lista **Número de secuencia**, junto al nombre del canal virtual.

Si se está utilizando un canal virtual personalizado en el entorno, haga clic en **Agregar**, especifique el nombre del canal virtual en el cuadro de texto **Canales virtuales** y seleccione el número de secuencia correspondiente en la lista **Número de secuencia** que hay junto a él. El nombre que especifique debe ser el nombre real del canal virtual, no un nombre descriptivo. Por ejemplo, CTXSBR en lugar de Citrix Browser Acceleration.

Estos parámetros solo surten efecto cuando se ha habilitado el parámetro multisequencia del equipo.

De forma predeterminada, los canales virtuales y sus asignaciones de secuencia son:

- Audio: 0
- Redirección de contenido de explorador web: 2
- Asignación de puertos COM del cliente: 3
- Asignación de unidades del cliente: 2
- Asignación de impresoras del cliente: 3
- Portapapeles: 2
- CTXDND: 1

- Plugins DVC (nombre estático de VC generado automáticamente a partir del nombre descriptivo del plug-in DVC o uno asignado por el administrador): 2
- Supervisión de la experiencia de usuario final: 1
- Transferencia de archivos (Receiver para HTML5): 2
- Transferencia de datos genérica: 2
- Control ICA: 1
- Editor de métodos de entrada: 1
- Asignación antigua de impresoras del cliente (COM1): 1, 3
- Asignación antigua de impresoras del cliente (COM2): 2, 3
- Asignación antigua de impresoras del cliente (LPT1): 1, 3
- Asignación antigua de impresoras del cliente (LPT2): 2, 3
- Administración de licencias: 1
- Redirección de Microsoft Teams/WebRTC: 1
- Receiver para móviles: 1
- Multitoque: 1
- Reenvío de puertos: 2
- Extensiones de audio y vídeo remotos (RAVE): 2
- Integrado (integración de ventanas transparentes): 1
- Sensor y ubicación: 1
- Tarjeta inteligente: 1
- Gráficos Thinwire: 1
- Estado de inicio de sesión/integración de IU transparente: 2
- Redirección TWAIN: 2
- USB: 2
- Fuente y teclado de latencia cero: 2
- Canal de datos de latencia cero: 2

Para obtener más información sobre las asignaciones y las prioridades de los canales virtuales, consulte el artículo [CTX131001](#) de Knowledge Center.

## Configuraciones de directiva de Redirección de puertos

September 22, 2021

La sección Redirección de puertos contiene configuraciones de directiva para la asignación de puertos LPT y COM del cliente.

Para los agentes Virtual Delivery Agent de **versiones anteriores a la 7.0**, utilice las siguientes configuraciones de directiva para configurar la redirección de puertos. Para los agentes Virtual Delivery

Agent **de las versiones 7.0 a 7.8**, configure estos parámetros con el Registro; consulte [Configurar la redirección de puertos COM y puertos LPT mediante el Registro](#). Para los agentes VDA de la versión **7.9**, utilice las siguientes configuraciones de directiva.

### **Conectar automáticamente puertos COM del cliente**

Esta configuración habilita o inhabilita la conexión automática de los puertos COM en los dispositivos del usuario cuando este inicia sesión en un sitio.

Los puertos COM del cliente no se conectan automáticamente de forma predeterminada.

### **Conectar automáticamente puertos LPT del cliente**

Esta configuración habilita o inhabilita la conexión automática de los puertos LPT en los dispositivos del usuario cuando este inicia sesión en un sitio.

Los puertos LPT del cliente no se conectan automáticamente de forma predeterminada.

### **Redirección de puertos COM del cliente**

Esta configuración permite o impide el acceso a los puertos COM en el dispositivo del usuario.

La redirección de puertos COM está prohibida de forma predeterminada.

Configuraciones de directiva relacionadas:

- Límite de ancho de banda de redirección de puertos COM
- Porcentaje límite de ancho de banda de redirección de puertos COM

### **Redirección de puertos LPT del cliente**

Esta configuración permite o impide el acceso a los puertos LPT en el dispositivo del usuario.

La redirección de puertos LPT está prohibida de forma predeterminada.

Los puertos LPT solo se utilizan por aplicaciones antiguas que envían trabajos de impresión a los puertos LPT y no a los objetos de impresión del dispositivo de usuario. La mayoría de las aplicaciones que se utilizan hoy en día pueden enviar trabajos de impresión a objetos de impresora. Esta configuración de directiva solo es necesaria para los servidores que alojan aplicaciones antiguas que imprimen en puertos LPT.

Tenga en cuenta que, aunque la redirección de puertos COM del cliente es bidireccional, la redirección de puertos LPT es solo de salida y se limita a `\\client\LPT1` y `\\client\LPT2` en una sesión ICA.

Configuraciones de directiva relacionadas:

- Límite de ancho de banda de redirección de puertos LPT
- Porcentaje límite de ancho de banda de redirección de puertos LPT

## Configuraciones de directiva de Impresión

September 22, 2021

La sección Impresión contiene configuraciones de directiva para administrar la impresión del cliente.

### Redirección de impresoras del cliente

Esta configuración controla si las impresoras cliente se asignan a un servidor cuando el usuario inicia sesión.

La asignación de impresoras cliente está permitida de forma predeterminada. Si esta configuración está inhabilitada, la impresora PDF para la sesión no se crea automáticamente.

Configuraciones de directiva relacionadas: Crear automáticamente las impresoras del cliente

### Impresora predeterminada

Esta configuración permite especificar cómo se establece la impresora predeterminada de un dispositivo del usuario en una sesión.

De forma predeterminada, la impresora actual del usuario se usa como predeterminada durante la sesión.

Para usar el parámetro de impresora predeterminada existente en el perfil de usuario de Windows o en Servicios de Escritorio remoto, seleccione No ajustar la impresora predeterminada del usuario. Si elige esta opción la impresora predeterminada no se guarda en el perfil y no cambia de acuerdo con otras propiedades de la sesión o del cliente. La impresora predeterminada de la sesión es la primera impresora que se haya creado automáticamente, que puede ser:

- La primera impresora agregada localmente al servidor de Windows en **Panel de control > Dispositivos e impresoras**.
- La primera impresora creada de forma automática, si no se agrega localmente ninguna impresora al servidor.

Esta opción se puede usar para presentar a los usuarios la impresora más próxima por medio de los parámetros del perfil (función conocida como impresión de proximidad).

## Asignaciones de impresora

Esta configuración proporciona una alternativa a las configuraciones Impresora predeterminada e Impresoras de la sesión. Utilice las configuraciones individuales Impresora predeterminada e Impresoras de la sesión para configurar comportamientos para un sitio, un grupo grande o una unidad organizativa. Utilice la configuración **Asignaciones de impresoras** para asignar un grupo grande de impresoras a varios usuarios.

Esta configuración especifica cómo se establece durante una sesión la impresora predeterminada en los dispositivos de usuario enumerados.

De forma predeterminada, la impresora actual del usuario se usa como predeterminada durante la sesión.

También especifica las impresoras de red que se crearán de forma automática en una sesión para cada dispositivo de usuario. De forma predeterminada, no hay impresoras especificadas.

- Al configurar el valor de impresora predeterminada:

Para usar la impresora predeterminada actual para el dispositivo del usuario, seleccione No ajustar.

Para usar el parámetro de impresora predeterminada existente en el perfil del usuario de Windows o en Servicios de Escritorio remoto, seleccione No ajustar. Si elige esta opción la impresora predeterminada no se guarda en el perfil y no cambia de acuerdo con otras propiedades de la sesión o del cliente. La impresora predeterminada de la sesión es la primera impresora que se haya creado automáticamente, que puede ser:

- La primera impresora agregada localmente al servidor de Windows en Panel de control > Dispositivos e impresoras.
  - La primera impresora creada de forma automática, si no se agrega localmente ninguna impresora al servidor.
- Al configurar el valor de impresoras de la sesión: para agregar impresoras, escriba la ruta UNC de la impresora que quiere crear automáticamente. Después de agregar la impresora, puede aplicar parámetros personalizados para la sesión actual en cada inicio de sesión.

## Preferencia de registro de sucesos de creación automática de impresoras

Esta configuración permite especificar los sucesos que se registran durante el proceso de creación automática de impresoras. Puede optar por no registrar los errores ni las advertencias, registrar solamente los errores o registrar los errores y las advertencias.

De forma predeterminada, se registran los errores y las advertencias.

Un ejemplo de advertencia es un suceso en el cual no se pudo instalar el controlador original de una impresora y se instaló el controlador de impresión universal. Para utilizar controladores de impresión universal en esta circunstancia, configure Uso de controladores de impresión universal en Usar solo impresión universal o Usar impresión universal solo si el controlador solicitado no está disponible.

## Impresoras de la sesión

Esta configuración permite especificar qué impresoras de red se crearán automáticamente en una sesión. Dentro de la sesión ICA/HDX, Citrix Print Manager Service (CpSvc.exe) crea una conexión de impresora de red durante el inicio de sesión para cada impresora de red especificada en la configuración de directiva **Impresoras de la sesión**. Elimina las impresoras durante el cierre de sesión. De forma predeterminada, no hay impresoras especificadas.

En la configuración de directiva **Impresoras de la sesión**, las impresoras de red pueden residir en un servidor de impresión de Windows o un servidor de impresión universal de Citrix (Universal Print Server).

- **Servidor de impresión de Windows:** Comparte una o más impresoras de red. También tiene los controladores nativos de impresora necesarios para usar las impresoras de red.
- **Universal Print Server:** Un servidor de impresión de Windows en el que se ha instalado el software de Citrix Universal Print Server.

Cuando se utiliza un servidor de impresión de Windows, Citrix Print Manager Service crea las conexiones de las impresoras de red mediante controladores de impresora nativos. El servidor de Citrix Virtual Apps debe tener instalados los controladores de impresora nativos.

Cuando se utiliza Citrix Universal Print Server, Citrix Print Manager Service crea las conexiones de las impresoras de red mediante controladores de impresora nativos, el controlador de impresora universal de Citrix o el controlador de impresora universal XPS de Citrix. El controlador que usted utiliza está controlado por la configuración de directiva Uso de controladores de impresión universal.

Actualmente, todos los controladores de impresora de Windows están dentro de la versión v3 o v4 de controlador. Para obtener más información, consulte [Support for the Microsoft V3 and V4 Printer Driver Architectures](#) (Compatibilidad para las arquitecturas de las versiones v3 y v4 de los controladores de impresora de Microsoft).

Para agregar impresoras de sesión y comprobar si aparecen en las sesiones, siga el procedimiento siguiente:

1. En Citrix Studio, vaya a la ficha **Directivas**.
2. Habilite la directiva de impresión de sesión en el cuadro de diálogo **Modificar directiva**.
3. En la directiva, agregue la impresora de sesión. Para agregar impresoras, escriba la ruta UNC de la impresora que quiere crear automáticamente. Después de agregar la impresora, puede

aplicar parámetros personalizados para la sesión actual en cada inicio de sesión. La impresora de sesión debe aparecer en la lista.

4. Una vez configurada la directiva, es posible que la aplicación publicada no muestre impresoras de sesión. Este problema puede producirse porque falta el controlador de impresora en el servidor de Citrix Virtual Apps o la directiva se ha creado pero no se ha habilitado.

Nota:

Si el controlador de impresora no se ha instalado en el servidor de Citrix Virtual Apps, es posible que experimente el error más común con las impresoras de sesión: que los administradores se olviden de instalar el controlador de impresora en el servidor de Citrix Virtual Apps.

5. Inicie el escritorio publicado y agregue manualmente la impresora de sesión en **Dispositivos e impresoras > Panel de control**.
6. Si esto falla, investigue la comunicación entre el servidor Citrix Virtual Apps y el servidor de impresión. Si hace falta, realice una prueba con RDP.

### **Esperar a que se creen las impresoras (escritorio de servidor)**

Esta configuración permite o impide la demora al conectarse a una sesión para dar tiempo a que las impresoras de escritorio del servidor se creen automáticamente.

De forma predeterminada, no hay demora en la conexión.

## **Configuraciones de directiva de Impresoras del cliente**

September 22, 2021

La sección Impresoras del cliente contiene configuraciones de directiva para las impresoras del cliente, como configuraciones para la creación automática de impresoras, la conservación de ciertas propiedades de la impresora y la conexión a servidores de impresión.

### **Crear automáticamente las impresoras del cliente**

Esta configuración permite especificar qué impresoras se crearán automáticamente. Esta configuración anula los parámetros predeterminados de creación automática de impresoras del cliente.

Todas las impresoras del cliente se crean automáticamente de forma predeterminada.

Esta configuración se aplica solamente si la configuración Redirección de impresoras del cliente está presente y establecida en Permitida.

Al agregar esta configuración a una directiva, seleccione una de las siguientes opciones:

- Crear automáticamente todas las impresoras del cliente: Crea de forma automática todas las impresoras del dispositivo del usuario.
- Crear automáticamente solo la impresora predeterminada del cliente: Crea de forma automática solo la impresora seleccionada como predeterminada en el dispositivo del usuario.
- Crear automáticamente solo las impresoras locales (no de red) del cliente: Crea de forma automática solo las impresoras conectadas directamente con el dispositivo del usuario por un puerto LPT, COM, USB, TCP/IP u otro puerto local.
- No crear automáticamente las impresoras del cliente: Desactiva la creación automática de todas las impresoras del cliente cuando el usuario inicia sesión. Esto hace que los parámetros de creación automática de impresoras del cliente de los Servicios de Escritorio remoto reemplacen esta configuración en las directivas que tengan menor prioridad.

### **Crear automáticamente una impresora universal genérica**

Esta configuración habilita o inhabilita la creación automática del objeto de impresora universal de Citrix genérico (Citrix Universal Printer) para las sesiones en las que se usa un dispositivo de usuario compatible con la impresión universal.

De forma predeterminada, el objeto genérico de impresora universal no se crea automáticamente.

Configuraciones de directiva relacionadas:

- Uso de controladores de impresión universal
- Preferencia de controlador universal

### **Crear automáticamente la impresora universal de PDF**

Este parámetro habilita o inhabilita la creación automática de Citrix PDF Printer para sesiones mediante la aplicación Citrix Workspace para Windows (a partir de VDA 7.19), la aplicación Citrix Workspace para HTML5 o la aplicación Citrix Workspace para Chrome.

De forma predeterminada, la impresora Citrix PDF Printer no se crea automáticamente.

### **Nombres de impresora del cliente**

Esta configuración permite seleccionar la convención de nomenclatura que se aplicará a las impresoras del cliente creadas automáticamente.

De forma predeterminada, se utilizan nombres de impresoras estándar.

Seleccione Nombres de impresoras estándar para usar nombres de impresora similares a “HPLaserJet 4 de nombre\_cliente en sesión 3”.

Seleccione Nombres de impresoras antiguos para usar nombres similares a los asignados a las impresoras cliente más antiguas y mantener la compatibilidad con versiones anteriores para usuarios o grupos que utilicen MetaFrame Presentation Server 3.0 u otra versión anterior. Un ejemplo de nombre de impresora antiguo es: “Cliente/nombre\_cliente#/HPLaserJet 4”. Esta opción es menos segura.

Nota: Esta opción se ofrece únicamente para mantener la compatibilidad con versiones anteriores de XenApp y XenDesktop.

### **Conexiones directas con servidores de impresión**

Esta configuración habilita o inhabilita las conexiones directas desde el escritorio virtual o desde el servidor que aloja las aplicaciones con un servidor de impresión para las impresoras del cliente alojadas en un recurso compartido de red accesible.

Las conexiones directas están habilitadas de forma predeterminada.

Habilite las conexiones directas si el servidor de impresión en red no está en una red WAN desde el escritorio virtual o servidor que aloja las aplicaciones. La comunicación directa da como resultado una impresión más rápida si el servidor de impresión en red y el escritorio virtual o servidor que aloja las aplicaciones están en la misma LAN.

Inhabilite las conexiones directas si es una red WAN o si el ancho de banda es limitado o tiene mucha latencia. Los trabajos de impresión se enrutan a través del dispositivo del usuario, desde donde se los redirige hacia el servidor de impresión en red. Los datos enviados al dispositivo del usuario se comprimen, por lo que se consume menos ancho de banda al transmitir los datos en la WAN.

Si hay dos impresoras de red con un mismo nombre, se usará la que esté en la misma red que el dispositivo del usuario.

### **Asignación y compatibilidad de controladores de impresora**

Esta configuración permite especificar reglas de sustitución de controladores para impresoras creadas automáticamente.

Esta configuración está definida para excluir Microsoft OneNote y el escritor de documentos XPS de la lista de impresoras cliente creadas automáticamente.

Al definir estas reglas, es posible permitir o impedir la creación de impresoras con un controlador específico. También es posible permitir que las impresoras creadas usen solamente controladores de

impresión universal. La sustitución de controladores sobrescribe (o asigna) los nombres de los controladores proporcionados por el dispositivo cliente y sustituyéndolo por un controlador equivalente en el servidor. Este proceso permite que las aplicaciones del servidor tengan acceso a las impresoras cliente que tienen los mismos controladores que el servidor pero distintos nombres de controladores.

Puede agregar una asignación de controlador, modificar una existente, sobrescribir la configuración personalizada para una asignación, quitar una asignación o cambiar el orden de entradas de controlador en la lista. Al agregar una asignación, se debe especificar el nombre del controlador de la impresora cliente y luego seleccionar el controlador de servidor con el que desea sustituirlo.

## **Retención de las propiedades de impresora**

Esta configuración permite especificar si se almacenan las propiedades de la impresora y dónde se almacenan.

De forma predeterminada, el sistema determina si las propiedades de la impresora se almacenan en el dispositivo del usuario, si está disponible, o en el perfil del usuario.

Al agregar esta configuración a una directiva, seleccione una de las siguientes opciones:

- Guardado solo en el dispositivo cliente se utiliza para los dispositivos de usuario que cuentan con un perfil obligatorio o móvil que no se guarda. Elija esta opción solo si todos los servidores de la comunidad están ejecutando XenApp 5 o una versión posterior y los usuarios usan Citrix Online Plug-in versiones 9 a 12.x, o Citrix Receiver 3.x.
- Conservado solo en el perfil de usuario se utiliza para los dispositivos de usuarios con un ancho de banda limitado (ya que reduce el tráfico de red) e inicios de sesión lentos o para los usuarios que tienen plug-ins antiguos. Esta opción almacena las propiedades de la impresora en el perfil del usuario existente en el servidor y evita cualquier intercambio de propiedades con el dispositivo del usuario. Utilice esta opción con MetaFrame Presentation Server 3.0 o una versión anterior y el cliente de MetaFrame Presentation Server 8.x o anterior. Tenga en cuenta que esto solo se puede aplicar si se utiliza un perfil móvil de Servicios de Escritorio remoto (RDS).
- Guardado en perfil solo si no se guarda en el cliente permite que el sistema determine dónde almacenar las propiedades de la impresora. Las propiedades de la impresora se almacenan en el dispositivo del usuario, cuando está disponible, o en el perfil del usuario. Aunque esta opción ofrece más flexibilidad, puede hacer que el inicio de sesión se prolongue y que parte del ancho de banda se utilice para realizar las comprobaciones del sistema.
- No conservar las propiedades de impresora. Evita que se almacenen las propiedades de la impresora.

## **Impresoras del cliente retenidas o restauradas**

Esta configuración habilita o inhabilita la conservación y la recreación de impresoras en el dispositivo del usuario. De forma predeterminada, las impresoras del cliente se conservan y se restauran automáticamente.

Las impresoras conservadas son impresoras creadas por el usuario que se vuelven a crear, o se recuerdan, al iniciar la sesión siguiente. Cuando Citrix Virtual Apps vuelve a crear una impresora conservada, aplica todas las configuraciones de directiva, excepto Crear automáticamente las impresoras del cliente.

Las impresoras restauradas son impresoras configuradas íntegramente por un administrador, con un estado guardado que queda vinculado de forma permanente con un puerto del cliente.

## **Controlador de impresora universal PDF de Citrix**

El controlador de impresora universal PDF de Citrix (o Citrix PDF Universal Printer) permite a los usuarios imprimir documentos abiertos con aplicaciones alojadas o aplicaciones ejecutadas en escritorios virtuales entregados por Citrix Virtual Apps and Desktops. Cuando un usuario selecciona la opción Citrix PDF Printer, el controlador convierte el archivo a documento PDF y transfiere este último al dispositivo local. El PDF se abre para verlo e imprimirlo en una impresora conectada localmente. PDF es uno de los formatos compatibles con la impresión universal de Citrix (además de EMF y XPS).

La impresora PDF se puede habilitar, configurar y establecer como predeterminada mediante una directiva de Citrix. La opción Impresora PDF de Citrix está disponible para los usuarios de la aplicación Citrix Workspace para Windows, Chrome y HTML5.

### **Nota:**

Se requiere un visor de PDF para dispositivos de punto final Windows. El cliente debe tener una aplicación que tenga una asociación de tipos de archivo registrada en Windows para poder abrir archivos PDF.

## **Configuraciones de directiva de Controladores**

January 4, 2021

La sección Controladores contiene configuraciones de directiva relacionadas con los controladores de impresoras.

## Instalación automática de controladores de impresora

### Nota

Esta directiva no es compatible con agentes VDA en esta versión.

Esta configuración habilita o inhabilita la instalación automática de los controladores de impresora del conjunto de controladores integrados de Windows o de paquetes de controladores del host mediante pnputil.exe /a.

De forma predeterminada, estos controladores se instalan según se requieren.

## Preferencia de controlador universal

Esta configuración especifica el orden en el que se usan los controladores de impresión universal, comenzando por la primera entrada en la lista.

De forma predeterminada, el orden de preferencia es:

- EMF
- XPS
- PCL5c
- PCL4
- PS

Es posible agregar, modificar o eliminar controladores y cambiar el orden de los controladores en la lista.

## Uso de controladores de impresión universal

Esta configuración permite especificar cuándo se usa la impresión universal.

De forma predeterminada, la impresión universal se utiliza exclusivamente si el controlador solicitado no está disponible.

La impresión universal emplea controladores de impresora genéricos en lugar de controladores específicos de modelos de impresora, lo que simplifica la gestión de los controladores en los equipos host. La disponibilidad de los controladores de impresión universal depende de la capacidad del software del dispositivo de usuario, del host y del servidor de impresión. En algunas configuraciones, es posible que la impresión universal no esté disponible.

Al agregar esta configuración a una directiva, seleccione una de las siguientes opciones:

- Usar solo los controladores específicos de la impresora indica que la impresora cliente usa solamente los controladores estándar específicos de modelo de impresora, los cuales se crean

automáticamente al iniciar sesión. Si el controlador solicitado no está disponible, la impresora cliente no podrá crearse de forma automática.

- Usar solo impresión universal. Especifica que no se usen los controladores específicos del modelo de impresora. Solo se usan controladores de impresión universal para crear impresoras.
- Usar impresión universal solo si el controlador solicitado no está disponible utiliza los controladores estándar específicos del modelo de impresora para la creación de impresoras, si están disponibles. Si el controlador no está disponible en el servidor, la impresora cliente se crea automáticamente mediante un controlador de impresora universal adecuado.
- Usar controladores específicos de la impresora solo si la impresión universal no está disponible usa el controlador de impresión universal si está disponible. Si el controlador no está disponible en el servidor, la impresora cliente se crea de forma automática con el controlador específico del modelo de impresora adecuado.

## Configuraciones de directiva de Universal Print Server

September 22, 2021

La sección Universal Print Server contiene configuraciones de directiva para administrar el servidor de impresión universal (Universal Print Server).

### Conjunto de cifrado SSL

Esta configuración especifica los conjuntos de cifrado SSL/TLS que utiliza el cliente de impresión universal (Universal Print Client) para conexiones cifradas del flujo de datos de impresión (CGP).

Para decidir qué paquete de conjunto de cifrado utiliza Universal Print Client para conexiones cifradas del servicio web de impresión (HTTPS/SOAP), consulte [CHANNEL].

Valor predeterminado: ALL

Esta configuración puede tener los valores: ALL, COM o GOV.

A continuación, se indican los conjuntos de cifrado correspondientes a cada valor:

#### **ALL:**

TLS\_ECDHE\_RSA\_AES256\_GCM\_SHA384

TLS\_ECDHE\_RSA\_AES256\_CBC\_SHA384

TLS\_ECDHE\_RSA\_AES128\_CBC\_SHA

#### **COM:**

TLS\_ECDHE\_RSA\_AES128\_CBC\_SHA

**GOV:**

TLS\_ECDHE\_RSA\_AES256\_GCM\_SHA384

TLS\_ECDHE\_RSA\_AES256\_CBC\_SHA384

### **Modo de conformidad de SSL**

Esta configuración especifica el nivel de conformidad con la publicación especial 800-52 de NIST que utiliza el cliente de impresión universal (Universal Print Client) para conexiones cifradas del flujo de datos de impresión (CGP).

Valor predeterminado: Ninguno.

Esta configuración puede tener los siguientes valores:

**Ninguno.**

Las conexiones cifradas del flujo de datos de impresión (CGP) utilizan el modo de conformidad predeterminado.

**SP800-52.**

Las conexiones cifradas del flujo de datos de impresión (CGP) utilizan el modo de conformidad de la publicación especial 800-52 de NIST.

### **Habilitado para SSL**

Esta configuración especifica si el cliente de impresión universal (Universal Print Client) utiliza SSL/TLS para conexiones del flujo de datos de impresión (CGP) y para conexiones del servicio web (HTTP/SOAP).

Cuando **Habilitar Universal Print Server** se establece en **Habilitado, con opción de reserva de la impresión remota nativa de Windows**, se recurre a conexiones mediante el proveedor de impresión de red de Microsoft Windows. Esta configuración no afecta a las conexiones a las que se recurre.

Valor predeterminado: Inhabilitada

Esta configuración puede tener los siguientes valores:

**Habilitada.**

El Universal Print Client usa SSL/TLS para conectarse al Universal Print Server.

**Inhabilitado.**

El Universal Print Client usa SSL/TLS para conectarse al Universal Print Server.

## **Modo FIPS de SSL**

Esta configuración especifica si el módulo criptográfico SSL/TLS que utilice el cliente de impresión universal (Universal Print Client) para conexiones del flujo de datos de impresión (CGP) se ejecutará en el modo FIPS.

Valor predeterminado: Inhabilitada

Esta configuración puede tener los siguientes valores:

### **Habilitada.**

El modo FIPS está activado.

### **Inhabilitado.**

El modo FIPS está desactivado.

## **Versión de protocolo SSL**

Esta configuración especifica la versión del protocolo SSL/TLS que utiliza el cliente de impresión universal (Universal Print Client).

Valor predeterminado: ALL

Esta configuración puede tener los siguientes valores:

### **ALL.**

Utilice las versiones 1.0, 1.1 o 1.2 de TLS.

### **TLSv1.**

Utilice TLS 1.0.

### **TLSv1.1.**

Utilice TLS 1.1.

### **TLSv1.2.**

Use TLS 1.2.

## **Puerto SSL del flujo de datos cifrado de impresión de Universal Print Server (CGP)**

Esta configuración especifica el número de puerto TCP para el flujo cifrado de datos de impresión (CGP) de Universal Print Server. Este puerto recibe datos para trabajos de impresión.

Valor predeterminado: 443

## **Puerto SSL del servicio web cifrado de Universal Print Server (HTTPS/SOAP)**

Esta configuración especifica el número de puerto TCP para el servicio web cifrado de Universal Print Server (HTTPS/SOAP). Este puerto recibe datos para comandos de impresión.

Valor predeterminado: 8443

## **Habilitar Universal Print Server**

Esta configuración habilita o inhabilita la funcionalidad de Universal Print Server en el escritorio virtual o en el servidor que aloja aplicaciones. Aplique esta configuración de directiva a las unidades organizativas (OU) que contienen los escritorios o servidores virtuales que alojan las aplicaciones.

De forma predeterminada, Universal Print Server está inhabilitado.

Al agregar esta configuración a una directiva, seleccione una de las siguientes opciones:

- **Habilitado, con opción de reserva de la impresión remota nativa de Windows.** Cuando es posible, Universal Print Server proporciona servicios a las conexiones con impresoras de red. Si Universal Print Server no está disponible, se usa el proveedor de impresión de Windows. El proveedor de impresión de Windows sigue administrando todas las impresoras que fueron creadas previamente con dicho proveedor.
- **Habilitado, sin opción de reserva de la impresión remota nativa de Windows.** Solo Universal Print Server proporciona servicios a las conexiones con impresoras de red. Si Universal Print Server no está disponible, la conexión con la impresora de red falla. Esta configuración inhabilita en efecto la impresión en red a través del proveedor de impresión de Windows. Las impresoras creadas previamente con el proveedor de impresión de Windows no se crearán mientras exista una directiva que contenga esta configuración.
- **Inhabilitado.** La función Universal Print Server está inhabilitada. No se intenta conectar a Universal Print Server al conectarse a una impresora de red con un nombre UNC. Las conexiones con impresoras remotas continúan mediante la utilidad de impresión remota nativa de Windows.

## **Puerto del flujo de datos de impresión de Universal Print Server (CGP)**

Esta configuración especifica el número de puerto TCP utilizado por el protocolo CGP de escucha de flujo de datos de impresión de Universal Print Server. Aplique esta configuración de directiva solamente a las unidades organizativas que contienen el servidor de impresión.

De forma predeterminada, el número de puerto es el 7229.

Los números de puerto válidos deben estar en el intervalo de 1 a 65535.

## **Límite de ancho de banda del flujo de entrada de impresión de Universal Print Server (kbps)**

Esta configuración especifica el límite superior (en kilobits por segundo) de la velocidad de transferencia de datos de impresión entregados desde cada trabajo de impresión a Universal Print Server mediante CGP. Aplique esta configuración de directiva a las unidades organizativas que contienen el escritorio virtual o el servidor que aloja aplicaciones.

De forma predeterminada, el valor es 0, lo cual no especifica un límite superior.

## **Puerto del servicio web de Universal Print Server (HTTP/SOAP)**

Esta configuración especifica el número de puerto TCP que utiliza el agente de escucha (HTTP/SOAP) del servicio web de Universal Print Server. Universal Print Server es un componente optativo que permite el uso de controladores de impresión universal de Citrix para la impresión en red. Cuando se utiliza Universal Print Server, los comandos de impresión se envían de los hosts de Citrix Virtual Apps and Desktops a Universal Print Server mediante SOAP a través de HTTP. Esta configuración modifica el puerto TCP predeterminado en que Universal Print Server escucha las solicitudes HTTP/SOAP entrantes.

Debe configurar de la misma manera el puerto HTTP del host y del servidor de impresión. Si los puertos no tienen la misma configuración, el software del host no se conectará a Universal Print Server. Esta configuración cambia el VDA en Citrix Virtual Apps and Desktops. Además, debe cambiar el puerto predeterminado en Universal Print Server.

De forma predeterminada, el número de puerto es el 8080.

Los números de puerto válidos deben estar en el intervalo de 0 a 65535.

## **Universal Print Servers para equilibrio de carga**

Esta configuración enumera los servidores de impresión universal que se usarán para equilibrar la carga de las conexiones de impresora establecidas al comienzo de las sesiones, después de evaluar otras configuraciones de impresión de Citrix. Para optimizar la creación de impresoras, Citrix recomienda que todos los servidores de impresión tengan el mismo conjunto de impresoras compartidas. No hay límite máximo para la cantidad de servidores de impresión que se pueden agregar para el equilibrio de carga.

Esta configuración también implementa la detección de fallos de impresora para la conmutación por error y la recuperación de conexiones de impresora. La disponibilidad de los servidores de impresión se comprueba periódicamente. Si se detecta un error del servidor, ese servidor se quita del esquema de equilibrio de carga y las conexiones de impresora en ese servidor se redistribuyen entre los otros

servidores de impresión disponibles. Cuando el servidor de impresión que falló se recupera, se lo devuelve al esquema de equilibrio de carga.

Haga clic en **Validar servidores** para comprobar: que cada servidor es un servidor de impresión, que la lista no contiene nombres de servidor duplicados y que todos los servidores tienen un conjunto idéntico de impresoras compartidas instaladas. Esta operación puede tardar varios minutos.

### **Umbral para servidores Universal Print Server fuera de servicio**

Esta configuración especifica cuánto tiempo debe esperar el equilibrador de carga a que se recupere un servidor de impresión no disponible antes de determinar que ese servidor está fuera de línea permanentemente y redistribuir su carga en otros servidores de impresión disponibles.

El valor umbral predeterminado es de 180 segundos.

## **Configuraciones de directiva de Impresión universal**

January 4, 2021

La sección Impresión universal contiene configuraciones de directiva para administrar la impresión universal.

### **Modo de procesamiento EMF de la impresión universal**

Esta configuración controla el método de procesamiento del archivo de cola de impresión EMF en el dispositivo de usuario Windows.

De forma predeterminada, los registros EMF se envían directamente a la impresora.

Al agregar esta configuración a una directiva, seleccione una de las siguientes opciones:

- Reprocesar EMF para la impresora fuerza el reprocesamiento del archivo de cola de EMF y su envío a través del subsistema GDI en el dispositivo del usuario. Puede usar esta configuración para los controladores que requieren el reprocesamiento de EMF pero que puede que no se seleccionen automáticamente en una sesión.
- Enviar directamente a la cola de impresión, cuando se usa con el controlador de impresora universal de Citrix, asegura que los registros EMF se envíen a la cola y se entreguen al dispositivo del usuario para el procesamiento. Normalmente, estos archivos de cola de impresión EMF se transfieren directamente a la cola de impresión del cliente. Para las impresoras y controladores que son compatibles con el formato EMF, este es el método de impresión más rápido.

## **Límite de compresión de imagen para la impresión universal**

Esta configuración define la calidad máxima y el nivel de compresión mínimo disponibles para las imágenes impresas con el controlador de impresora universal de Citrix.

De forma predeterminada, el límite de compresión de imagen está definido en Mejor calidad (compresión sin pérdida).

Si se ha seleccionado Sin compresión, la compresión está inhabilitada para la impresión EMF solamente.

Al agregar esta configuración a una directiva, seleccione una de las siguientes opciones:

- Sin compresión
- Mejor calidad (compresión sin pérdida)
- Alta calidad
- Calidad estándar
- Calidad reducida (compresión máxima)

Cuando agregue esta configuración a una directiva que incluye ya la configuración Valores predeterminados de optimización de impresión universal, tenga en cuenta lo siguiente:

- Si el nivel de compresión en Límite de compresión de imagen para la impresión universal es inferior al nivel definido en Valores predeterminados de optimización de impresión universal, las imágenes se comprimen según el nivel definido en la configuración Límite de compresión de imagen para la impresión universal.
- Si la compresión está inhabilitada, las opciones Calidad de imagen deseada y Habilitar la compresión intensa de la configuración Valores predeterminados de optimización de impresión universal no tienen ningún efecto en la directiva.

## **Valores predeterminados de optimización de impresión universal**

Esta configuración especifica los valores predeterminados para la optimización de la impresión cuando se crea el controlador de impresión universal para una sesión.

- Calidad de imagen deseada especifica el límite predeterminado de compresión de imagen aplicable a la impresión universal. De forma predeterminada, la Calidad estándar está habilitada, de manera que los usuarios solo pueden imprimir imágenes con la compresión de calidad estándar o reducida.
- Habilitar la compresión intensa habilita o inhabilita la reducción de ancho de banda más allá del nivel de compresión definido por Calidad de imagen deseada, sin pérdida de calidad de imagen. La compresión intensa está inhabilitada de forma predeterminada.

- La configuración de Almacenamiento en caché de imágenes y fuentes especifica si las imágenes y fuentes que aparecen varias veces en el flujo de impresión se almacenan en caché, para que cada imagen individual se envíe solo una vez a la impresora. De forma predeterminada, las fuentes e imágenes incrustadas se almacenan en caché. Tenga en cuenta que estas configuraciones solo se aplican si el dispositivo del usuario admite este comportamiento.
- Permitir a los no administradores modificar estos parámetros especifica si los usuarios pueden cambiar los parámetros predeterminados de optimización de la impresión en una sesión. De forma predeterminada, los usuarios no pueden cambiar los parámetros predeterminados de la optimización de impresión.

Nota: Todas estas opciones son compatibles con la impresión EMF. En el caso de la impresión XPS, solo se admite la opción Calidad de imagen deseada.

Cuando agregue esta configuración a una directiva que incluye ya la configuración Límite de compresión de imagen para la impresión universal, tenga en cuenta lo siguiente:

- Si el nivel de compresión en Límite de compresión de imagen para la impresión universal es inferior al nivel definido en Valores predeterminados de optimización de impresión universal, las imágenes se comprimen según el nivel definido en la configuración Límite de compresión de imagen para la impresión universal.
- Si la compresión está inhabilitada, las opciones Calidad de imagen deseada y Habilitar la compresión intensa de la configuración Valores predeterminados de optimización de impresión universal no tienen ningún efecto en la directiva.

### **Preferencia de vista previa en impresión universal**

Esta configuración permite especificar si se usará la función de vista previa de impresión para las impresoras universales genéricas o creadas automáticamente.

De forma predeterminada, no se utiliza la vista previa de impresión para estas impresoras.

Al agregar esta configuración a una directiva, seleccione una de las siguientes opciones:

- No usar vista previa en las impresoras de creación automática o universales genéricas
- Usar vista previa solo para impresoras de creación automática
- Usar vista previa solo para impresoras universales genéricas
- Usar vista previa para impresoras de creación automática y universales genéricas

### **Límite de calidad de la impresión universal**

Esta configuración especifica la cantidad máxima de puntos por pulgada (PPP) disponibles para generar los productos impresos en una sesión.

De forma predeterminada, Sin límite está habilitado, y permite a los usuarios seleccionar la calidad de impresión máxima permitida por la impresora a la que están conectados.

Cuando esta configuración está definida, limita la calidad de impresión máxima disponible para los usuarios en términos de resolución de salida. Tanto la calidad de impresión misma como la capacidad de calidad de impresión de la impresora a la que se conectan los usuarios quedan limitadas por el parámetro configurado. Por ejemplo, si se configura como Resolución media (600 PPP), los usuarios están limitados a imprimir con una calidad máxima de 600 PPP y la configuración Calidad de impresión en la ficha Avanzado del cuadro de diálogo Impresora universal muestra parámetros de resolución solo hasta la calidad media inclusive (600 PPP).

Al agregar esta configuración a una directiva, seleccione una de las siguientes opciones:

- Borrador (150 PPP)
- Baja resolución (300 PPP)
- Resolución media (600 PPP)
- Alta resolución (1200 PPP)
- Sin límite

## Configuraciones de directiva de Seguridad

September 22, 2021

La sección Seguridad contiene la configuración de directiva para configurar el cifrado de sesiones y el cifrado de los datos de inicio de sesión.

### Nivel de cifrado mínimo de SecureICA

Esta configuración permite especificar el nivel mínimo de cifrado para los datos de sesión enviados entre el servidor y el dispositivo de usuario.

**Importante:** Para Virtual Delivery Agent 7.x, esta configuración de directiva se puede usar solo para habilitar el cifrado de los datos de inicio de sesión con el cifrado RC5 de 128 bits. Hay otras configuraciones que se proporcionan únicamente para la compatibilidad con versiones anteriores de Citrix Virtual Apps and Desktops.

Para VDA 7.x, el cifrado de los datos de inicio de sesión se configura mediante los parámetros básicos del grupo de entrega del VDA. Si se selecciona “Habilitar Secure ICA” para el grupo de entrega, los datos de la sesión se cifran mediante RC5 (128 bits). Si no se selecciona la opción Habilitar Secure ICA para el grupo de entrega, los datos de la sesión se cifran con Cifrado básico.

Al agregar esta configuración a una directiva, seleccione una de las siguientes opciones:

- Básico. Cifra la conexión de cliente mediante un algoritmo distinto de RC5. Este nivel de cifrado protege el flujo de datos para que no pueda leerse directamente, pero puede ser descifrado. De forma predeterminada, el servidor utiliza el cifrado básico para el tráfico entre el cliente y el servidor.
- RC5 (128 bits) solo inicios de sesión. Cifra los datos de inicio de sesión mediante un cifrado RC5 de 128 bits y cifra la conexión de cliente mediante un cifrado básico.
- RC5 (40 bits). Cifra la conexión de cliente mediante un cifrado RC5 de 40 bits.
- RC5 (56 bits). Cifra la conexión de cliente mediante un cifrado RC5 de 56 bits.
- RC5 (128 bits). Cifra la conexión de cliente mediante un cifrado RC5 de 128 bits.

La configuración especificada para el cifrado cliente-servidor puede interactuar con cualquier otra configuración de cifrado existente en el entorno y en el sistema operativo Windows. Si se establece un cifrado de alta prioridad en un servidor o un dispositivo de usuario, se pueden sobrescribir las configuraciones especificadas en los recursos publicados.

Se pueden elevar los niveles de cifrado para proteger aún más las comunicaciones y la integridad de los mensajes de ciertos usuarios. Si una directiva exige un nivel de cifrado mayor, se impide la conexión de Citrix Receivers que usen un nivel de cifrado inferior.

SecureICA no realiza ninguna autenticación ni comprueba la integridad de los datos. Para proporcionar un cifrado integral de extremo a extremo para su sitio, use SecureICA con cifrado TLS.

SecureICA no utiliza algoritmos compatibles con FIPS. Si esto supone algún problema, configure el servidor y Citrix Receivers para que no utilicen SecureICA.

Por motivos de confidencialidad, SecureICA usa el cifrado de bloques RC5 como se describe en RFC 2040. El tamaño del bloque es de 64 bits (un múltiplo de unidades de palabras de 32 bits). La longitud de la clave es de 128 bits. La cantidad de rondas es 12.

Las claves del cifrado de bloques RC5 se negocian cuando se crea una sesión. La negociación se lleva a cabo mediante el algoritmo Diffie-Hellman. Esta negociación utiliza parámetros públicos de Diffie-Hellman, que se almacenan en el Registro de Windows cuando se instala el Virtual Delivery Agent. Los parámetros públicos no son secretos. El resultado de la negociación de Diffie-Hellman es una clave secreta, de la que se derivan las claves de sesión para el cifrado de bloques RC5. Se utilizan claves de sesión independientes para el inicio de sesión de los usuarios y para la transferencia de datos, y también se utilizan claves de sesión independientes para el tráfico hacia y desde el Virtual Delivery Agent. Por lo tanto, hay cuatro claves de sesión para cada sesión. No se almacenan ni las claves secretas ni las claves de sesión. Los vectores de inicialización del cifrado de bloques RC5 también se derivan de la clave secreta.

## Configuraciones de directiva de Límites de servidor

February 6, 2020

La sección Límites de servidor contiene la configuración de directiva para controlar las conexiones inactivas.

### Intervalo de temporizador de servidor inactivo

Esta configuración determina cuánto tiempo, en milésimas de segundo, se mantendrá una sesión de usuario ininterrumpida si este no realiza entradas.

De forma predeterminada, las conexiones inactivas no se desconectan (intervalo de temporizador de servidor inactivo = 0). Citrix recomienda establecer este valor a un mínimo de 60 000 milisegundos (60 segundos).

Para mostrar la directiva, seleccione **Versiones múltiples**, borre las versiones de SO de sesión única y luego seleccione **Límites del servidor**.

#### Nota

Cuando se utiliza esta configuración de directiva, es posible que los usuarios vean el cuadro de diálogo “Idle timer expired” si la sesión ha estado inactiva durante el tiempo especificado. Este mensaje es un cuadro de diálogo de Microsoft; por tanto, no lo controlan las configuraciones de directiva de Citrix. Para obtener más información, consulte <http://support.citrix.com/article/CX118618>.

## Configuraciones de directiva de Límites de sesión

February 6, 2020

La sección **Límites de sesión** contiene configuraciones de directiva para controlar el tiempo que las sesiones pueden permanecer conectadas antes de un cierre forzoso.

#### Importante:

Las configuraciones descritas en este artículo no se aplican a los agentes VDA de Windows Server. Para obtener más información acerca de la configuración de límites de tiempo de sesión para los agentes VDA de servidor, consulte [Microsoft KB - Session Time Limits](#).

### **Temporizador de sesión desconectada**

Esta configuración habilita o inhabilita un temporizador para determinar cuánto tiempo permanece desconectado y bloqueado un escritorio antes de que se cierre la sesión. Si este minuterero está habilitado, la sesión desconectada se cierra cuando el minuterero expira.

De forma predeterminada, las sesiones desconectadas no se cierran.

### **Intervalo de temporizador de sesiones desconectadas**

Esta configuración especifica cuánto tiempo, en minutos, puede permanecer desconectado y bloqueado un escritorio antes de que se cierre la sesión.

De forma predeterminada, este período es de 1440 minutos (24 horas).

### **Temporizador de conexión de sesión**

Esta configuración habilita o inhabilita un temporizador para especificar la duración máxima de una conexión sin interrupciones entre un dispositivo del usuario y un escritorio. Si este temporizador está habilitado, la sesión se desconecta o se cierra cuando caduca el temporizador. La configuración de **Finalizar sesión cuando se alcancen los límites de tiempo** determina el siguiente estado de la sesión.

De manera predeterminada, este temporizador está inhabilitado.

### **Intervalo de temporizador de conexión de sesiones**

Esta configuración especifica el número máximo de minutos de una conexión sin interrupciones entre un dispositivo del usuario y un escritorio.

De forma predeterminada, la duración máxima es 1440 minutos (24 horas).

### **Temporizador de sesión inactiva**

Esta configuración habilita o inhabilita un temporizador que especifica cuánto tiempo se puede mantener ininterrumpida una conexión entre un dispositivo de usuario y un escritorio si el usuario no suministra ninguna entrada. Cuando se agota el tiempo de este temporizador, la sesión pasa al estado desconectado y se aplica el **Temporizador de sesión desconectada**. Si el **Temporizador de sesión desconectada** está inhabilitado, la sesión no se cierra.

De manera predeterminada, este temporizador está habilitado.

## Intervalo de temporizador de sesiones inactivas

Esta configuración especifica cuánto tiempo se mantiene ininterrumpida la conexión entre el dispositivo del usuario y un escritorio si el usuario no realiza entradas.

De forma predeterminada, las conexiones inactivas se mantienen durante 1440 minutos (24 horas).

## Configuraciones de la directiva Fiabilidad de la sesión

September 22, 2021

La sección Fiabilidad de la sesión contiene las configuraciones de directiva para gestionar las conexiones que usan fiabilidad de la sesión.

### Conexiones de fiabilidad de la sesión

Esta configuración permite o impide que las sesiones permanezcan abiertas durante una pérdida de conectividad de red. La Reconexión automática de clientes, junto con la Fiabilidad de la sesión, permiten a los usuarios reconectarse automáticamente a sus sesiones de la aplicación Citrix Workspace después de recuperarse de una interrupción en la red. De forma predeterminada, la Fiabilidad de la sesión está permitida.

Para la aplicación de Citrix Workspace 1808 y versiones posteriores y Citrix Receiver para Windows 4.7 y versiones posteriores, la configuración de Studio se aplica en el cliente. La directiva de Studio reemplaza el objeto de directiva de grupo de Citrix Receiver en los clientes. Las actualizaciones de estas directivas en Studio sincronizan la Fiabilidad de la sesión desde el servidor hasta el cliente.

#### Nota:

- Cuando se trata de Citrix Receiver para Windows 4.7 y versiones posteriores o aplicaciones Citrix Workspace para Windows, establezca la directiva en Studio.
- Cuando se trata de Citrix Receiver para Windows anterior a 4.7, establezca directivas en Studio y en la plantilla del objeto de directiva de grupo de Citrix Receiver en el cliente para un comportamiento uniforme.

Cuando la conectividad de red se ve interrumpida, la fiabilidad de la sesión mantiene las sesiones activas y en la pantalla del usuario. Los usuarios siguen viendo la aplicación que están utilizando hasta que vuelve la conexión.

Con la función Fiabilidad de la sesión, la sesión permanece activa en el servidor. Para indicar que se ha perdido la conectividad, la pantalla del usuario se oscurece. La sesión del usuario puede quedar con-

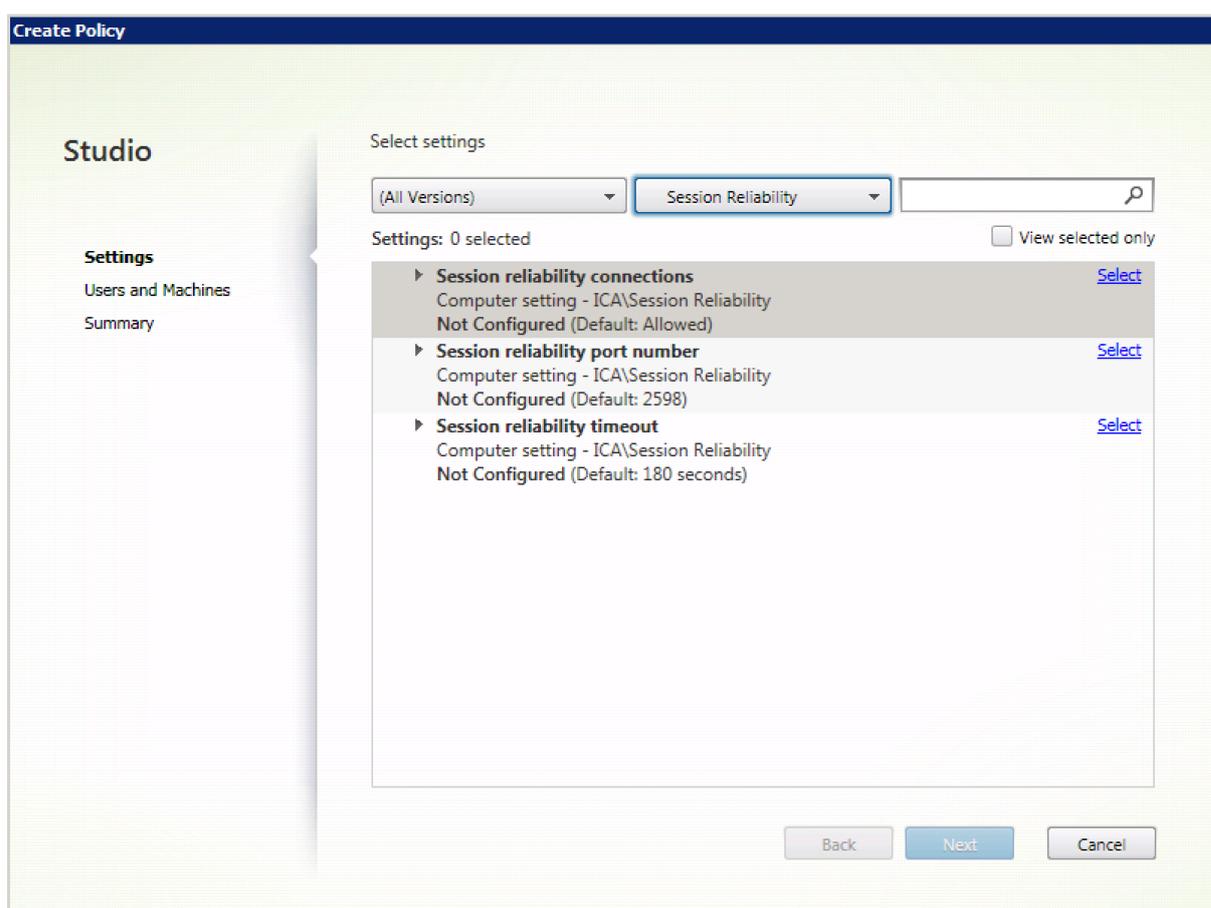
gelada durante la interrupción y puede reanudar la interacción con la aplicación después de restablecerse la conexión de red. La función Fiabilidad de la sesión vuelve a conectar a los usuarios sin pedirles que repitan la autenticación.

Si usa tanto la fiabilidad de la sesión como la reconexión automática de clientes, las dos actúan de manera secuencial. La Fiabilidad de la sesión cierra (o desconecta) la sesión del usuario una vez haya transcurrido el tiempo especificado en Tiempo de espera de fiabilidad de la sesión. A continuación, se aplicará la configuración de directiva de Reconexión automática de clientes y se intentará reconectar al usuario con la sesión desconectada.

De forma predeterminada, la Fiabilidad de la sesión está permitida.

Para inhabilitar la fiabilidad de la sesión:

1. Inicie Citrix Studio.
2. Abra la directiva **Conexiones de fiabilidad de la sesión**.
3. Establezca la directiva en **Prohibida**.



## Número de puerto para fiabilidad de la sesión

Esta configuración especifica el número de puerto TCP para conexiones de fiabilidad de la sesión entrantes.

De forma predeterminada, el número de puerto es el 2598.

Para cambiar el número de puerto de Fiabilidad de la sesión:

1. Inicie Citrix Studio.
2. Abra la directiva **Número de puerto para fiabilidad de la sesión**.
3. Modifique el número de puerto.
4. Haga clic en **OK**.

## Tiempo de espera de fiabilidad de la sesión

Esta configuración especifica el tiempo en segundos que el proxy de fiabilidad de la sesión espera a que se reconecte un usuario, antes de dejar que la sesión sea desconectada.

Aunque se puede alargar el tiempo que se mantiene abierta una sesión, esta función está diseñada para la comodidad del usuario, por lo que no le pedirá que repita la autenticación. Cuanto más tiempo permanezca abierta la sesión, mayor será la probabilidad de que el usuario deje el dispositivo sin supervisión, por lo que podría ser potencialmente accesible a usuarios no autorizados.

De forma predeterminada, el tiempo de espera es de 180 segundos (3 minutos).

Para modificar el tiempo de espera de Fiabilidad de la sesión:

1. Inicie Citrix Studio.
2. Abra la directiva **Tiempo de espera de fiabilidad de la sesión**.
3. Cambie el valor del tiempo de espera.
4. Haga clic en **OK**.

## Configuraciones de directiva de Marca de agua de la sesión

February 6, 2020

La sección “Marca de agua de la sesión” contiene configuraciones para definir esta función. Habilitar esta función provoca un aumento significativo en el consumo del ancho de banda de la red y el consumo de la CPU por parte de la máquina VDA. Recomendamos configurar la marca de agua de la sesión para máquinas VDA concretas en función de los recursos de hardware disponibles.

### **Importante**

Habilite la función de marca de agua de la sesión para que las demás configuraciones de directiva de marca de agua sean efectivas. Para una mejor experiencia de usuario, no habilite más de dos elementos textuales de la marca de agua.

### **Habilitar marca de agua de la sesión**

Cuando habilita esta configuración, aparece una marca de agua textual opaca que muestra información específica de la sesión en la pantalla de la sesión. Las demás configuraciones de marca de agua dependen de que esta configuración esté habilitada.

De forma predeterminada, la marca de agua de la sesión está inhabilitada.

### **Incluir dirección IP del cliente**

Cuando habilita esta configuración, la sesión muestra la dirección IP del cliente actual como una marca de agua.

De forma predeterminada, “Incluir dirección IP del cliente” está inhabilitado.

### **Incluir la hora de la conexión**

Cuando habilita esta configuración, la marca de agua de la sesión muestra la hora de la conexión. El formato es: aaaa/mm/dd hh:mm. La hora que aparece se basa en el reloj del sistema y la zona horaria.

De forma predeterminada, “Incluir la hora de la conexión” está inhabilitado.

### **Incluir nombre de usuario de inicio de sesión**

Cuando habilita esta configuración, la sesión muestra el nombre del usuario que ha iniciado la sesión como una marca de agua. El formato es: NOMBREDEUSUARIO@NOMBREDEDOMINIO. Recomendamos que el nombre de usuario tenga un máximo de 20 caracteres. Si un nombre de usuario contiene más de 20 caracteres, pueden aparecer fuentes de caracteres demasiado pequeñas o puede haber truncamiento de caracteres, con lo que disminuye la eficacia de la marca de agua.

De forma predeterminada, “Incluir nombre de usuario de inicio de sesión” está habilitado.

### **Incluir nombre de host del VDA**

Cuando habilita esta configuración, la sesión muestra el nombre de host del VDA perteneciente a la sesión ICA actual como una marca de agua.

De forma predeterminada, “Incluir nombre de host del VDA” está habilitado.

### **Incluir dirección IP del VDA**

Cuando habilita esta configuración, la sesión muestra la dirección IP del VDA perteneciente a la sesión ICA actual como una marca de agua.

De forma predeterminada, “Incluir dirección IP del VDA” está inhabilitado.

### **Estilo de la marca de agua de la sesión**

Esta configuración controla si se muestra una sola etiqueta de texto de la marca de agua o varias etiquetas. Elija **Múltiple** o **Única** en el menú desplegable **Valor**.

La opción **Múltiple** muestra cinco etiquetas de marca de agua en la sesión. Una en el centro y cuatro en las esquinas.

La opción **Única** muestra una sola etiqueta de marca de agua en el centro de la pantalla de la sesión.

De forma predeterminada, el “Estilo de la marca de agua de la sesión” es “Múltiple”.

### **Texto personalizado de la marca de agua**

Esta configuración especifica una cadena de texto personalizada (por ejemplo, el nombre corporativo) a mostrar en la marca de agua de la sesión. Cuando configura una cadena no vacía, el texto se muestra en una nueva línea que se agrega a la información ya habilitada en la marca de agua.

La cantidad máxima de caracteres que puede contener el texto personalizado de la marca de agua es de 25 caracteres Unicode. Si configura una cadena más larga, se truncará a los 25 caracteres.

No hay texto predeterminado.

### **Transparencia de la marca de agua**

Puede especificar una opacidad de la marca de agua que oscile entre 0 y 100. Cuanto mayor sea el valor especificado, más opaca será la marca de agua.

De forma predeterminada, el valor es 17.

## Parámetros de directiva de control de zona horaria

January 4, 2021

La sección Control de zona horaria contiene parámetros de directiva relacionados con la hora local usada para las sesiones.

### Calcular hora local para clientes antiguos

Este parámetro habilita o inhabilita el cálculo de la zona horaria local de los dispositivos del usuario que envían información inexacta sobre la zona horaria al servidor.

De forma predeterminada, el servidor calcula la zona horaria local cuando es necesario.

Este parámetro está diseñado para su uso con versiones anteriores de Citrix Receiver o clientes ICA que no envían al servidor información detallada acerca de la zona horaria. Cuando se usa con instancias de Citrix Receiver que envían al servidor información detallada acerca de la zona horaria, como las versiones compatibles de Citrix Receiver para Windows, esta configuración no tiene ningún efecto.

### Restaurar la zona horaria del SO de escritorio al desconectar o al cerrar la sesión

Este parámetro determina si el parámetro de zona horaria de un VDA para SO de sesión única se restaura en la zona horaria original de la máquina cuando el usuario se desconecta o cierra la sesión. Si habilita este parámetro, el VDA restaura la zona horaria de la máquina a su configuración original cuando el usuario se desconecta o cierra la sesión. Para que este parámetro surta efecto, establezca **Usar la hora local del cliente** en **Usar la zona horaria del cliente**.

De manera predeterminada, esta configuración está habilitada.

### Usar la hora local del cliente

Este parámetro permite determinar la configuración de zona horaria de la sesión del usuario. Las opciones son la zona horaria de la sesión de usuario ( zona horaria del servidor ) o la zona horaria del dispositivo de usuario (zona horaria del cliente).

De forma predeterminada, se usa la zona horaria de la sesión del usuario.

Para activar esta configuración, habilite el parámetro **Permitir redirección de zona horaria** en el Editor de directivas de grupo. Este parámetro se encuentra en **Directiva de equipo local > Configuración del equipo > Plantillas administrativas > Componentes de Windows > Servicios de Escritorio remoto > Host de sesión de Escritorio remoto > Redirección de dispositivo o recurso**.

Si el VDA es un VDA de SO de sesión única que se ejecuta en un SO multisesión, establezca el derecho de usuario local **Cambiar zona horaria** en **Todos**. Este derecho de usuario se puede encontrar en **Directiva del equipo local > Configuración del equipo > Parámetros de Windows > Parámetros de seguridad > Directivas locales > Asignación de derechos de usuario**.

**Nota:**

En un SO de sesión única, los **usuarios** se incluyen en la asignación de derechos de usuario **Cambiar zona horaria**, aunque no en un SO multisesión. En un SO multisesión, la zona horaria se sincroniza mediante la siguiente directiva de grupo: Configuración del equipo\Plantillas administrativas\Componentes de Windows\Servicios de Escritorio remoto\Host de sesión de Escritorio remoto\Redirección de dispositivo o recurso\Permitir redirección de zona horaria. Esta directiva no se aplica cuando el servidor no es un host de sesión de Escritorio remoto en el VDA del SO multisesión (instalado con el comando `/ServerVDI`). En un SO multisesión, de forma predefinida y por diseño, los usuarios no tienen el derecho local de cambiar la zona horaria.

## Configuraciones de directiva de Dispositivos TWAIN

February 6, 2020

La sección Dispositivos TWAIN contiene configuraciones de directiva relacionadas con la asignación de dispositivos TWAIN del cliente, tales como cámaras digitales o escáneres, y con la optimización de la transferencia de imágenes del servidor al cliente.

**Nota**

TWAIN 2.0 se admite con Citrix Receiver para Windows 4.5.

### Redirección de dispositivos TWAIN del cliente

Esta configuración permite o impide el acceso de los usuarios a los dispositivos TWAIN del dispositivo del usuario desde aplicaciones de tratamiento de imágenes alojadas en servidores. De forma predeterminada, la redirección de dispositivos TWAIN está permitida.

Configuraciones de directiva relacionadas:

- Nivel de compresión TWAIN
- Límite de ancho de banda de redirección de dispositivos TWAIN
- Porcentaje límite de ancho de banda de redirección de dispositivos TWAIN

## Nivel de compresión TWAIN

Esta configuración permite especificar el nivel de compresión para la transferencia de imágenes del cliente al servidor. Utilice Baja para obtener la mejor calidad de imagen, Media para una calidad de imagen intermedia o Alta para una imagen de baja calidad. De forma predeterminada, se aplica la compresión media.

## Configuraciones de directiva de Dispositivos USB

September 22, 2021

La sección **Dispositivos USB** contiene las configuraciones de directiva para gestionar la redirección de archivos para dispositivos USB.

### Reglas de optimización de dispositivos USB del cliente

Las reglas referentes a la optimización de dispositivos USB del cliente se pueden aplicar a los dispositivos para inhabilitar la optimización o para cambiar el modo de optimización.

Cuando el usuario conecta un dispositivo USB, el host comprueba si la configuración de la **directiva USB** permite el dispositivo. Si el dispositivo está permitido, el host comprueba luego las **reglas de optimización para dispositivos USB del cliente** definidas para el dispositivo. Si no se especifica ninguna regla, el dispositivo no está optimizado. El modo de captura (04) es el modo recomendado para los dispositivos de firma. Para otros dispositivos cuyo rendimiento se degrada con la latencia alta, los administradores pueden habilitar el modo interactivo (02). Consulte las descripciones de los modos disponibles en la tabla de este artículo.

### Información útil

- Para usar tabletas y paneles táctiles de firma electrónica Wacom, se recomienda inhabilitar el protector de pantalla. Al final de esta sección, se ofrecen los pasos necesarios para inhabilitar el protector de pantalla.
- Se ha preconfigurado la optimización de la serie de tabletas STU y paneles táctiles de firma electrónica Wacom en la instalación de directivas de Citrix Virtual Apps and Desktops.
- Los dispositivos de firma funcionan en Citrix Virtual Apps and Desktops, y no requieren controladores para usarlos como dispositivos de firma. Wacom dispone de software adicional que se puede instalar para personalizar más el dispositivo. Consulte <http://www.wacom.com/>.

- **Tabletas de dibujo.** Algunos dispositivos de dibujo pueden ser dispositivos de interfaz humana (HID) en buses PCI o ACPI y no se admiten. Conecte esos dispositivos a un controlador de host USB en el cliente para que se redirijan dentro de una sesión de Citrix Virtual Desktops.

Las reglas de directivas tienen el formato de expresiones etiqueta=valor, separadas por un espacio en blanco. Se admiten las siguientes etiquetas:

---

Nombre de la etiqueta	Descripción
Modo	El modo de optimización se admite para dispositivos de entrada de class= <b>03</b> . Los modos admitidos son: Sin optimización: Valor <b>01</b> . Modo interactivo: Valor <b>02</b> . Recomendado para dispositivos como tabletas con lápiz y punteros 3D Pro. Modo de captura: Valor <b>04</b> . Apropriados para dispositivos como paneles táctiles de firma.
VID	Identificador del proveedor, tomado del descriptor del dispositivo, como un número hexadecimal de cuatro dígitos.
PID	Identificador del producto, proveniente del descriptor del dispositivo, como un número hexadecimal de cuatro dígitos.
REV	Identificador de revisión, tomado del descriptor del dispositivo, como un número hexadecimal de cuatro dígitos.
Class	Clase, proveniente del descriptor del dispositivo o de un descriptor de la interfaz.
SubClass	Subclase, proveniente del descriptor del dispositivo o de un descriptor de la interfaz.
Prot	Protocolo proveniente del descriptor del dispositivo o de un descriptor de la interfaz.

---

## Ejemplos

Mode=00000004 VID=067B PID=1230 class=03 #El dispositivo de entrada opera en el modo de captura

Mode=00000002 VID=067B PID=1230 class=03 #El dispositivo de entrada opera en el modo interactivo (opción predeterminada)

Mode=00000001 VID=067B PID=1230 class=03 #El dispositivo de entrada opera sin optimización

Mode=00000100 VID=067B PID=1230 #Configuración de optimización inhabilitada en el dispositivo (valor predeterminado)

Mode=00000200 VID=067B PID=1230 # Configuración de optimización habilitada en el dispositivo

## Inhabilitar el protector de pantalla en paneles táctiles de firma electrónica de Wacom

Para usar tabletas y paneles táctiles de firma electrónica Wacom, Citrix recomienda inhabilitar el protector de pantalla. Puede hacerlo de la siguiente manera:

1. Instale **Wacom-STU-Driver** después de redirigir el dispositivo.
2. Instale **Wacom-STU-Display MSI** para acceder al panel de control del panel táctil de firma electrónica.
3. Vaya a **Control Panel > Wacom STU Display > STU430 o STU530** (Panel de control > Monitor Wacom STU) y seleccione la ficha de su modelo.
4. Elija **Change** y, a continuación, seleccione **Yes** cuando aparezca la ventana de seguridad UAC.
5. Seleccione **Disable slideshow** y haga clic en **Apply**.

Cuando el parámetro esté establecido en un panel de firma electrónica que se utiliza como modelo, se aplicará a todos los modelos.

## Redirección de dispositivos USB del cliente

Esta configuración permite o impide la redirección de dispositivos USB desde el dispositivo del usuario y hacia él.

De forma predeterminada, los dispositivos USB no se redirigen.

## Reglas de redirección de dispositivos USB del cliente

Esta configuración especifica las reglas de redirección para dispositivos USB.

De forma predeterminada, no se especifica ninguna regla.

Cuando un usuario conecta un dispositivo USB, el dispositivo host consulta cada regla de directiva hasta que encuentra una coincidencia, es decir una directiva donde figure el dispositivo en cuestión. La primera coincidencia para cualquier dispositivo se considera definitiva. Si la primera coincidencia es una regla para Permitir (Allow), el dispositivo se coloca en comunicación remota con el escritorio virtual. Si la primera coincidencia es una regla para Denegar (Deny), el dispositivo solamente está disponible en el escritorio local. Si no hay coincidencias, se usan las reglas predeterminadas.

Las reglas de directivas tienen el formato {Allow:|Deny:} seguidas de un conjunto de expresiones etiqueta=valor, separadas por un espacio en blanco. Se admiten las siguientes etiquetas:

---

Nombre de la etiqueta	Descripción
VID	Identificador del proveedor tomado del descriptor del dispositivo
PID	Identificador del producto tomado del descriptor del dispositivo
REL	Identificador de la versión tomado del descriptor del dispositivo
Class	Clase, tomada del descriptor del dispositivo o de un descriptor de la interfaz
SubClass	Subclase, tomada del descriptor del dispositivo o de un descriptor de la interfaz
Prot	Protocolo tomado del descriptor del dispositivo o de un descriptor de la interfaz

---

Al crear reglas de directivas, recuerde:

- Las reglas no distinguen entre mayúsculas y minúsculas.
- Las reglas pueden tener un comentario optativo al final que se introduce con el signo #.
- Se ignoran las líneas en blanco y las que son exclusivamente de comentario.
- Las etiquetas deben utilizar el operador de coincidencia = (por ejemplo, VID=067B\_).
- Cada regla debe comenzar en una línea nueva o formar parte de una lista de reglas, separadas por punto y coma.
- Consulte los códigos de clase USB que están disponibles en el sitio web de USB Implementers Forum, Inc.

Ejemplos de reglas de directivas USB definidas por el administrador:

- Permitir: VID=067B PID=0007 # Otra Industria, Otra unidad de Flash
- Denegar: Class=08 subclass=05 # Almacenamiento masivo
- Para crear una regla que rechace todos los dispositivos USB, use “DENY:” sin otras etiquetas.

## **Redirección de dispositivos USB Plug and Play del cliente**

Esta configuración permite o impide que los dispositivos Plug and Play, tales como cámaras o terminales de punto de venta (POS), se usen en sesiones de cliente.

De forma predeterminada, la redirección de dispositivos Plug and Play está permitida. Si se establece como Permitida, todos los dispositivos Plug and Play que pertenecen a usuarios o grupos específicos se redirigen. Si se establece como Prohibida, ningún dispositivo se redirige.

## Configurar redirección automática de dispositivos USB

Los dispositivos USB se redirigen automáticamente cuando la funcionalidad de USB está habilitada y la configuración de las preferencias de usuario para USB está definida para conectar automáticamente los dispositivos USB.

### Nota:

En Receiver para Windows 4.2, los dispositivos USB también se redirigen automáticamente cuando se trabaja en modo Desktop Appliance y la barra de conexión no está presente. En versiones anteriores de Citrix Receiver para Windows, los dispositivos USB también se redirigen automáticamente cuando funcionan en modo de dispositivo de escritorio o con aplicaciones alojadas en máquinas virtuales (VM).

No siempre es mejor redirigir todos los dispositivos USB. Los usuarios pueden redirigir explícitamente dispositivos seleccionándolos en la lista de dispositivos USB que no se redirigen automáticamente. Para evitar que los dispositivos USB se incluyan o redirijan, use DeviceRules en el dispositivo de punto final del cliente o en el VDA. Consulte las Guías de administración para obtener más detalles.

### Precaución

Utilizar el Editor del Registro de forma incorrecta puede provocar problemas graves que podrían conllevar la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

## Parámetros de preferencias de usuario para la redirección automática de dispositivos USB

Directiva:

1. Abra el **Editor de directivas de grupo local** y vaya a **Plantillas administrativas > Componentes de Citrix > Citrix Receiver > Uso remoto de dispositivos cliente > Uso remoto de USB genérico**.
2. Abra **Nuevos dispositivos USB**, seleccione **Habilitado** y haga clic en **Aceptar**.
3. Abra **Dispositivos USB existentes**, seleccione **Habilitado** y haga clic en **Aceptar**.

Citrix Receiver:

1. Vaya a **Preferencias de Citrix Receiver > Conexiones**.
2. Asegúrese de que las siguientes opciones estén seleccionadas:
  - Conectar dispositivos automáticamente al comenzar una sesión

- Cuando se conecta un nuevo dispositivo mientras se ejecuta una sesión, conectar el dispositivo automáticamente.

3. Haga clic en **OK**.

Todas las claves de Registro y los cambios de directiva se aplican al dispositivo cliente de Windows.

### **Redirección de impresoras USB simples**

La mejor solución para impresoras USB simples es utilizar el controlador de impresora universal dedicado y el canal virtual para realizar la impresión. De forma predeterminada, las impresoras USB simples no se redirigen automáticamente.

Las impresoras simples se detectan mediante datos heurísticos, y se espera que las impresoras avanzadas con funciones de escaneo, por ejemplo, puedan tener que redirigirse con la ayuda de la funcionalidad de USB para funcionar correctamente.

Utilice este Registro para establecer si las impresoras simples se redirigen automáticamente:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Nombre: AutoRedirectPrinters

Tipo: DWORD

Datos: 00000000

El valor predeterminado es 0 (no redirige automáticamente). Al establecer un valor distinto de cero, se permite que el soporte USB redirija las impresoras USB simples.

También puede implementar directivas de Active Directory en esta clave de Registro y anular el valor que no corresponda a la directiva si ambos están presentes:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Nombre: AutoRedirectAudio

Tipo: DWORD

Datos: 00000000

### **Redirección de dispositivos de sonido simples**

Al igual que las impresoras simples, la mejor experiencia de usuario se logra mediante el canal virtual de audio dedicado de ICA para enviar datos de audio desde dispositivos de sonido simples. Sin embargo, es posible que deba redirigir algunos dispositivos especializados mediante el soporte USB. Los datos heurísticos se utilizan para determinar qué dispositivos son dispositivos de sonido simples.

Utilice este Registro para establecer si los dispositivos de sonido simples se redirigen automáticamente:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Nombre: AutoRedirectAudio

Tipo: DWORD

Datos: 00000000

El valor predeterminado es 0 (no redirige automáticamente). Al establecer un valor distinto de cero, redirige los dispositivos de sonido simples mediante la funcionalidad de USB.

También puede utilizar las directivas de Active Directory para implementar este valor en la clave de Registro y anular el valor que no corresponda a la directiva si ambos están presentes:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Nombre: AutoRedirectVideo

Tipo: DWORD

Datos: 00000000

### **Redirección de dispositivos de almacenamiento simples (dispositivo de almacenamiento masivo)**

Para los dispositivos de almacenamiento simples, obtiene la mejor experiencia de usuario mediante el canal virtual dedicado, como la asignación de unidades del cliente que también realiza la optimización. Además de la simple lectura o escritura de archivos, para realizar ciertas tareas especiales como grabar un CD/DVD o acceder a dispositivos de sistemas de archivos cifrados, es posible que el dispositivo aún deba redirigirse con la funcionalidad de USB genérico.

Los datos heurísticos se utilizan para determinar qué dispositivos son dispositivos de almacenamiento simples. Utilice esta clave de Registro para establecer si los dispositivos de almacenamiento simples se redirigen automáticamente:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Nombre: AutoRedirectStorage

Tipo: DWORD

Datos: 00000000

El valor predeterminado es 0 (no redirige automáticamente). Al establecer un valor distinto de cero, redirige los dispositivos de almacenamiento simples mediante la funcionalidad de USB.

También puede utilizar las directivas de Active Directory para implementar este valor en la siguiente clave de Registro y anular el valor que no corresponda a la directiva si ambos están presentes:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Nombre: AutoRedirectStorage

Tipo: DWORD

Datos: 00000000

Nota:

El acceso de solo lectura al dispositivo de almacenamiento simple no se puede configurar si está utilizando la funcionalidad de USB genérico, mientras que se puede configurar si se usa la asignación de unidades del cliente.

### **Dispositivo de memoria USB con redirección de cifrado de hardware**

Los dispositivos de memoria USB con cifrado de hardware suelen consistir en una partición de almacenamiento cifrada y una segunda partición de *utilidad* que contiene una utilidad para desbloquear la partición cifrada. Para los dispositivos de memoria USB, obtendrá la mejor experiencia de usuario mediante la asignación de unidades del cliente dedicada, como el canal virtual HDX de la asignación de unidades del cliente/asignación dinámica de dispositivos de memoria en formato thumb-drive que también realiza la optimización.

La redirección de USB genérico es necesaria para clientes que no son de Windows (por ejemplo, clientes de Linux) y casos en los que el cliente ha restringido (bloqueado) el acceso de los usuarios a las funciones locales en el cliente. La redirección de USB genérico puede redirigir cualquier dispositivo de almacenamiento USB sin cifrado de hardware a las sesiones de VDA del SO de sesión única y SO multisesión.

Antes de la versión Citrix Virtual Apps and Desktops 7 1808, los dispositivos de memoria USB con cifrado de hardware no podían redirigirse de ninguna manera útil a las sesiones en VDA de SO de sesión única y SO multisesión. Una nueva mejora de funciones introducida en Citrix Virtual Apps and Desktops 7 1808 admite el redireccionamiento USB genérico de dispositivos de memoria USB con cifrado de hardware en sesiones de VDA de SO de sesión única y SO multisesión.

Después de que se redirija el dispositivo, ninguna de sus unidades aparece en el cliente local. Por lo tanto, si se requiere desbloquear la unidad, desbloquéela en la sesión. Esta función requiere la actualización de Windows KB4074590.

### **Dispositivos simples de imagen fija (escáneres y cámaras digitales)**

Para los dispositivos simples de imagen fija, obtendrá la mejor experiencia de usuario mediante el canal virtual dedicado, como el canal virtual TWAIN, que también realiza la optimización. Estos dispositivos deben cumplir con los estándares de la industria. Si un dispositivo no es conforme o si no se usa de acuerdo con las intenciones originales, la redirección de USB genérico podría ser la única

forma de usar el dispositivo. Los datos heurísticos se utilizan para determinar qué dispositivos son dispositivos simples de imagen fija.

Utilice esta clave de Registro para establecer si los dispositivos simples de imagen fija se redirigen automáticamente:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Nombre: AutoRedirectImage

Tipo: DWORD

Datos: 00000000

El valor predeterminado es 0 (no redirige automáticamente). Al establecer un valor distinto de cero, redirige los dispositivos simples de imagen fija mediante el USB genérico.

También puede utilizar las directivas de Active Directory para implementar este valor en la siguiente clave de Registro y anular el valor que no corresponda a la directiva si ambos están presentes:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Nombre: AutoRedirectImage

Tipo: DWORD

Datos: 00000000

### **Parámetros específicos del dispositivo**

Los procesos heurísticos utilizados para seleccionar dispositivos optimizables de Citrix (como impresoras, dispositivos de sonido, vídeo, almacenamiento e imágenes fijas) no siempre coinciden con lo que usted quiere. Es posible que quiera controlar la redirección automática de los dispositivos que no figuran en la lista anterior. Puede controlar la redirección automática según el dispositivo.

Por ejemplo, no es necesario redireccionar el lector de códigos de barras DemoTech 2000 mediante la funcionalidad de USB. Tiene un identificador de proveedor de 12AB y un identificador de producto de 5678. Estos números hexadecimales se pueden encontrar en el Administrador de dispositivos.

Para evitar que esto se redirija automáticamente, cree esta clave de Registro específica del dispositivo:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

Nombre: AutoRedirect

Tipo: DWORD

Datos: 00000000

Un valor de 0 evita que el dispositivo se redirija automáticamente. Un valor distinto de cero indica que el dispositivo debe considerarse para la redirección automática (según las preferencias del usuario). Hay un único carácter de espacio entre el proveedor y los identificadores de producto.

También puede implementar este valor mediante las directivas de Active Directory en esta clave de Registro. Anula el valor que no corresponda a la directiva si ambos están presentes:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices\VID12AB  
PID5678

Nombre: AutoRedirect

Tipo: DWORD

Datos: 00000000

La configuración de AutoRedirect específica del dispositivo tiene prioridad sobre los valores más generales de AutoRedirectXXX explicados anteriormente. Los procesos heurísticos predeterminados para dispositivos optimizados de Citrix pueden malinterpretar un dispositivo como genérico. Por lo tanto, establezca el valor de AutoRedirect específico del dispositivo en 1 para redirigirlo automáticamente.

## Configuraciones de directiva de Presentación visual

September 22, 2021

La sección Presentación visual contiene configuraciones de directiva para controlar la calidad de las imágenes enviadas desde los escritorios virtuales al dispositivo del usuario.

### Profundidad de color preferida para gráficos simples

Esta configuración de directiva se encuentra disponible en las versiones de VDA 7.6 FP3 y las versiones posteriores. La opción de 8 bits está disponible en las versiones de VDA 7.12 y las versiones posteriores.

Esta configuración hace posible reducir la profundidad de color en los gráficos sencillos que se envían a través de la red. Reducir el color a 8 o 16 bits por píxel ofrece una mejora potencial de la capacidad de respuesta en conexiones de poco ancho de banda, a costa de una pequeña degradación de la calidad de imagen. La profundidad de color de 8 bits no se admite cuando la configuración de directiva [Usar códec de vídeo para compresión](#) está definida en “Para la pantalla entera”.

El valor predeterminado es la profundidad de color preferida de 24 bits por píxel.

Los VDA vuelven a la profundidad de color de 24 bits (predeterminada) si la opción de 8 bits se aplica a VDA 7.11 y versiones anteriores.

## Velocidad de fotogramas de destino

Esta configuración especifica la cantidad máxima de fotogramas por segundo que se envían desde el escritorio virtual al dispositivo de usuario.

De forma predeterminada, el valor máximo es 30 fotogramas por segundo.

Establecer una cantidad alta de fotogramas por segundo (por ejemplo, 30) mejora la experiencia del usuario, pero requiere más ancho de banda. Reducir la cantidad de fotogramas por segundo (por ejemplo, a 10) maximiza la escalabilidad del servidor a expensas de la experiencia del usuario. Para los dispositivos de usuario con CPU lentas, especifique un valor inferior para mejorar la experiencia de usuario.

La velocidad máxima permitida es de 60 fotogramas por segundo.

## Calidad visual

Esta configuración especifica la calidad visual de las imágenes que se muestran en el dispositivo del usuario.

De forma predeterminada, se establece en Media.

Para especificar la calidad de la imagen, seleccione una de las siguientes opciones:

- **Baja:** Se recomienda para redes con ancho de banda limitado donde la calidad visual se puede sacrificar para ganar en interactividad
- **Media:** Ofrece la mejor eficiencia de rendimiento y de ancho de banda en la mayoría de los casos de uso
- **Alta:** Opción recomendada cuando se requiere calidad de imagen sin pérdida
- **Gradual sin pérdida:** Envía imágenes con pérdida al dispositivo de usuario durante los períodos de mayor actividad en la red, e imágenes sin pérdida cuando la actividad en la red disminuye. Esta configuración mejora el rendimiento en conexiones de ancho de banda limitado.
- **Siempre sin pérdida:** En situaciones en que resulta totalmente necesario conservar la calidad de la imagen, seleccione “Siempre sin pérdida” para que nunca se envíen datos incompletos al dispositivo del usuario. Por ejemplo, al mostrar radiografías, donde una pérdida de calidad sería inaceptable.

## Configuraciones de directiva de Imágenes en movimiento

February 6, 2020

La sección Imágenes en movimiento contiene configuraciones que le permiten quitar o modificar la compresión para imágenes dinámicas.

### Calidad de imagen mínima

Nota: Para Virtual Delivery Agent 7.x, esta configuración de directiva solo se aplica cuando la configuración de directiva Modo de gráficos antiguo está habilitada.

Esta configuración especifica la calidad de imagen mínima aceptable para la pantalla adaptable. Cuanto menor sea la compresión que se utilice, mayor es la calidad de las imágenes que se muestran. Elija la compresión entre las opciones Superalta, Muy alta, Alta, Normal y Baja.

De forma predeterminada, esta opción se establece en Normal.

### Compresión de imágenes en movimiento

Esta configuración especifica si se habilita o no la pantalla adaptable. La pantalla adaptable ajusta automáticamente la calidad de imagen de los vídeos y las diapositivas de transición de las presentaciones según el ancho de banda disponible. Si la pantalla adaptable está habilitada, los usuarios pueden ver presentaciones de ejecución fluida, sin pérdida de calidad.

De manera predeterminada, la función de pantalla adaptable está habilitada.

Desde la versión 7.0 hasta la versión 7.6 de VDA, esta opción de configuración se aplica solo cuando el modo de gráficos antiguo está habilitado. Para VDA 7.6 FP1 y versiones posteriores, esta opción de configuración se aplica cuando el modo de gráficos antiguo está habilitado, o bien cuando el modo de gráficos antiguo está inhabilitado y no se usa ningún códec de vídeo para comprimir los gráficos.

Cuando el modo de gráficos antiguo está habilitado, la sesión debe reiniciarse para que los cambios de la directiva surtan efecto. La pantalla adaptable y la presentación progresiva se excluyen mutuamente; es decir, habilitar la pantalla adaptable inhabilita la presentación progresiva y viceversa. Sin embargo, tanto la presentación progresiva como la pantalla adaptable se pueden inhabilitar al mismo tiempo. La presentación progresiva, como función de versiones anteriores, no se recomienda para XenApp o XenDesktop. Establecer un umbral de presentación progresiva inhabilitará la pantalla adaptable.

## Nivel de compresión progresiva

Nota: Para Virtual Delivery Agent 7.x, esta configuración de directiva solo se aplica cuando la configuración de directiva Modo de gráficos antiguo está habilitada.

Esta configuración permite una presentación inicial con menor detalle pero más rápida.

De forma predeterminada, no se aplica la compresión progresiva.

La imagen más detallada aparece cuando está ya disponible, definida por la configuración de compresión con pérdida normal. Use la compresión Muy alta o Superalta para una presentación mejorada de gráficos que usan mucho ancho de banda, como las fotografías.

Para que la compresión progresiva sea efectiva, el nivel de compresión debe ser mayor que el definido en la configuración Nivel de compresión con pérdida.

Nota: Un mayor nivel de compresión asociado a la compresión progresiva también mejora la interactividad de imágenes dinámicas en las conexiones de cliente. La calidad de una imagen dinámica, como un modelo tridimensional en movimiento, disminuye temporalmente hasta que la imagen deja de moverse; en ese momento, se aplica la configuración del nivel de compresión con pérdida normal.

Configuraciones de directiva relacionadas:

- Valor de umbral de compresión progresiva
- Compresión intensa progresiva

## Valor de umbral de compresión progresiva

Nota: Para Virtual Delivery Agent 7.x, esta configuración de directiva solo se aplica cuando la configuración de directiva Modo de gráficos antiguo está habilitada.

Esta configuración indica el valor máximo de ancho de banda (en kilobits por segundo), para una conexión a la que se aplica la compresión progresiva. Se aplica exclusivamente a las conexiones de cliente con un ancho de banda menor.

El umbral predeterminado es de 2 147 483 647 kilobits por segundo.

Configuraciones de directiva relacionadas:

- Valor de umbral de compresión progresiva
- Compresión intensa progresiva

## Velocidad de fotogramas mínima de destino

Esta configuración especifica la velocidad de fotogramas por segundo mínima que el sistema intenta mantener para imágenes dinámicas cuando la conexión cuenta con poco ancho de banda.

De forma predeterminada, el valor es de 10 fps.

Desde la versión 7.0 hasta la versión 7.6 de VDA, esta opción de configuración se aplica solo cuando el modo de gráficos antiguo está habilitado. A partir de la versión 7.6 FP1 de VDA, esta opción de configuración se aplica cuando el modo de gráficos antiguo está habilitado o inhabilitado.

## **Configuraciones de directiva de Imágenes fijas**

January 4, 2021

La sección Imágenes fijas contiene configuraciones que permiten quitar o modificar la compresión para imágenes estáticas.

### **Compresión de color adicional**

Esta configuración habilita o inhabilita el uso de la compresión de color adicional en imágenes enviadas a través de conexiones cliente que tienen una limitación de ancho de banda, con lo que se mejora la capacidad de respuesta al reducir la calidad de las imágenes presentadas.

De forma predeterminada, la compresión de color adicional está inhabilitada.

Cuando está habilitada, la compresión adicional de color se aplica solamente cuando el ancho de banda de la conexión del cliente está por debajo del valor especificado en Umbral de compresión de color adicional. Cuando el ancho de banda de la conexión de cliente es superior al umbral o la configuración está Inhabilitada, no se aplica la compresión.

### **Umbral de compresión de color adicional**

Nota: Para Virtual Delivery Agent 7.x, esta configuración de directiva solo se aplica cuando la configuración de directiva Modo de gráficos antiguo está habilitada.

Esta configuración indica el valor máximo de ancho de banda de una conexión (en kilobits por segundo), por debajo del cual se aplicará la compresión de color adicional. Si el ancho de banda de la conexión de cliente cae por debajo del valor establecido, se aplica la compresión de color adicional (si está habilitada).

El umbral predeterminado es de 8192 kilobits por segundo.

## **Compresión intensa**

Nota: Para Virtual Delivery Agent 7.x, esta configuración de directiva solo se aplica cuando la configuración de directiva Modo de gráficos antiguo está habilitada.

Esta configuración habilita o inhabilita la reducción del ancho de banda más allá de la compresión progresiva sin reducir la calidad de la imagen, mediante un algoritmo para gráficos más avanzado pero que requiere un uso más intensivo de CPU.

La compresión intensa está inhabilitada de forma predeterminada.

Si se la habilita, la compresión intensa se aplica a todas las configuraciones de compresión con pérdida. Se admite en la aplicación Citrix Workspace, pero no tiene ningún efecto en otros plug-ins.

Configuraciones de directiva relacionadas:

- Nivel de compresión progresiva
- Valor de umbral de compresión progresiva

## **Nivel de compresión con pérdida**

Nota: Para Virtual Delivery Agent 7.x, esta configuración de directiva solo se aplica cuando la configuración de directiva Modo de gráficos antiguo está habilitada.

Esta configuración permite controlar el grado de compresión con pérdida de información usado para las imágenes transmitidas a través de conexiones de cliente que tienen un ancho de banda limitado. En tales casos, la presentación de imágenes sin comprimir puede tardar mucho.

De forma predeterminada, se utiliza una compresión media.

Para mejorar la capacidad de respuesta al usar imágenes que consumen mucho ancho de banda, use la compresión alta. En aquellos casos en los que es muy importante mantener toda la información de la imagen, como, por ejemplo, al ver imágenes de rayos X en situaciones en las que no es aceptable perder calidad, se recomienda no utilizar compresión con pérdida.

Configuración de directiva relacionada: Valor de umbral de compresión con pérdida

## **Valor de umbral de compresión con pérdida**

Nota: Para Virtual Delivery Agent 7.x, esta configuración de directiva solo se aplica cuando la configuración de directiva Modo de gráficos antiguo está habilitada.

Esta configuración indica el valor máximo de ancho de banda (en kilobits por segundo) de una conexión a la que se aplicará compresión con pérdida.

El umbral predeterminado es de 2 147 483 647 kilobits por segundo.

Si se agrega la configuración Nivel de compresión con pérdida a una directiva y no se especifica ningún umbral, se puede incrementar la velocidad de presentación de mapas de bits con gran nivel de detalle, tales como fotografías, en una LAN.

Configuración de directiva relacionada: Nivel de compresión con pérdida

## Configuraciones de directiva de WebSockets

September 22, 2021

La sección “WebSockets” contiene configuraciones de directiva para acceder con la aplicación Citrix Workspace para HTML5 a los escritorios virtuales y las aplicaciones alojadas. La función WebSockets aumenta la seguridad y reduce la sobrecarga al llevar a cabo una comunicación bidireccional entre las aplicaciones basadas en exploradores web y los servidores, sin abrir varias conexiones HTTP.

### Conexiones con WebSockets

Esta configuración permite o prohíbe conexiones de WebSockets.

De forma predeterminada, las conexiones de WebSockets están prohibidas.

### Número de puerto de WebSockets

Esta configuración identifica el puerto para conexiones entrantes de WebSocket.

De forma predeterminada, el valor es de 8008.

### Lista de servidores de origen de WebSockets de confianza

Esta configuración proporciona una lista separada por comas de los servidores de origen de confianza (suele ser la aplicación Citrix Workspace para Web), expresados como direcciones URL. El servidor solo acepta conexiones de WebSockets procedentes de alguna de estas direcciones.

De forma predeterminada, se utiliza el carácter comodín \* para confiar en todas las URL de la aplicación Citrix Workspace para Web.

Para escribir una dirección en la lista, use la siguiente sintaxis:

<protocolo>://<Nombre de dominio completo del host>:[puerto]

El protocolo debe ser HTTP o HTTPS. Si no se especifica el puerto, se usa el puerto 80 para HTTP y el puerto 443 para HTTPS.

El carácter comodín \* se puede utilizar en la URL si no se trata de una dirección IP (10.105.\*.\*).

## Configuraciones de la directiva Administración de carga

September 22, 2021

La sección Administración de carga contiene configuraciones de directiva para habilitar y configurar la administración de carga entre los servidores que entregan máquinas con SO multisesión Windows.

Para obtener información sobre cómo calcular el índice del patrón de carga, consulte [CTX202150](#).

### Tolerancia de inicios de sesión simultáneos

Esta configuración especifica la cantidad máxima de inicios de sesión simultáneos que un servidor puede aceptar.

De forma predeterminada, este valor está establecido en 2.

Cuando esta configuración está habilitada, el equilibrio de carga intenta evitar tener más de la cantidad especificada de inicios de sesión activos en un servidor VDA al mismo tiempo. Sin embargo, el límite no se aplica estrictamente. Para reforzar el límite (y provocar que fallen los inicios de sesión simultáneos que superan la cantidad especificada), cree la siguiente clave del Registro:

```
HKLM\Software\Citrix\DesktopServer\LogonTolerancelHardLimit
```

```
Tipo: DWORD
```

```
Valor: 1
```

### Uso de CPU

Esta configuración especifica el nivel de uso de CPU (como un porcentaje), alcanzado el cual, el servidor notifica carga completa. Cuando está habilitada, el valor predeterminado en el que el servidor notifica carga completa es del 90%.

De forma predeterminada, esta configuración está inhabilitada y el uso de la CPU queda excluido al calcular la carga.

### Prioridad de procesos excluidos para el uso de CPU

Esta configuración especifica el nivel de prioridad en el que el uso de la CPU de un proceso se excluye del índice de carga de Uso de CPU.

De forma predeterminada, este valor está establecido en Por debajo de lo normal o Baja.

## **Uso del disco**

Esta configuración especifica la longitud de la cola de disco en la que el servidor notifica carga completa al 75%. Cuando está habilitada, el valor predeterminado para la longitud de la cola de disco es 8.

De forma predeterminada, esta configuración está inhabilitada y el uso del disco queda excluido al calcular la carga.

## **Número máximo de sesiones**

Esta configuración especifica el número máximo de sesiones que un servidor puede alojar. Cuando está habilitada, el valor predeterminado para la cantidad máxima de sesiones que un servidor puede alojar es 250.

De manera predeterminada, esta configuración está habilitada.

## **Uso de memoria**

Esta configuración especifica el nivel de uso de la memoria (como un porcentaje) alcanzado el cual, el servidor notifica carga completa. Cuando está habilitada, el valor predeterminado en el que el servidor notifica carga completa es del 90%.

De forma predeterminada, esta configuración está inhabilitada y el uso de la memoria queda excluido al calcular la carga.

## **Carga base de uso de memoria**

Esta configuración especifica una aproximación del uso de memoria del sistema operativo base y define, en MB, el uso de memoria por debajo del cual se considera que el servidor tiene carga cero.

De forma predeterminada, este valor está establecido en 768 MB.

## **Configuraciones de directiva de Profile Management**

September 22, 2021

Esta sección contiene configuraciones de directiva para habilitar la administración de perfiles del componente Profile Management y especificar qué grupos incluir y excluir en el procesamiento de Profile Management.

Para otra información, como los nombres de los parámetros del archivo INI equivalentes y la versión de Profile Management necesaria para cualquier configuración de directiva en particular, consulte [Directivas de Profile Management](#).

## Configuraciones avanzadas de directiva

September 22, 2021

### Reintentos de acceso a archivos bloqueados

Establece el número de reintentos al acceder a archivos bloqueados.

Si esta directiva está inhabilitada, se utilizará el valor predeterminado de cinco reintentos. Si esta directiva no está configurada aquí, se utiliza el valor del archivo INI. Si esta directiva no está configurada aquí ni en el archivo INI, se utiliza el valor predeterminado.

### Procesar cookies de Internet al cerrar la sesión

Algunas implementaciones dejan cookies de Internet a las que el archivo Index.dat no hace referencia. Estas cookies adicionales que permanecen en el sistema de archivos después de múltiples consultas pueden sobrecargar los perfiles. Habilite esta directiva para forzar el procesamiento de Index.dat y eliminar las cookies adicionales. Esta directiva alarga los tiempos de desconexión, de manera que se recomienda habilitarla solamente si ocurre el problema citado.

Si esta directiva no está configurada aquí, se utiliza el valor del archivo INI. Si esta directiva no está configurada aquí ni en el archivo INI, no se procesará Index.dat.

### Inhabilitar configuración automática

Profile Management examina todos los entornos de Citrix Virtual Desktops para detectar, por ejemplo, la presencia de discos Personal vDisk y configura la directiva de grupo como corresponda. Solo se ajustan las directivas de Profile Management que tengan el estado No configurada, para conservar las personalizaciones que haya realizado. Esta función aumenta la velocidad de implementación y simplifica la optimización. La función no requiere ninguna configuración, pero puede inhabilitar la configuración automática al actualizar (para conservar la configuración de versiones anteriores) o durante la solución de problemas. La configuración automática no funciona en entornos de Citrix Virtual Apps u otros.

Puede considerar la configuración automática como un comprobador de configuraciones dinámico que define automáticamente la configuración de directiva predeterminada según los entornos en ejecución. Elimina la necesidad de definir la configuración manualmente. Los entornos en ejecución incluyen:

- SO de Windows
- Versiones del SO de Windows
- Presencia de Citrix Virtual Desktops
- Presencia de discos Personal vDisk

Es posible que la configuración automática cambie las directivas siguientes si el entorno cambia:

- Reescritura activa
- Guardar siempre en caché
- Eliminar perfiles guardados en caché local al cerrar la sesión
- Demora antes de eliminar perfiles en caché
- Streaming de perfiles

Consulte esta tabla para ver el estado predeterminado de las directivas en diferentes sistemas operativos:

---

	SO multisesión	SO de sesión única
Reescritura activa	Habilitado	<i>Inhabilitado</i> si el disco Personal vDisk se está utilizando; de lo contrario, habilitado.
Guardar siempre en caché	Inhabilitada	<i>Inhabilitado</i> si el disco Personal vDisk se está utilizando; de lo contrario, habilitado.
Eliminar perfiles guardados en caché local al cerrar la sesión	Habilitado	<i>Inhabilitado</i> si el disco Personal vDisk se está utilizando, si Citrix Virtual Desktops está asignado o si Citrix Virtual Desktops no está instalado; de lo contrario, habilitado.
Demora antes de eliminar perfiles en caché	0 segundos	60 segundos si los cambios del usuario no son persistentes; de lo contrario, 0 segundos.
Streaming de perfiles	Habilitado	<i>Inhabilitado</i> si el disco Personal vDisk se está utilizando; de lo contrario, habilitado.

---

Sin embargo, con la configuración automática inhabilitada, todas las directivas anteriores también quedan **inhabilitadas** de forma predeterminada.

A partir de Profile Management 1909, puede disfrutar de una mejor experiencia con el menú Inicio en Windows 10 (desde la versión 1607 en adelante), y Windows Server 2016 y versiones posteriores. Esta mejora se logra mediante la configuración automática de las siguientes directivas:

- Agregue “Appdata\Local\Microsoft\Windows\Caches”y “Appdata\Local\Packages”a “Carpetas para reflejar”.
- Agregue “Appdata\Local\Microsoft\Windows\UsrClass.Dat\*”a “Archivos para sincronizar”.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado aquí ni en el archivo INI, se activa la configuración automática. Por eso, es posible que los parámetros de Profile Management cambien si el entorno cambia.

### **Cerrar la sesión del usuario si hay algún problema**

Si esta directiva está inhabilitada o no está configurada, los usuarios reciben un perfil temporal si ocurre algún problema (por ejemplo, si el almacén de los usuarios no está disponible). Si está habilitada, se muestra un mensaje de error y se cierra la sesión de los usuarios. Eso puede simplificar la solución del problema.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si este parámetro no se define ni aquí ni en el archivo INI, se ofrece un perfil temporal.

### **Customer Experience Improvement Program**

De forma predeterminada, se habilita el programa para la mejora de la experiencia de usuario CEIP (Customer Experience Improvement Program) para ayudar a mejorar la calidad y el rendimiento de los productos Citrix mediante el envío de información de uso y estadísticas anónimas.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

### **Habilitar itinerancia del índice de búsqueda de Outlook**

Para ofrecer una experiencia de búsqueda de Outlook nativo por usuario, puede activar la itinerancia automáticamente de los datos de búsqueda de Outlook junto con el perfil del usuario. Esto requiere espacios adicionales en el almacén de usuarios para guardar el índice de búsqueda de Outlook.

Debe cerrar la sesión y volver a iniciarla para que esta directiva surta efecto.

## **Base de datos del índice de búsqueda de Outlook: Copia de seguridad y restauración**

Este parámetro configura lo que Profile Management hace durante el inicio de sesión cuando se activa Habilitar la itinerancia del índice de búsqueda de Outlook.

Si este parámetro está habilitado, Profile Management guarda una copia de seguridad de la base de datos del índice de búsqueda cada vez que la base de datos se monta correctamente al iniciar sesión. Profile Management trata la copia de seguridad como la copia correcta de la base de datos del índice de búsqueda. Cuando se produce un error al intentar montar la base de datos del índice de búsqueda porque la base de datos resulta dañada, Profile Management revierte automáticamente la base de datos del índice de búsqueda a la última copia correcta que se conoce.

Nota: Profile Management elimina la copia de seguridad guardada anteriormente después de que se haya guardado correctamente una nueva copia de seguridad. La copia de seguridad consume el espacio de almacenamiento disponible de los archivos VHDX.

## **Configuraciones básicas de directiva**

September 22, 2021

Esta sección contiene configuraciones de directiva relacionadas con una configuración básica de Profile Management.

### **Habilitar Profile Management**

De forma predeterminada, para facilitar la instalación, Profile Management no procesa inicios de sesión ni cierres de sesión. Habilite Profile Management únicamente después de realizar todas las tareas de instalación y de probar de qué manera funcionan los perfiles de usuario Citrix en su entorno.

Si esta directiva no está configurada aquí, se utiliza el valor del archivo INI. Si esta directiva no está configurada aquí ni en el archivo INI, Profile Management no procesa los perfiles de usuario de Windows de ninguna manera.

### **Grupos procesados**

Se pueden utilizar tanto grupos locales de equipo como grupos de dominio (local, global y universal). El formato de los grupos de dominio debe especificarse con este formato: NOMBRE DEL DOMINIO\NOMBRE DEL GRUPO.

Si esta directiva está configurada aquí, Profile Management procesará solo los miembros de estos grupos de usuarios. Si esta directiva está inhabilitada, Profile Management procesará todos los usuarios.

Si esta directiva no está configurada aquí, se utiliza el valor del archivo INI. Si esta directiva no está configurada ni aquí ni en el archivo INI, se procesarán los miembros de todos los grupos de usuarios.

### **Grupos excluidos**

Puede utilizar grupos locales de equipo y grupos de dominio (local, global y universal) para evitar que se procesen determinados perfiles de usuario. Especifique los grupos de dominio así: NOMBRE DE DOMINIO\NOMBRE DE GRUPO.

Si este parámetro está configurado aquí, Profile Management excluye a los miembros de estos grupos de usuarios. Si está inhabilitado, Profile Management no excluye a ningún usuario. Si este parámetro no se define aquí, se utiliza el valor del archivo INI. Si este parámetro no está configurado aquí ni en el archivo INI, no se excluye ningún miembro de ningún grupo.

### **Procesar inicios de sesión de administradores locales**

Especifica si se procesan los inicios de sesión de miembros del grupo BUILTIN\Administrators. Si esta directiva está inhabilitada o no está configurada en sistemas operativos multisesión (por ejemplo, entornos de Citrix Virtual Apps), Profile Management entiende que se deben procesar los inicios de sesión de los usuarios de dominio, no los de los administradores locales. En sistemas operativos de sesión única (como, por ejemplo, entornos de Citrix Virtual Desktops), los inicios de sesión de administradores locales sí se procesan. Esta directiva permite que los usuarios del dominio con derechos de administrador local, normalmente usuarios de Citrix Virtual Desktops con escritorios virtuales asignados, puedan omitir el procesamiento, y puedan iniciar sesión y solucionar problemas de Profile Management en el escritorio.

Nota: Es posible que haya inicios de sesión de usuarios de dominio sujetos a restricciones impuestas por la pertenencia a grupos, por lo general para garantizar el cumplimiento de normas de las licencias de los productos.

Si esta directiva está inhabilitada, Profile Management no procesa los inicios de sesión de los administradores locales. Si esta directiva no está configurada aquí, se utiliza el valor del archivo INI. Si esta directiva no está configurada aquí ni en el archivo INI, no se procesan los administradores.

### **Ruta al almacén de usuarios**

Establece la ruta al directorio (el almacén de usuarios) en el que se guarda la configuración del usuario (cambios de registro y archivos sincronizados).

La ruta puede:

- Una ruta relativa. Esta ruta debe ser relativa al directorio principal (que se configura generalmente como el atributo #homeDirectory# para un usuario en Active Directory).

- Una ruta UNC. Esta ruta especifica generalmente un recurso compartido del servidor o un espacio de nombres DFS.
- Estar inhabilitada o sin configurar. En este caso, se asume el valor #homeDirectory#\Windows.

Se pueden usar los siguientes tipos de variable para esta directiva:

- Variables de entorno del sistema entre signos de porcentaje (por ejemplo, %ProfVer%). Las variables de entorno del sistema generalmente requieren una configuración adicional.
- Atributos del objeto de usuario de Active Directory, entre signos de almohadilla (por ejemplo, #sAMAccountName#).
- Variables de Profile Management. Para obtener más información, consulte la documentación sobre las Variables de Profile Management.

Las variables de entorno del usuario no se pueden utilizar, excepto en el caso de %username% y %userdomain%. También puede crear atributos personalizados para definir las variables organizativas, como ubicaciones o usuarios. Los atributos distinguen mayúsculas y minúsculas.

Ejemplos:

- \server\share#sAMAccountName# almacena la configuración del usuario en la ruta UNC \server\share\JohnSmith (si #sAMAccountName# se resuelve como JohnSmith para el usuario actual)
- \server\profiles\$%USERNAME%.%USERDOMAIN%!CTX\_OSNAME!!CTX\_OSBITNESS! podría expandirse a \server\profiles\$\JohnSmith.DOMAINCONTROLLER1\Win8x64

Importante: Independientemente de los atributos o las variables que utilice, compruebe que este parámetro se expande hasta la carpeta del nivel inmediatamente superior al de la carpeta donde se encuentra NTUSER.DAT. Por ejemplo, si este archivo se encuentra en \server\profiles\$\JohnSmith.Finance\Win8x64\UPM\_Profile, defina la ruta al almacén de usuarios como \server\profiles\$\JohnSmith.Finance\Win8x64 (no la subcarpeta \UPM\_Profile).

Para obtener más información sobre el uso de variables para especificar la ruta al almacén de usuarios, consulte los temas siguientes:

- Compartir los perfiles de usuario de Citrix en varios servidores de archivos
- Administrar perfiles dentro y entre las unidades organizativas
- Alta disponibilidad y recuperación ante desastres con Profile Management

Si la Ruta al almacén de usuarios está inhabilitada, la configuración del usuario se guarda en el subdirectorio Windows del directorio principal.

Si esta directiva está inhabilitada, la configuración del usuario se guarda en el subdirectorio Windows del directorio principal. Si esta directiva no está configurada aquí, se utiliza el valor del archivo INI. Si esta directiva no está configurada aquí ni en el archivo INI, se utiliza el directorio Windows de la unidad del directorio principal.

## Migrar almacén de usuarios

Especifica la ruta de acceso a la carpeta donde se guardó anteriormente (la ruta del almacén de usuarios que utilizó en su momento) la configuración del usuario (cambios del Registro y archivos sincronizados).

Si este parámetro se configura, la configuración del usuario guardada en el almacén de usuarios anterior se migra al almacén de usuarios actual especificado en la directiva “Ruta al almacén de usuarios”

.

La ruta puede ser una ruta UNC absoluta o una ruta relativa al directorio principal.

En los dos casos puede utilizar estos tipos de variables: Variables de entorno del sistema entre signos de porcentaje y atributos del objeto de usuario de Active Directory entre signos de almohadilla.

Ejemplos:

- La carpeta `Windows\ \%ProfileVer%` almacena la configuración del usuario en una subcarpeta denominada `Windows\W2K3` del almacén de usuarios (si `%ProfileVer%` es una variable de entorno del sistema que se resuelve en `W2K3`).
- `\\server\share\ \#SAMAccountName#` almacena la configuración del usuario en la ruta UNC `\\server\share\ <JohnSmith>` (si `#SAMAccountName#` se resuelve en `JohnSmith` para el usuario actual).

En la ruta, puede usar variables de entorno del usuario, excepto `%username%` y `%userdomain%`.

Si este parámetro está inhabilitado, la configuración del usuario se guarda en el almacén de usuarios actual.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si este parámetro no se configura aquí ni en el archivo INI, la configuración del usuario se guarda en el almacén de usuarios actual.

## Reescritura activa

Los archivos y las carpetas (pero no las entradas del Registro del sistema) que se modifican pueden sincronizarse con el almacén de usuarios a mitad de una sesión, antes de cerrarla.

Si esta directiva no está configurada aquí, se utiliza el valor del archivo INI. Si esta directiva no está configurada aquí ni en el archivo INI, se considera habilitada.

Compatibilidad con perfiles sin conexión

Esta directiva permite que los perfiles se sincronicen con el almacén de usuarios en la primera oportunidad disponible. Está pensada para usuarios de equipos portátiles o dispositivos móviles que cambian de equipo a menudo. Cuando se produce una desconexión de red, los perfiles permanecen intactos en el equipo portátil o dispositivo itinerante, incluso después de reiniciar o hibernar. A medida que

los usuarios móviles trabajan, sus perfiles se actualizan de forma local, y finalmente se sincronizan con el almacén de usuarios cuando se vuelve a establecer la conexión de red.

Si esta directiva no está configurada aquí, se utiliza el valor del archivo INI. Si esta directiva no está configurada aquí ni en el archivo INI, los perfiles sin conexión están inhabilitados.

### **Registro de reescritura activa**

Use esta directiva junto con “Reescritura activa”. Las entradas del Registro que se modifican se pueden sincronizar con el almacén de usuarios en medio de una sesión.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si no configura este parámetro aquí ni en el archivo INI, el registro de reescritura activa queda inhabilitado.

### **Compatibilidad con perfiles sin conexión**

Habilita la función de perfiles sin conexión. Esta función está diseñada para equipos que suelen eliminarse de redes, normalmente portátiles o dispositivos móviles, no servidores o escritorios.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si este parámetro no se define ni aquí ni en el archivo INI, se inhabilita la funcionalidad de perfiles sin conexión.

## **Configuraciones de directiva de Multiplataforma**

November 30, 2020

Esta sección contiene configuraciones de directiva relacionadas con la función de configuración multiplataforma de Profile Management.

### **Habilitar configuración multiplataforma**

De forma predeterminada, para facilitar la implementación, la configuración multiplataforma está inhabilitada. Active el procesamiento habilitando esta directiva, pero antes asegúrese de planificar y probar esta funcionalidad rigurosamente.

Si esta directiva no está configurada aquí, se utiliza el valor del archivo INI. Si esta directiva no está configurada aquí ni en el archivo INI, no se aplicará la configuración multiplataforma.

## **Grupos de usuarios de configuración multiplataforma**

Introduzca uno o varios grupos de usuarios de Windows. Por ejemplo, podría utilizar este parámetro para procesar solamente los perfiles de un grupo de usuarios de prueba. Si esta directiva está configurada, la función Configuración multiplataforma de Profile Management procesará solamente los miembros de estos grupos de usuarios. Si esta directiva está inhabilitada, la función procesa todos los usuarios especificados en la directiva Grupos procesados.

Si esta directiva no está configurada aquí, se utiliza el valor del archivo INI. Si esta directiva no está configurada aquí ni en el archivo INI, se procesarán todos los grupos de usuarios.

## **Ruta de definiciones multiplataforma**

Identifica la ubicación de red de los archivos de definición que se han copiado del paquete de descarga. Debe ser una ruta UNC. Los usuarios deben tener acceso de lectura en esa ubicación y los administradores deben tener acceso de escritura. La ubicación debe ser un punto compartido de archivos SMB (Server Message Block) o CIFS (Common Internet File System).

Si esta directiva no está configurada aquí, se utiliza el valor del archivo INI. Si esta directiva no está configurada aquí ni en el archivo INI, no se aplicará la configuración multiplataforma.

## **Ruta del almacén de configuración multiplataforma**

Establece la ruta al almacén de configuración multiplataforma, que es la carpeta donde se guarda la configuración multiplataforma de los usuarios. Los usuarios deben contar con acceso de escritura en esta zona. La ruta puede ser una ruta UNC absoluta o una ruta relativa al directorio principal.

Esta es la zona común del almacén de usuarios donde se ubican los datos de perfil compartidos entre múltiples plataformas. Los usuarios deben contar con acceso de escritura en esta zona. La ruta puede ser una ruta UNC absoluta o una ruta relativa al directorio principal. Se pueden usar las mismas variables que para la Ruta al almacén de usuarios.

Si esta directiva está inhabilitada, se utiliza la ruta `Windows\PM_CP`. Si esta directiva no está configurada aquí, se utiliza el valor del archivo INI. Si esta directiva no está configurada aquí ni en el archivo INI, se utiliza el valor predeterminado.

## **Origen para crear configuración multiplataforma**

Especifica una plataforma como plataforma base si esta directiva está habilitada en la unidad organizativa (OU) de dicha plataforma. Esta directiva migra los datos desde los perfiles de la plataforma base al almacén de configuración multiplataforma.

Los conjuntos de perfiles de cada plataforma se guardan en una unidad organizativa aparte. Esto significa que es necesario seleccionar de qué plataforma se quieren usar los datos de perfil como base para el almacén de configuración multiplataforma. La plataforma así seleccionada será la plataforma base. Si el almacén de configuración multiplataforma contiene un archivo de definición sin datos, o los datos en caché de un perfil de plataforma individual son más recientes que los datos de la definición en el almacén, Profile Management migrará los datos del perfil de la plataforma individual al almacén, a menos que se inhabilite esta directiva.

**Importante:**

Si esta directiva está habilitada en varias unidades organizativas o en varios objetos de usuario o máquina, la plataforma en la que inicie sesión el primer usuario se convertirá en el perfil base. De manera predeterminada, esta directiva está Habilitada.

## Configuraciones de directiva de Sistema de archivos

November 30, 2020

Esta sección contiene directivas para establecer qué archivos y directorios de un perfil de usuario se sincronizan entre el sistema en el que el perfil está instalado y el almacén de usuarios.

## Configuraciones de directiva de Exclusiones

September 22, 2021

Esta sección contiene configuraciones de directiva para establecer qué archivos y directorios de un perfil de usuario se excluyen del proceso de sincronización.

### Lista de exclusión de archivos

Lista de archivos que se ignoran durante la sincronización. Los nombres de archivo deben ser rutas relativas al perfil de usuario (%USERPROFILE%). Se puede usar comodines y se aplican de forma recursiva.

Ejemplos:

- Escritorio\Desktop.ini ignora el archivo Desktop.ini de la carpeta Escritorio
- %USERPROFILE%\*.tmp ignora todos los archivos con la extensión TMP en el perfil entero

- AppData\Roaming\MyApp\*.tmp ignora todos los archivos con la extensión TMP en una parte del perfil

Si esta directiva está inhabilitada, no se excluirá ningún archivo. Si esta directiva no está configurada aquí, se utiliza el valor del archivo INI. Si esta directiva no está configurada aquí ni en el archivo INI, no se excluirá ningún archivo.

## Habilitar lista de exclusión predeterminada de directorios

Lista predeterminada de directorios que se omiten durante la sincronización. Use esta directiva para especificar directorios de exclusión de objeto de directiva de grupo (GPO) sin tener que rellenarlos manualmente.

Si se inhabilita esta directiva, Profile Management no excluye ningún directorio de forma predeterminada. Si esta directiva no está configurada aquí, Profile Management usa el valor del archivo INI. Si esta directiva no está configurada aquí ni en el archivo INI, Profile Management no excluye ningún directorio de manera predeterminada.

## Lista de exclusión de directorios

Lista de carpetas que se ignoran durante la sincronización. Los nombres de carpeta deben especificarse como rutas relativas al perfil de usuario (%USERPROFILE%).

Ejemplo:

- “Escritorio” ignora la carpeta Escritorio en el perfil del usuario

Si esta directiva está inhabilitada, no se excluirá ninguna carpeta. Si esta directiva no está configurada aquí, se utiliza el valor del archivo INI. Si esta directiva no está configurada ni aquí ni en el archivo INI, no se excluirá ninguna carpeta.

## Comprobación de exclusiones al iniciar sesión

Esta configuración estipula lo que hace Profile Management si un perfil del almacén de usuarios contiene archivos o carpetas excluidos.

Si esta configuración está inhabilitada o establecida en el valor predeterminado **Sincronizar carpetas o archivos excluidos al iniciar sesión**, Profile Management sincroniza estos archivos o carpetas excluidos que hubiera en el almacén de usuarios con el perfil local cuando un usuario inicia sesión.

Si esta configuración se establece en **Omitir carpetas o archivos excluidos al iniciar sesión**, Profile Management omite los archivos o carpetas excluidos que hubiera en el almacén de usuarios cuando un usuario inicia sesión.

Si esta configuración se establece en **Eliminar carpetas o archivos excluidos al iniciar sesión**, Profile Management elimina los archivos o carpetas excluidos que hubiera en el almacén de usuarios cuando un usuario inicia sesión.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si este parámetro no se define ni aquí ni en el archivo INI, los archivos o carpetas excluidos se sincronizan del almacén de usuarios al perfil local cuando un usuario inicia sesión.

### **Procesamiento de archivos grandes: Archivos que se crearán como enlaces simbólicos**

Para mejorar el rendimiento en el inicio de sesión y procesar archivos de gran tamaño, se crea un enlace simbólico, en lugar de copiar archivos en esta lista.

Puede usar comodines en directivas que hagan referencia a archivos; por ejemplo, `!ctx_localappdata!\Microsoft\Outlook\*.OST`.

Para procesar el archivo de la carpeta sin conexión (`*.ost`) de Microsoft Outlook, la carpeta **Outlook** no debe estar excluida en Profile Management.

**Nota:** Tenga en cuenta que no se puede acceder a esos archivos simultáneamente desde varias sesiones.

## **Configuraciones de directiva de Sincronización**

September 22, 2021

Esta sección contiene configuraciones de directiva para especificar qué archivos y carpetas de un perfil de usuario se sincronizarán entre el sistema en el que el perfil está instalado y el almacén de usuarios.

### **Directorios que sincronizar**

Profile Management sincroniza el perfil completo de cada usuario entre el sistema en el que se instala y el almacén de usuarios. No es necesario agregar las subcarpetas del perfil del usuario a la lista para incluirlas.

Las rutas de la lista deben ser relativas al perfil de usuario.

Ejemplo:

- Escritorio\excluir\incluir hace que la subcarpeta llamada “incluir” se sincronice aun cuando la carpeta llamada “Escritorio\excluir” no se sincronice

La inhabilitación de esta directiva tiene el mismo efecto que habilitarla con una lista vacía.

Si esta directiva no está configurada aquí, se utiliza el valor del archivo INI. Si esta directiva no está configurada ni aquí ni en el archivo INI, se sincronizarán solo las carpetas del perfil de usuario que no se hayan excluido.

### **Archivos que sincronizar**

Profile Management sincroniza el perfil completo de cada usuario entre el sistema en el que se instala y el almacén de usuarios. No es necesario agregar archivos del perfil del usuario a la lista para incluirlos.

Esta directiva se puede utilizar para incluir archivos que se encuentran en las carpetas excluidas. Las rutas de la lista deben ser relativas al perfil de usuario. Es posible utilizar comodines, pero solo se permiten para los nombres de archivo. No es posible anidar los comodines y se aplican de forma recursiva.

Ejemplos:

- `AppData\Local\Microsoft\Office\Access.qat` especifica un archivo que se encuentra en un nivel inferior de una carpeta excluida en la configuración predeterminada
- `AppData\Local\MyApp*.cfg` especifica todos los archivos con la extensión `.cfg` en la carpeta `AppData\Local\MyApp` del perfil y sus subcarpetas

La inhabilitación de esta directiva tiene el mismo efecto que habilitarla con una lista vacía.

Si esta directiva no está configurada aquí, se utiliza el valor del archivo INI. Si esta directiva no está configurada ni aquí ni en el archivo INI, se sincronizarán solo los archivos del perfil de usuario que no hayan sido excluidos.

### **Carpetas para reflejar**

Esta directiva puede ayudar a solucionar problemas relacionados con las carpetas transaccionales (también conocidas como carpetas de referencia). Estas carpetas contienen archivos interdependientes, donde un archivo hace referencia a otros. El reflejo de las carpetas permite a Profile Management procesar una carpeta transaccional y su contenido como una sola entidad, evitando la sobrecarga del perfil. Por ejemplo, puede reflejar la carpeta de cookies de Internet Explorer de manera que `Index.dat` se sincronice con las cookies para las que se crea un índice. En estas situaciones, prevalece la última escritura. De manera que los archivos en las carpetas reflejadas que se han modificado en más de una sesión se sobrescribirán con la última actualización, lo que generará una pérdida de cambios del perfil.

Por ejemplo, piense en cómo `Index.dat` hace referencia a las cookies mientras un usuario consulta Internet. Si un usuario abre dos sesiones de Internet Explorer, cada una en un servidor diferente, y

consulta distintos sitios en cada sesión, las cookies de cada sitio se agregarán al servidor apropiado. Cuando el usuario se desconecte de la primera sesión (o a mitad de una sesión, si está habilitada la función Reescritura activa), las cookies de la segunda sesión deberían sustituir aquellas de la primera sesión. Sin embargo, éstas se combinan, y las referencias a las cookies en Index.dat se vuelven obsoletas. Las consultas adicionales que se hagan en sesiones nuevas resultarán en combinaciones repetidas y en una carpeta de cookies saturada.

La posibilidad de reflejar la carpeta de cookies resuelve el problema al sobrescribir las cookies con las de la última sesión cada vez que el usuario cierra la sesión. De esta manera, Index.dat permanece siempre actualizado.

Si esta directiva no está configurada aquí, se utiliza el valor del archivo INI. Si esta directiva no está configurada ni aquí ni en el archivo INI, no se reflejará ninguna carpeta.

## Contenedor de perfiles

Un contenedor de perfiles es una solución de perfil basada en VHDX que permite especificar las carpetas que se van a contener en el disco de perfil. El contenedor de perfiles conecta el disco de perfil que contiene esas carpetas, eliminando así la necesidad de guardar una copia de las carpetas en el perfil local. Al hacerlo, se reducen los tiempos de inicio de sesión.

Para utilizar un contenedor de perfiles, habilite esta directiva y agregue las rutas relativas de las carpetas a la lista. Se recomienda incluir en la lista las carpetas que contienen archivos de caché grandes. Por ejemplo, agregue la carpeta de caché de contenido de **Citrix Files** a la lista: `AppData\Local\Citrix\Citrix Files\PartCache`.

Existen dos casos a tener en cuenta:

- El contenedor de perfiles no admite el acceso simultáneo desde varias sesiones.
- El contenedor de perfiles no puede contener el perfil entero.

Si esta directiva no está configurada aquí, se utiliza el valor del archivo INI. Si esta directiva no está configurada aquí ni en el archivo INI, se considera inhabilitada.

## Configuraciones de directiva de Redirección de carpetas

November 30, 2020

Esta sección contiene configuraciones de directiva para especificar si desea redirigir las carpetas que suelen aparecer en perfiles a una ubicación de red compartida.

## Conceder acceso a administradores

Esta configuración permite que un administrador pueda acceder al contenido de las carpetas redirigidas de un usuario.

### Nota:

Este parámetro otorga permisos a los administradores que tienen acceso completo y sin restricciones al dominio.

De forma predeterminada, esta configuración está inhabilitada y los usuarios tienen acceso exclusivo al contenido de sus carpetas redirigidas.

## Incluir nombre de dominio

Esta configuración habilita la inclusión de la variable de entorno `%userdomain%` como parte de la ruta UNC especificada para carpetas redirigidas.

De forma predeterminada, esta configuración está inhabilitada y la variable de entorno `%userdomain%` no se incluye como parte de la ruta UNC especificada para carpetas redirigidas.

## Configuraciones de directiva de AppData(Roaming)

November 30, 2020

Esta sección contiene configuraciones de directiva para redirigir el contenido de la carpeta **AppData(Roaming)** a una ubicación de red compartida.

### Ruta de AppData(Roaming)

Esta configuración especifica la ubicación de red a la que se redirige el contenido de la carpeta **AppData(Roaming)**.

De forma predeterminada, esta configuración está inhabilitada y no se especifica ninguna ubicación.

Si esta configuración no está definida aquí, Profile Management no redirige la carpeta especificada.

### Parámetros de redirección para AppData(Roaming)

Esta configuración especifica cómo redirigir el contenido de la carpeta **AppData(Roaming)**.

De forma predeterminada, el contenido se redirige a una ruta UNC.

Si esta configuración no está definida aquí, Profile Management no redirige la carpeta especificada.

## Configuraciones de directiva de Contactos

September 22, 2021

Esta sección contiene configuraciones de directiva para redirigir el contenido de la carpeta **Contactos** a una ubicación de red compartida.

### Ruta de Contactos

Esta configuración especifica la ubicación de red a la que se redirige el contenido de la carpeta **Contactos**.

De forma predeterminada, esta configuración está inhabilitada y no se especifica ninguna ubicación.

Si esta configuración no está definida aquí, Profile Management no redirige la carpeta especificada.

### Parámetros de redirección para Contactos

Esta configuración especifica cómo redirigir el contenido de la carpeta **Contactos**.

De forma predeterminada, el contenido se redirige a una ruta UNC.

Si esta configuración no está definida aquí, Profile Management no redirige la carpeta especificada.

## Configuraciones de directiva de Escritorio

November 30, 2020

Esta sección contiene configuraciones de directiva para redirigir el contenido de la carpeta **Escritorio** a una ubicación de red compartida.

## Ruta de Escritorio

Esta configuración especifica la ubicación de red a la que se redirige el contenido de la carpeta **Escritorio**.

De forma predeterminada, esta configuración está inhabilitada y no se especifica ninguna ubicación.

Si esta configuración no está definida aquí, Profile Management no redirige la carpeta especificada.

## Parámetros de redirección para Escritorio

Esta configuración especifica cómo redirigir el contenido de la carpeta **Escritorio**.

De forma predeterminada, el contenido se redirige a una ruta UNC.

Si esta configuración no está definida aquí, Profile Management no redirige la carpeta especificada.

## Configuraciones de directiva de Documentos

January 4, 2021

Esta sección contiene configuraciones de directiva para redirigir el contenido de la carpeta **Documentos** a una ubicación de red compartida.

## Ruta de Documentos

Esta configuración especifica la ubicación de red a la que se redirigen los archivos en la carpeta **Documentos**.

De forma predeterminada, esta configuración está inhabilitada y no se especifica ninguna ubicación.

Si esta configuración no está definida aquí, Profile Management no redirige la carpeta especificada.

La configuración **Ruta de Documentos** debe estar habilitada no solo para redirigir archivos a la carpeta **Documentos**, sino también para redirigir archivos a las carpetas Música, Imágenes y Vídeos.

## Parámetros de redirección para Documentos

Esta configuración especifica cómo redirigir el contenido de la carpeta **Documentos**.

De forma predeterminada, el contenido se redirige a una ruta UNC.

Para controlar cómo redirigir el contenido de la carpeta **Documentos**, elija una de las siguientes opciones:

- Redirigir a esta ruta UNC. Redirige contenido a la ruta UNC especificada en la configuración de directiva de Ruta de Documentos.
- Redirigir al directorio principal del usuario. Redirige contenido al directorio principal de los usuarios, configurado generalmente como el atributo #homeDirectory# para usuarios en Active Directory.

Si esta configuración no está definida aquí, Profile Management no redirige la carpeta especificada.

## Configuraciones de directiva de Descargas

January 4, 2021

Esta sección contiene configuraciones de directiva para redirigir el contenido de la carpeta **Descargas** a una ubicación de red compartida.

### Ruta de Descargas

Esta configuración especifica la ubicación de red a la que se redirigen los archivos de la carpeta **Descargas**.

De forma predeterminada, esta configuración está inhabilitada y no se especifica ninguna ubicación.

Si esta configuración no está definida aquí, Profile Management no redirige la carpeta especificada.

### Parámetros de redirección para Descargas

Esta configuración especifica cómo redirigir el contenido de la carpeta **Descargas**.

De forma predeterminada, el contenido se redirige a una ruta UNC.

Si esta configuración no está definida aquí, Profile Management no redirige la carpeta especificada.

## Configuraciones de directiva de Favoritos

November 30, 2020

Esta sección contiene configuraciones de directiva para redirigir el contenido de la carpeta **Favoritos** a una ubicación de red compartida.

### **Ruta de Favoritos**

Esta configuración especifica la ubicación de red a la que se redirige el contenido de la carpeta **Favoritos**.

De forma predeterminada, esta configuración está inhabilitada y no se especifica ninguna ubicación.

Si esta configuración no está definida aquí, Profile Management no redirige la carpeta especificada.

### **Parámetros de redirección para Favoritos**

Esta configuración especifica cómo redirigir el contenido de la carpeta **Favoritos**.

De forma predeterminada, el contenido se redirige a una ruta UNC.

Si esta configuración no está definida aquí, Profile Management no redirige la carpeta especificada.

## **Configuraciones de directiva de Vínculos**

November 30, 2020

Esta sección contiene configuraciones de directiva para redirigir el contenido de la carpeta **Vínculos** a una ubicación de red compartida.

### **Ruta de Vínculos**

Esta configuración especifica la ubicación de red a la que se redirige el contenido de la carpeta **Vínculos**.

De forma predeterminada, esta configuración está inhabilitada y no se especifica ninguna ubicación.

Si esta configuración no está definida aquí, Profile Management no redirige la carpeta especificada.

## Parámetros de redirección para Vínculos

Esta configuración especifica cómo redirigir el contenido de la carpeta **Vínculos**.

De forma predeterminada, el contenido se redirige a una ruta UNC.

Si esta configuración no está definida aquí, Profile Management no redirige la carpeta especificada.

## Configuraciones de directiva de Música

November 30, 2020

Esta sección contiene configuraciones de directiva para redirigir el contenido de la carpeta **Música** a una ubicación de red compartida.

### Ruta de Música

Esta configuración especifica la ubicación de red a la que se redirige el contenido de la carpeta **Música**.

De forma predeterminada, esta configuración está inhabilitada y no se especifica ninguna ubicación.

Si esta configuración no está definida aquí, Profile Management no redirige la carpeta especificada.

### Configuraciones de redirección para Música

Esta configuración especifica cómo redirigir el contenido de la carpeta **Música**.

De forma predeterminada, el contenido se redirige a una ruta UNC.

Para controlar cómo redirigir el contenido de la carpeta **Música**, elija una de las siguientes opciones:

- Redirigir a esta ruta UNC. Redirige contenido a la ruta UNC especificada en la configuración de directiva de Ruta de Música.
- Redirección relativa a la carpeta **Documentos**. Redirige contenido a una carpeta relativa a la carpeta **Documentos**.

Para redirigir contenido a una carpeta relativa a la carpeta **Documentos**, es necesario habilitar la configuración **Ruta de Documentos**.

Si esta configuración no está definida aquí, Profile Management no redirige la carpeta especificada.

## Configuraciones de directiva de Imágenes

November 30, 2020

Esta sección contiene configuraciones de directiva para redirigir el contenido de la carpeta **Imágenes** a una ubicación de red compartida.

### Ruta de Imágenes

Esta configuración especifica la ubicación de red a la que se redirige el contenido de la carpeta **Imágenes**.

De forma predeterminada, esta configuración está inhabilitada y no se especifica ninguna ubicación.

Si esta configuración no está definida aquí, Profile Management no redirige la carpeta especificada.

### Parámetros de redirección para Imágenes

Esta configuración especifica cómo redirigir el contenido de la carpeta **Imágenes**.

De forma predeterminada, el contenido se redirige a una ruta UNC.

Para controlar cómo redirigir el contenido de la carpeta **Imágenes**, elija una de las siguientes opciones:

- Redirigir a esta ruta UNC. Redirige contenido a la ruta UNC especificada en la configuración de directiva de Ruta de Imágenes.
- Redirección relativa a la carpeta Documentos. Redirige contenido a una carpeta relativa a la carpeta Documentos.

Para redirigir contenido a una carpeta relativa a la carpeta **Documentos**, es necesario habilitar la configuración **Ruta de Documentos**.

Si esta configuración no está definida aquí, Profile Management no redirige la carpeta especificada.

## Configuraciones de directiva de Juegos guardados

November 30, 2020

Esta sección contiene configuraciones de directiva para redirigir el contenido de la carpeta **Juegos guardados** a una ubicación de red compartida.

## Parámetros de redirección para Juegos guardados

Esta configuración especifica cómo redirigir el contenido de la carpeta **Juegos guardados**.

De forma predeterminada, el contenido se redirige a una ruta UNC.

Si esta configuración no está definida aquí, Profile Management no redirige la carpeta especificada.

## Ruta de Juegos guardados

Esta configuración especifica la ubicación de red a la que se redirige el contenido de la carpeta **Juegos guardados**.

De forma predeterminada, esta configuración está inhabilitada y no se especifica ninguna ubicación.

Si esta configuración no está definida aquí, Profile Management no redirige la carpeta especificada.

## Configuraciones de directiva de Menú Inicio

November 30, 2020

Esta sección contiene configuraciones de directiva para redirigir el contenido de la carpeta **Menú Inicio** a una ubicación de red compartida.

## Parámetros de redirección para Menú Inicio

Esta configuración especifica cómo redirigir el contenido de la carpeta **Menú Inicio**.

De forma predeterminada, el contenido se redirige a una ruta UNC.

Si esta configuración no está definida aquí, Profile Management no redirige la carpeta especificada.

## Ruta de Menú Inicio

Esta configuración especifica la ubicación de red a la que se redirige el contenido de la carpeta **Menú Inicio**.

De forma predeterminada, esta configuración está inhabilitada y no se especifica ninguna ubicación.

Si esta configuración no está definida aquí, Profile Management no redirige la carpeta especificada.

## Configuraciones de directiva de Búsquedas

November 30, 2020

Esta sección contiene configuraciones de directiva para redirigir el contenido de la carpeta **Búsquedas** a una ubicación de red compartida.

### Parámetros de redirección para Búsquedas

Esta configuración especifica cómo redirigir el contenido de la carpeta **Búsquedas**.

De forma predeterminada, el contenido se redirige a una ruta UNC.

Si esta configuración no está definida aquí, Profile Management no redirige la carpeta especificada.

### Ruta de Búsquedas

Esta configuración especifica la ubicación de red a la que se redirige el contenido de la carpeta **Búsquedas**.

De forma predeterminada, esta configuración está inhabilitada y no se especifica ninguna ubicación.

Si esta configuración no está definida aquí, Profile Management no redirige la carpeta especificada.

## Configuraciones de directiva de Vídeos

November 30, 2020

Esta sección contiene configuraciones de directiva para redirigir el contenido de la carpeta **Vídeos** a una ubicación de red compartida.

### Parámetros de redirección para Vídeos

Esta configuración especifica cómo redirigir el contenido de la carpeta **Vídeos**.

De forma predeterminada, el contenido se redirige a una ruta UNC.

Para controlar cómo redirigir el contenido de la carpeta **Vídeos**, elija una de las siguientes opciones:

- Redirigir a esta ruta UNC. Redirige contenido a la ruta UNC especificada en la configuración de directiva de Ruta de Vídeos.

- Redirección relativa a la carpeta **Documentos**. Redirige contenido a una carpeta relativa a la carpeta **Documentos**.

Para redirigir contenido a una carpeta relativa a la carpeta **Documentos**, es necesario habilitar la configuración **Ruta de Documentos**.

Si esta configuración no está definida aquí, Profile Management no redirige la carpeta especificada.

## **Ruta de Vídeos**

Esta configuración especifica la ubicación de red a la que se redirige el contenido de la carpeta **Vídeos**.

De forma predeterminada, esta configuración está inhabilitada y no se especifica ninguna ubicación.

Si esta configuración no está definida aquí, Profile Management no redirige la carpeta especificada.

## **Configuraciones de directiva de Registro**

November 30, 2020

Esta sección contiene configuraciones de directiva para definir la captura de registros de Profile Management.

### **Acciones de Active Directory**

Esta configuración habilita o inhabilita el registro detallado de las acciones realizadas en Active Directory.

De forma predeterminada, esta configuración está inhabilitada.

Cuando habilite esta configuración, compruebe que la configuración **Habilitar registro** también está habilitada.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se registran los errores y la información general.

## Información común

Esta configuración habilita o inhabilita el registro detallado de información común.

De forma predeterminada, esta configuración está inhabilitada.

Cuando habilite esta configuración, compruebe que la configuración **Habilitar registro** también está habilitada.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se registran los errores y la información general.

## Advertencias comunes

Esta configuración habilita o inhabilita el registro detallado de advertencias comunes.

De forma predeterminada, esta configuración está inhabilitada.

Cuando habilite esta configuración, compruebe que la configuración **Habilitar registro** también está habilitada.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se registran los errores y la información general.

## Habilitar registro

Esta configuración habilita o inhabilita el registro de Profile Management en el modo de depuración (registro detallado). En modo de depuración, la información detallada de estado se registra en los archivos de registro ubicados en “%SystemRoot%\System32\Logfiles\UserProfileManager”.

De forma predeterminada, esta configuración está inhabilitada y solo se registran los errores.

Citrix recomienda habilitar esta configuración solo cuando vaya a solucionar problemas de Profile Management.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, solo se registran los errores.

## Acciones del sistema de archivos

Esta configuración habilita o inhabilita el registro detallado de las acciones realizadas en el sistema de archivos.

De forma predeterminada, esta configuración está inhabilitada.

Cuando habilite esta configuración, compruebe que la configuración **Habilitar registro** también está habilitada.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se registran los errores y la información general.

## **Notificaciones del sistema de archivos**

Esta configuración habilita o inhabilita el registro detallado de las notificaciones de los sistemas de archivos.

De forma predeterminada, esta configuración está inhabilitada.

Cuando habilite esta configuración, compruebe que la configuración **Habilitar registro** también está habilitada.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se registran los errores y la información general.

## **Cierre de sesión**

Esta configuración habilita o inhabilita el registro detallado de los cierres de sesión de los usuarios.

De forma predeterminada, esta configuración está inhabilitada.

Cuando habilite esta configuración, compruebe que la configuración **Habilitar registro** también está habilitada.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se registran los errores y la información general.

## **Inicio de sesión**

Esta configuración habilita o inhabilita el registro detallado de los inicios de sesión de los usuarios.

De forma predeterminada, esta configuración está inhabilitada.

Cuando habilite esta configuración, compruebe que la configuración **Habilitar registro** también está habilitada.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se registran los errores y la información general.

### **Tamaño máximo del archivo de registro**

Esta configuración permite especificar el valor máximo permitido para el archivo de registro de Profile Management en bytes.

De forma predeterminada, este valor está establecido en 1.048.576 bytes (1 MB).

Citrix recomienda aumentar el tamaño de este archivo a 5 MB o más si dispone de suficiente espacio en disco. Si el archivo de registro supera el tamaño máximo indicado, se elimina una copia de seguridad (.bak) del archivo, se cambia el nombre del archivo de registro a .bak y se crea un nuevo archivo de registro.

El archivo de registro se crea en %SystemRoot%\System32\Logfiles\UserProfileManager.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se utiliza el valor predeterminado.

### **Ruta al archivo de registro**

Esta configuración especifica una ruta alternativa en la que guardar el archivo de registros de Profile Management.

De forma predeterminada, esta configuración está inhabilitada y los archivos de registro se guardan en la ubicación predeterminada: %SystemRoot%\System32\Logfiles\UserProfileManager.

La ruta puede corresponder a una unidad local o a una unidad remota en la red (una ruta UNC). Las rutas remotas pueden ser útiles en entornos distribuidos de gran tamaño, pero pueden crear un tráfico de red significativo, lo cual puede ser inadecuado para los archivos de registros. En el caso de máquinas virtuales aprovisionadas, con una unidad de disco duro persistente, defina una ruta local a dicha unidad. Esto garantiza que los archivos de registro se conservarán cuando la máquina se reinicie. Para máquinas virtuales sin disco duro persistente, la definición de una ruta UNC permite conservar los archivos de registros, pero la cuenta de sistema de las máquinas debe tener acceso de escritura en el punto compartido UNC. Use una ruta local para los equipos portátiles gestionados con la función de perfiles sin conexión.

Si se usa una ruta UNC para los archivos de registro, Citrix recomienda aplicar una lista de control de acceso a la carpeta donde se guardan los mismos, para garantizar que solo tengan acceso a ellos las cuentas de los usuarios y equipos autorizados.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se utilizará la ubicación predeterminada “%SystemRoot%\System32\Logfiles\UserProfileManager”.

### **Información de usuario personalizada**

Esta configuración habilita o inhabilita el registro detallado de la información de usuario personalizada.

De forma predeterminada, esta configuración está inhabilitada.

Cuando habilite esta configuración, compruebe que la configuración **Habilitar registro** también está habilitada.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se registran los errores y la información general.

### **Valores de directivas al iniciar y cerrar la sesión**

Esta configuración habilita o inhabilita el registro detallado de valores de directivas cuando un usuario inicia y cierra sesión.

De forma predeterminada, esta configuración está inhabilitada.

Cuando habilite esta configuración, compruebe que la configuración **Habilitar registro** también está habilitada.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se registran los errores y la información general.

### **Acciones del Registro del sistema**

Esta configuración habilita o inhabilita el registro detallado de las acciones realizadas en el Registro del sistema.

De forma predeterminada, esta configuración está inhabilitada.

Cuando habilite esta configuración, compruebe que la configuración **Habilitar registro** también está habilitada.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se registran los errores y la información general.

## Diferencias en el Registro del sistema al cerrar la sesión

Esta configuración habilita o inhabilita el registro detallado de las diferencias en el Registro cuando un usuario cierra sesión.

De forma predeterminada, esta configuración está inhabilitada.

Cuando habilite esta configuración, compruebe que la configuración **Habilitar registro** también está habilitada.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se registran los errores y la información general.

## Configuraciones de directiva de Gestión de perfiles

September 22, 2021

Esta sección contiene configuraciones de directiva para definir la forma en que Profile Management gestiona los perfiles de usuario.

### Demora antes de eliminar perfiles en caché

Esta configuración especifica una extensión opcional para el intervalo de demora, en segundos, antes de que Profile Management elimine los perfiles almacenados en caché local al cerrar sesión.

Un valor de 0 elimina los perfiles inmediatamente al final del proceso de cierre de sesión. Profile Management comprueba los cierres de sesión cada minuto, por lo que un valor de 60 garantiza que los perfiles se eliminan entre uno y dos minutos después de que los usuarios hayan cerrado la sesión (dependiendo de cuando tuvo lugar la última comprobación). Ampliar la demora es útil si sabe que un proceso mantiene abiertos los archivos o el subárbol User del Registro durante el cierre de sesión. Con grandes perfiles, esto también puede acelerar el cierre de sesión.

De forma predeterminada, este valor está establecido en 0 y Profile Management elimina inmediatamente los perfiles almacenados en caché local.

Cuando habilite esta configuración, compruebe que Eliminar perfiles guardados en caché local al cerrar la sesión también está habilitada.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, los perfiles se eliminan inmediatamente.

## **Eliminar perfiles guardados en caché local al cerrar la sesión**

Esta configuración especifica si los perfiles almacenados en caché local se eliminan cuando el usuario cierra la sesión.

Si se habilita este parámetro, la caché de perfiles local del usuario se borra después del cierre de sesión. Citrix recomienda habilitar este parámetro para servidores de terminales.

De forma predeterminada, esta configuración está inhabilitada y la caché de perfiles local de un usuario se conserva después de cerrar sesión.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, los perfiles almacenados en caché no se eliminan.

## **Gestión de conflictos de perfiles locales**

Esta configuración define el comportamiento de Profile Management si el mismo perfil de usuario consta en el almacén de usuarios y en Windows como perfil local (no un perfil de usuario de Citrix).

De forma predeterminada, Profile Management utiliza el perfil de Windows local, pero no lo cambia de ninguna manera.

Para controlar el comportamiento de Profile Management, elija una de las siguientes opciones:

- Usar el perfil local. Profile Management utiliza el perfil local, pero no lo cambia de ninguna manera.
- Eliminar el perfil local. Profile Management elimina el perfil de usuario local de Windows y, a continuación, importa el perfil de usuario de Citrix desde el almacén de usuarios.
- Cambiar el nombre del perfil local. Profile Management cambia el nombre del perfil de usuario local de Windows (para conservar una copia de seguridad) y, a continuación, importa el perfil de usuario de Citrix desde el almacén de usuarios.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si este parámetro no se define ni aquí ni en el archivo INI, se utilizan los perfiles locales existentes.

## **Migración de perfiles existentes**

Esta configuración especifica los tipos de perfil migrados al almacén de usuarios durante el inicio de sesión si un usuario no tiene ningún perfil actual en el almacén de usuarios.

Profile Management puede migrar perfiles existentes inmediatamente durante el inicio de sesión si un usuario no tiene perfil en el almacén de usuarios. Al finalizar este proceso, Profile Management utiliza

el perfil del almacén de usuarios tanto en la sesión actual como en cualquier otra sesión configurada con la ruta al mismo almacén de usuarios.

De forma predeterminada, se migran los perfiles locales y móviles al almacén de usuarios durante el inicio de sesión.

Para especificar los tipos de perfil que se migran al almacén de usuarios durante el inicio de sesión, elija una de las siguientes opciones:

- Perfiles locales e itinerantes
- Locales
- Itinerancia
- Ninguno (inhabilitado)

Si selecciona **Ninguno**, el sistema utiliza el mecanismo de Windows existente para crear perfiles, como si fuera un entorno donde Profile Management no está instalado.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si este parámetro no se define ni aquí ni en el archivo INI, se migran los perfiles locales e itinerantes existentes.

### **Migración automática de perfiles de aplicación existentes**

Este parámetro habilita o inhabilita la migración automática de perfiles de aplicación existentes en varios sistemas operativos. Los perfiles de aplicación incluyen tanto los datos de aplicación de la carpeta **AppData** como las entradas del Registro de `HKEY_CURRENT_USER\SOFTWARE`. Este parámetro puede ser útil cuando se quiere migrar los perfiles de aplicación a través de varios sistemas operativos.

Por ejemplo, supongamos que actualiza la versión 1803 de su sistema operativo Windows 10 a la versión 1809 de Windows 10. Si este parámetro está habilitado, Profile Management migra automáticamente la configuración de la aplicación existente a la versión 1809 de Windows 10 la primera vez que cada usuario inicia sesión. Como consecuencia, se migran tanto los datos de aplicación de la carpeta **AppData** como las entradas del Registro de `HKEY_CURRENT_USER\SOFTWARE`.

Si existen varios perfiles de aplicación, Profile Management realiza la migración con esta prioridad:

1. Perfiles del mismo tipo de SO (SO de sesión única a SO de sesión única y SO multisesión a SO multisesión).
2. Perfiles de la misma familia de sistemas operativos Windows; por ejemplo, de Windows 10 a Windows 10 o de Windows Server 2016 a Windows Server 2016.
3. Perfiles de una versión anterior del sistema operativo; por ejemplo, de Windows 7 a Windows 10 o de Windows Server 2012 a Windows Server 2016.
4. Perfiles del sistema operativo más cercano.

**Nota:** Debe especificar el nombre corto del sistema operativo; para ello, incluya la variable “!CTX\_OSNAME!” en la ruta al almacén de usuarios. Así, Profile Management puede localizar los perfiles de aplicación existentes.

Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no se define ni aquí ni en el archivo INI, se considera inhabilitado de forma predefinida.

### **Ruta al perfil de plantilla**

Esta configuración especifica la ruta al perfil que Profile Management deberá utilizar como plantilla para crear perfiles de usuario.

La ruta especificada debe ser la ruta completa a la carpeta que contiene el archivo de Registro NTUSER.DAT y todas las carpetas y los archivos necesarios para el perfil de plantilla.

Nota: No incluya NTUSER.DAT en la ruta. Por ejemplo, para el archivo \\myservername\myprofiles\template\ntuser se definiría la ubicación como \\myservername\myprofiles\template.

Utilice rutas absolutas, ya sean rutas UNC o rutas del equipo local. Puede utilizar las últimas, por ejemplo, para especificar permanentemente un perfil de plantilla en una imagen de Citrix Provisioning Services. No se admite el uso de rutas relativas.

Nota: Esta configuración no admite la expansión de atributos de Active Directory, variables de entorno de sistema ni las variables %USERNAME% y %USERDOMAIN%.

De forma predeterminada, esta configuración está inhabilitada y los perfiles de usuario nuevos se crean a partir del perfil de usuario predeterminado del dispositivo donde un usuario inicia sesión por primera vez.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, no se utiliza ninguna plantilla.

### **El perfil de plantilla anula el perfil local**

Esta configuración permite que el perfil de plantilla anule el perfil local cuando se crean perfiles de usuario.

Si un usuario no tiene perfil de usuario de Citrix, pero existe un perfil de usuario local de Windows, de forma predeterminada se utiliza el perfil local (y se migra al almacén de usuarios si esto no está inhabilitado). Al habilitar esta configuración de directiva, el perfil de plantilla anula el perfil local que se usa durante la creación de perfiles de usuario.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, no se utiliza ninguna plantilla.

### **El perfil de plantilla sobrescribe el perfil móvil**

Esta configuración permite que el perfil de plantilla anule o sobrescriba el perfil móvil al crear perfiles de usuario.

Si un usuario no tiene perfil de usuario de Citrix, pero existe un perfil de usuario móvil de Windows, de forma predeterminada se utiliza el perfil móvil (y se migra al almacén de usuarios si esto no está inhabilitado). Al habilitar esta configuración de directiva, el perfil de plantilla anula el perfil móvil utilizado durante la creación de perfiles de usuario.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, no se utiliza ninguna plantilla.

### **Perfil de plantilla utilizado como perfil de Citrix obligatorio para todos los inicios de sesión**

Esta configuración permite que Profile Management use el perfil de plantilla como perfil predeterminado para crear todos los perfiles de usuario.

De forma predeterminada, esta configuración está inhabilitada y los perfiles de usuario nuevos se crean a partir del perfil de usuario predeterminado del dispositivo donde un usuario inicia sesión por primera vez.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, no se utiliza ninguna plantilla.

## **Configuraciones de directiva de Registro del sistema**

November 30, 2020

Esta sección contiene configuraciones de directiva para especificar qué claves del Registro se incluyen o excluyen en el procesamiento de Profile Management.

### **Lista de exclusión**

Lista de claves de registro en el subárbol de HKCU que se ignoran durante el cierre de sesión.

Ejemplo: Software\Policies

Si esta directiva está inhabilitada, no se excluye ninguna clave del Registro. Si esta directiva no está configurada aquí, se utiliza el valor del archivo INI. Si esta directiva no está configurada aquí ni en el archivo INI, no se excluye ninguna clave del Registro.

## **Lista de inclusión**

Lista de claves de registro en el subárbol de HKCU que se procesan durante el cierre de sesión.

Ejemplo: Software\Adobe.

Si esta directiva está habilitada, solo se procesarán las claves de la lista. Si esta directiva está inhabilitada, se procesará el subárbol HKCU completo. Si esta directiva no está configurada aquí, se utiliza el valor del archivo INI. Si esta directiva no está configurada aquí ni en el archivo INI, se procesará el subárbol HKCU completo.

## **Habilitar lista de exclusión predeterminada: Profile Management 5.5**

Lista predeterminada de claves del Registro en el subárbol HKCU que no se sincronizan con el perfil de usuario. Use esta directiva para especificar archivos de exclusión de objeto de directiva de grupo (GPO) sin tener que rellenarlos manualmente.

Si se inhabilita esta directiva, Profile Management no excluye ninguna clave de Registro de forma predeterminada. Si esta directiva no está configurada aquí, Profile Management usa el valor del archivo INI. Si esta directiva no está configurada aquí ni en el archivo INI, Profile Management no excluye ninguna clave de Registro de manera predeterminada.

## **Copia de seguridad de NTUSER.DAT**

Habilita la creación de una copia de seguridad de la versión correcta más reciente de NTUSER.DAT para poder volver a ella en caso de dañarse el archivo.

Si esta directiva no está configurada aquí, Profile Management usa el valor del archivo INI. Si esta directiva no está configurada aquí ni en el archivo INI, Profile Management no hace una copia de seguridad de NTUSER.DAT.

## **Configuraciones de directiva para Perfiles de usuario de streaming**

September 22, 2021

Esta sección contiene configuraciones de directiva para especificar la forma en que Profile Management procesa los perfiles de usuario distribuidos por streaming.

## **Guardar siempre en caché**

Esta configuración especifica si Profile Management guarda en caché los archivos distribuidos por streaming tan pronto como sea posible cuando un usuario inicia una sesión. El almacenamiento en caché de archivos cuando un usuario inicia sesión ahorra en ancho de banda de la red, por lo que la experiencia del usuario mejora.

Use esta configuración junto con la configuración **Streaming de perfiles**.

De forma predeterminada, esta configuración está inhabilitada y los archivos distribuidos por streaming no se almacenan en caché tan pronto como sea posible cuando un usuario inicia sesión.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si este parámetro no se define ni aquí ni en el archivo INI, se considera inhabilitado.

## **Tamaño de caché**

Esta configuración especifica un límite inferior, en MB, del tamaño de los archivos que se distribuyen por streaming. Profile Management almacena en caché los archivos de este tamaño o más grandes tan pronto como sea posible cuando un usuario inicia sesión.

De forma predeterminada, este valor está establecido en 0 (cero) y se usa la función de guardado del perfil entero en caché. Cuando la función de guardado del perfil entero en caché está habilitada, Profile Management obtiene todo el contenido del perfil en el almacén de usuarios, cuando un usuario inicia sesión, como una tarea en segundo plano.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si este parámetro no se define ni aquí ni en el archivo INI, se considera inhabilitado.

## **Streaming de perfiles**

Esta configuración habilita o inhabilita la función de streaming de perfiles de usuario de Citrix. Cuando está habilitada, las carpetas y los archivos incluidos en un perfil se obtienen del almacén de usuarios y se envían al equipo local solo cuando los usuarios acceden a estos archivos y carpetas después de iniciar una sesión. Las entradas del Registro y los archivos del área de archivos pendientes se obtienen inmediatamente.

De forma predeterminada, el streaming de perfiles está inhabilitado.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si este parámetro no se define ni aquí ni en el archivo INI, se considera inhabilitado.

## **Grupos de perfiles de usuarios de streaming**

Esta configuración especifica qué perfiles de usuario dentro de una unidad organizativa se distribuyen por streaming, en función de los grupos de usuarios de Windows.

Cuando está habilitada, solo los perfiles de usuario en los grupos de usuarios especificados se distribuyen por streaming. Todos los demás perfiles de usuario se procesan con normalidad.

De forma predeterminada, esta configuración está inhabilitada y todos los perfiles de usuario dentro de una unidad organizativa se procesan con normalidad.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se procesan todos los perfiles de usuario.

## **Para habilitar la exclusión de streaming de perfiles**

Cuando la exclusión de streaming de perfiles está habilitada, Profile Management no distribuye por streaming las carpetas especificadas en la lista de exclusiones, con lo que todas las carpetas se obtienen inmediatamente desde el almacén de usuarios al equipo local cuando un usuario inicia sesión.

Para obtener más información, consulte [Perfiles de usuario de streaming](#).

## **Tiempo de espera para bloqueo del área de archivos pendientes**

Esta configuración especifica el período de tiempo (en días) transcurrido el cual, los archivos de los usuarios se escriben de nuevo en el almacén de usuarios desde el área de archivos pendientes en el caso de que el almacén de usuarios quede bloqueado cuando un servidor no responde. Esto evita la saturación en el área de archivos pendientes y garantiza que el almacén de usuarios siempre contenga los archivos más actualizados.

De forma predeterminada, este valor está establecido en 1 (un) día.

Si este parámetro no se define aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se utiliza el valor predeterminado.

## **Configuración de directiva de personalización de usuario**

January 4, 2021

Para habilitar el montaje de capas de usuarios dentro de Virtual Delivery Agents, utilice los parámetros de configuración para especificar:

- En qué lugar de la red se accede a las capas de usuarios.
- El tamaño al que pueden llegar los discos nuevos de capas de usuarios.

Para ello, estas dos directivas aparecen en la lista de directivas disponibles:

- Ruta del repositorio de capas de usuarios: Introduzca una ruta con el formato “\nombre o dirección del servidor\nombre de la carpeta” en el campo Valor.
- Tamaño de las capas de usuarios en GB: Cambie el valor predeterminado de 0 al tamaño máximo (en GB) al que la capa de usuarios puede llegar. Si mantiene el valor predeterminado, el tamaño máximo de las capas de usuarios es de 10 GB.

Nota:

El hecho de cambiar el tamaño de las capas de usuarios en la directiva no cambia el tamaño de las capas existentes.

El tamaño predeterminado de las capas es 0.

Para obtener más información, consulte [Capa de personalización de usuarios](#).

## Configuraciones de directiva de Virtual Delivery Agent

January 4, 2021

La sección Virtual Desktop Agent (VDA) contiene configuraciones de directiva que controlan la comunicación entre el Virtual Desktop Agent y los Controllers de un sitio.

Importante: El agente VDA requiere información proporcionada por estos parámetros para registrarse en un Delivery Controller, si no se utiliza la función de actualización automática. Puesto que se requiere esta información para el proceso de registro, es necesario configurar las siguientes configuraciones con el Editor de directivas de grupo, a menos que usted proporcione esta información durante la instalación de Virtual Desktop Agent:

- Máscara de red IPv6 para el registro de Controller
- Puerto de registro de Controller
- SID de Controller
- Controllers
- Usar solo el registro de Controller con IPv6
- GUID del sitio

## **Máscara de red IPv6 para el registro de Controller**

Esta configuración de directiva permite que los administradores puedan restringir VDA a una sola sub-red preferida (en lugar de una dirección IP global, si está registrado). Esta configuración especifica la dirección IPv6 y de la red en la que se registrará VDA. VDA se registrará solo en la primera dirección que coincida con la máscara de red especificada. Esta configuración solo es válida si la configuración de directiva Usar solo registro de Controller con IPv6 está habilitada.

De forma predeterminada, esta configuración está en blanco.

## **Puerto de registro de Controller**

Use esta configuración solamente si Habilitar actualización automática de Controller está inhabilitada.

Esta configuración especifica el número de puerto TCP/IP que VDA utiliza para registrarse con un Controller cuando se usa un registro basado en el Registro del sistema.

De forma predeterminada, el número de puerto es el 80.

## **SID de Controller**

Use esta configuración solamente si Habilitar actualización automática de Controller está inhabilitada.

Esta configuración especifica una lista separada por espacios de identificadores de seguridad (SID) de Controllers que VDA usa para registrarse con un Controller cuando se usa un registro basado en el Registro del sistema. Este es un parámetro opcional que se puede usar con la configuración Controllers para restringir la lista de Controllers utilizados para el registro.

De forma predeterminada, esta configuración está en blanco.

## **Controllers**

Use esta configuración solamente si Habilitar actualización automática de Controller está inhabilitada.

Esta configuración especifica una lista separada por espacios de nombres de dominio completos (FQDN) de Controllers que el VDA usa para registrarse con un Controller cuando se usa un registro basado en el Registro del sistema. Esta es una configuración optativa que puede utilizarse junto con la configuración SIDs de Controller.

De forma predeterminada, esta configuración está en blanco.

## **Habilitar actualización automática de Controller**

Esta configuración permite que el VDA se registre con un Controller automáticamente después de la instalación.

Después de que el VDA se registre, el Controller con el que se registró envía una lista actualizada de los SID y FQDN del Controllers al VDA. VDA escribe esta lista en almacenamiento persistente. Cada Controller también comprueba la base de datos del sitio cada 90 minutos para verificar la información sobre los Controllers; si un Controller se ha agregado o quitado desde la última comprobación, o si se ha producido un cambio en la directiva, Controller envía listas actualizadas a los VDA registrados. Los VDA aceptarán conexiones de todos los Controllers de la lista más reciente que hayan recibido.

De manera predeterminada, esta configuración está habilitada.

## **Usar solo el registro de Controller con IPv6**

Esta configuración controla qué tipo de dirección usa el VDA para registrarse con un Controller:

- Cuando está habilitada, el VDA se registra con el Controller mediante la dirección IPv6 de la máquina. Cuando el VDA se comunica con el Controller, se utiliza el siguiente orden de direcciones: dirección IP global, dirección local única (ULA), dirección local de vínculo (si no hay otras direcciones IPv6 disponibles).
- Cuando está inhabilitada, el VDA se registra y se comunica con el Controller mediante la dirección IPv4 de la máquina.

De manera predeterminada, esta configuración está inhabilitada.

## **GUID del sitio**

Use esta configuración solamente si Habilitar actualización automática de Controller está inhabilitada.

Esta configuración especifica el identificador único global (GUID) del sitio que utiliza VDA para registrarse con un Controller cuando se usa el registro basado en Active Directory.

De forma predeterminada, esta configuración está en blanco.

## **Configuraciones de directiva de HDX 3D Pro**

February 6, 2020

La sección HDX 3D Pro contiene configuraciones de directiva para habilitar y definir los parámetros de la herramienta de configuración de la calidad de imagen para los usuarios. La herramienta permite que los usuarios ajusten el equilibrio entre calidad de imagen y capacidad de respuesta en tiempo real para optimizar el uso del ancho de banda disponible.

### **Habilitar sin pérdida**

Esta configuración especifica si los usuarios pueden o no habilitar e inhabilitar la compresión sin pérdida mediante la herramienta de configuración de la calidad de imagen. De forma predeterminada, los usuarios no tienen la opción de habilitar la compresión sin pérdida.

Cuando un usuario habilita la compresión sin pérdida, la calidad de imagen se establece automáticamente en el valor máximo disponible en la herramienta de configuración de la imagen. De forma predeterminada, se puede utilizar la compresión basada en CPU o GPU, según la capacidad del dispositivo del usuario y el equipo host.

### **Parámetros de calidad de HDX 3D Pro**

Esta configuración especifica los valores mínimos y máximos que definen el intervalo de ajuste de la calidad de imagen disponible para los usuarios en la herramienta de configuración de la calidad de imagen.

Especifique valores de calidad de imagen entre 0 y 100, ambos valores incluidos. El valor máximo debe ser mayor o igual que el valor mínimo.

## **Configuraciones de directiva de Supervisión**

September 22, 2021

La sección Supervisión contiene configuraciones de directiva para la supervisión de procesos, recursos y errores de aplicaciones.

El ámbito de estas directivas se puede definir según el sitio, el grupo de entrega, el tipo de grupo de entrega, la unidad organizativa y las etiquetas.

### **Directivas para la supervisión de procesos y recursos**

Cada punto de datos de la CPU, la memoria y los procesos se recopila del VDA y se almacena en la base de datos de Supervisión. El envío de puntos de datos desde el VDA consume ancho de banda

y su almacenamiento consume un espacio considerable en la base de datos de supervisión. Si no quiere supervisar datos de procesos o de recursos (o ninguno de los dos) de un ámbito concreto (por ejemplo, un grupo de entrega o una unidad organizativa específicos), se recomienda inhabilitar la directiva.

### **Habilitar supervisión de procesos**

Habilite esta configuración para permitir la supervisión de procesos que se ejecutan en las máquinas con agentes VDA. Las estadísticas (por ejemplo, acerca del uso de la CPU y la memoria) se envían a Monitoring Service. Las estadísticas se utilizan para notificaciones en tiempo real e informes históricos en Director.

La opción predeterminada de esta configuración es “Inhabilitada”.

### **Habilitar supervisión de recursos**

Habilite esta configuración para permitir la supervisión de los contadores de rendimiento en las máquinas con agentes VDA. Las estadísticas (por ejemplo, acerca de la CPU y la memoria, IOPS y la latencia de datos) se envían a Monitoring Service. Las estadísticas se utilizan para notificaciones en tiempo real e informes históricos en Director.

La opción predeterminada de esta configuración es “Habilitada”.

### **Escalabilidad**

Los datos de la CPU y la memoria se envían desde cada VDA a la base de datos en intervalos de 5 minutos. Los datos de procesos (si la opción está habilitada) se envían a la base de datos en intervalos de 10 minutos. Los datos de IOPS y latencia disco se envían a la base de datos cada hora.

### **Datos de CPU y memoria**

De forma predeterminada, la opción de datos de CPU y memoria está **habilitada**. Los valores de retención de datos son los siguientes (licencia Platinum):

---

Granularidad de datos	Cantidad de días
Datos de 5 minutos	1 día
Datos de 10 minutos	7 días
Datos por hora	30 días

---

Granularidad de datos	Cantidad de días
Datos diarios	90 días

---

### Datos de IOPS y latencia de disco

Los datos de IOPS y latencia de disco están **habilitados** de forma predeterminada. Los valores de retención de datos son los siguientes (licencia Platinum):

---

Granularidad de datos	Cantidad de días
Datos por hora	3 días
Datos diarios	90 días

---

Con esta configuración de retención de datos, se necesitan aproximadamente 276 KB de espacio para almacenar los datos de la CPU, la memoria las IOPS y la latencia de disco provenientes de un VDA en un periodo de un año.

---

Cantidad de máquinas	Almacenamiento aproximado requerido
1	276 KB
1000	270 MB
40 000	10,6 GB

---

### Datos de procesos

Los datos de procesos están **inhabilitados** de forma predeterminada. Se recomienda habilitar los datos de procesos en un subconjunto de máquinas si fuera necesario. La configuración predeterminada de retención para datos de procesos es la siguiente:

---

Granularidad de datos	Cantidad de días
Datos de 10 minutos	1 día
Datos por hora	7 días

---

Si se habilitan los datos de procesos, con la configuración predeterminada de retención de datos, consumirían aproximadamente 1,5 MB por cada VDA y 3 MB por cada VDA de Terminal Services (VDA de TS) en un periodo de un año.

Cantidad de máquinas	Almacenamiento aproximado requerido para el VDA	Almacenamiento aproximado requerido para el VDA de Terminal Services
1	1,5 MB	3 MB
1000	1,5 GB	3 GB

**Nota**

Estos números no incluyen el espacio de índice. Además, todos esos cálculos son aproximados y pueden variar de una implementación a otra.

**Configuraciones opcionales**

Puede modificar la configuración de retención predeterminada para que se adapte a sus necesidades. Sin embargo, eso consume almacenamiento extra. Al habilitar los siguientes parámetros, puede obtener más precisión en los datos de uso de procesos. Las configuraciones que se pueden habilitar son:

**EnableMinuteLevelGranularityProcessUtilization****EnableDayLevelGranularityProcessUtilization**

Estas configuraciones se pueden habilitar desde el cmdlet Monitoring de PowerShell: [Set-MonitorConfiguration](#)

**Directivas para la supervisión de fallos de aplicaciones**

De forma predeterminada, la ficha **Fallos y errores de aplicación** muestra solo los errores de aplicaciones en los VDA de SO multisesión. Puede modificar las configuraciones de supervisión de fallos en aplicaciones con las siguientes directivas de supervisión:

**Habilitar supervisión de fallos y errores de aplicación**

Use esta configuración para definir la supervisión de los fallos de aplicaciones y supervisar errores y fallos (bloqueos del sistema y excepciones no controladas) o ambos. Para inhabilitar la supervisión

de fallos de aplicaciones, establezca el campo **Valor** en **Ninguno**. El valor predeterminado de esta configuración es “Solo fallos de aplicación”.

### **Habilitar supervisión de fallos y errores de aplicación en VDA de SO de sesión única**

De forma predeterminada, solo se supervisan los fallos de las aplicaciones alojadas en agentes VDA de SO multisesión. Para supervisar los VDA de SO de sesión única, establezca la directiva en **Permitida**. De forma predeterminada, esta configuración está establecida en **Prohibida**.

### **Lista de aplicaciones excluidas de la supervisión de fallos y errores**

Especifique una lista de las aplicaciones que no se supervisarán para buscar fallos. De forma predeterminada, esta lista está vacía.

### **Sugerencias para la planificación de almacenamiento**

**Directiva de grupo.** Si no quiere supervisar los datos de recursos o procesos, ambos se pueden desactivar mediante la directiva de grupo. Para obtener más información, consulte la sección Directiva de grupo de [Creación de directivas](#).

**Limpieza de datos.** La configuración predeterminada de retención de datos se puede modificar para limpiar los datos antes y así liberar espacio de almacenamiento. Para obtener más información sobre los parámetros de limpieza de datos, consulte Granularidad y retención de datos en [Acceder a datos mediante la API](#).

## **Configuraciones de directiva de IP virtual**

February 6, 2020

#### **Importante:**

La multisesión de Windows 10 Enterprise no admite virtualización de IP de Escritorio remoto (IP virtual) y nosotros no admitimos IP virtual ni bucle invertido virtual en multisesión con Windows 10 Enterprise.

La sección IP virtual contiene configuraciones de directiva que controlan si las sesiones tienen su propia dirección virtual de bucle invertido.

## **Funcionalidad de bucle invertido de IP virtual**

Cuando esta configuración está habilitada, cada sesión tiene su propia dirección virtual de bucle invertido. Cuando está inhabilitada, las sesiones no tienen direcciones de bucle invertido individuales.

De forma predeterminada, esta configuración está inhabilitada.

## **Lista de programas para bucle invertido de IP virtual**

Esta configuración especifica los archivos ejecutables de aplicaciones que pueden usar direcciones virtuales de bucle invertido. Al agregar programas a la lista, especifique solamente el nombre del archivo ejecutable, no es necesario especificar la ruta completa.

De forma predeterminada, no hay archivos ejecutables especificados.

## **Configurar la redirección de puertos COM y puertos LPT mediante el Registro**

September 22, 2021

En las versiones de VDA desde 7.0 a 7.8, los parámetros de puertos COM y puertos LPT solo se pueden configurar mediante el Registro. Para versiones de VDA anteriores a 7.0 y a partir de VDA 7.9, estos parámetros se pueden configurar en Studio. Para obtener más información, consulte [Configuraciones de directiva de Redirección de puertos](#) y [Configuraciones de directiva de ancho de banda](#).

Las configuraciones de directiva de Redirección de puertos COM y puertos LPT se encuentran en HKLM\Software\Citrix\GroupPolicy\Defaults\Deprecated en la imagen o la máquina VDA.

Para habilitar la redirección de puertos COM y puertos LPT, agregue nuevas claves de Registro de tipo REG\_DWORD, como se muestra a continuación:

Precaución: Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

---

Clave del Registro	Descripción	Valores permitidos
AllowComPortRedirection	Permitir o impedir la redirección de puertos COM	1 (Permitir) o 0 (Prohibir)

Clave del Registro	Descripción	Valores permitidos
LimitComBw	Límite de ancho de banda para el canal de redirección de puertos COM	Valor numérico
LimitComBWPercent	Límite de ancho de banda para el canal de redirección de puertos COM como un porcentaje del ancho de banda total de la sesión	Valor numérico comprendido entre 0 y 100
AutoConnectClientComPorts	Conectar automáticamente los puertos COM del dispositivo de usuario	1 (Permitir) o 0 (Prohibir)
AllowLptPortRedirection	Permitir o impedir la redirección de puertos LPT	1 (Permitir) o 0 (Prohibir)
LimitLptBw	Límite de ancho de banda para el canal de redirección de puertos LPT	Valor numérico
LimitLptBwPercent	Límite de ancho de banda para el canal de redirección de puertos LPT como un porcentaje del ancho de banda total de la sesión	Valor numérico comprendido entre 0 y 100
AutoConnectClientLptPorts	Conectar automáticamente los puertos LPT del dispositivo de usuario	1 (Permitir) o 0 (Prohibir)

Después de configurar estos parámetros, modifique los catálogos de máquinas para usar la nueva imagen maestra o el equipo físico actualizado. Los escritorios se actualizan con la nueva configuración la próxima vez que los usuarios cierran la sesión.

## Configuración de directivas de Connector for Configuration Manager 2012

September 22, 2021

La sección de Connector for Configuration Manager 2012 contiene los parámetros de directiva para configurar la versión 7.5 del agente Citrix Connector Agent.

Importante: Las directivas acerca de advertencias, cierres de sesión y mensajes de reinicio solo se aplican a implementaciones en catálogos de máquinas con SO multisesión administradas manualmente o mediante Provisioning Services. Para esos catálogos de máquinas, el servicio Connector avisa a los usuarios cuando hay instalaciones de aplicaciones o actualizaciones de software pendientes.

En caso de catálogos administrados por MCS, use Studio para notificar a los usuarios. En caso de catálogos de máquinas con SO de sesión única administrados manualmente, utilice Configuration Manager para notificar a los usuarios. En caso de catálogos de máquinas con SO de sesión única administradas por Provisioning Services, utilice Provisioning Services para notificar a los usuarios.

### **Frecuencia de advertencias por adelantado**

Este parámetro define el intervalo de frecuencia con que aparecen los mensajes de advertencia para los usuarios.

Los intervalos se establecen con el formato ddd.hh:mm:ss, donde:

- ddd son los días, un parámetro optativo, con un rango de 0 a 999.
- hh son las horas, con un rango de 0 a 23.
- hh son los minutos, con un rango de 0 a 59.
- hh son los segundos, con un rango de 0 a 59.

De forma predeterminada, el valor del intervalo es de 1 hora (01:00:00).

### **Texto del mensaje de advertencia por adelantado**

Este parámetro contiene el texto a modificar del mensaje para los usuarios, donde se les notifica que va a haber actualizaciones de software o un periodo de mantenimiento para lo cual necesitan cerrar sesión.

De forma predeterminada, el mensaje contiene este texto: {TIMESTAMP} Please save your work. The server will go offline for maintenance in {TIMELEFT}.

### **Título del mensaje de advertencia por adelantado**

Este parámetro contiene el texto modificable del título del mensaje de advertencia dirigido a los usuarios.

De manera predeterminada, el título es Upcoming Maintenance.

## **Periodo de advertencia por adelantado**

Este parámetro define el tiempo de antelación con que aparecen por primera vez los mensajes de advertencia sobre el mantenimiento.

El tiempo se establece con el formato ddd.hh:mm:ss, donde:

- ddd son los días, un parámetro optativo, con un rango de 0 a 999.
- hh son las horas, con un rango de 0 a 23.
- hh son los minutos, con un rango de 0 a 59.
- hh son los segundos, con un rango de 0 a 59.

De forma predeterminada, el valor es de 16 horas (16:00:00), lo que indica que el primer mensaje de advertencia aparece aproximadamente 16 horas antes del mantenimiento.

## **Texto del mensaje final de cierre de sesión forzado**

Este parámetro contiene el texto modificable del mensaje donde se avisa a los usuarios que se ha comenzado un cierre de sesión forzoso.

De manera predeterminada, el mensaje contiene el texto siguiente: The server is currently going offline for maintenance.

## **Título del mensaje final de cierre de sesión forzado**

Este parámetro contiene el texto modificable del título del mensaje donde se avisa a los usuarios que se ha comenzado un cierre de sesión forzoso.

De manera predeterminada, el título es Notification From IT Staff.

## **Periodo de gracia de cierre de sesión forzado**

Este parámetro define el tiempo que transcurre desde que se notifica a los usuarios que deben cerrar sesión hasta que se aplica el cierre de sesión forzoso para procesar el mantenimiento pendiente.

El tiempo se establece con el formato ddd.hh:mm:ss, donde:

- ddd son los días, un parámetro optativo, con un rango de 0 a 999.
- hh son las horas, con un rango de 0 a 23.
- hh son los minutos, con un rango de 0 a 59.
- hh son los segundos, con un rango de 0 a 59.

De manera predeterminada, el periodo de gracia para el cierre de sesión forzoso es de 5 minutos (00:05:00).

### **Texto del mensaje de cierre de sesión forzado**

Este parámetro contiene el texto modificable del mensaje donde se avisa a los usuarios que deben guardar su trabajo y cerrar la sesión antes de que comience el cierre de sesión forzado.

De manera predeterminada, el mensaje contiene este texto: {TIMESTAMP} Please save your work and log off. The server will go offline for maintenance in {TIMELEFT}.

### **Título del mensaje de cierre de sesión forzado**

Este parámetro contiene el texto modificable del título del mensaje de advertencia sobre el cierre de sesión forzado.

De manera predeterminada, el título es Notification From IT Staff.

### **Modo administrado por imagen**

El servicio Connector Agent detecta automáticamente si se está ejecutando en una máquina clonada administrada por Provisioning Services o MCS. El agente bloquea las actualizaciones de Configuration Manager en clones administrados por imagen, e instala automáticamente las actualizaciones en la imagen maestra del catálogo.

Después de actualizar una imagen maestra, use Studio para orquestar el reinicio de los clones del catálogo de MCS. El servicio Connector Agent orquesta automáticamente el reinicio de los clones del catálogo de PVS durante las ventanas de mantenimiento de Configuration Manager. Si quiere anular este comportamiento para que Configuration Manager instale el software en los clones de catálogo, cambie el modo administrado por imagen a Inhabilitada.

### **Texto del mensaje de reinicio**

Este parámetro contiene el texto modificable del mensaje donde se avisa a los usuarios de que el servidor está a punto de reiniciarse.

De manera predeterminada, el mensaje contiene el texto siguiente: The server is currently going offline for maintenance.

### **Intervalo regular para ejecutar la tarea del agente**

Este parámetro determina la frecuencia con la que se ejecuta la tarea del agente Citrix Connector Agent.

El tiempo se establece con el formato ddd.hh:mm:ss, donde:

- ddd son los días, un parámetro optativo, con un rango de 0 a 999.
- hh son las horas, con un rango de 0 a 23.
- hh son los minutos, con un rango de 0 a 59.
- hh son los segundos, con un rango de 0 a 59.

De forma predeterminada, el parámetro del intervalo regular es de 5 minutos (00:05:00).

## Administrar

September 22, 2021

La administración de un sitio de Citrix Virtual Apps and Desktops abarca varios elementos y tareas.

### Licencias

Es necesaria una conexión válida al servidor de licencias de Citrix cuando se crea un sitio. Más adelante, podrá realizar varias tareas de licencias desde Studio, como agregar licencias, cambiar sus tipos o modelos, además de gestionar a los administradores de licencias. También podrá acceder a la consola License Administration Console desde Studio.

### Aplicaciones

Administre aplicaciones en grupos de entrega y, opcionalmente, en grupos de aplicaciones.

### Zonas

En una implementación de puntos geográficamente alejados, puede usar zonas para mantener las aplicaciones y los escritorios más cerca de los usuarios finales, lo que mejora el rendimiento. Cuando se instala y se configura un sitio, todos los Controllers, los catálogos de máquinas y las conexiones de host están en una zona principal. Posteriormente, puede usar Studio para crear zonas satélite que contengan esos elementos. Una vez que el sitio tenga más de una zona, podrá indicar en qué zona se colocarán las conexiones de host, los catálogos de máquinas recién creados o los Controllers recién agregados. También podrá mover elementos entre zonas.

### Conexiones y recursos

Si usa un hipervisor o un servicio de nube para alojar máquinas que van a entregar aplicaciones y escritorios a los usuarios, cree la primera conexión a ese hipervisor o servicio de nube al crear un sitio. Los detalles de almacenamiento y de red de dicha conexión conforman sus *recursos*. Posteriormente, puede cambiar esa conexión y sus recursos, además de crear nuevas conexiones. También puede administrar las máquinas que usan una conexión configurada.

### Caché de host local

La Caché de host local permite que la intermediación de operaciones en un sitio continúe cuando se interrumpa la conexión entre un Delivery Controller y la base de datos del sitio.

## IP virtual y bucle invertido virtual

La función de dirección IP virtual de Microsoft proporciona una dirección IP exclusiva a una aplicación publicada, asignada dinámicamente para cada sesión. La función de bucle invertido virtual de Citrix permite configurar aplicaciones que dependen de la comunicación con el host local (127.0.0.1 de forma predeterminada) para utilizar una dirección de bucle invertido virtual exclusiva en el intervalo de host local (127.\*).

## Delivery Controllers

Este artículo contiene procedimientos y aspectos a tener en cuenta a la hora de agregar y quitar Controllers de un sitio. Asimismo, se describe cómo mover los Controllers a otra zona o sitio, y cómo mover un VDA a otro sitio.

## Registro de VDA con Controllers

Para que un VDA pueda facilitar la entrega de aplicaciones y escritorios, debe registrarse en un Controller (establecer comunicación con él). Las direcciones del Controller se pueden especificar de varias maneras, todas ellas descritas en este artículo. Es importante que los agentes VDA tengan información actualizada a medida que se agreguen, se muevan o se eliminen Controllers del sitio.

## Sesiones

El mantenimiento de la actividad de las sesiones es fundamental para ofrecer la mejor experiencia de uso. Existen varias funciones que pueden optimizar la fiabilidad de sesiones, reducir los problemas, el tiempo de inactividad y la pérdida de la productividad.

- Fiabilidad de la sesión
- Reconexión automática de clientes
- ICA Keep-Alive
- Control del espacio de trabajo
- Itinerancia de sesiones

## Usar las búsquedas en Studio

Si quiere ver información acerca de las máquinas, las sesiones, los catálogos de máquinas, las aplicaciones o los grupos de entrega en Studio, utilice la función flexible de búsqueda.

## Etiquetas

Utilice etiquetas para identificar elementos tales como máquinas, aplicaciones, grupos y directivas. A continuación, puede ajustar determinadas operaciones para aplicarlas a elementos con una etiqueta determinada.

## IPv4 o IPv6

Citrix Virtual Apps and Desktops admite IPv4 puro, IPv6 puro, así como implementaciones de doble pila que usan redes IPv4 e IPv6 superpuestas. En este artículo, se describen y se muestran estas im-

plementaciones. También se describen las configuraciones de directivas Citrix que determinan el uso de IPv4 o IPv6.

### Perfiles de usuario

De forma predeterminada, Citrix Profile Management se instala automáticamente al instalar un VDA. Si usa esta solución de perfiles, consulte este artículo para obtener información general; consulte la documentación de Profile Management para obtener información detallada.

### Citrix Insight Services

Citrix Insight Services (CIS) es una plataforma de Citrix para instrumentación, telemetría y generación de información empresarial.

## Licencias

August 9, 2022

#### Nota:

Ni Studio ni Director admiten Citrix License Server VPX.

Puede usar Studio para administrar y realizar un rastreo de las licencias, siempre y cuando el servidor de licencias esté en el mismo dominio que Studio o en un dominio de confianza. Para obtener información sobre otras tareas relacionadas con las licencias, consulte la [documentación sobre el sistema de licencias](#) y [Licencias de varios tipos](#).

Debe ser un administrador total de licencias para llevar a cabo las tareas que se describen en este artículo, excepto para ver la información de las licencias. Para ver la información de licencias en Studio, un administrador debe tener al menos el permiso de lectura de licencias de administración delegada; los roles de administrador total y de administrador de solo lectura integrados tienen esos permisos.

La siguiente tabla ofrece una lista de las ediciones y los modelos de licencia admitidos:

Productos	Ediciones	Modelos de licencia
Citrix Virtual Apps	Premium, Advanced, Standard	Simultánea
Citrix Virtual Desktops	Premium, Advanced, Standard	Usuario por dispositivo y simultánea

Para obtener más información sobre el uso compartido de licencias, consulte [Licencias concurrentes](#).

**Importante:**

License Server VPX se ha retirado y no recibirá más correcciones de mantenimiento o seguridad. Se recomienda a los clientes que usen 11.16.6 o versiones anteriores de License Server VPX que migren a [la versión más reciente del Servidor de licencias para Windows](#) lo antes posible.

## **Versiones Current Release (CR) y Long Term Service Release (LTSR) compatibles**

Para obtener información sobre las versiones Current Release (CR), Long Term Service Release (LTSR) y LS compatibles, consulte la documentación de la [versión Current Release de Citrix Virtual Apps and Desktops](#).

### **Ver información de licencias**

Seleccione **Configuración > Licencias** en el panel de navegación de Studio. Se muestra un resumen del uso de licencias y los parámetros del sitio, junto con una lista de todas las licencias instaladas actualmente en el servidor de licencias especificado.

Compruebe que la configuración de licencias del sitio, que incluye el tipo de producto, la edición de las licencias y el modelo de licencia, coincide con las licencias que utiliza el servidor de licencias configurado. De lo contrario, es posible que tenga que descargar o asignar las licencias de salida para que coincidan con la configuración de licencias del sitio.

Para descargar una licencia de Citrix:

1. Seleccione **Configuración > Licencias** en el panel de navegación de Studio.
2. Seleccione **Asignar licencias** en el panel Acciones.
3. Introduzca el código de acceso de licencia (License Access Code) suministrado por Citrix en un mensaje de correo electrónico.
4. Seleccione un producto y elija **Asignar licencias**. Todas las licencias disponibles para ese producto se asignarán y se descargarán. Una vez que se asignan y se descargan todas las licencias para un código de acceso de licencia específico, no se puede volver a usar ese código. Si tiene que llevar a cabo otras transacciones con ese código, inicie sesión en My Account.

Para agregar licencias almacenadas en el equipo local o en la red:

1. Seleccione **Configuración > Licencias** en el panel de navegación de Studio.
2. Seleccione **Agregar licencias** en el panel Acciones.
3. Vaya a un archivo de licencias y agréguelo al servidor de licencias.

Para cambiar el servidor de licencias:

1. Seleccione **Configuración > Licencias** en el panel de navegación de Studio.

2. Seleccione **Cambiar servidor de licencias** en el panel Acciones.
3. Escriba la dirección del servidor de licencias en el formato *nombre:puerto*, donde el nombre es una dirección DNS, NetBIOS o IP. Si no especifica un número de puerto, se utiliza el puerto predeterminado (27000).

Para seleccionar el tipo de licencia que se va a utilizar:

- Al configurar el sitio, después de especificar el servidor de licencias, se le solicita que seleccione el tipo de licencia que va a utilizar. Si no existen licencias en el servidor, se selecciona automáticamente la opción para utilizar el producto durante un período de prueba de 30 días sin una licencia.
- Si existen licencias en el servidor, se muestran los detalles y se puede seleccionar una de ellas. O bien puede agregar un archivo de licencia al servidor y seleccionar ese archivo.

Para cambiar la edición y el modelo de licencia del producto:

1. Seleccione **Configuración > Licencias** en el panel de navegación de Studio.
2. Seleccione **Modificar edición de producto** en el panel Acciones.
3. Actualice las opciones pertinentes.

Para acceder a la consola License Administration Console, en el panel Acciones, seleccione **License Administration Console**. La consola aparece inmediatamente o bien, si el panel de mandos está configurado con la protección por contraseña, se le pedirán las credenciales de la consola License Administration Console. Para obtener más información acerca de cómo usar la consola, consulte la documentación de licencias.

Para agregar un administrador de licencias:

1. Seleccione **Configuración > Licencias** en el panel de navegación de Studio.
2. Seleccione la ficha Administradores de licencias en el panel central.
3. Seleccione **Agregar administrador de licencias** en el panel Acciones.
4. Vaya al usuario que quiere agregar como administrador y elija los permisos correspondientes.

Para modificar los permisos de un administrador de licencias o eliminarlo:

1. Seleccione **Configuración > Licencias** en el panel de navegación de Studio.
2. Seleccione la ficha Administradores de licencias en el panel central y, a continuación, seleccione el administrador en cuestión.
3. Seleccione **Modificar administrador de licencias** o **Eliminar administrador de licencias** en el panel Acciones.

Para agregar un grupo de administradores de licencias:

1. Seleccione **Configuración > Licencias** en el panel de navegación de Studio.
2. Seleccione la ficha Administradores de licencias en el panel central.

3. Seleccione **Agregar grupo de administradores de licencias** en el panel Acciones.
4. Vaya al grupo de usuarios que quiere que actúen como administradores y elija los permisos correspondientes. Cuando se agrega un grupo de Active Directory se dan permisos de administrador de licencias a los usuarios de ese grupo.

Para modificar los permisos de un grupo de administradores de licencias o eliminar dicho grupo:

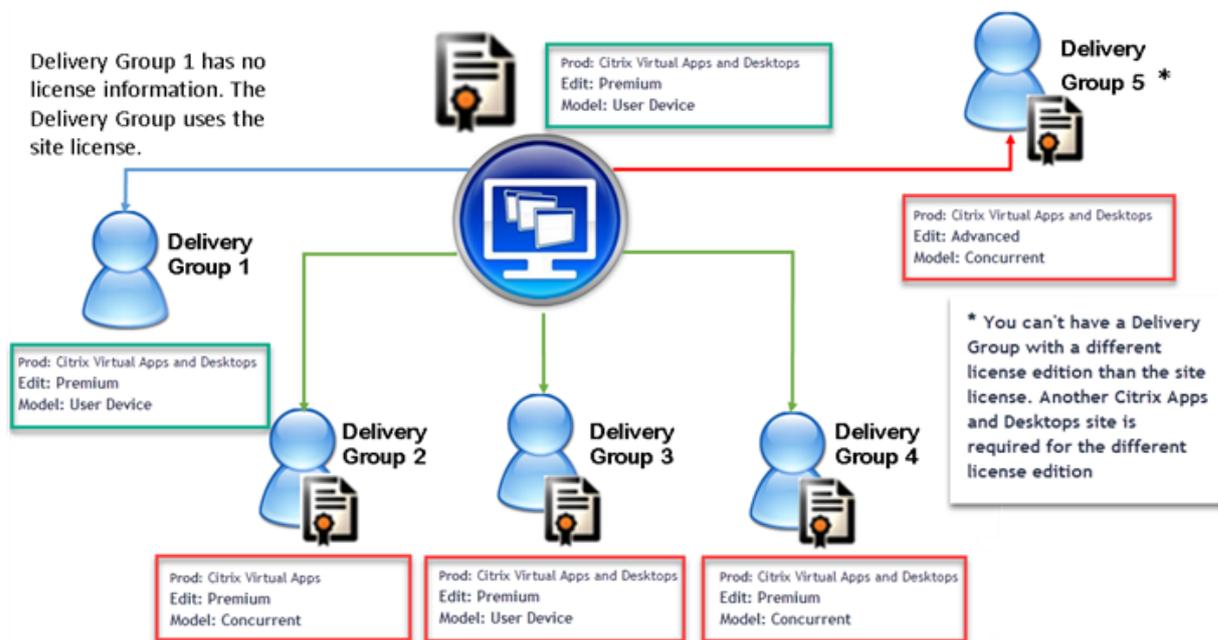
1. Seleccione **Configuración > Licencias** en el panel de navegación de Studio.
2. Seleccione la ficha Administradores de licencias en el panel central y, a continuación, seleccione el grupo de administradores en cuestión.
3. Seleccione **Modificar grupo de administradores de licencias** o **Eliminar grupo de administradores de licencias** en el panel Acciones.

## Licencias de varios tipos

March 10, 2022

Con licencias de varios tipos, puede usar tipos de licencias diferentes para grupos de entrega en un único sitio de Citrix Virtual Apps and Desktops. El **tipo de licencia** es una combinación única del ID de producto (XDT o MPS) y el modelo (UserDevice o Concurrent). Los grupos de entrega deben utilizar la misma edición del producto (PLT/Premium o ENT/Advanced) configurada en el nivel de sitio. Observe las [consideraciones especiales](#) al final de este artículo al configurar licencias de varios tipos para sus implementaciones de Citrix Virtual Apps and Desktops.

Si no se configura el uso de licencias de varios tipos, solo podrá utilizar tipos distintos de licencias cuando se configuren en sitios independientes. Los grupos de entrega usan la licencia del sitio. Para obtener información importante sobre limitaciones de notificación al configurar licencias de varios tipos, consulte [Consideraciones especiales](#).



Para determinar los grupos de entrega que consumen los distintos tipos de licencias, utilice estos cmdlets de Broker PowerShell:

- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup
- Get-BrokerDesktopGroup

Para instalar licencias, utilice:

- Citrix Studio
- Citrix Licensing Manager
- License Administration Console
- citrix.com

Las fechas de Subscription Advantage son únicas para cada archivo de licencia, producto y modelo. Los grupos de entrega que se configuren de manera diferente podrían tener diferentes fechas de Subscription Advantage entre sí.

### Tabla de compatibilidad de licencias

En esta tabla se indican los nombres de productos antiguos, los nombres de productos nuevos y los nombres de funciones asociadas. Las cuatro columnas de compatibilidad especifican qué combinaciones de producto y modelo de licencia son compatibles para licencias de varios tipos. Por ejemplo, todos los tipos con una **X** en la columna **1** son compatibles. CCU y CCS son licencias simultáneas y UD son licencias de usuario/dispositivo.

Old Name	New Name	Feature	Multi-type licensing compatibility			
			1	2	3	4
Citrix XenApp Standard	Citrix XenApp Standard	MPS_STD_CCU	X			
Citrix XenApp Advanced	Citrix Virtual Apps Standard	MPS_ADV_CCU		X		
Citrix XenApp Enterprise	Citrix Virtual Apps Advanced	MPS_ENT_CCU			X	
Citrix XenApp Platinum	Citrix Virtual Apps Premium	MPS_PLT_CCU				X
CSP - Citrix XenApp Base	Citrix Virtual Apps Base	XDT_ADV_UD		X		
CSP Premium	Citrix Virtual Apps and Desktops Premium	XDT_PLT_UD				X
Citrix XenDesktop VDI Edition (XDT-U)	Citrix Virtual Desktops - Per User/Device	XDT_STD_UD	X			
Citrix XenDesktop VDI Edition (XDT-C)	Citrix Virtual Desktops - Concurrent	XDT_STD_CCS	X			
Citrix XenDesktop Enterprise Edition (XDT-C)	Citrix Virtual Apps and Desktops Advanced - Concurrent	XDT_ENT_CCS			X	
Citrix XenDesktop Enterprise Edition (XDT-U)	Citrix Virtual Apps and Desktops Advanced - Per User/Device	XDT_ENT_UD			X	
Citrix XenDesktop Platinum Edition (XDT-C)	Citrix Virtual Apps and Desktops Premium - Concurrent	XDT_PLT_CCS				X
Citrix XenDesktop Platinum Edition (XDT-U)	Citrix Virtual Apps and Desktops Premium - Per User/Device	XDT_PLT_UD				X

## SDK de Broker PowerShell

El objeto **DesktopGroup** tiene estas dos propiedades que puede manipular mediante los cmdlets `New-BrokerDesktopGroup` y `Set-BrokerDesktopGroup` asociados.

Nombre	Valor	Restricción
LicenseModel	Un parámetro (Concurrent o UserDevice) que especifica el modelo de licencias para el grupo. Si no se especifica ninguno, se utiliza el modelo de licencias para todo el sitio.	Si está inhabilitada la activación o desactivación de la función, no se puede establecer ninguna de las propiedades.
ProductCode	Una cadena de texto de XDT (para Citrix Virtual Desktops) o MPS (para Citrix Virtual Apps) que especifica el ID de licencia del producto para el grupo. Si no se especifica ninguno, se utiliza el código de producto para todo el sitio.	Si está inhabilitada la activación o desactivación de la función, no se puede establecer ninguna de las propiedades.

Para obtener más información sobre **LicenseModel** y **ProductCode**, consulte [about\\_Broker\\_Licensing](#).

### **New-BrokerDesktopGroup**

Crea un grupo de escritorio para administrar la intermediación de grupos de escritorios. Para obtener más información sobre este cmdlet, consulte <https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerDesktopGroup/>.

### **Set-BrokerDesktopGroup**

Inhabilita o habilita un grupo existente de escritorios intermediados o altera su configuración. Para obtener más información sobre este cmdlet, consulte <https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/>

### **Get-BrokerDesktopGroup**

Recupera los grupos de escritorio que coincidan con los criterios especificados. El resultado del cmdlet Get-BrokerDesktopGroup incluye las propiedades **ProductCode** y **LicenseModel** del grupo. Si las propiedades no se han establecido mediante New-BrokerDesktopGroup ni Set-BrokerDesktopGroup, se devuelven valores nulos. Si es nulo, se utiliza el código de producto y el modelo de licencia que ya se utiliza para todo el sitio. Para obtener más información sobre este cmdlet, consulte <https://citrix.github.io/delivery-controller-sdk/Broker/Get-BrokerDesktopGroup/>.

## **Configurar diferentes productos y modelos de licencia para cada grupo de entrega**

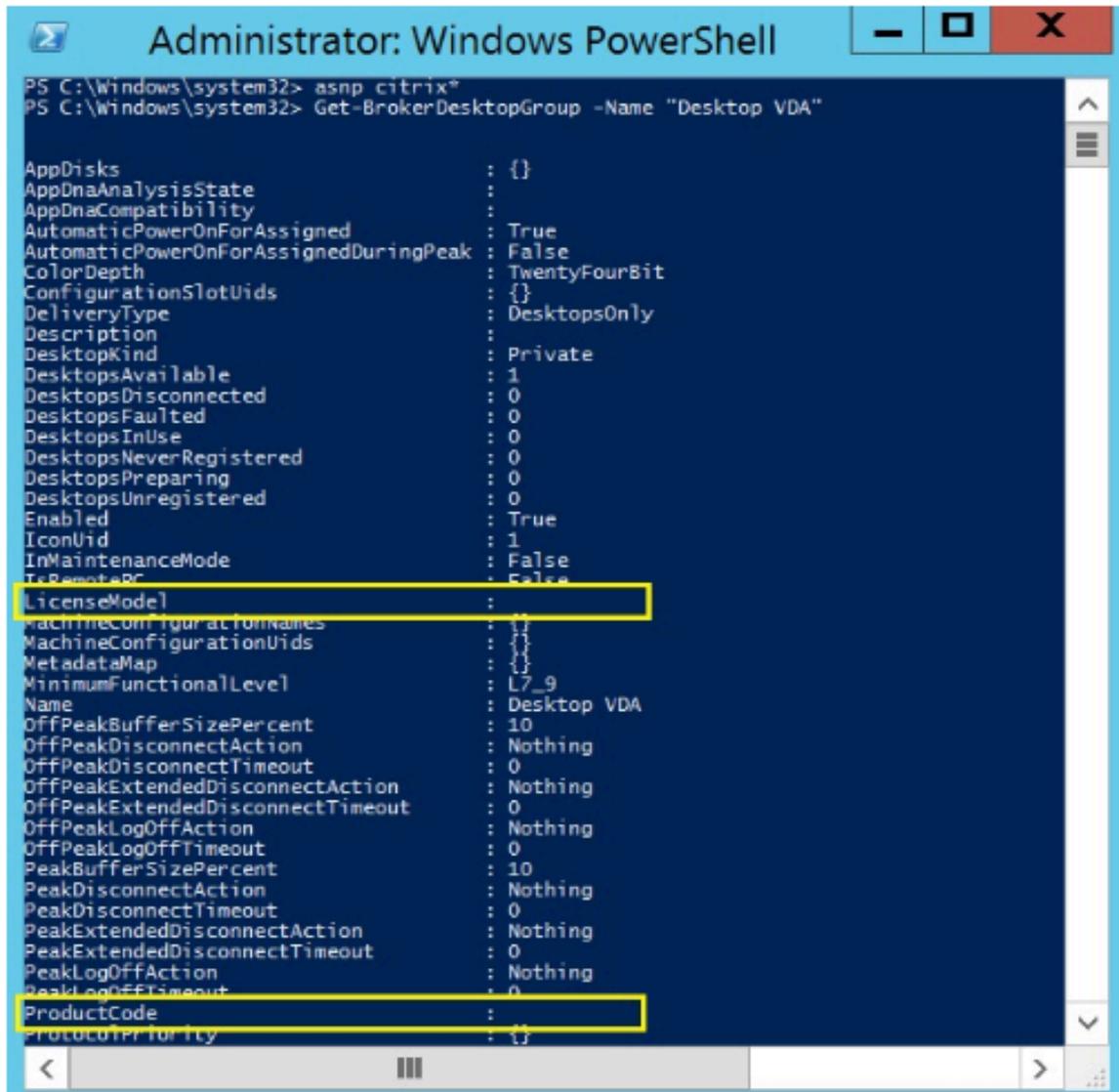
1. Abra PowerShell con derechos de administrador y agregue el complemento de Citrix.



2. Ejecute el comando **Get-BrokerDesktopGroup -Name "DeliveryGroupName"** para ver la configuración de licencias actual. Busque los parámetros **LicenseModel** y **ProductCode**. Si no ha configurado estos parámetros antes, es posible que estén vacíos.

Nota:

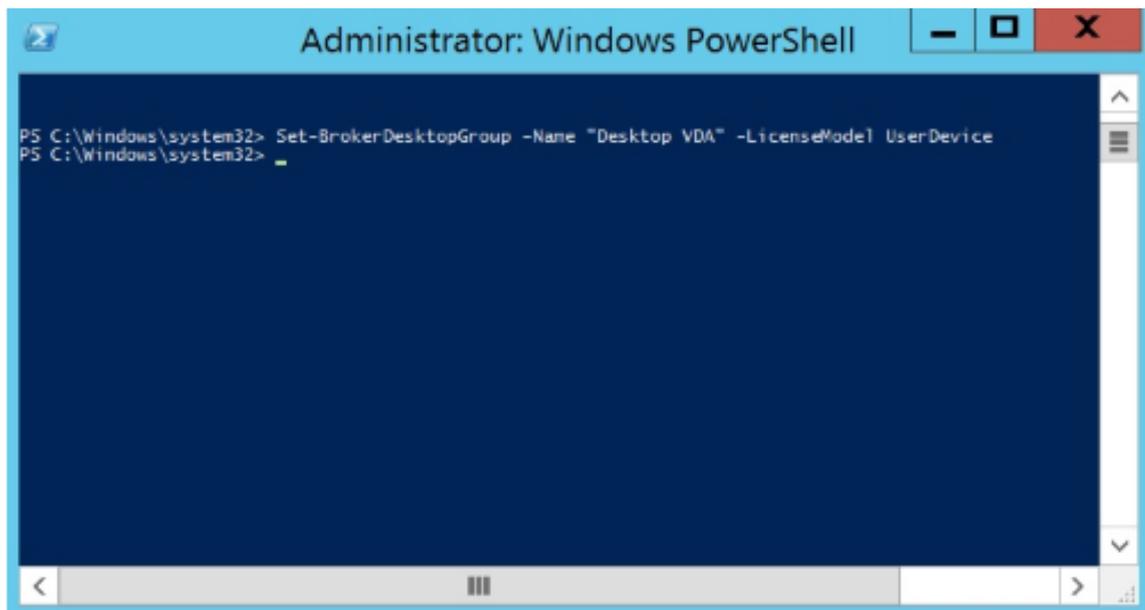
Si un grupo de entrega no tiene una información de licencias establecida, se utiliza de manera predeterminada la directiva **Site level Site license**.



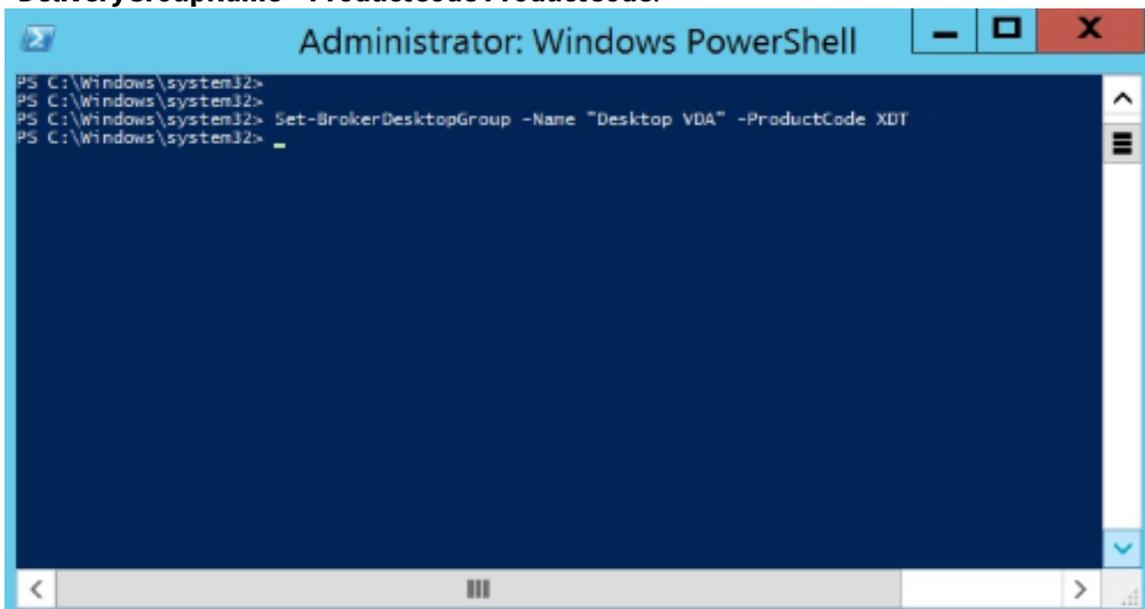
```
Administrator: Windows PowerShell
PS C:\Windows\system32> asnp citrix*
PS C:\Windows\system32> Get-BrokerDesktopGroup -Name "Desktop VDA"

AppDisks                : {}
AppDnaAnalysisState     :
AppDnaCompatibility     :
AutomaticPowerOnForAssigned : True
AutomaticPowerOnForAssignedDuringPeak : False
ColorDepth              : TwentyFourBit
ConfigurationSlotUids   : {}
DeliveryType            : DesktopsOnly
Description              :
DesktopKind              : Private
DesktopsAvailable       : 1
DesktopsDisconnected    : 0
DesktopsFaulted         : 0
DesktopsInUse           : 0
DesktopsNeverRegistered : 0
DesktopsPreparing       : 0
DesktopsUnregistered    : 0
Enabled                  : True
IconUid                  : 1
InMaintenanceMode       : False
IsRemotePC               : False
LicenseModel             :
MachineConfigurationNames : {}
MachineConfigurationUids : {}
MetadataMap              : {}
MinimumFunctionalLevel   : L7_9
Name                     : Desktop VDA
OffPeakBufferSizePercent : 10
OffPeakDisconnectAction  : Nothing
OffPeakDisconnectTimeout : 0
OffPeakExtendedDisconnectAction : Nothing
OffPeakExtendedDisconnectTimeout : 0
OffPeakLogOffAction      : Nothing
OffPeakLogOffTimeout     : 0
PeakBufferSizePercent    : 10
PeakDisconnectAction     : Nothing
PeakDisconnectTimeout    : 0
PeakExtendedDisconnectAction : Nothing
PeakExtendedDisconnectTimeout : 0
PeakLogOffAction         : Nothing
PeakLogOffTimeout        : 0
ProductCode              :
ProtocolPriority          : {}
```

3. Para cambiar el modelo de licencia, ejecute el comando **Set-BrokerDesktopGroup -Name "DeliveryGroupName"-LicenseModel LicenseModel**.



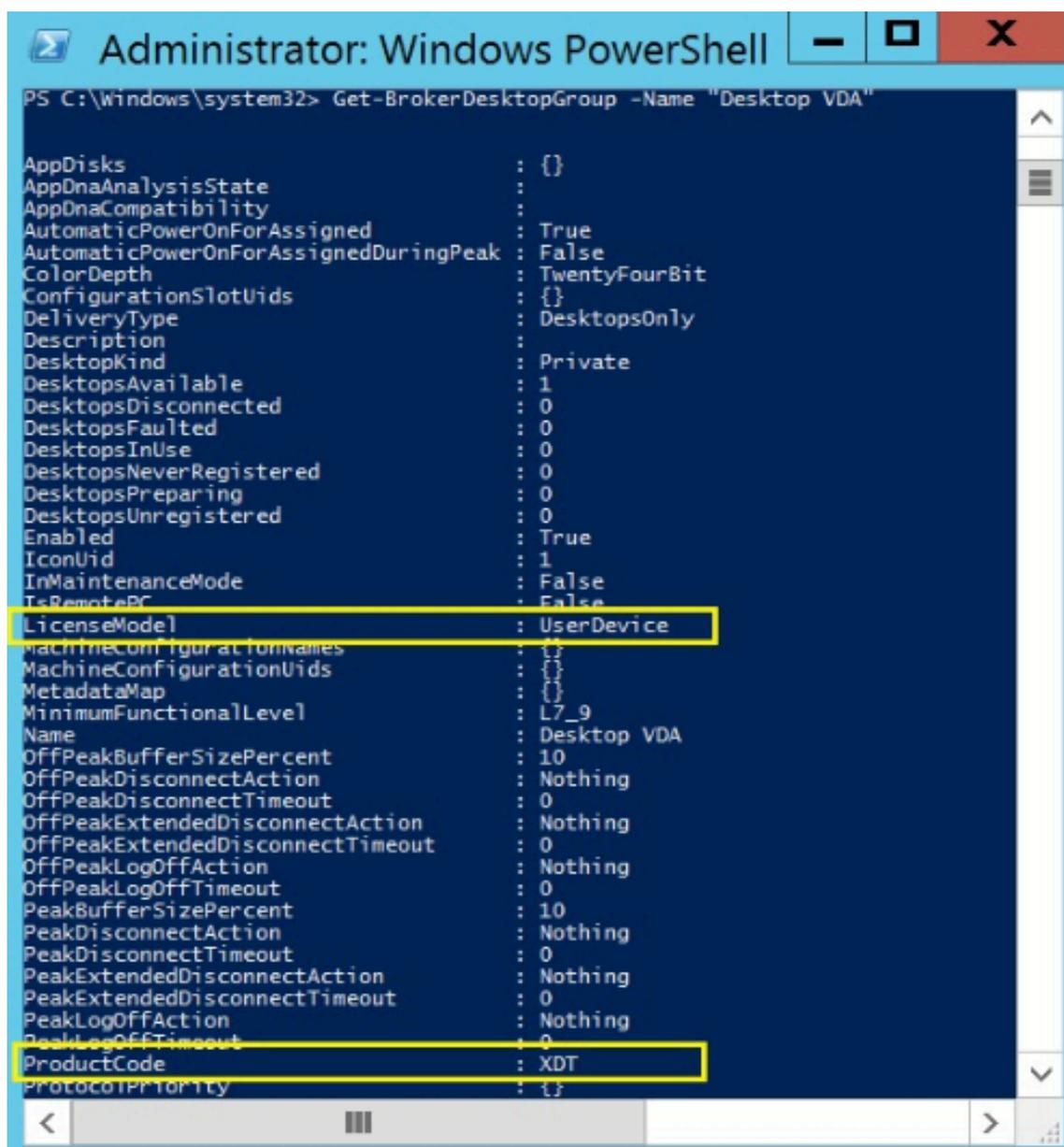
4. Para cambiar el producto de licencia, ejecute el comando **Set-BrokerDesktopGroup -Name "DeliveryGroupName"-ProductCode ProductCode**.



5. Introduzca el comando **Get-BrokerDesktopGroup -Name "DeliveryGroupName"** para validar los cambios.

Nota:

No puede mezclar ni combinar distintas ediciones en el mismo sitio. Por ejemplo, licencias Premium y Advanced. Se requieren varios sitios si tiene licencias con diferentes ediciones.



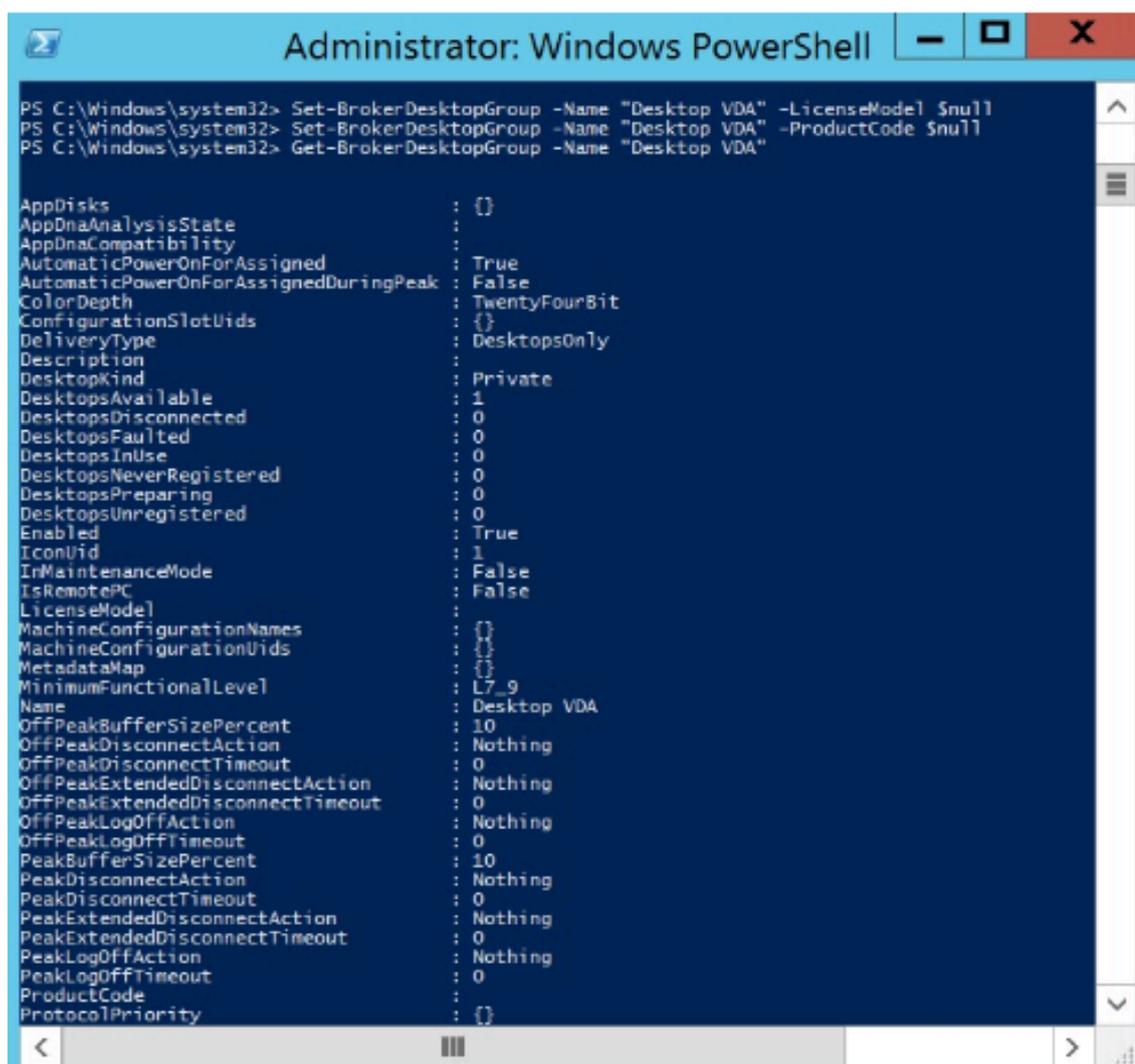
```
Administrator: Windows PowerShell
PS C:\Windows\system32> Get-BrokerDesktopGroup -Name "Desktop VDA"

AppDisks                : {}
AppDnaAnalysisState     :
AppDnaCompatibility     :
AutomaticPowerOnForAssigned : True
AutomaticPowerOnForAssignedDuringPeak : False
ColorDepth              : TwentyFourBit
ConfigurationSlotUids   : {}
DeliveryType            : DesktopsOnly
Description              :
DesktopKind              : Private
DesktopsAvailable       : 1
DesktopsDisconnected    : 0
DesktopsFaulted         : 0
DesktopsInUse           : 0
DesktopsNeverRegistered : 0
DesktopsPreparing       : 0
DesktopsUnregistered    : 0
Enabled                 : True
IconUid                 : 1
InMaintenanceMode       : False
IsRemotePC              : False
LicenseMode              : UserDevice
MachineConfigurationNames : {}
MachineConfigurationUids : {}
MetadataMap             : {}
MinimumFunctionalLevel  : L7_9
Name                    : Desktop VDA
OffPeakBufferSizePercent : 10
OffPeakDisconnectAction  : Nothing
OffPeakDisconnectTimeout : 0
OffPeakExtendedDisconnectAction : Nothing
OffPeakExtendedDisconnectTimeout : 0
OffPeakLogOffAction      : Nothing
OffPeakLogOffTimeout    : 0
PeakBufferSizePercent   : 10
PeakDisconnectAction     : Nothing
PeakDisconnectTimeout   : 0
PeakExtendedDisconnectAction : Nothing
PeakExtendedDisconnectTimeout : 0
PeakLogOffAction        : Nothing
PeakLogOffTimeout       : 0
ProductCode              : XDT
ProtocolPriority         : {}
```

6. Para quitar la configuración de licencias, ejecute los mismos comandos que los descritos anteriormente, **Set-BrokerDesktopGroup**, y establezca el valor en **\$null**.

Nota:

En Studio, no se muestra la configuración de licencias para cada grupo de entrega. Utilice PowerShell para ver la configuración actual.



```

Administrator: Windows PowerShell

PS C:\Windows\system32> Set-BrokerDesktopGroup -Name "Desktop VDA" -LicenseModel $null
PS C:\Windows\system32> Set-BrokerDesktopGroup -Name "Desktop VDA" -ProductCode $null
PS C:\Windows\system32> Get-BrokerDesktopGroup -Name "Desktop VDA"

AppDisks                : {}
AppDnaAnalysisState     :
AppDnaCompatibility     :
AutomaticPowerOnForAssigned : True
AutomaticPowerOnForAssignedDuringPeak : False
ColorDepth              : TwentyFourBit
ConfigurationSlotUids   : {}
DeliveryType            : DesktopsOnly
Description              :
DesktopKind             : Private
DesktopsAvailable       : 1
DesktopsDisconnected    : 0
DesktopsFaulted        : 0
DesktopsInUse           : 0
DesktopsNeverRegistered : 0
DesktopsPreparing      : 0
DesktopsUnregistered   : 0
Enabled                 : True
IconUid                 : 1
InMaintenanceMode      : False
IsRemotePC              : False
LicenseModel            :
MachineConfigurationNames : {}
MachineConfigurationUids : {}
MetadataMap             : {}
MinimumFunctionalLevel  : L7_9
Name                    : Desktop VDA
OffPeakBufferSizePercent : 10
OffPeakDisconnectAction : Nothing
OffPeakDisconnectTimeout : 0
OffPeakExtendedDisconnectAction : Nothing
OffPeakExtendedDisconnectTimeout : 0
OffPeakLogOffAction     : Nothing
OffPeakLogOffTimeout    : 0
PeakBufferSizePercent   : 10
PeakDisconnectAction    : Nothing
PeakDisconnectTimeout   : 0
PeakExtendedDisconnectAction : Nothing
PeakExtendedDisconnectTimeout : 0
PeakLogOffAction        : Nothing
PeakLogOffTimeout       : 0
ProductCode             :
ProtocolPriority         : {}

```

## Ejemplo

En este ejemplo de cmdlet de PowerShell, se representa cómo establecer varios tipos de licencias para dos grupos de entrega existentes; también se crea y se establece un tercer grupo de entrega.

Para ver el producto de licencia y el modelo de licencia asociado a un grupo de entrega, use el cmdlet de PowerShell **Get-BrokerDesktopGroup**.

1. El primer grupo de entrega se establece como XenApp y Concurrent.

**Set-BrokerDesktopGroup -Name "Delivery group for Citrix Virtual Apps Premium Concurrent"-ProductCode MPS -LicenseModel Concurrent**

2. El segundo grupo de entrega se establece como XenDesktop y Concurrent.

**Set-BrokerDesktopGroup -Name "Delivery group for Citrix Virtual Desktops Premium Concurrent"-ProductCode XDT -LicenseModel Concurrent**

3. El tercer grupo de entrega se crea y se establece como XenDesktop y UserDevice.

**New-BrokerDesktopGroup -Name “Delivery group for Citrix Virtual Desktops Premium UserDevice”-PublishedName “MyDesktop”-DesktopKind Private -ProductCode XDT -LicenseModel UserDevice**

## Consideraciones especiales

Las licencias de varios tipos presentan una funcionalidad distinta de las licencias habituales de Citrix Virtual Apps and Desktops.

No hay alertas ni notificaciones de Director o Studio para los grupos de entrega configurados para usar un tipo que difiera de la configuración del sitio:

- No se informa cuando se acerca el límite de caducidad de la licencia, ni cuando comienza o caduca a su vez el período de gracia complementario.
- No se informa cuando un grupo concreto tiene un problema.

Los grupos de entrega configurados para licencias de varios tipos consumen SOLAMENTE ese tipo de licencia y no reierten a la configuración del sitio una vez que se han consumido todas.

Aunque los nombres de las ediciones de licencia de Citrix Virtual Apps Standard y Citrix Virtual Desktops Standard indican que ambos son Standard, no son de la misma edición. La función de licencias de varios tipos no funciona con las licencias de Citrix Virtual Apps Standard y Citrix Virtual Desktops Standard.

## Preguntas frecuentes sobre licencias

November 4, 2022

### Nota:

- Para los recursos sobre continuidad de negocio relacionados con la pandemia provocada por la COVID-19, consulte [CTX27055](#).
- Para obtener información general sobre cómo mantener la continuidad del negocio, consulte [Continuidad de negocio —a demanda](#).
- Para obtener más información acerca de la versión actual de Citrix License Server, consulte [Licensing](#).

## ¿Cómo funcionan las licencias de Citrix Virtual Apps and Desktops?

El sistema de licencias de Citrix Virtual Apps and Desktops ofrece modelos de licencia simultánea y de usuario/dispositivo.

### **Usuario/dispositivo:**

El modelo flexible de usuario/dispositivo se complementa bien con:

- El uso de escritorios en toda la empresa.
- Sistemas de licencias subyacentes a la virtualización de escritorios de Microsoft.
- Sistemas de licencias simultáneas para clientes con usuarios que solo necesitan acceso ocasional a sus aplicaciones y escritorios virtuales.

Sistemas de licencias de usuario/dispositivo que proporcionan a los usuarios acceso a sus aplicaciones y escritorios virtuales desde una cantidad ilimitada de dispositivos. Las licencias de dispositivo proporcionan una cantidad ilimitada de accesos de usuario a sus escritorios y aplicaciones virtuales desde un único dispositivo. Este enfoque le proporciona la máxima flexibilidad y se complementa mejor con los sistemas de licencias de virtualización de escritorios de Microsoft.

#### **Importante:**

No puede asignar licencias manualmente a usuarios o dispositivos. El Servidor de licencias o el servicio de nube son los que las asignan. Con el sistema de licencias de usuario/dispositivo, una vez asignada una licencia, no se puede asignar a otro usuario hasta que hayan transcurrido 90 días de inactividad.

### **Simultáneas:**

Las licencias simultáneas permiten una conexión a una cantidad ilimitada de aplicaciones y escritorios virtuales para cualquier usuario y dispositivo. Las licencias solo se consumen durante sesiones activas. Si la sesión se desconecta o finaliza, la licencia se devuelve al grupo de licencias.

Para obtener más información sobre el sistema de licencias de usuario/dispositivo, consulte [Licencias de usuario o dispositivo](#), y para las licencias simultáneas, [Licencias simultáneas](#).

## ¿Es posible probar Citrix Virtual Apps and Desktops antes de adquirir licencias?

Sí. Puede descargar el software de Citrix Virtual Apps and Desktops y ejecutarlo en modo de prueba. El modo de prueba le permite usar Citrix Virtual Apps and Desktops de manera local durante 30 días, para 10 conexiones y sin licencia.

Citrix Virtual Apps and Desktops Services para Citrix Cloud está disponible como servicio de prueba sometido a aprobación. Acuda a un representante de Citrix para obtener más información.

## **¿Cómo define Citrix la simultaneidad en Citrix Virtual Apps and Desktops?**

El modelo simultáneo de Citrix Virtual Apps and Desktops permite una conexión a una cantidad ilimitada de aplicaciones y escritorios virtuales para cualquier usuario y dispositivo. Las licencias solo se consumen durante sesiones activas. Si la sesión se desconecta o finaliza, la licencia se devuelve al grupo de licencias para volver a utilizarse más adelante.

## **¿Cómo asigna Citrix licencias a los usuarios en el modelo de licencias de usuario/dispositivo?**

Con el modelo de licencias de usuario/dispositivo, el Servidor de licencias asigna la licencia a un ID único de usuario. Permite que solamente un usuario disponga de conexiones ilimitadas desde dispositivos ilimitados. Si un usuario se conecta a un escritorio o dispositivo, el usuario necesita que se le asigne una licencia para acceder a un escritorio o una aplicación virtuales. El Servidor de licencias o el servicio de nube son los que la asignan. No puede asignar estas licencias manualmente. La licencia se asigna al usuario, no al dispositivo compartido. Una vez asignada una licencia, no se puede asignar a otro usuario hasta que hayan transcurrido 90 días de inactividad.

## **¿Cómo define Citrix un dispositivo con licencia en el modelo de licencias de usuario/dispositivo?**

Un dispositivo con licencia requiere un ID único de dispositivo de punto final. En el modelo de usuario/dispositivo, un dispositivo es cualquier elemento de equipo que haya autorizado para que cualquier persona pueda utilizar para acceder a instancias de Citrix Virtual Apps and Desktops. Para un dispositivo compartido, una única licencia de usuario/dispositivo de Citrix Virtual Apps and Desktops puede admitir varios usuarios que comparten el dispositivo. Por ejemplo, un dispositivo compartido puede ser la estación de trabajo de un aula o la estación de trabajo de una clínica en un hospital.

## **¿Puedo convertir mis licencias simultáneas de Citrix Virtual Desktops Standard Edition en el modelo de usuario/dispositivo?**

No puede convertir licencias simultáneas de Citrix Virtual Desktops Standard Edition en licencias de usuario/dispositivo de Citrix Virtual Desktops Standard Edition. Del mismo modo, no puede convertir licencias de usuario/dispositivo de Citrix Virtual Desktops Standard Edition en licencias simultáneas de Citrix Virtual Desktops Standard Edition.

Si tiene licencias simultáneas de Citrix Virtual Desktops Standard Edition y quiere el modelo de licencias de usuario/dispositivo, actualice la versión de Citrix Virtual Apps and Desktops a Advanced o Premium Edition.

De	A licencia simultánea de Standard Edition	A licencia de usuario/dispositivo de Standard Edition	A licencia de usuario/dispositivo de Advanced Edition	A licencia de usuario/dispositivo de Premium Edition
Licencias simultáneas de Citrix Virtual Desktops Standard Edition	N/D	Conversión de licencia simultánea a usuario/dispositivo NO permitida	No puede convertir modelos de licencia, pero puede actualizar la versión a Citrix Virtual Apps and Desktops Advanced o Premium Edition.	No puede convertir modelos de licencia, pero puede actualizar la versión a Citrix Virtual Apps and Desktops Advanced o Premium Edition.
Licencias de usuario/dispositivo de Citrix Virtual Desktops Standard Edition	Conversión de licencia de usuario/dispositivo a simultánea NO permitida	N/D	N/D	N/D

### ¿En qué se diferencia el sistema de licencias simultáneas del sistema de licencias de usuario/dispositivo?

Las licencias simultáneas se basan en conexiones simultáneas de dispositivos. Una licencia simultánea solo se considera en uso después de que un dispositivo establezca una conexión activa. Una vez finalizada la conexión, la licencia simultánea vuelve al grupo de licencias para poder ser utilizada inmediatamente. Se recomienda este modelo de licencia para usos ocasionales. Las licencias de usuario/dispositivo se ceden por un período y no están disponibles para otros usuarios hasta que caduque la cesión.

### En el modelo de usuario/dispositivo, ¿se pueden asignar licencias a usuarios y dispositivos de la misma empresa?

Sí. Ambos tipos pueden estar presentes en la misma empresa. El Servidor de licencias asigna de manera óptima licencias a usuarios o dispositivos en función del uso. No puede asignar estas licencias manualmente.

## ¿Cómo puedo decidir a cuántos usuarios o dispositivos conceder licencias?

Puede analizar los requisitos de los casos de uso para determinar la cantidad adecuada de licencias. El sistema de licencias por usuario/dispositivo permiten un acceso ilimitado a aplicaciones virtuales ilimitadas y escritorios virtuales ilimitados desde una cantidad ilimitada de dispositivos. El sistema de licencias simultáneas permite un acceso ilimitado a escritorios virtuales ilimitados y aplicaciones virtuales ilimitadas desde un único dispositivo que puede utilizar una cantidad ilimitada de usuarios. Puede plantearse utilizar la siguiente fórmula:

```
1 (Number of total users) - (number of users that only access
   exclusively
2 with shared devices) + (number shared devices) = total number
3 of licenses to buy.
4
5 For example, there are 1000 total users at the hospital. If 700 of them
   access only
6 Citrix Virtual Desktops from 300 shared devices in the hospital, the
   number of
7 licenses to purchase is 1000 - 700 + 300 = 600 licenses.
8 <!--NeedCopy-->
```

## En el modelo de usuario/dispositivo, ¿cuál es la cantidad máxima de dispositivos que un usuario con licencia puede usar para conectarse a mi entorno?

Cada usuario con licencia tiene derecho a utilizar una cantidad ilimitada de dispositivos con o sin conexión.

## En el modelo de usuario/dispositivo, ¿cuál es la cantidad máxima de usuarios que pueden acceder a un dispositivo con licencia?

Cada dispositivo con licencia puede acomodar una cantidad ilimitada de usuarios dentro de una organización.

## En el modelo de usuario/dispositivo, ¿cuál es la cantidad máxima de escritorios virtuales o aplicaciones web de Remote Browser Isolation (RBI) que un usuario con licencia puede utilizar en un momento dado?

Cada usuario con licencia puede conectarse a una cantidad ilimitada de escritorios virtuales o aplicaciones web.

## **¿Cuál es la cantidad máxima de aplicaciones virtuales que un usuario con licencia puede utilizar en un momento dado?**

Cada usuario con licencia puede conectarse a una cantidad ilimitada de aplicaciones virtuales.

## **¿Qué sucede si un usuario con licencia deja de trabajar para mi organización?**

Cuando un usuario con licencia deja de trabajar para la organización, se puede liberar la licencia de ese usuario sin tener que notificar a Citrix de ello. Use la utilidad `udadmin` para liberar la licencia. Si no libera la licencia, el Servidor de licencias libera automáticamente cualquier licencia que sume 90 días de inactividad. Esta información está sujeta a los términos especificados en el CLUF.

## **¿Qué sucede si un usuario con licencia está ausente durante un período prolongado?**

Si un usuario con licencia se ausenta durante un período prolongado, se puede liberar su licencia sin necesidad de notificar a Citrix. De este modo, la licencia está disponible para ser reasignada. Use la utilidad `udadmin` para liberar la licencia.

## **¿Qué sucede si reemplazamos un dispositivo con licencia en mi organización?**

Si reemplaza un dispositivo con licencia, se puede liberar su licencia sin necesidad de notificar a Citrix. De este modo, la licencia está disponible para ser reasignada. Use la utilidad `udadmin` para liberar la licencia.

## **¿Qué sucede si un dispositivo con licencia está fuera de servicio durante un período prolongado?**

Cuando un dispositivo con licencia está fuera de servicio durante un período prolongado, se puede liberar su licencia sin necesidad de notificar a Citrix. De este modo, la licencia está disponible para ser reasignada. Use la utilidad `udadmin` para liberar la licencia. Si no libera la licencia, el Servidor de licencias libera automáticamente cualquier licencia que sume 90 días de inactividad. Esta información está sujeta a los términos especificados en el CLUF.

## **¿Puedo cambiar las licencias de usuario a licencias de dispositivo y viceversa tras asignarlas?**

Sí. Este cambio ocurre automáticamente. El Servidor de licencias asigna licencias a usuarios o dispositivos en función del uso. Si los patrones de uso cambian, es posible que el Servidor de licencias

cambie la asignación en función del nuevo uso. El Servidor de licencias siempre asigna licencias de la manera más económica para el cliente. Además, el Servidor de licencias supervisa las licencias para identificar las licencias **no utilizadas** después de un período de asignación de 90 días. Puede reasignar las licencias identificadas como no utilizadas a otros usuarios o dispositivos después del período de asignación de 90 días.

**En el modelo de licencia simultánea, ¿cuál es la cantidad máxima de escritorios virtuales que un usuario con licencia de Citrix Virtual Apps and Desktops puede utilizar en un momento dado?**

Un dispositivo de punto final puede acomodar muchos usuarios y permite conexiones ilimitadas.

**¿Puedo adquirir licencias de Citrix Virtual Apps and Desktops para aumentar la cantidad de usuarios/dispositivos con licencia en mi entorno de Citrix Virtual Apps and Desktops?**

Sí. Puede adquirir licencias de Citrix Virtual Apps and Desktops para aumentar la cantidad de usuarios/dispositivos con licencia en su entorno de Citrix Virtual Apps and Desktops.

**¿Puedo implementar licencias simultáneas desde una versión anterior de Citrix Virtual Apps and Desktops y nuevas licencias de usuario/dispositivo o simultáneas en un único Servidor de licencias?**

Sí. Puede seguir usando el mismo Servidor de licencias para implementaciones con licencias simultáneas o de usuario/dispositivo.

**¿Puedo implementar licencias simultáneas y licencias de usuario/dispositivo en un único Servidor de licencias?**

Sí. Puede seguir usando el mismo Servidor de licencias para implementaciones con licencias simultáneas y de usuario/dispositivo.

**¿Puedo implementar varias ediciones de licencias de Citrix Virtual Apps and Desktops en un mismo Servidor de licencias?**

Sí. El Servidor de licencias administra simultáneamente las licencias para ambos Citrix Virtual Apps and Desktops. Le recomendamos que instale la versión más reciente del Servidor de licencias. Si no está seguro de si la versión del servidor de licencias que está utilizando es la más actualizada, verifíquelo comparando su versión con el número en el [sitio de descargas de Citrix](#).

## **¿Puede un solo sitio usar licencias de Citrix Virtual Apps y Citrix Virtual Apps and Desktops?**

Dependiendo de la versión, un único sitio de Citrix Virtual Apps o Citrix Virtual Apps and Desktops puede admitir ambos modelos de licencias: usuario/dispositivo o licencias simultáneas. Un único sitio de Citrix Virtual Apps o Citrix Virtual Apps and Desktops solo puede admitir una edición. Para obtener más información, consulte [Licencias de varios tipos](#).

Las versiones mínimas que admiten licencias de varios tipos son XenApp y XenDesktop 7.15 Long Term Service Release (LTSR) y Citrix Virtual Apps and Desktops 7 1808.

## **¿Puedo seleccionar licencias simultáneas de Citrix Virtual Apps como modelo de producto si tengo instaladas licencias simultáneas para Citrix Virtual Apps and Desktops o licencias de usuario/dispositivo para Citrix Virtual Apps and Desktops en el Servidor de licencias?**

Si utiliza Citrix Virtual Apps como una función de las ediciones Citrix Virtual Apps and Desktops Advanced o Premium, su modelo de licencia para Citrix Virtual Apps es el mismo que el de su edición Advanced o Premium de Citrix Virtual Apps and Desktops. Si ha adquirido Citrix Virtual Apps and Desktops, configure su sistema de licencias como Citrix Virtual Apps and Desktops, aunque tenga previsto utilizar únicamente la funcionalidad de Citrix Virtual Apps. Seleccione Citrix Virtual Apps como modelo de producto solo si tiene licencias independientes simultáneas de Citrix Virtual Apps instaladas en el Servidor de licencias.

## **Licencias de descubierto**

En esta sección se responden las preguntas acerca de las licencias de descubierto.

**¿Cómo obtener licencias de descubierto?** El descubierto de licencias está disponible para todas las licencias de usuario/dispositivo. Cuando adquiere licencias de usuario/dispositivo, recibe un descubierto de licencias del 10%. Ese descubierto pasa a estar disponible después de que asigne todas las licencias adquiridas y de evaluación. La función de descubierto se ofrece como una comodidad, no como un derecho de licencias. Si utiliza las licencias de descubierto con frecuencia, sería más conveniente adquirir más licencias.

**¿Cómo identificar un descubierto de licencias?** La información de uso, incluida la cantidad de licencias en descubierto, está disponible en Citrix Licensing Manager. Studio también contiene información sobre el uso de licencias de descubierto.

## **¿Qué ocurre cuando se utiliza una licencia de descubierto?**

Se asigna una licencia desde las licencias instaladas para permitir el acceso al entorno de Citrix Virtual

Apps and Desktops. Esa licencia de descubierta ofrece el mismo acceso y la misma funcionalidad que las demás licencias.

**¿Puedo recibir una alerta cuando se utilicen mis licencias de descubierta?**

Por el momento, no existen alertas concretas cuando se utilizan las licencias de descubierta.

**¿Durante cuánto tiempo puede utilizarse una licencia de descubierta?**

Debe adquirir las licencias de descubierta dentro de los 30 días siguientes al primer uso.

**¿Qué componentes de producto se incluyen en cada edición de Citrix Virtual Apps y Citrix Virtual Apps and Desktops?**

Para ver una tabla de funciones completa por edición, consulte [Funciones de Citrix Virtual Apps and Desktops](#).

**¿Qué licencias conceder a los entornos de Citrix Virtual Desktops para que cumplan las normas del contrato de licencia del usuario final de Citrix Virtual Apps and Desktops?**

Para implementar Citrix Virtual Apps and Desktops siguiendo el modelo de licencia de usuario/dispositivo o simultánea de modo que cumpla las normas del CLUF de Citrix Virtual Apps and Desktops, aplique los archivos de licencia al Servidor de licencias. A continuación, el Servidor de licencias controla y supervisa el cumplimiento de las licencias. Se recomienda configurar el producto en función de lo que se haya adquirido. Por ejemplo, si compra Citrix Virtual Apps and Desktops Premium pero solo quiere utilizar la función Citrix Virtual Apps, configure el producto en Citrix Virtual Apps and Desktops para cumplir las normas. Para obtener más información, consulte el [Centro de conformidad de las licencias de producto](#).

**¿Qué licencias conceder a los entornos de Citrix Virtual Apps para que cumplan las normas del contrato de licencia del usuario final de Citrix Virtual Apps?**

Para implementar Citrix Virtual Apps siguiendo el modelo de licencia simultánea de modo que cumpla las normas del CLUF de Citrix Virtual Apps, aplique los archivos de licencia al Servidor de licencias. A continuación, el Servidor de licencias controla y supervisa el cumplimiento de las licencias.

**¿Las ediciones Advanced y Premium de Citrix Virtual Apps and Desktops incluyen licencias simultáneas de Citrix Virtual Apps?**

Las licencias de usuario/dispositivo de Citrix Virtual Apps and Desktops Advanced y Premium incluyen licencias simultáneas de Citrix Virtual Apps solamente por motivos de compatibilidad. Estas licencias simultáneas solo deben usarse con versiones anteriores de producto que no sean compatibles con las

licencias de usuario/dispositivo. El uso de las licencias simultáneas de compatibilidad incluidas con las licencias de usuario/dispositivo solo está permitido con las versiones de XenApp anteriores a 6.5 y las versiones de XenDesktop anteriores a 5.0 Service Pack 1.

## ¿Cómo puedo obtener mi archivo de licencia?

Se le envía el código de acceso a la licencia por correo electrónico. Existen tres maneras de generar archivos de licencia mediante el código de acceso a la licencia:

- Se utiliza la caja de herramientas Manage Licenses (Administrar licencias) disponible desde la página My Account (Mi cuenta) en citrix.com
- Se utiliza Citrix Studio para asignar la compra y el archivo de licencia se instala automáticamente en Citrix License Server.
- Se utiliza Citrix Licensing Manager, incluido en Citrix License Server, para asignar la compra e instalar el archivo de licencias.

Para obtener más información, consulte [Licensing](#) en la documentación de Citrix Licensing y [Licencias](#) en la documentación de Citrix Virtual Apps and Desktops.

## ¿Qué puertos TCP utilizan las licencias de Citrix?

- El número de puerto del Servidor de licencias es 27000
- El número de puerto del demonio de proveedor es 7279
- El número de puerto web de la consola de administración es 8082
- El puerto de Web Services for Licensing es 8083

## ¿Qué es Citrix License Server?

Citrix License Server es un sistema que permite compartir licencias por toda la red. Para obtener más información, consulte [Descripción general de las operaciones de licencia](#).

## ¿Puedo virtualizar o agrupar Citrix License Server en clústeres?

Sí. Puede virtualizar o agrupar Citrix License Server en clústeres. Para obtener más información, consulte [Servidores de licencias agrupados en clústeres](#).

## ¿Qué ventajas obtengo si virtualizo Citrix License Server?

La virtualización de Citrix License Server ofrece una solución de redundancia. Esta solución permite la movilidad entre varios servidores físicos sin que haya tiempo de inactividad.

## ¿Hay alguna limitación a tener en cuenta si virtualizo Citrix License Server?

No.

## ¿Citrix License Server administra todas las licencias de mi implementación de Citrix Virtual Apps and Desktops?

Citrix License Server administra todas las licencias que se reciban para Citrix Virtual Apps and Desktops, excepto las licencias de la edición Premium utilizadas con Citrix Gateway. Los Servidores de licencias integrados en los dispositivos de red como sea necesario para esos dispositivos de red orientados a la seguridad administran esas licencias.

## ¿Qué es Citrix Licensing Manager?

Citrix Licensing Manager habilita la descarga y asignación de archivos de licencias desde el Servidor de licencias donde se ha instalado Citrix Licensing Manager. Citrix Licensing Manager es el método de administración recomendado del Servidor de licencias, que permite lo siguiente:

- Registrar el código corto del servidor de licencias en Citrix Cloud y quitar fácilmente el registro.
- Configurar cuentas de usuario y grupo.
- Utilice el panel de mandos para mostrar las licencias instaladas, las que se están utilizando, las vencidas y las disponibles, así como las fechas de Customer Success Services.
- Exportar datos de uso de licencias para usarlos en informes.
- Configurar el período de retención de datos de uso histórico. El período predeterminado para la retención de datos es 180 días.
- Instalación simplificada de archivos de licencias en el servidor de licencias mediante un código de acceso de licencias o un archivo descargado.
- Habilitar e inhabilitar el período de gracia complementario.
- Configurar el programa Customer Experience Improvement Program (CEIP) y Call Home.
- Comprueba manual o automáticamente las licencias de renovación de Customer Success Services y le notifica o instala las licencias si las encuentra.
- Notifica acerca del estado del Servidor de licencias: si falta una licencia inicial, si hay problemas de hora, fallos de carga, etc.
- Modificar estos puertos:
  - Servidor de licencias (predeterminado: 27000)
  - Demonio de proveedor (predeterminado: 7279)
  - Web Services For Licensing (predeterminado: 8083)

Para obtener más información, consulte [Citrix Licensing Manager](#).

## ¿Qué es Citrix License Administration Console?

License Administration Console es una interfaz que permite administrar las licencias para la infraestructura de Citrix. La consola también permite configurar el servidor de licencias y ver el uso de las licencias en un momento dado.

Puede usar Studio para administrar y realizar un seguimiento de las licencias, siempre y cuando el Servidor de licencias esté en el mismo dominio que Studio o en un dominio de confianza.

Para obtener más información, consulte [License Administration Console](#).

## ¿Cuál es el período de asignación de una licencia?

El período de asignación de una licencia es el tiempo que una licencia de Citrix Virtual Apps and Desktops se asigna a un usuario o dispositivo. El período de asignación de licencia predeterminado es de 90 días.

## ¿Cómo libero una licencia de usuario/dispositivo autorizada?

Para liberar la asignación de una licencia de usuario/dispositivo autorizada, utilice la utilidad `udadmin` de acuerdo con las condiciones del CLUF. A continuación, el Servidor de licencias asigna la licencia al siguiente usuario/dispositivo apropiado.

## ¿Cómo sé cuántas licencias ha adquirido mi organización?

Puede ver todas las licencias compradas y acceder a ellas en cualquier momento (las 24 horas del día, los 7 días de la semana) desde su caja de herramientas segura **Manage Licenses** (Administrar licencias) en su página **My Account** (Mi cuenta) en <https://www.citrix.com>.

## ¿Cómo sé cuántas licencias están en uso en un momento dado?

Citrix Licensing Manager, License Administration Console y Studio ofrecen datos sobre el uso de licencias en tiempo real.

## ¿Qué sucede si supero la cantidad de licencias de usuario/dispositivo compradas?

Las licencias de usuario/dispositivo incluyen un 10% de descubierto, que se incluye cuando se generan licencias. El descubierto también se incluye en el recuento de licencias instaladas. Si el pico de uso supera el recuento instalado, incluido el descubierto, se deniega el acceso a más usuarios. Deberá adquirir e implementar una nueva licencia para permitir el acceso a más usuarios.

Cuando todas las licencias están en uso, incluidas las licencias en descubierto, el período de gracia complementario posibilita un número ilimitado de conexiones a un producto. El período de gracia complementario le proporciona tiempo para determinar por qué ha superado la cantidad máxima de licencias y comprar otras licencias sin interrumpir el trabajo de los usuarios. Este período dura 15 días como máximo o hasta que instale más licencias Retail, lo que ocurra antes. Para obtener más información, consulte [Período de gracia complementario](#).

Director muestra los estados del período de gracia. Para obtener más información, consulte [Paneles del panel de mandos de Director](#).

### **¿Qué sucede si supero la cantidad de licencias simultáneas compradas?**

Cuando todas las licencias están en uso, el período de gracia complementario posibilita un número ilimitado de conexiones a un producto. El período de gracia complementario le proporciona tiempo para determinar por qué ha superado la cantidad máxima de licencias y comprar otras licencias sin interrumpir el trabajo de los usuarios. Este período dura 15 días como máximo o hasta que instale más licencias Retail, lo que ocurra antes. Para obtener más información, consulte [Período de gracia complementario](#).

Director muestra los estados del período de gracia. Para obtener más información, consulte [Paneles del panel de mandos de Director](#).

### **¿Existe algún requisito de licencia para las opciones de servicio de Citrix Virtual Apps and Desktops: Long Term Service Release (LTSR) o Current Release (CR)?**

Las opciones de servicio de Citrix Virtual Apps and Desktops, como Long Term Service Release, son una ventaja del programa Customer Success Services. Debe tener activo Customer Success Services para poder beneficiarse de LTSR. Para obtener más información, consulte [Citrix Virtual Apps, Citrix Virtual Apps and Desktops y las opciones de servicio de Citrix Hypervisor](#).

### **¿Cómo funcionan las horas agrupadas de RBI Service?**

Cuando compra un mínimo de 25 usuarios del servicio, recibe 5000 horas de derechos para usar el servicio, agrupados para todos los usuarios. Las compras posteriores de los derechos de usuario no aumentan el derecho a horas agrupadas. Para aumentar el derecho a horas de servicio, compre paquetes complementarios.

## Mantenimiento y recuperación ante desastres del servidor de licencias

Para obtener información acerca de la recuperación ante desastres y el mantenimiento de su Servidor de licencias, consulte [Mantenimiento y recuperación ante desastres](#) en la documentación de Citrix Licensing.

## ¿Puedo usar acceso con Remote PC con licencias CCU?

Sí.

Para obtener información, consulte [Acceso con Remote PC](#).

## Preguntas frecuentes e información sobre licencias específicas de productos

- [Citrix ADC](#)
- [Citrix Cloud](#)
- [Citrix Endpoint Management](#)
- [Citrix Gateway](#)
- [Citrix Hypervisor](#)

## Aplicaciones

April 19, 2024

### Introducción

Si su implementación usa solo grupos de entrega (y no grupos de aplicaciones), tiene que agregar aplicaciones a los grupos de entrega. Si también tiene grupos de aplicaciones, por lo general, debe agregar aplicaciones a los grupos de aplicaciones. Esta recomendación facilita la administración. Una aplicación siempre debe pertenecer al menos a un grupo de entrega o un grupo de aplicaciones.

En el asistente para agregar aplicaciones, seleccione uno o varios grupos de entrega, o uno o más grupos de aplicaciones, pero no ambos. Aunque puede cambiar posteriormente la asociación de una aplicación a un grupo (por ejemplo, puede mover la aplicación desde un grupo de aplicaciones a un grupo de entrega), se recomienda no hacerlo para no incrementar la complejidad. Mantenga sus aplicaciones en un tipo de grupo.

Al asociar una aplicación a más de un grupo de entrega o más de un grupo de aplicaciones, puede producirse un problema de visibilidad si no dispone de permisos suficientes para ver la aplicación en

todos esos grupos. En tales casos, consulte a un administrador con más permisos o haga que amplíen su ámbito para incluir todos los grupos a los que se haya agregado la aplicación.

Si publica dos aplicaciones con el mismo nombre (quizá desde distintos grupos) para los mismos usuarios, cambie la propiedad Nombre de la aplicación (para el usuario) en Studio; de lo contrario, los usuarios verán nombres duplicados en la aplicación Citrix Workspace.

Puede cambiar las propiedades de una aplicación (parámetros) al agregarla, o más tarde. También puede cambiar la carpeta de la aplicación donde está colocada la aplicación, ya sea al agregarla, o más tarde.

Para obtener más detalles, consulte:

- [Crear grupos de entrega](#)
- [Crear grupos de aplicaciones](#)
- [Etiquetas](#)

## Agregar aplicaciones

Puede agregar aplicaciones al crear un grupo de entrega o un grupo de aplicaciones; los procedimientos correspondientes se describen en los artículos [Crear grupos de entrega](#) y [Crear grupos de aplicaciones](#). El procedimiento siguiente describe cómo agregar aplicaciones después de crear un grupo.

Información útil:

- No se pueden agregar aplicaciones a grupos de entrega de acceso con Remote PC.
- El asistente para agregar aplicaciones no puede usarse para quitar aplicaciones de los grupos de entrega o de los grupos de aplicaciones. Se trata de dos operaciones diferentes.

Para agregar una o varias aplicaciones:

1. Seleccione **Aplicaciones** en el panel de navegación de Studio y, a continuación, seleccione **Agregar aplicaciones** en el panel Acciones.
2. El asistente para agregar aplicaciones se inicia con la página **Introducción**, que se puede eliminar de futuros inicios de este asistente.
3. El asistente le guiará a través de las páginas Grupos, Aplicaciones y Resumen, que se describen a continuación. Cuando haya terminado con cada página, haga clic en **Siguiente** hasta llegar a la página Resumen.

Como alternativa al paso 1 si quiere agregar aplicaciones a un grupo de entrega o un grupo de aplicaciones:

- Para agregar aplicaciones a un solo grupo de entrega, en el paso 1, seleccione **Grupos de entrega** en el panel de navegación de Studio y, a continuación, seleccione un grupo de entrega

en el panel central y, a continuación, seleccione **Agregar aplicaciones** en el panel Acciones. El asistente no mostrará la página **Grupos**.

- Para agregar aplicaciones a un solo grupo de aplicaciones, en el paso 1, seleccione **Aplicaciones** en el panel de navegación de Studio y, a continuación, seleccione un **Grupo de aplicaciones** en el panel central y, a continuación, seleccione la entrada **Agregar aplicaciones** bajo el nombre del grupo de aplicaciones en el panel Acciones. El asistente no mostrará la página **Grupos**.

## Grupos

Esta página contiene una lista de todos los grupos de entrega en el sitio. Si también se han creado grupos de aplicaciones, la página muestra la lista de grupos de aplicaciones y grupos de entrega. Puede elegir de cada grupo, pero no de ambos grupos. En otras palabras, no se pueden agregar aplicaciones a un grupo de aplicaciones y a un grupo de entrega a la vez. Por lo general, si está utilizando grupos de aplicaciones, las aplicaciones deben agregarse a grupos de aplicaciones en lugar de grupos de entrega.

Al agregar una aplicación, se debe marcar la casilla de verificación junto a un grupo de entrega o un grupo de aplicaciones (si están disponibles) como mínimo, porque cada aplicación siempre debe estar asociada con, al menos, un grupo.

## Aplicaciones

Haga clic en la lista desplegable **Agregar** para ver los orígenes de aplicación.

- **Desde el menú Inicio:** Se trata de las aplicaciones que se detectan en una máquina de los grupos de entrega seleccionados. Cuando se selecciona este origen, se abre una nueva página con una lista de aplicaciones detectadas. Marque las casillas de verificación de las aplicaciones que quiere agregar y, a continuación, haga clic en **Aceptar**.

Este origen no se puede seleccionar si usted (1) seleccionó grupos de aplicaciones que no tienen grupos de entrega asociados, (2) seleccionó grupos de aplicaciones con grupos de entrega asociados que no contienen máquinas, o (3) seleccionó un grupo de entrega que no contiene máquinas.

- **Definidas manualmente:** Se trata de las aplicaciones que se encuentran en el sitio o en la red. Cuando se selecciona este origen, se abre una nueva página donde se escribe la ruta al archivo ejecutable, al directorio de trabajo, los argumentos de línea de comandos opcionales y los nombres simplificados para administradores y usuarios. Después de introducir la información, haga clic en Aceptar.
- **Existentes:** Se trata de aplicaciones agregadas anteriormente al sitio. Cuando se selecciona este origen, se abre una nueva página con una lista de aplicaciones detectadas. Marque las

casillas de verificación de las aplicaciones que quiere agregar y, a continuación, haga clic en **Aceptar**.

Este origen no se puede seleccionar si el sitio no contiene ninguna aplicación.

- **App-V:** Se trata de las aplicaciones presentes en paquetes de App-V. Cuando se selecciona este origen, se abre una nueva página donde se puede seleccionar el servidor de App-V o la biblioteca de aplicaciones. En la pantalla resultante, marque las casillas de las aplicaciones que quiere agregar y, a continuación, haga clic en **Aceptar**. Para obtener más información, consulte el artículo de App-V.

Este origen no se puede seleccionar si App-V no está configurado en el sitio.

- **Grupo de aplicaciones:** Grupos de aplicaciones. Cuando se selecciona este origen, se abre una nueva página con una lista de Grupos de aplicaciones. (Aunque la pantalla también lista las aplicaciones de cada grupo, solo se puede seleccionar el grupo, no las aplicaciones individualmente). Se agregarán las aplicaciones actuales del grupo y las que se agreguen a él en el futuro. Marque las casillas de los grupos de aplicaciones que quiere agregar y, a continuación, haga clic en **Aceptar**.

Este origen no se puede seleccionar si (1) no hay grupos de aplicaciones o (2) si los grupos de entrega seleccionados no admiten grupos de aplicaciones (por ejemplo, los grupos de entrega contienen máquinas de asignación estática).

Como se indica en la tabla, algunas de las entradas de la lista desplegable Agregar no se pueden seleccionar si no existe ningún origen válido de ese tipo. Los orígenes que no son compatibles (por ejemplo, no se puede agregar grupos de aplicaciones a otros grupos de aplicaciones) no se incluyen en la lista desplegable. Las aplicaciones que ya se han agregado a los grupos que eligió no se podrán seleccionar de nuevo.

Para agregar una aplicación desde un AppDisk asignado, seleccione **Desde el menú Inicio**. Si la aplicación no está disponible allí, seleccione **Definidas manualmente** y facilite los datos pertinentes. Si se produce un error de acceso a la carpeta, configúrela como **compartida** y vuelva a agregar la aplicación a través de la opción **Definidas manualmente**.

Puede cambiar las propiedades de una aplicación (parámetros) en esta página, o más tarde.

De forma predeterminada, las aplicaciones que agregue se colocan en una carpeta denominada **Applications**. Puede cambiar la aplicación desde esta página, o más tarde. Si intenta agregar una aplicación y ya existe una con el mismo nombre en la misma carpeta, se le pedirá cambiar el nombre de la aplicación que está agregando. Puede aceptar el nuevo nombre sugerido, o rechazarlo y darle otro nombre, o seleccionar una carpeta diferente. Por ejemplo, si **app** ya existe en la carpeta **Applications** y se intenta agregar otra aplicación denominada también **app** a esa carpeta, se le sugerirá el nombre **app\_1**.

## Resumen

Si agrega como máximo 10 aplicaciones, sus nombres aparecerán en la lista **Aplicaciones para agregar**. Si agrega más de 10 aplicaciones, se indica la cantidad total.

Revise la información de resumen y, a continuación, haga clic en **Finalizar**.

## Cambiar la asociación de una aplicación a un grupo

Después de agregar una aplicación, puede cambiar los grupos de entrega y los grupos de aplicaciones con los que la aplicación está asociada.

Puede arrastrar y colocar para asociar una aplicación con un grupo adicional. Esta es una alternativa al uso de comandos en el panel Acciones.

Si una aplicación está asociada a más de un grupo de entrega o más de un grupo de aplicaciones, se puede usar la prioridad de grupos para especificar el orden en que se comprueban los grupos para encontrar las aplicaciones. De forma predeterminada, todos los grupos tienen prioridad 0 (la máxima prioridad). Si los grupos tienen la misma prioridad, se les aplica el equilibrio de carga.

Una aplicación se puede asociar a grupos de entrega que contengan máquinas compartidas (no privadas) que puedan entregar aplicaciones. También puede seleccionar grupos de entrega con máquinas compartidas que entreguen solo escritorios si 1) el grupo de entrega contiene máquinas compartidas y se creó con una versión de XenDesktop 7.x anterior a 7.9 y 2) usted tiene el permiso Modificar grupo de entrega. El tipo de grupo de entrega se convierte automáticamente a “escritorios y aplicaciones” cuando se confirma la selección en el diálogo de propiedades.

1. Seleccione **Aplicaciones** en el panel de navegación de Studio y, a continuación, seleccione la aplicación en el panel central.
2. Seleccione **Propiedades** en el panel Acciones.
3. Seleccione la página **Grupos**.
4. Para agregar un grupo, haga clic en la lista desplegable **Agregar** y seleccione **Grupos de aplicaciones** o **Grupos de entrega**. (Si aún no ha creado ningún grupo de aplicaciones, la única entrada que verá será Grupos de entrega.) A continuación, seleccione uno o varios grupos disponibles. Los grupos que no son compatibles con la aplicación, o que ya están asociados a ella, no se pueden seleccionar.
5. Para quitar un grupo, seleccione uno o varios grupos y, a continuación, haga clic en **Quitar**. Si al quitar la asociación de grupo la aplicación ya no estará asociada a ningún grupo de aplicaciones o grupo de entrega, se le alertará de que la aplicación será eliminada.
6. Para cambiar la prioridad de un grupo, seleccione el grupo y, a continuación, haga clic en **Modificar prioridad**. Seleccione un valor de prioridad y, a continuación, haga clic en **Aceptar**.
7. Cuando haya terminado, haga clic en **Aplicar** para aplicar los cambios y dejar abierta la ventana, o haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

## Duplicar, habilitar o inhabilitar, cambiar de nombre o eliminar una aplicación

Las siguientes acciones están disponibles:

- **Duplicar:** Puede que necesite duplicar una aplicación para crear otra versión de esta con parámetros o propiedades diferentes. Cuando se duplica una aplicación, se le cambia el nombre de manera automática con un sufijo único y se coloca junto a la original. También puede que le convenga duplicar una aplicación para agregarla a un grupo distinto (Después de la duplicación, el modo más sencillo de mover una aplicación es arrastrarla y colocarla en otro grupo.)
- **Habilitar o inhabilitar:** La habilitación o inhabilitación de una aplicación son acciones diferentes de habilitar o inhabilitar un grupo de entrega o un grupo de aplicaciones.
- **Cambio de nombre:** Solo se puede cambiar el nombre de una aplicación a la vez. Si intenta agregar una aplicación y ya existe una con el mismo nombre en la misma carpeta o el mismo grupo, se le pedirá que especifique un nombre diferente.
- **Eliminar:** Al eliminar una aplicación, se la quita de los grupos de aplicaciones o grupos de entrega con los que estaba asociada, pero no del origen que se utilizó para agregarla originalmente. Eliminar una aplicación es una acción diferente de quitarla de un grupo de entrega o un grupo de aplicaciones.

Para duplicar, habilitar, inhabilitar, cambiar de nombre o eliminar una aplicación:

1. Seleccione **Aplicaciones** en el panel de navegación de Studio.
2. Seleccione una o más aplicaciones en el panel central y, a continuación, seleccione la tarea correspondiente en el panel Acciones.
3. Confirme la acción, cuando se le solicite.

## Quitar aplicaciones de un grupo de entrega

La aplicación debe estar asociada (pertenecer) a al menos un grupo de entrega o un grupo de aplicaciones. Si intenta quitar una aplicación de un grupo de entrega y con ello la aplicación ya no estaría asociada con ningún grupo de entrega o grupo de aplicaciones, se le notificará que la aplicación será eliminada si decide continuar. En estos casos, si quiere poder entregar la aplicación, debe volver a agregarla desde un origen válido.

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo de entrega. En el panel inferior central, seleccione la ficha **Aplicaciones** y, a continuación, la aplicación que quiere quitar.
3. Seleccione **Quitar aplicación** en el panel Acciones.
4. Confirme la eliminación.

## Quitar aplicaciones de un grupo de aplicaciones

Una aplicación debe pertenecer al menos a un grupo de entrega o a un grupo de aplicaciones. Si intenta quitar una aplicación de un grupo de aplicaciones y con ello la aplicación ya no pertenecería a ningún grupo de entrega o grupo de aplicaciones, se le notificará que la aplicación será eliminada si decide continuar. En estos casos, si quiere poder entregar la aplicación, debe volver a agregarla desde un origen válido.

1. Seleccione **Aplicaciones** en el panel de navegación de Studio.
2. Seleccione el grupo de aplicaciones en el panel central y, a continuación, seleccione una o más aplicaciones en el panel central.
3. Seleccione **Quitar del grupo de aplicaciones** en el panel Acciones.
4. Confirme la eliminación.

## Cambiar las propiedades de la aplicación

Solo se pueden cambiar las propiedades de una aplicación a la vez.

Para cambiar las propiedades de una aplicación:

1. Seleccione **Aplicaciones** en el panel de navegación de Studio.
2. Seleccione una aplicación y, a continuación, seleccione **Modificar propiedades de aplicación** en el panel Acciones.
3. Seleccione la página que contiene la propiedad que quiere cambiar.
4. Cuando haya terminado, haga clic en **Aplicar** para aplicar los cambios que haya realizado y dejar la ventana abierta, o bien haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

En la siguiente lista, la página se indica entre paréntesis.

---

Propiedad	Página
Categoría/carpeta donde aparece la aplicación en la aplicación Citrix Workspace	Entrega
Argumentos de línea de comandos; consulte Transferir parámetros a aplicaciones publicadas	Ubicación
Grupos de entrega y grupos de aplicaciones donde la aplicación está disponible	Grupos
Descripción	Identificación
Extensiones de archivo y asociación de tipos de archivo: qué extensiones abre automáticamente la aplicación	Asociación de tipos de archivos

---

Propiedad	Página
Icono	Entrega
Palabras clave para StoreFront	Identificación
Límites: consulte Configurar límites para aplicaciones	Entrega
Nombre: los nombres que ven el usuario y el administrador	Identificación
Ruta al archivo ejecutable; consulte Transferir parámetros a aplicaciones publicadas	Ubicación
Acceso directo en el escritorio de usuario: habilitarlo o inhabilitarlo	Entrega
Visibilidad: limita qué usuarios pueden ver la aplicación en la aplicación Citrix Workspace (aunque una aplicación sea invisible, se la puede iniciar; para que además de no estar visible, tampoco esté disponible, agréguela a otro grupo)	Limitar visibilidad
Directorio de trabajo	Ubicación

---

Es posible que los cambios en las aplicaciones no se efectúen de cara a los usuarios actuales de las aplicaciones hasta que cierren sus sesiones.

### **Configurar límites para aplicaciones**

Configurar límites para aplicaciones puede ayudarle a administrar el uso de esas aplicaciones. Por ejemplo, puede usar límites para aplicaciones si quiere controlar la cantidad de usuarios que acceden a una aplicación de forma simultánea. Del mismo modo, los límites para aplicaciones se pueden usar con el fin de controlar la cantidad de instancias simultáneas de aplicaciones que consumen muchos recursos, lo que puede ayudar a mantener el rendimiento del servidor y evitar el deterioro del servicio.

Esta función limita la cantidad de inicios de aplicaciones que usan como intermediario el Controller (por ejemplo, desde la aplicación Citrix Workspace y StoreFront), no la cantidad de aplicaciones en ejecución que se inician mediante otros métodos. Esto significa que los límites para aplicaciones ayudan a los administradores a la hora de administrar el uso simultáneo, pero no se aplican en todos los casos. Por ejemplo, no se pueden aplicar límites para aplicaciones cuando el Controller está en modo de conexión por concesión.

De forma predeterminada, no hay ningún límite en la cantidad de instancias de aplicación que pueden ejecutarse al mismo tiempo. Existen varias configuraciones de límite para las aplicaciones. Puede definir una o todas:

- La cantidad máxima de instancias simultáneas de una aplicación que hayan iniciado todos los usuarios del grupo de entrega.
- Una instancia de aplicación por usuario en el grupo de entrega.
- La cantidad máxima de instancias simultáneas de una aplicación por cada máquina (solo PowerShell).

Si se define un límite, se generará un mensaje de error cuando un usuario intente iniciar una aplicación más veces que el número del límite configurado. Si se configura más de un límite, se informa un error cuando se alcanza el primer límite.

Ejemplos de uso de los límites para aplicaciones:

- **Límite para la cantidad máxima de instancias simultáneas:** En un grupo de entrega, se configura la cantidad máxima de 15 instancias simultáneas de la aplicación Alfa. Posteriormente, los usuarios de ese grupo de entrega tienen 15 instancias de esa aplicación que se ejecutan al mismo tiempo. Si un usuario de ese grupo de entrega intenta iniciar Alfa, se generará un mensaje de error y Alfa no se iniciará porque eso superaría el límite de instancias simultáneas de aplicación (15).
- **Límite para una instancia de aplicación por usuario:** En otro grupo de entrega, se habilita la opción de una instancia por usuario para la aplicación Beta. El usuario Marcos inicia correctamente la aplicación Beta. Más tarde en la misma jornada, mientras esa aplicación se sigue ejecutando en la sesión de Marcos, este intenta iniciar otra instancia de Beta. Se generará un mensaje de error y Beta no se iniciará porque eso superaría el límite de una instancia por usuario.
- **Límites de cantidad máxima de instancias simultáneas y una instancia de aplicación por usuario:** En otro grupo de entrega, se configura una cantidad máxima de 10 instancias simultáneas y se habilita la opción de una instancia por usuario de la aplicación Delta. Posteriormente, cuando diez usuarios de ese grupo de entrega tienen cada uno una instancia de Delta en ejecución, si otro usuario de ese grupo intenta iniciar Delta, recibirá un mensaje de error y Delta no se iniciará. Si alguno de los diez usuarios actuales intenta iniciar una segunda instancia de esa aplicación, recibirá un mensaje de error y la segunda instancia no se iniciará.
- **Cantidad máxima de instancias simultáneas por máquina y con restricciones de etiqueta:** La aplicación A tiene requisitos de licencia y rendimiento que estipulan cuántas instancias se pueden ejecutar al mismo tiempo en un servidor específico, así como cuántas instancias pueden ejecutarse simultáneamente en todos los servidores del sitio.

El límite de instancias de aplicación por máquina afecta a todos los servidores del sitio (no solo a las máquinas en un grupo de entrega en particular). Supongamos que su sitio contiene tres

servidores. Para la aplicación A, se configura el límite de 2 instancias de aplicación por máquina. Por lo tanto, no se permitirá el inicio de más de seis instancias de aplicación en todo el sitio. (Este es el límite de dos instancias de A en cada uno de los tres servidores.)

Para restringir el uso de una aplicación a solo ciertas máquinas dentro de un grupo de entrega (además de limitar las instancias en todas las máquinas en todo el sitio), use la función de etiquetado para esas máquinas y configure el límite de cantidad máxima de instancias por máquina para esa aplicación.

Si también se inician instancias de aplicación sin Controller como broker (por ejemplo, durante la interrupción de servicios de un Controller) y se superan los límites configurados, los usuarios no podrán iniciar más instancias hasta que cierren las instancias necesarias para dejar de superar el límite. No se forzará el cierre de las instancias que superen el límite, sino que se seguirán ejecutando hasta que el usuario las cierre.

Si inhabilita la movilidad de sesión, inhabilite también el límite de una instancia de aplicación por usuario. Si habilita el límite de una instancia de aplicación por usuario, no configure uno de los dos valores que permiten sesiones nuevas en dispositivos nuevos. Para obtener información acerca de la movilidad, consulte el artículo Sesiones.

Para configurar el límite de instancias máximas por grupo de entrega y el límite de una instancia por usuario:

1. Seleccione **Aplicaciones** en el panel de navegación de Studio y, a continuación, seleccione una aplicación.
2. Seleccione **Modificar propiedades de aplicación** en el panel Acciones.
3. En la página **Entrega**, seleccione una de las siguientes opciones.
  - Permitir el uso ilimitado de la aplicación. No hay límite para la cantidad de instancias ejecutadas a la vez. Esta es la opción predeterminada.
  - Establecer límites para la aplicación. Hay dos tipos de límite; especifique uno o ambos.
    - Especifique la cantidad máxima de instancias que pueden ejecutarse simultáneamente.
    - Ponga el límite de una instancia de aplicación por usuario.
4. Haga clic en **Aceptar** para aplicar el cambio y cierre el cuadro de diálogo, o pinche en **Aplicar** para aplicar el cambio y deje abierto el cuadro de diálogo.

Para configurar el límite de instancias máximas por máquina (solo PowerShell):

- En PowerShell (mediante el SDK de PowerShell remoto para implementaciones de Citrix Cloud o el SDK de PowerShell para implementaciones locales), indique el cmdlet `BrokerApplication` apropiado con el parámetro `MaxPerMachineInstances`.

- Para obtener ayuda, utilice el cmdlet `Get-Help`. Por ejemplo:

```
Get-Help Set-BrokerApplication -Parameter MaxPerMachineInstances
```

## Transferir parámetros a aplicaciones publicadas

Utilice la página **Ubicación** de las propiedades de la aplicación para introducir la línea de comandos y transferir los parámetros a las aplicaciones publicadas.

Al asociar una aplicación publicada con tipos de archivos, los símbolos “%\*” (porcentaje y asterisco entre comillas) se agregan al final de la línea de comandos de la aplicación. Estos símbolos actúan como marcadores de posición para los parámetros transferidos a los dispositivos de usuario.

Si una aplicación publicada no se inicia cuando se espera, verifique que la línea de comandos contiene los símbolos correctos. De forma predeterminada, los parámetros proporcionados por los dispositivos de usuario se validan si se agregan los símbolos “%\*”. Para las aplicaciones publicadas que utilizan parámetros personalizados suministrados por el dispositivo de usuario, se agregan los símbolos “%\*” a la línea de comandos para omitir la validación de la línea de comandos. Si los símbolos no aparecen en la línea de comandos de la aplicación, agréguelos manualmente.

Si la ruta del archivo ejecutable contiene nombres de directorios con espacios (como `C:\Program Files`), escriba la línea de comandos de la aplicación entre comillas para indicar que los espacios pertenecen a la línea de comandos. Para ello, agregue dobles comillas al principio y al final de la ruta. Asimismo, deberá agregar otro conjunto de comillas dobles al principio y al final de los símbolos %\*. Incluya un espacio entre la comilla de cierre de la ruta y la de apertura de los símbolos %\*.

Por ejemplo, la línea de comandos de la aplicación publicada Reproductor de Windows Media es:

```
“C:\Program Files\Windows Media Player\mplayer1.exe” “%*”
```

## Administrar carpetas de aplicaciones

De forma predeterminada, las aplicaciones nuevas que se agreguen a los grupos de entrega se colocan en una carpeta denominada **Aplicaciones**. Puede indicar una carpeta distinta cuando cree el grupo de entrega, cuando agregue una aplicación o más tarde.

Información útil:

- No se puede eliminar o cambiar el nombre a la carpeta Aplicaciones, pero puede mover todas las aplicaciones que contiene a otras carpetas que cree.
- El nombre de las carpetas puede contener entre 1 y 64 caracteres. Se permiten los espacios en blanco.
- Las carpetas se pueden anidar en hasta cinco niveles.
- Las carpetas no tienen que contener aplicaciones: pueden ser carpetas vacías.

- En Studio, las carpetas se incluyen en una lista alfabética a menos que las mueva o especifique otra ubicación al crearlas.
- Puede tener más de una carpeta con el mismo nombre, siempre y cuando cada una tenga otra carpeta principal. Del mismo modo, puede tener más de una aplicación con el mismo nombre, siempre y cuando cada una esté en una carpeta diferente.
- Para poder ver las aplicaciones en las carpetas, debe tener el permiso de Ver aplicaciones. Para quitar, cambiar el nombre o eliminar una carpeta que contenga aplicaciones, debe tener el permiso de Modificar propiedades de aplicación para todas las aplicaciones que contenga dicha carpeta.
- La mayoría de los procedimientos siguientes requieren acciones mediante el panel Acciones de Studio. También puede utilizar los menús contextuales o arrastrar y colocar. Por ejemplo, si crea o mueve por error una carpeta a una ubicación, la puede arrastrar y colocar en la ubicación correcta.

Para administrar las carpetas de aplicaciones, seleccione **Aplicaciones** en el panel de navegación de Studio. Utilice la siguiente lista como guía.

- **Para ver todas las carpetas (también las anidadas):** haga clic en **Mostrar todo**, situado sobre la lista de carpetas.
- **Para crear una carpeta en el nivel más alto (no anidada):** Seleccione la carpeta Aplicaciones. Para colocar la nueva carpeta en una carpeta existente distinta de Aplicaciones, seleccione esa carpeta. A continuación, seleccione **Crear carpeta** en el panel Acciones. Escriba un nombre.
- **Para cambiar una carpeta:** Seleccione esa carpeta y, a continuación, seleccione **Mover carpeta** en el panel Acciones. Solo puede mover una carpeta a la vez, a menos que la carpeta que quiere mover contenga carpetas anidadas (La forma más fácil de mover una carpeta es arrastrarla y colocarla en el sitio correspondiente.)
- **Para cambiar el nombre de una carpeta:** Seleccione esa carpeta y, a continuación, seleccione **Cambiar nombre de carpeta** en el panel Acciones. Escriba un nombre.
- **Para eliminar una carpeta:** Seleccione esa carpeta y, a continuación, seleccione **Eliminar carpeta** en el panel Acciones. Si elimina una carpeta que contiene aplicaciones y otras carpetas, esos objetos también se eliminarán. Cuando se elimina una aplicación, se quita la asignación de la misma del grupo de entrega; no se quita la aplicación de la máquina.
- **Para mover aplicaciones a una carpeta:** Seleccione una o varias aplicaciones. A continuación, seleccione **Mover aplicación** en el panel Acciones. Seleccione la carpeta.

También puede colocar las aplicaciones en una carpeta específica (incluso una nueva) en la página **Aplicación** de los asistentes Crear grupo de entrega y Crear grupo de aplicaciones. De forma predefinida, las aplicaciones agregadas se colocan en la carpeta **Aplicaciones**, haga clic en **Cambiar** para seleccionar o crear una carpeta.

## Controlar el inicio local de aplicaciones en escritorios publicados

Cuando los usuarios inician una aplicación publicada desde un escritorio publicado, puede controlar si la aplicación se inicia en esa sesión de escritorio o como una aplicación publicada. La aplicación Citrix Workspace busca la ruta de instalación de la aplicación en el Registro de Windows del VDA y, si está presente, inicia la instancia local de la aplicación. De lo contrario, se inicia una instancia alojada de la aplicación. Si inicia una aplicación que no está instalada en el VDA, se inicia la aplicación alojada. Para obtener más información, consulte [Iniciar vPrefer](#).

En PowerShell (mediante el SDK de PowerShell remoto en implementaciones de Citrix Cloud o el SDK de PowerShell en implementaciones locales), puede cambiar esta acción.

En `New-Broker Application` o el cmdlet `Set-BrokerApplication`, utilice la opción `LocalLaunchDisabled`. Por ejemplo:

```
Set-BrokerApplication -LocalLaunchDisabled <Boolean>
```

De forma predeterminada, el valor de esta opción es `false` (`-LocalLaunchDisabled $false`). Al iniciar una aplicación publicada desde un escritorio publicado, la aplicación se inicia en esa sesión de escritorio.

Si establece el valor de la opción en `true` (`-LocalLaunchDisabled $true`), se inicia la aplicación publicada. Eso crea una sesión adicional, por separado del escritorio publicado (que usa la aplicación Citrix Workspace para Windows), para la aplicación publicada.

Requisitos y limitaciones:

- El valor `ApplicationType` de la aplicación debe ser `HostedOnDesktop`.
- Esta opción solo está disponible a través del SDK de PowerShell apropiado. Actualmente no está disponible en la interfaz gráfica de Studio.
- Esta opción requiere, como mínimo: StoreFront 3.14, Citrix Receiver para Windows 4.11 y Delivery Controller 7.17.

## Aplicaciones de la Plataforma universal de Windows

January 19, 2023

Para obtener información sobre las aplicaciones de la Plataforma universal de Windows (UWP), consulte esta documentación de Microsoft:

- [¿Qué es una aplicación de la Plataforma universal de Windows \(UWP\)?](#)
- [Administrador de paquetes de Windows](#)

## Requisitos y limitaciones

Citrix Virtual Apps and Desktops admite el uso de aplicaciones UWP con VDA en estas máquinas con Windows:

- Windows 10 y versiones posteriores
- Windows Server 2016 y versiones posteriores

Los VDA deben ser como mínimo de la versión 7.11.

Las siguientes funciones de Citrix Virtual Apps and Desktops no se ofrecen o están limitadas cuando se usan aplicaciones UWP:

- La asociación de tipo de archivo no se ofrece.
- La función Acceso a aplicaciones locales no se ofrece.
- Vista previa dinámica. Si las aplicaciones que se ejecutan en la sesión se solapan, la vista previa mostrará el icono predeterminado. Las API de Win32 para Vista previa dinámica no se admiten en aplicaciones UWP.
- Comunicación remota con el centro de actividades: Las aplicaciones UWP pueden usar el Centro de actividades para mostrar mensajes en la sesión. Actualmente, estos mensajes no se redirigen al dispositivo de punto final para mostrarlos al usuario.

No se permite iniciar aplicaciones UWP y aplicaciones que no son de UWP desde el mismo servidor. En su lugar, coloque las aplicaciones UWP y las aplicaciones que no son de UWP en grupos de entrega o grupos de aplicaciones independientes.

Como se enumeran todas las aplicaciones UWP instaladas en la máquina, Citrix recomienda inhabilitar el acceso de los usuarios a la Tienda Windows. Eso impide que un usuario acceda a las aplicaciones UWP que haya instalado otro usuario.

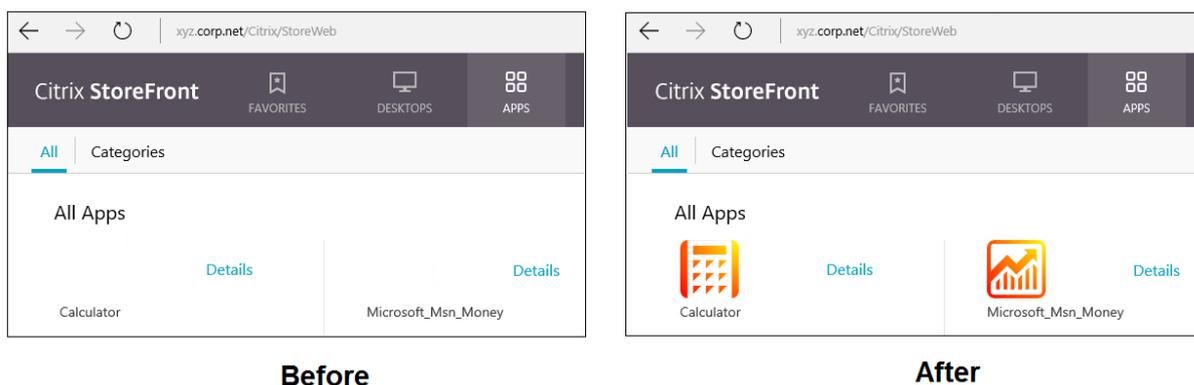
Durante la carga lateral, la aplicación UWP se instala en la máquina y empieza a estar disponible para otros usuarios. Cuando otro usuario inicia la aplicación, esta se instala, y el sistema operativo actualiza su base de datos de AppX para indicar que ese usuario la ha instalado.

Es posible que, en un cierre de sesión correcto iniciado desde una aplicación UWP publicada que se inició en una ventana fija o integrada, la sesión del VDA no pueda cerrarse y que se fuerce el cierre de sesión del usuario. Cuando esto ocurre, quedan varios procesos pendientes en la sesión del VDA que impiden un cierre correcto. Para resolver este problema, puede determinar cuál es el proceso que impide el cierre de sesión de VDA y agregarlo al valor de la clave de Registro “LogoffCheckSysModules” según las instrucciones proporcionadas en [CTX891671](#).

Es posible que los nombres principales y las descripciones de las aplicaciones UWP no sean correctos. Modifique y corrija esas propiedades al agregar las aplicaciones a un grupo de entrega.

Consulte [Problemas conocidos](#) para resolver problemas adicionales.

Actualmente, algunas aplicaciones UWP tienen iconos blancos con transparencia habilitada, lo que vuelve al icono invisible en el fondo de pantalla blanco de StoreFront. Para evitar este problema, se puede cambiar el fondo. Por ejemplo, en la máquina de StoreFront, modifique el archivo `C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css`. Al final del archivo, agregue `.storeapp-icon { background-image: radial-gradient( circle at top right, yellow, red ); }`. En el gráfico siguiente, se muestra un antes y un después de este ejemplo.



En Windows Server 2016 y versiones posteriores, es posible que el Administrador del servidor también se inicie cuando se inicie una aplicación universal. Para evitar que esto ocurra, impida que el Administrador del servidor se inicie automáticamente durante el inicio de sesión con la clave de Registro `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon`. Para obtener información detallada, consulte <https://blog.rmilne.ca/2014/05/30/how-to-hide-server-manager-at-logon/>.

## Instalar y publicar aplicaciones UWP

La funcionalidad de aplicaciones UWP está habilitada de forma predeterminada.

Para instalar una o más aplicaciones UWP en agentes VDA (o en una imagen maestra), use uno de los siguientes métodos:

- Lleve a cabo una instalación sin conexión desde la Tienda Windows para empresas, mediante una herramienta como Administración y mantenimiento de imágenes de implementación (DISM) para implementar las aplicaciones en la imagen de escritorio. Para obtener más información, consulte [Administrador de paquetes de Windows](#).
- Realice una instalación de prueba de las aplicaciones. Para obtener más información, consulte [Sideload line of business \(LOB\) apps in Windows client devices](#).
- Instale las aplicaciones UWP para cada usuario previsto directamente desde la Tienda Windows para empresas.

Para agregar (publicar) una o varias aplicaciones UWP en Citrix Virtual Apps o Citrix Virtual Desktops:

1. Una vez que las aplicaciones UWP se hayan instalado en la máquina, agréguelas a un grupo de entrega o a un grupo de aplicaciones. Puede hacerlo cuando cree un grupo de entrega o más tarde. En la página **Aplicaciones**, en el menú **Agregar**, seleccione **Desde el menú Inicio**.
2. Cuando aparezca la lista de aplicaciones, marque las aplicaciones UWP que quiera publicar.
3. Continúe con el asistente o cierre el cuadro de diálogo de edición.

Para obtener información sobre los requisitos de configuración adicionales al utilizar User Profile Manager (UPM), consulte

[Aplicaciones Windows: Tienda Microsoft](#).

Para inhabilitar el uso de aplicaciones UWP en un VDA, agregue el parámetro del Registro **EnableUWASeamlessSupport** a `HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle` y establézcalo en **0**.

## Desinstalar aplicaciones UWP

Cuando desinstale una aplicación UWP con un comando como `Remove-AppXPackage`, el elemento se desinstala solo para los administradores. Para quitar la aplicación de las máquinas de los usuarios que puedan haberlas iniciado y utilizado, debe ejecutar el comando de eliminación en cada máquina. No puede desinstalar el paquete AppX de todas las máquinas de los usuarios con un comando.

## Zonas

June 27, 2024

Las implementaciones que incluyen ubicaciones muy alejadas, conectadas mediante una red WAN, pueden presentar problemas debido a la latencia de la red y la confiabilidad. Existen dos opciones para mitigar esos problemas:

- Implementar varios sitios, cada uno con su propia base de datos SQL Server del sitio.  
Se recomienda esta opción para implementaciones de empresa de gran tamaño. Se trata de varios sitios que se administran por separado, y cada uno necesita su propia base de datos SQL Server del sitio. Cada sitio es una implementación independiente de Citrix Virtual Apps.
- Configurar varias zonas en un único sitio.

Configurar zonas puede ayudar a los usuarios de regiones remotas a conectarse a recursos sin que las conexiones recorran necesariamente grandes segmentos de red WAN. Utilizar zonas permite una administración efectiva de sitios desde una única consola de Citrix Studio, Citrix Director y la base de datos del sitio. Esto disminuye los costes de implementación, personal, licencias y operación de otros sitios que contienen bases de datos separadas en ubicaciones remotas.

Las zonas pueden resultar útiles en implementaciones de todos los tamaños. Puede usar zonas para mantener las aplicaciones y los escritorios más cerca de los usuarios finales, lo que mejora el rendimiento. Una zona puede tener uno o varios Controllers instalados localmente por redundancia y resistencia, pero no es necesario.

La cantidad de Controllers configurados en el sitio puede afectar al rendimiento de algunas operaciones, como agregar nuevos Controllers al sitio mismo. Para evitar este problema, se recomienda limitar la cantidad a no más de 50 zonas en su sitio de Citrix Virtual Apps o Citrix Virtual Desktops.

Si la latencia de red de las zonas es superior a 250 milisegundos RTT, se recomienda implementar varios sitios en lugar de varias zonas.

En este artículo, el término “local” se refiere a la zona que se analiza. Por ejemplo, “un VDA se registra en el Controller local” significa que el VDA se registra en un Controller de la zona donde está situado el VDA.

Las zonas de esta versión son similares (pero no idénticas) a las zonas de XenApp 6.5 o versiones anteriores. Por ejemplo, en esta implementación de zonas, no hay recopiladores de datos. Todos los Controllers de un sitio se comunican con una base de datos del sitio situada en la zona principal. Además, la conmutación por error y las zonas favoritas funcionan de otra forma en esta versión.

## Tipos de zona

Un sitio siempre tiene una zona principal. También puede tener una o varias zonas satélite. Las zonas satélite se pueden usar para: recuperación ante desastres, centros de datos geográficamente alejados, sucursales, una nube o la zona de disponibilidad de una nube.

### Zona principal:

La zona principal tiene el nombre predeterminado “Principal” y contiene la base de datos SQL Server del sitio (y servidores SQL de alta disponibilidad, si los hay), Studio, Director, Citrix StoreFront, el servidor de licencias Citrix y Citrix Gateway. La base de datos del sitio debe estar siempre en la zona principal.

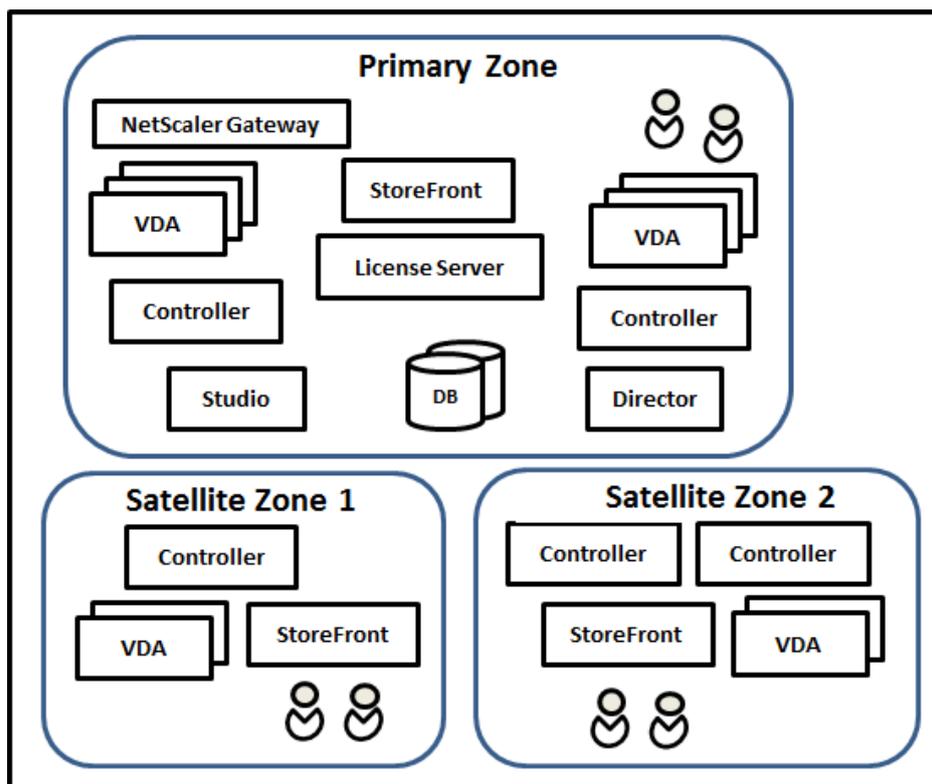
La zona principal también debe tener al menos dos Controllers para la redundancia. Asimismo, puede tener uno o varios VDA con aplicaciones estrechamente ligadas a la base de datos y la infraestructura.

### Zona satélite:

Una zona satélite contiene uno o varios VDA, Controllers, servidores de StoreFront y servidores de Citrix Gateway. En condiciones normales, los Controllers de una zona satélite se comunican directamente con la base de datos situada en la zona principal.

Una zona satélite, especialmente una grande, también puede contener un hipervisor que se usa para aprovisionar y/o almacenar máquinas de esa zona. Al configurar una zona satélite, puede asociarle una conexión de hipervisor o servicio de nube. (Compruebe que los catálogos de máquinas que utilizan esa conexión están en la misma zona.)

Un sitio puede tener zonas satélite con distintas configuraciones, en función de sus necesidades concretas y su entorno. En la siguiente imagen, se representa una zona principal y ejemplos de zonas satélite.



En la imagen:

- **Zona principal:** Contiene dos Controllers, Studio, Director, StoreFront, el servidor de licencias y la base de datos del sitio (además de implementaciones de alta disponibilidad de SQL Server). La zona principal también contiene varios VDA y un Citrix Gateway.
- **Zona satélite 1: varios VDA con un Controller:** Contiene un Controller, agentes VDA y un servidor de StoreFront. Los VDA de esta zona satélite se registran en el Controller local. El Controller local se comunica con la base de datos del sitio y el servidor de licencias situados en la zona principal.

Si falla la red WAN, la función Caché de host local permite que el Controller de la zona satélite siga actuando como broker en conexiones a los VDA de esa zona. Una implementación así puede ser adecuada en una oficina donde los trabajadores utilicen un sitio local de StoreFront y el Controller local para acceder a sus recursos locales incluso aunque falle el vínculo WAN que

conecta su oficina a la red de la empresa.

- **Zona satélite 2: varios VDA con Controllers redundantes:** Contiene dos Controllers, agentes VDA y un servidor de StoreFront. Este es el tipo de zona más resistente. Ofrece protección contra errores simultáneos de red WAN y uno de los Controllers locales.

## **Dónde se registran los VDA y dónde conmutan por error los Controllers**

En un sitio que contiene zonas principal y satélite, con agentes VDA como mínimo de la versión 7.7:

- Un VDA de la zona principal se registra en un Controller de la zona principal. Un VDA de la zona principal no intentará nunca registrarse en un Controller de una zona satélite.
- Un VDA de una zona satélite se registra en el Controller local, si es posible. (Este se considera el Controller favorito.) Si no hay Controllers locales disponibles (por ejemplo, debido a que no pueden aceptar más registros de VDA o porque se ha producido un error en ellos), el VDA intentará registrarse en un Controller de la zona principal. En este caso, el VDA permanecerá registrado en la zona principal incluso aunque un Controller de la zona satélite vuelva a estar disponible. Un VDA de una zona satélite no intentará nunca registrarse en un Controller de otra zona satélite.
- Cuando está habilitada la actualización automática para la detección de Controllers por parte de los VDA y se especifica una lista de direcciones de Controller durante la instalación de VDA, se selecciona aleatoriamente un Controller de esa lista para el registro inicial (independientemente de la zona en que resida ese Controller). Una vez se reinicie la máquina que contiene el VDA, ese VDA empezará el registro en un Controller de su zona local.
- Si falla un Controller de una zona satélite, si puede, conmutará por error a otro Controller local. Si no hay Controllers locales disponibles, se producirá una conmutación por error a un Controller de la zona principal.
- Si se mueve un Controller dentro o fuera de una zona y su actualización automática está habilitada, los VDA de ambas zonas recibirán listas actualizadas que indicarán qué Controllers son locales y cuáles están en la zona principal, para que los VDA sepan en cuál se pueden registrar y de cuál pueden aceptar conexiones.
- Si se mueve un catálogo de máquinas a otra zona, los VDA de ese catálogo volverán a registrarse en los Controllers de la zona a la que se haya movido el catálogo. (Cuando mueva un catálogo a otra zona, compruebe que esa zona y la zona con la conexión de host asociada estén bien conectadas. Si hay ancho de banda limitado o alta latencia, mueva la conexión de host a la misma zona que contiene el catálogo de máquinas asociado.)

Si fallan todos los Controllers de la zona principal:

- Studio no puede conectarse al sitio.
- No se puede establecer conexiones con los VDA de la zona principal.

- El rendimiento del sitio se degradará cada vez más hasta que los Controllers de la zona principal vuelvan a estar disponibles.

En caso de sitios que contienen versiones de VDA anteriores a 7.7:

- Un VDA en una zona satélite aceptará solicitudes de Controllers de su zona local y la zona principal. (A partir de la versión 7.7, los agentes VDA pueden aceptar solicitudes de Controller de otras zonas satélite.)
- Un VDA de una zona satélite se registrará en un Controller de la zona principal o de la zona local de forma aleatoria. (A partir de la versión 7.7, los agentes VDA prefieren la zona local.)

### **Preferencia de zonas**

Para usar la función Preferencia de zonas, debe utilizar como mínimo StoreFront 3.7 y Citrix Gateway 11.0-65.x.

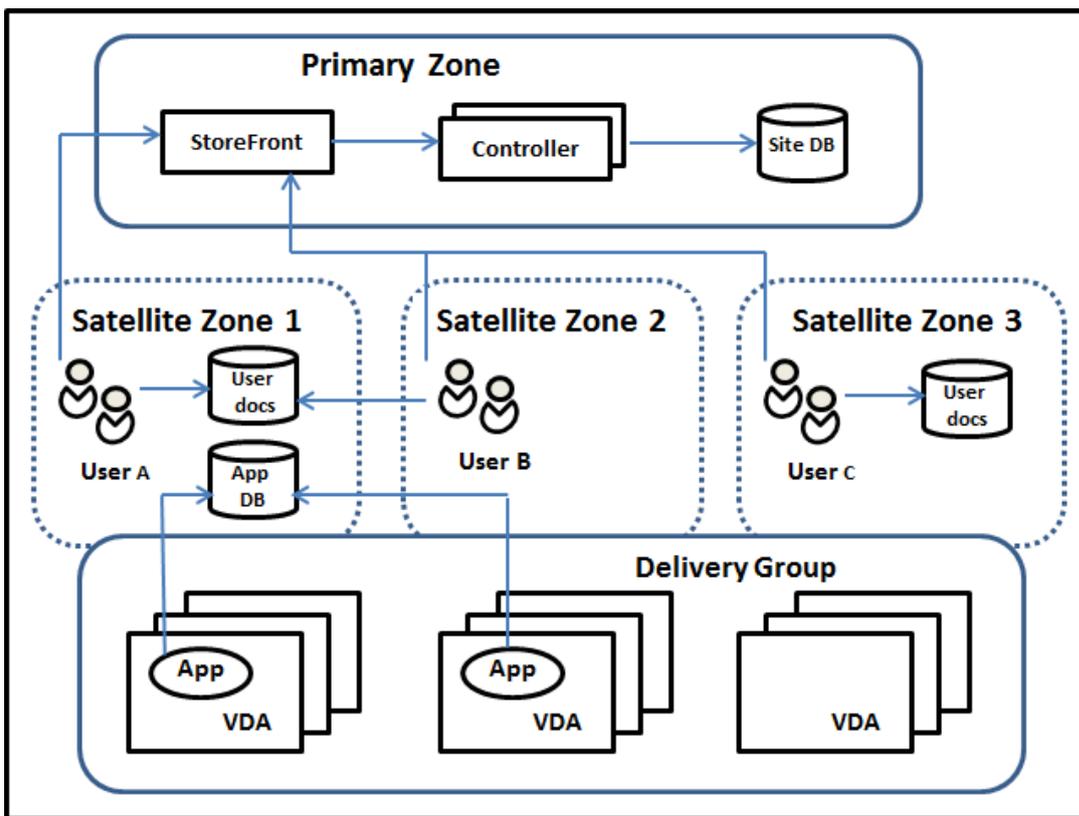
En un sitio de varias zonas, la función Preferencia de zonas ofrece más flexibilidad al administrador para controlar qué VDA se utiliza para iniciar una aplicación o un escritorio.

### **Cómo funciona la preferencia de zonas**

Existen tres preferencias distintas de zonas. Es posible que prefiera utilizar un VDA en una zona particular, en función de:

- Dónde se almacenan los datos de la aplicación. Esto se conoce como zona particular de la aplicación.
- La ubicación de los datos principales del usuario (por ejemplo, un perfil o un directorio particular en un recurso compartido de red). Esto se conoce como zona particular del usuario.
- La ubicación actual del usuario (dónde se está ejecutando la aplicación Citrix Workspace). Esto se conoce como ubicación del usuario.

En el gráfico siguiente, se muestra un ejemplo de configuración de varias zonas.



En este ejemplo, los VDA están distribuidos en tres zonas satélite, pero pertenecen todos al mismo grupo de entrega. Por lo tanto, el intermediario (broker) puede elegir qué VDA usar cuando un usuario lanza una solicitud de inicio. En este ejemplo, hay varios lugares donde los usuarios pueden ejecutar sus puntos finales de la aplicación Citrix Workspace: el usuario A usa un dispositivo con la aplicación Citrix Workspace en la zona satélite 1; el usuario B usa un dispositivo en la zona satélite 2. Los documentos de los usuarios pueden almacenarse en una serie de ubicaciones; por ejemplo: ambos usuarios, A y B, utilizan un recurso compartido en la zona satélite 1, mientras que el usuario C usa un recurso de la zona satélite C. Además, una de las aplicaciones publicadas utiliza una base de datos que se encuentra en la zona satélite 1.

Para asociar un usuario o una aplicación a una zona, configure una zona particular específica para ese usuario o esa aplicación. A partir de ahí, el broker que se encuentra en el Delivery Controller usa esas asociaciones para seleccionar la zona donde se iniciará una sesión, si los recursos están disponibles. Puede hacer lo siguiente:

- Configurar la zona particular de un usuario agregándolo a una zona.
- Configurar la zona particular de una aplicación modificando las propiedades de esta.

Un usuario o una aplicación pueden tener solo una zona particular en un momento dado. (Puede darse una excepción para los usuarios cuando hay varias pertenencias a zonas porque esos usuarios forman parte de grupos de usuarios; consulte la sección “Otras consideraciones” para resolverla. Sin embargo, incluso en este caso, el broker utiliza una sola zona particular.)

Aunque se puedan configurar las preferencias de zonas para usuarios y aplicaciones, el broker selecciona una sola zona preferida para el inicio. El orden predeterminado de prioridad para seleccionar la zona preferida es: zona particular de la aplicación > zona particular del usuario > ubicación del usuario. Puede restringir la secuencia; consulte Adaptar la preferencia de zonas. Cuando un usuario inicia una aplicación:

- Si la aplicación tiene configurada una asociación de zona (es decir, una zona particular de la aplicación), entonces la zona preferida es la zona particular de esa aplicación.
- En cambio, si la aplicación no tiene configurada una asociación de zona pero el usuario sí la tiene (una zona particular de usuario), entonces la zona preferida es la zona particular del usuario.
- Si ni la aplicación ni el usuario tienen configurada una asociación de zona, entonces la zona preferida es la zona donde el usuario ejecuta la instancia de la aplicación Citrix Workspace (la ubicación del usuario). Si esa zona no está definida, se seleccionan un VDA y una zona aleatorios. El equilibrio de carga se aplica a todos los VDA de la zona preferida. Si no hay ninguna zona preferida, el equilibrio de carga se aplica a todos los VDA del grupo de entrega.

### Adaptar la preferencia de zonas

Al configurar (o quitar) la zona particular de un usuario o una aplicación, puede limitar más cómo se utilizará (o no) la preferencia de zonas.

- **Uso obligatorio de la zona particular del usuario.** En un grupo de entrega, puede especificar que una sesión deba iniciarse en la zona particular del usuario (si la tiene), sin conmutación por error a otra zona si los recursos no estuvieran disponibles en esa zona particular. Esta restricción es útil para evitar el riesgo de copia de perfiles o archivos de datos grandes entre las zonas. En otras palabras, cuando se prefiere negar el inicio de una sesión a iniciarla en otra zona.
- **Uso obligatorio de la zona particular de la aplicación.** Del mismo modo, cuando configure la zona particular de una aplicación, puede indicar que la aplicación deba iniciarse solo en esa zona, sin conmutación por error a otra zona aunque los recursos no estuvieran disponibles en la zona particular de la aplicación.
- **Sin zona particular de aplicación, e ignorar la zona particular configurada del usuario.** Si no especifica ninguna zona particular para una aplicación, también puede indicar que no se tenga en cuenta ninguna zona de usuario configurada para iniciar esa aplicación. Por ejemplo, si prefiere que los usuarios ejecuten una aplicación concreta en un VDA cercano a la máquina que están utilizando (donde se está ejecutando la aplicación Citrix Workspace), puede indicarlo mediante la preferencia de zona “ubicación del usuario” aunque algunos usuarios tengan otra zona particular.

## **Cómo afecta la preferencia de zonas al uso de sesiones**

Cuando un usuario inicia una aplicación o un escritorio, el broker prefiere usar la zona preferida en lugar de usar una sesión existente.

Si el usuario que inicia la aplicación o escritorio ya tiene una sesión apropiada para el recurso que se va a iniciar (por ejemplo, una que puede usar la función de compartir sesiones para una aplicación, o bien una sesión que ya ejecuta el recurso que se va a iniciar), pero esa sesión se está ejecutando en un VDA que se encuentra en otra zona, no la preferida de la aplicación o el usuario, el sistema puede crear una nueva sesión. Con lo que el inicio se produce en la zona correcta (si tiene capacidad disponible), en vez de reconectarse a una sesión en una zona menos ventajosa para los requisitos de sesión del usuario.

Para que no exista una sesión “huérfana” con la que ya no se pueda establecer conexión, se permite volverse a conectar a las sesiones desconectadas incluso aunque estén en una zona no preferida.

El orden de preferencia para elegir una sesión para el inicio es:

1. Reconectarse a una sesión existente en la zona preferida.
2. Reconectarse a una sesión desconectada existente en una zona que no sea la preferida.
3. Iniciar una sesión nueva en la zona preferida.
4. Reconectarse una sesión conectada existente en una zona que no sea la preferida.
5. Iniciar una sesión nueva en una zona que no sea la preferida.

## **Otras consideraciones de preferencia de zonas**

- Si configura la zona particular de un grupo de usuarios (por ejemplo, un grupo de seguridad), los usuarios de ese grupo (por pertenencia directa o indirecta) se asocian a la zona especificada. No obstante, un usuario puede pertenecer a varios grupos de seguridad y, por lo tanto, puede tener otras zonas particulares configuradas por pertenecer a otros grupos. En tales casos, la determinación de la zona particular de ese usuario puede ser ambigua.

Si un usuario tiene configurada una zona particular que no adquirió por pertenecer a grupos, esa es la zona que se usa para la preferencia de zonas. Se ignoran las asociaciones de zona que se adquieran por pertenecer a grupos.

Si el usuario tiene varias asociaciones de zonas que adquirió únicamente por pertenecer a grupos, el broker escoge una zona aleatoria de entre ellas. Tras la elección del broker, se utiliza la misma zona para los inicios subsiguientes de sesión hasta que cambie la pertenencia del usuario a los grupos.

- La preferencia de zona “ubicación del usuario” requiere que el Citrix Gateway a través del cual se conecta el dispositivo de punto final detecte la aplicación Citrix Workspace en ese dispositivo de punto final. El dispositivo Citrix Gateway debe estar configurado para asociar intervalos de

direcciones IP a zonas concretas, y la identidad de la zona detectada debe transferirse a través de StoreFront al Controller.

Para obtener más información acerca de la preferencia de zonas, consulte [Zone Preference Internals](#).

## Requisitos, consejos y consideraciones

- Puede colocar los siguientes elementos en una zona: Controllers, catálogos de máquinas, conexiones de host, usuarios y aplicaciones. Si un catálogo de máquinas usa una conexión de host, el catálogo y la conexión deben estar en la misma zona. (sin embargo, con una conexión disponible de latencia baja y ancho de banda alto, pueden estar en diferentes zonas).
- Colocar elementos en una zona satélite afecta al modo en que el sitio interactúa con ellos y con otros objetos relacionados con esos elementos.
  - Cuando se colocan máquinas de Controller en una zona satélite, se presupone que esas máquinas tienen una buena conexión (local) con hipervisores y máquinas VDA en la misma zona satélite. Por tanto, se utilizan preferentemente los Controllers de esa zona satélite en lugar de Controllers de la zona principal para la gestión de esos hipervisores y esas máquinas VDA.
  - Cuando se coloca una conexión de hipervisor en una zona satélite, se presupone que todos los hipervisores administrados a través de esa conexión de hipervisor también residen en esa zona satélite. Por tanto, se utilizan preferentemente los Controllers de esa zona satélite en lugar de Controllers de la zona principal para la comunicación por esa conexión de hipervisor.
  - Cuando se coloca un catálogo de máquinas en una zona satélite, se presupone que todas las máquinas VDA de ese catálogo están en la zona satélite. Se utilizan preferentemente Controllers locales (en lugar de Controllers de la zona principal) cuando los VDA intentan registrarse en el sitio, después de que se haya activado el mecanismo de actualización automática de los Controllers tras el primer registro de cada VDA.
  - También se pueden asociar instancias de Citrix Gateway a zonas. A diferencia de los demás elementos que se describen aquí, esto se realiza como parte de la configuración del enrutamiento óptimo de HDX de StoreFront, en lugar de hacerse como parte de la configuración del sitio. Cuando se asocia un Citrix Gateway a una zona, se utiliza preferentemente ese Citrix Gateway cuando se utilizan las conexiones HDX a las máquinas VDA de esa zona.
- Cuando se crea un sitio de producción y, luego, se crean el primer catálogo de máquinas y el primer grupo de entrega, todos esos elementos se encuentran en la zona principal: no se pueden crear zonas satélite hasta después de completar la configuración inicial (si crea un sitio vacío, la zona principal contendrá al principio solo un Controller; puede crear zonas satélite antes o después de crear un catálogo de máquinas y un grupo de entrega).

- Cuando crea la primera zona satélite con uno o varios elementos, todos los demás elementos de su sitio siguen estando en la zona principal.
- La zona principal se denomina “Principal” de forma predeterminada, y usted puede cambiar ese nombre. Aunque la pantalla de Studio indica cuál es la zona principal, se recomienda usar un nombre de fácil identificación para la zona principal. Puede reasignar la zona principal (es decir, puede convertir otra zona en la zona principal), pero esta debe contener siempre la base de datos del sitio y los servidores de alta disponibilidad.
- La base de datos del sitio debe estar siempre en la zona principal.
- Después de crear una zona, puede mover elementos de una zona a otra. Tenga en cuenta que esta flexibilidad permite llegar a separar elementos que funcionan mejor en cercanía; por ejemplo, mover un catálogo de máquinas a otra zona que la conexión (host) que crea las máquinas del catálogo podría afectar al rendimiento. Por lo tanto, tenga en mente los posibles efectos imprevistos antes de mover elementos entre zonas. Mantenga el catálogo y la conexión de host que éste usa en la misma zona o en zonas bien conectadas (por ejemplo, conectadas a través de una red de baja latencia y alto ancho de banda).
- Para obtener un rendimiento óptimo, instale Studio y Director solo en la zona principal. Si quiere otra instancia de Studio en una zona satélite (por ejemplo, si una zona satélite que contiene Controllers se usa para la conmutación por error en caso de que la zona principal deje de ser accesible), ejecute Studio como una aplicación publicada localmente. Asimismo, puede acceder a Director desde una zona satélite porque se trata de una aplicación web.
- Preferiblemente, Citrix Gateway de una zona satélite debe usarse para conexiones de usuario provenientes de otras zonas o ubicaciones externas, aunque puede usarse para conexiones desde dentro de la zona.
- Recuerde: Para usar la función Preferencia de zonas, debe utilizar como mínimo StoreFront 3.7 y Citrix Gateway 11.0-65.x.

### **Límites a la calidad de conexión**

Los Controllers de la zona satélite llevan a cabo interacciones SQL directamente con la base de datos del sitio. Eso impone algunos límites en la calidad del enlace entre la zona satélite y la zona principal que contiene la base de datos del sitio. Los límites concretos dependen de la cantidad de agentes VDA y sesiones de usuario en esos VDA que se implementan en la zona satélite. Por lo tanto, zonas satélite con pocos VDA y pocas sesiones pueden funcionar con una conexión de peor calidad a la base de datos que las zonas satélite que tengan grandes cantidades de agentes VDA y muchas sesiones.

Para obtener más información, consulte [Latency and SQL Blocking Query Improvements](#).

## Impacto de latencia en la intermediación de rendimiento

Aunque las zonas permiten a los usuarios estar en los enlaces de mayor latencia, siempre que haya un broker local, la latencia adicional influye inevitablemente en la experiencia del usuario final. Para la mayor parte de las tareas, los usuarios experimentan lentitud provocada por viajes de ida y vuelta entre los Controllers de la zona satélite y la base de datos del sitio.

En el inicio de aplicaciones, se producen demoras extras mientras el proceso de intermediación de sesiones identifica al VDA adecuado al que enviar las solicitudes de inicio de sesión.

## Crear y administrar zonas

Un administrador total puede realizar todas las tareas de creación y administración de zonas. Sin embargo, también se puede crear un rol personalizado que permita crear, modificar o eliminar una zona. Mover elementos entre zonas no requiere permisos de zonas (excepto el permiso de lectura de zonas). Sin embargo, debe tener permiso para modificar los elementos que esté moviendo. Por ejemplo, para mover un catálogo de máquinas de una zona a otra, debe tener el permiso de modificar ese catálogo de máquinas. Para obtener más información, consulte el artículo Administración delegada.

**Si utiliza Citrix Provisioning:** La consola de Citrix Provisioning que se incluye en esta versión no reconoce zonas, por lo que Citrix recomienda usar Studio para crear catálogos de máquinas que quiera colocar en las zonas satélite. Use el asistente de Studio para crear el catálogo y especificar la zona satélite correspondiente. A continuación, utilice la consola de Citrix Provisioning para aprovisionar las máquinas de ese catálogo. (Si crea el catálogo mediante el asistente de Citrix Provisioning, este se colocará en la zona principal y deberá usar Studio para moverlo posteriormente a la zona satélite.)

## Crear una zona

1. Seleccione **Configuración > Zonas** en el panel de navegación de Studio.
2. Seleccione **Crear zona** en el panel Acciones.
3. Escriba un nombre para la zona y una descripción (opcional). El nombre debe ser único dentro del sitio.
4. Seleccione los elementos que se van a colocar en la nueva zona. Puede filtrar o buscar la lista de elementos de la que seleccionarlos. También puede crear una zona vacía. Para ello, simplemente no seleccione ningún elemento.
5. Haga clic en **Guardar**.

Como alternativa a este método, puede seleccionar uno o varios elementos en Studio y, a continuación, seleccionar **Crear zona** en el panel Acciones.

### **Cambiar el nombre o la descripción de una zona**

1. Seleccione **Configuración > Zonas** en el panel de navegación de Studio.
2. Seleccione una zona en el panel central y, a continuación, seleccione **Modificar zona** en el panel Acciones.
3. Cambie el nombre y/o la descripción de la zona. Si cambia el nombre de la zona principal, tenga en cuenta que la zona debe ser fácilmente identificable como zona principal.
4. Haga clic en **Aceptar** o en **Aplicar**.

### **Mover elementos de una zona a otra**

1. Seleccione **Configuración > Zonas** en el panel de navegación de Studio.
2. Seleccione una zona en el panel central y, a continuación, seleccione uno o varios elementos.
3. Arrastre los elementos a la zona de destino o seleccione **Mover elementos** en el panel Acciones y, a continuación, especifique la zona a la que moverlos.

Aparecerá un mensaje de confirmación con una lista de los elementos seleccionados y preguntará si quiere moverlos a todos.

**Recuerde:** Si un catálogo de máquinas usa una conexión de host a un hipervisor o un servicio de nube, ambos (el catálogo y la conexión) deben estar en la misma zona. De lo contrario, el rendimiento puede verse afectado. Si mueve un elemento, mueva el otro.

### **Eliminar una zona**

Una zona debe estar vacía antes de que se pueda eliminar. No se puede eliminar la zona principal.

1. Seleccione **Configuración > Zonas** en el panel de navegación de Studio.
2. Seleccione una zona en el panel central.
3. Seleccione **Eliminar zona** en el panel Acciones. Si la zona no está vacía (contiene elementos), se le pedirá que seleccione la zona a la que se moverán los elementos.
4. Confirme la eliminación.

### **Agregar una zona particular a un usuario**

Configurar la zona particular de un usuario también se conoce como *agregar un usuario a una zona*.

1. Seleccione **Configuración > Zonas** en el panel de navegación de Studio y, a continuación, seleccione una zona en el panel central.
2. Seleccione **Agregar usuarios a la zona** en el panel Acciones.

3. En el cuadro de diálogo **Agregar usuarios a la zona**, haga clic en **Agregar** y, a continuación, seleccione los usuarios y los grupos de usuarios que quiera agregar a la zona. Si especifica usuarios que ya tienen su zona particular, aparecerá un mensaje con dos opciones: **Sí**, que equivale a agregar solo a los usuarios especificados que no tengan ninguna zona particular; **No**, que equivale a volver al diálogo de selección de usuarios.
4. Haga clic en **OK**.

Para los usuarios que tengan una zona particular configurada, puede definir que las sesiones se inicien solo desde su zona particular correspondiente:

1. Cree o modifique un grupo de entrega.
2. En la página **Usuarios**, marque la casilla **Las sesiones deben iniciarse en la zona particular del usuario, si está configurada**.

Todas las sesiones que inicie un usuario de ese grupo de entrega deberán iniciarse desde las máquinas que se encuentren en la zona particular de ese usuario. Si un usuario del grupo de entrega no tiene configurada una zona particular, este parámetro no tiene ningún efecto.

### Eliminar la zona particular de un usuario

Este procedimiento también se conoce como quitar un usuario de una zona.

1. Seleccione **Configuración > Zonas** en el panel de navegación de Studio y, a continuación, seleccione una zona en el panel central.
2. Seleccione **Quitar usuarios de la zona** en el panel Acciones.
3. En el cuadro de diálogo **Agregar usuarios a la zona**, haga clic en **Quitar** y, a continuación, seleccione los usuarios y los grupos que quiera quitar de la zona. Tenga en cuenta que esta acción solo quita a los usuarios de la zona; esos usuarios siguen formando parte de los grupos de entrega y los grupos de aplicaciones.
4. Confirme la eliminación cuando se le solicite.

### Administrar zonas particulares de aplicaciones

Configurar la zona particular de una aplicación también se conoce como agregar una aplicación a una zona. De forma predeterminada, en un entorno de varias zonas, una aplicación no tiene ninguna zona particular.

La zona particular de una aplicación se especifica en las propiedades de la aplicación. Puede configurar las propiedades de una aplicación cuando la agregue a un grupo o más adelante. Para ello, deberá seleccionar la aplicación en Studio y modificar sus propiedades.

- Al [crear un grupo de entrega](#), [crear un grupo de aplicaciones](#) o al [agregar aplicaciones a grupos existentes](#), seleccione **Propiedades** en la página **Aplicaciones** del asistente.

- Para cambiar las propiedades de una aplicación después de agregarla, seleccione **Aplicaciones** en el panel de navegación de Studio. Seleccione una aplicación y, a continuación, seleccione **Modificar propiedades de aplicación** en el panel Acciones.

En la página **Zonas** de las propiedades o ajustes de la aplicación:

- Si quiere que la aplicación tenga una zona particular:
  - Marque el botón de opción **Usar la zona seleccionada para determinar donde se inicia esta aplicación** y, a continuación, seleccione la zona de la lista desplegable.
  - Si quiere que la aplicación solo se inicie desde la zona seleccionada (ninguna otra), marque la casilla situada debajo de la selección de zonas.
- Si no quiere que la aplicación tenga una zona particular:
  - Seleccione la opción **No configurar una zona particular para esta aplicación**.
  - Si no quiere que el broker tenga en cuenta ninguna de las zonas de usuario configuradas cuando se inicie esta aplicación, marque la casilla situada bajo el botón de opción. En ese caso, no se utilizará ninguna zona particular de aplicación o usuario para determinar dónde iniciar esta aplicación.

## Otras acciones que implican especificar zonas

Cuando se agrega una conexión de host o se crea un catálogo de máquinas (aparte del momento en que se crea un sitio), se puede especificar una zona a la que se asignará el objeto, si ya se ha creado al menos una zona satélite.

En la mayoría de los casos, la zona principal es la opción predeterminada. Si utiliza Machine Creation Services para crear un catálogo de máquinas, se selecciona automáticamente la zona que esté configurada para la conexión de host.

Si el sitio no contiene zonas satélite, se presupone la selección de la zona principal y el cuadro de selección de zonas no aparece.

## Conexiones y recursos

September 22, 2021

### Introducción

Cuando se crea un sitio, también se puede crear la primera conexión a los recursos de alojamiento. Posteriormente, se puede cambiar esa conexión y crear otras nuevas. La configuración de una conex-

ión implica seleccionar el tipo de conexión entre los servicios de nube o los hipervisores compatibles. El almacenamiento y la red que seleccione forman los recursos necesarios para dicha conexión.

Los administradores de solo lectura pueden ver los detalles de conexiones y recursos. Debe ser un administrador total para realizar tareas de administración de conexiones y recursos. Para obtener más información, consulte [Administración delegada](#).

### **Dónde encontrar información acerca de los tipos de conexión**

Puede utilizar las plataformas de virtualización admitidas para alojar y administrar máquinas en el entorno de Citrix Virtual Apps o Citrix Virtual Desktops. El artículo [Requisitos del sistema](#) enumera los tipos compatibles. Puede utilizar las soluciones admitidas de implementación en la nube para alojar componentes de producto y aprovisionar máquinas virtuales. Estas soluciones agrupan recursos de procesamiento para construir nubes privadas, públicas o híbridas de Infraestructura como servicio (IaaS).

Para obtener más información, consulte las siguientes fuentes de información.

- **Microsoft Azure Resource Manager:**

- Artículo [Entornos de virtualización para el Administrador de recursos de Azure](#).
- Documentación de Microsoft.

- **Amazon Web Services (AWS):**

- [Citrix y AWS](#).
- Documentación de AWS.
- Al crear una conexión en Studio, debe proporcionar los valores de la clave de la **API** y de la clave secreta. Puede exportar el archivo de claves que contiene esos valores de AWS y, a continuación, importarlos. Incluya la región, la zona de disponibilidad, el nombre de la nube VPC, las direcciones de subred, el nombre de dominio, los nombres de los grupos de seguridad y las credenciales.
- Para configurar una conexión de host de AWS con el fin de utilizar roles de IAM, introduzca **role\_based\_auth** como valor para los campos “clave de acceso” y “clave secreta”. Asimismo, se requiere un rol de IAM que defina la directiva y los permisos requeridos por Citrix al agregarse a las instancias de Delivery Controllers o Cloud Connectors alojadas de AWS.
- El archivo de credenciales para la cuenta raíz de AWS, (que se puede obtener de la consola de AWS), no está en el mismo formato que los archivos de credenciales descargados para los usuarios estándar de AWS. Por lo tanto, Studio no puede usar el archivo para rellenar los campos de la clave de la **API** y de la clave secreta. Compruebe que está utilizando archivos de credenciales IAM de AWS.

- **Citrix Hypervisor (anteriormente XenServer):**
  - [Entornos de virtualización de Citrix Hypervisor.](#)
  - Documentación sobre Citrix Hypervisor.
- **Nutanix Acropolis:**
  - [Entornos de virtualización de Nutanix.](#)
  - Documentación de Nutanix.
- **VMware:**
  - [Entornos de virtualización VMware.](#)
  - Documentación del producto VMware.
- **Microsoft Hyper-V:**
  - Artículo [Entornos de virtualización de Microsoft System Center Virtual Machine Manager.](#)
  - Documentación de Microsoft.
- **Microsoft Azure (Classic):**
  - Este tipo de host ha sido [retirado](#).
  - Artículo [Entornos de virtualización de Microsoft Azure.](#)
  - Documentación de Microsoft.
- **CloudPlatform:**
  - Este tipo de host ha sido [retirado](#).
  - Documentación de CloudPlatform.
  - Al crear una conexión en Studio, debe proporcionar los valores de la clave de la **API** y de la clave secreta. Puede exportar el archivo de claves que contiene esos valores desde CloudPlatform y, a continuación, importarlos en Studio.

## Almacenamiento de host

Se admite un producto de almacenamiento si lo administra un hipervisor compatible. Citrix Support ayuda a los proveedores de los productos de almacenamiento a resolver problemas, y documentará esos problemas en Knowledge Center según sea necesario.

Cuando se aprovisionan máquinas, los datos se clasifican por tipo:

- Datos de sistema operativo (SO), que incluye las imágenes maestras.
- Datos temporales, que incluyen todos los datos no persistentes escritos en las máquinas aprovisionadas por MCS, archivos de paginación de Windows, datos de los perfiles de usuario y todos los datos que se sincronicen con ShareFile. Estos datos se descartan cada vez que la máquina se reinicia.

- Datos personales guardados en los Personal vDisks.

Si se ofrece un almacenamiento por separado para cada tipo de datos se puede reducir la carga y mejorar el rendimiento de IOPS en cada dispositivo de almacenamiento, lo que hace un uso óptimo de los recursos del host. También habilita el almacenamiento apropiado para los distintos tipos de datos, ya que la persistencia y resistencia son más importantes para algunos tipos de datos que para otros.

El almacenamiento puede ser compartido (ubicado centralmente, separado de los hosts y utilizado por todos los hosts) o local, en un hipervisor. Por ejemplo, el almacenamiento compartido central puede ser uno o varios volúmenes de almacenamiento en clúster de servidores Windows Server 2012 (con o sin almacenamiento conectado), o un dispositivo de un proveedor de almacenamiento. El almacenamiento central también puede ofrecer sus propias optimizaciones, tales como rutas de control del almacenamiento del hipervisor y acceso directo a través de plugins asociados.

El almacenamiento local de los datos temporales evita que haya que atravesar la red para acceder al almacenamiento compartido. Almacenar datos también reduce la carga (IOPS) en el dispositivo de almacenamiento compartido. El almacenamiento compartido puede ser más costoso, por lo que el almacenamiento de datos local puede reducir el gasto. Estas ventajas deben tenerse en cuenta frente a la disponibilidad de almacenamiento suficiente en los servidores de hipervisor.

Cuando se crea una conexión, se elige uno de los dos métodos de administración del almacenamiento: el almacenamiento compartido por los hipervisores, o el almacenamiento local en cada hipervisor.

Cuando se usa el almacenamiento local en uno o varios hosts de Citrix Hypervisor para el almacenamiento de datos temporales, compruebe que cada ubicación de almacenamiento que forma parte de la agrupación tenga un nombre único. (Para modificar un nombre en XenCenter, haga clic con el botón secundario en el espacio de almacenamiento y modifique la propiedad de nombre.)

### **Almacenamiento compartido por los hipervisores**

El método de almacenamiento compartido por los hipervisores guarda los datos que necesitan persistencia a largo plazo en una ubicación central, lo que proporciona una copia de seguridad y una administración centralizadas. Ese almacenamiento guarda los discos de SO y los discos Personal vDisk.

Cuando se selecciona este método, se puede elegir si usar almacenamiento local (en servidores de la misma agrupación de hipervisores) para datos de máquina temporales. Este método no requiere persistencia ni tanta resistencia como los datos del almacenamiento compartido. Esto se denomina *caché de datos temporales*. El disco local ayuda a reducir el tráfico hacia el almacenamiento de SO principal. Este disco se borra cada vez que se reinicia la máquina. Se accede al disco a través de una memoria caché de escritura. Tenga en cuenta que, si usa almacenamiento local para datos temporales, el VDA provisionado queda asociado a un host de hipervisor específico. Si ese host falla, la máquina virtual no se puede iniciar.

**Excepción:** Si usa volúmenes de almacenamiento en clúster o CSV (Clustered Storage Volumes), Microsoft System Center Virtual Machine Manager no permite la creación de discos caché de datos temporales en el almacenamiento local.

Cuando se crea una conexión, si se habilita la opción para almacenar datos temporales localmente, se pueden habilitar y configurar valores no predeterminados para el tamaño de la memoria y del disco de caché de cada VM cuando se crea un catálogo de máquinas que usa esa conexión. No obstante, los valores predeterminados se ajustan al tipo de conexión y son suficientes en la mayoría de los casos. Para obtener más información, consulte [Crear catálogos de máquinas](#).

El hipervisor también puede ofrecer tecnologías de optimización a través de la caché local de lectura de las imágenes de los discos. Por ejemplo, Citrix Hypervisor ofrece IntelliCache. Esto también puede reducir el tráfico de red hacia el almacenamiento central.

### Almacenamiento local en el hipervisor

El método de almacenamiento local en el hipervisor almacena datos localmente en el hipervisor. Con este método, las imágenes maestras y otros datos del SO se transfieren a todos los hipervisores utilizados en el sitio, tanto para la creación inicial de las máquinas como para las actualizaciones de las imágenes. Esto da como resultado un tráfico importante en la red de administración. La transferencia de imágenes consume también mucho tiempo y las imágenes no llegan a todos los hosts al mismo tiempo.

Cuando se selecciona este método, se puede elegir si se quiere usar el almacenamiento compartido para los discos Personal vDisk, para ofrecer resistencia y funcionalidad a los sistemas de recuperación antes desastres y copia de seguridad.

### Crear una conexión y recursos

Si quiere, puede crear la primera conexión cuando crea el sitio. El asistente para la creación de sitios contiene las páginas relacionadas con la conexión, como se describe más abajo: Conexión, Administración del almacenamiento, Selección del almacenamiento y Red.

Si crea una conexión después de crear un sitio, empiece en el paso 1.

#### **Importante:**

Los recursos de host (almacenamiento y red) deben estar disponibles antes de crear la conexión.

1. Seleccione **Configuración > Alojamiento** en el panel de navegación de **Studio**.
2. Seleccione **Agregar conexiones y recursos** en el panel **Acciones**.
3. El asistente lo guiará por las páginas siguientes (el contenido específico de las páginas depende del tipo de conexión seleccionado). Después de completar cada página, haga clic en **Siguiente** hasta llegar a la página **Resumen**.

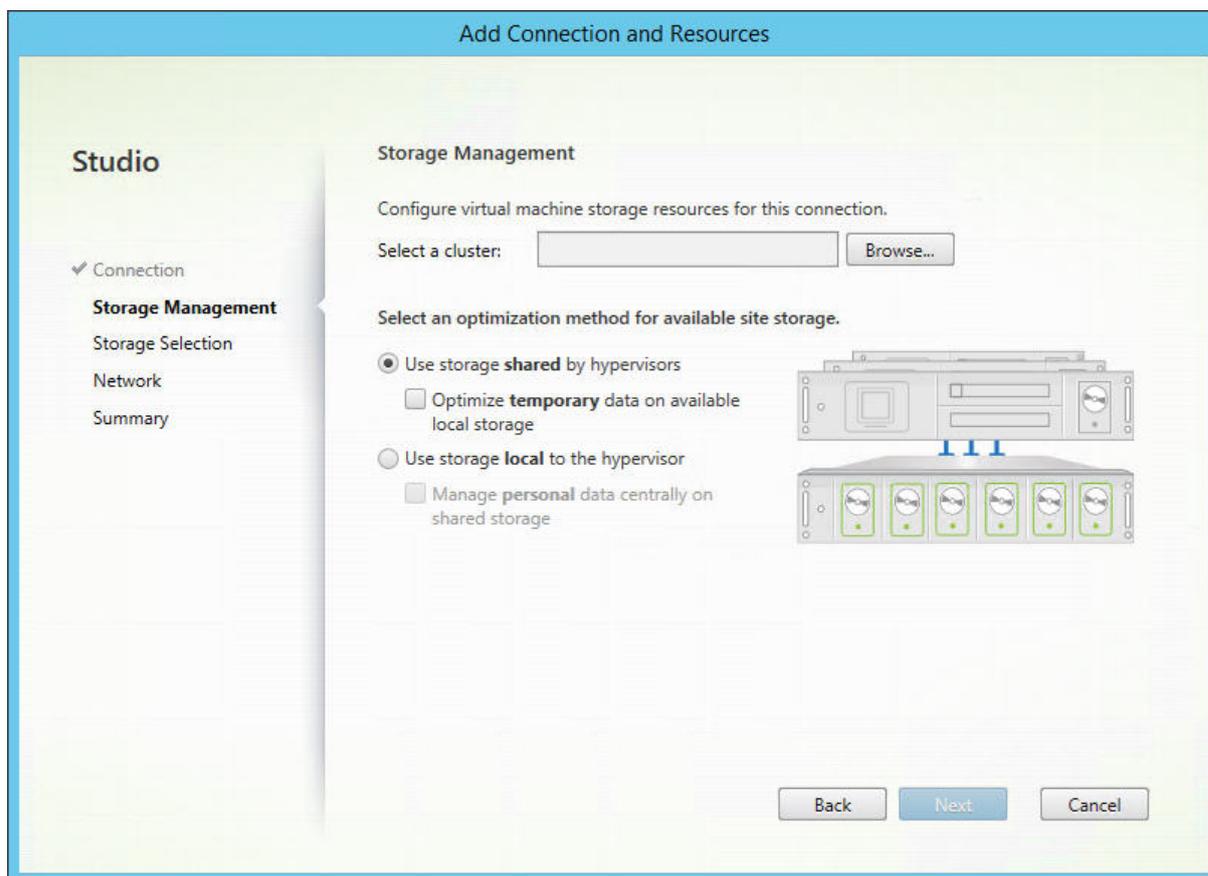
## Conexión

The screenshot shows the 'Add Connection and Resources' wizard in Citrix Studio. The 'Connection' tab is selected in the left-hand navigation pane. The main area is divided into two sections: 'Connection' and 'Create virtual machines using:'. In the 'Connection' section, the 'Create a new Connection' radio button is selected. Below it, the 'Connection type' is set to 'Citrix XenServer'. The 'Connection address' field contains 'Example: http://xenserver.example.com', the 'User name' field contains 'Example: root', the 'Password' field is empty, and the 'Connection name' field contains 'Example: MyConnection'. In the 'Create virtual machines using:' section, the 'Studio tools (Machine Creation Services)' radio button is selected. At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

En la página **Conexión**:

- Para crear una conexión, seleccione **Crear una nueva conexión**. Para crear una conexión basada en la misma configuración de host que una conexión existente, seleccione **Usar una conexión existente** y, a continuación, seleccione la conexión correspondiente.
- Seleccione el hipervisor o servicio de nube que está utilizando en el campo **Tipo de conexión**.
- Los campos de dirección de la conexión y credenciales difieren en función del tipo de conexión seleccionado. Introduzca la información requerida.
- Escriba un nombre para la conexión. Este nombre aparece en Studio.
- Elija la herramienta que usa para crear máquinas virtuales: herramientas de Studio (tales como Machine Creation Services o Citrix Provisioning) u otras herramientas.

## Administración del almacenamiento



Para obtener más información sobre los tipos y métodos de administración de almacenamiento, consulte Almacenamiento de host.

Si está configurando una conexión con un host de Hyper-V o VMware, busque y seleccione el nombre del clúster. Otros tipos de conexión no requieren un nombre de clúster.

Seleccione un método de administración del almacenamiento: puede ser almacenamiento compartido por los hipervisores o almacenamiento local en cada hipervisor.

- Si elige el almacenamiento compartido por los hipervisores, indique si quiere conservar los datos temporales en almacenamiento local disponible (Puede especificar valores no predeterminados para el tamaño del almacenamiento en los catálogos de máquinas que usen esta conexión.) **Excepción:** Si usa volúmenes de almacenamiento en clúster o CSV (Clustered Storage Volumes), Microsoft System Center Virtual Machine Manager no permite crear discos de caché de datos temporales en el almacenamiento local, por lo que el intento de configurar esa administración de almacenamiento en Studio falla.
- Si elige usar el almacenamiento local en cada hipervisor, indique si quiere administrar los datos personales (Personal vDisk) en el almacenamiento compartido.

Si usa almacenamiento compartido en una agrupación de Citrix Hypervisor, indique si quiere usar

IntelliCache para reducir la carga en el dispositivo de almacenamiento compartido. Consulte [Usar IntelliCache para conexiones de Citrix Hypervisor](#).

## Selección del almacenamiento

**Add Connection and Resources**

**Studio**

- ✓ Connection
- ✓ Storage Management
- Storage Selection**
- Network
- Summary

**Storage Selection**

When using local storage, you must select the type of data to store on each local storage device; machine operating system data, temporary data, and if not storing personal user data remotely, personal user data. At least one device must be selected for each data type.

Select data storage locations:

Show storage devices as groups Show all storage devices

Name	OS	Temporary
datastore1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
localdisk1	<input type="checkbox"/>	<input type="checkbox"/>
localdisk2	<input type="checkbox"/>	<input type="checkbox"/>
localdisk3	<input type="checkbox"/>	<input type="checkbox"/>

Select shared storage to store personal user data on personal vDisks:

1 storage device selected Select...

Back Next Cancel

Para obtener más información sobre la selección del almacenamiento, consulte Almacenamiento de hosts.

Seleccione al menos un dispositivo de almacenamiento en el host para cada tipo de datos. El método de administración de almacenamiento seleccionado en la página anterior afecta a qué tipos de datos estarán disponibles para seleccionar en esta página. Es necesario seleccionar al menos un dispositivo de almacenamiento para cada tipo de datos admitido antes de pasar a la página siguiente del asistente.

La parte inferior de la página **Selección de almacenamiento** contiene más opciones de configuración si se seleccionó alguna de las opciones siguientes en la página anterior.

- Si eligió almacenamiento compartido por los hipervisores y marcó la casilla **Optimizar datos temporales en el almacenamiento local disponible**, puede seleccionar los dispositivos de almacenamiento local (ubicados en la misma agrupación de hipervisores) que quiere usar para los datos temporales.

- Si eligió almacenamiento local en el hipervisor, y marcó la casilla **Administrar datos personales de forma centralizada en almacenamiento compartido**, puede seleccionar qué dispositivos compartidos quiere usar para los datos personales (datos de Personal vDisk).

Se mostrará la cantidad de dispositivos de almacenamiento seleccionados en ese momento (en el gráfico anterior, “1 storage device selected”). Cuando se pasa el puntero sobre ese texto, aparecen los nombres de los dispositivos seleccionados (a menos que no haya ninguno configurado).

1. Haga clic en **Seleccionar** para cambiar los dispositivos de almacenamiento que quiere usar.
2. En el cuadro de diálogo **Seleccionar almacenamiento**, seleccione o deje sin seleccionar las casillas de cada dispositivo de almacenamiento, y haga clic en **Aceptar**.

## Red

En la página **Red**, introduzca un nombre para los recursos. Este es el nombre que aparece en Studio para identificar la combinación de almacenamiento y red asociada a la conexión.

Seleccione una o varias redes que usan las VM.

## Resumen

En la página **Resumen**, revise sus selecciones. Cuando haya terminado, haga clic en **Finalizar**.

**Recuerde:** Si eligió guardar los datos temporales localmente, puede configurar valores no predeterminados para el almacenamiento de datos temporales cuando cree el catálogo de máquinas que contendrá las máquinas que usen esta conexión. Consulte [Creación de catálogos de máquinas](#).

## Modificar parámetros de conexión

No haga uso de este procedimiento para cambiar el nombre de una conexión o para crear una conexión. Esas son operaciones diferentes. Cambie la dirección solo si la máquina host actual tiene una nueva dirección. Si introduce la dirección de una máquina distinta se rompen los catálogos de máquinas de la conexión.

No puede cambiar los parámetros de **GPU** de una conexión porque los catálogos de máquinas que acceden a este recurso deben usar una imagen maestra de GPU específica apropiada. Cree una conexión.

1. Seleccione **Configuración > Alojamiento** en el panel de navegación de **Studio**.
2. Seleccione la conexión y, a continuación, seleccione **Modificar conexión** en el panel **Acciones**.
3. Siga las instrucciones que se indican a continuación para conocer los parámetros disponibles cuando se modifica una conexión.

4. Cuando haya terminado, haga clic en **Aplicar** para aplicar los cambios que haya hecho y deje la ventana abierta, o haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

Página **Propiedades de la conexión:**

- Para cambiar la dirección de conexión y las credenciales, seleccione **Modificar configuración** y, a continuación, escriba la nueva información.
- Si quiere especificar los servidores de alta disponibilidad para una conexión de Citrix Hypervisor, seleccione **Modificar servidores HA**. Citrix recomienda seleccionar todos los servidores de la agrupación para permitir la comunicación con Citrix Hypervisor en caso de que falle el servidor principal de la agrupación.

Página **Avanzada:**

- En el caso de una conexión Wake On LAN de Microsoft System Center Configuration Manager (ConfMgr), utilizada con el acceso con Remote PC, introduzca información sobre la transmisión de paquetes, Magic Packets y el **proxy de reactivación de ConfMgr**.
- Con las opciones del umbral de limitación, puede especificar una cantidad máxima de acciones de energía permitidas en una conexión. Estos parámetros pueden resultar útiles si los parámetros de administración de energía permiten que se inicien demasiadas o demasiado pocas máquinas al mismo tiempo. Todos los tipos de conexión tienen valores predeterminados concretos que son adecuados en la mayoría de los casos y no se deberían cambiar.
- En las opciones **Acciones simultáneas (de cualquier tipo)** y **Actualizaciones de inventario de Personal vDisk simultáneas**, se especifican dos valores: el número máximo absoluto que se puede dar de forma simultánea en esta conexión y un porcentaje máximo de todas las máquinas que utilizan esta conexión. Debe especificar valores absolutos y porcentuales. El límite real aplicado es el valor más bajo.

Por ejemplo, en una implementación con 34 máquinas, si **Acciones simultáneas (de cualquier tipo)** está establecido en un valor absoluto de 10 y un valor de porcentaje de 10, el límite real aplicado es 3 (es decir, 10 por ciento de 34, redondeado al número entero más cercano que sea menor que el valor absoluto de 10 máquinas).

- La opción **Máximo de acciones nuevas por minuto** es un número absoluto. No hay ningún valor porcentual.
- Introduzca la información en el campo **Opciones de conexión** únicamente con la ayuda de un representante de asistencia técnica de Citrix o instrucciones explícitas de la documentación.

## Activar o desactivar el modo de mantenimiento de una conexión

Si activa el modo de mantenimiento de una conexión, impide que cualquier otra acción de energía nueva afecte a las máquinas almacenadas en la conexión. Los usuarios no se pueden conectar a una

máquina mientras está en modo de mantenimiento. Si los usuarios ya están conectados, los cambios del modo de mantenimiento se efectúan cuando se cierra la sesión.

1. Seleccione **Configuración > Alojamiento** en el panel de navegación de **Studio**.
2. Seleccione la conexión. Para activar el modo de mantenimiento, seleccione **Activar modo de mantenimiento** en el panel **Acciones**. Para desactivar el modo de mantenimiento, seleccione **Desactivar modo de mantenimiento**.

También puede activar o desactivar el modo de mantenimiento en máquinas individuales. También puede activar o desactivar el modo de mantenimiento en las máquinas de los catálogos o grupos de entrega.

## Eliminar una conexión

La eliminación de una conexión puede provocar la eliminación de una gran cantidad de máquinas y la pérdida de datos. Compruebe que se haya hecho copia de seguridad de los datos de usuario en las máquinas afectadas, si fueran útiles.

Antes de eliminar una conexión, compruebe que:

- Todos los usuarios hayan cerrado la sesión en las máquinas almacenadas en la conexión.
- No existan sesiones de usuario desconectadas en ejecución.
- El modo de mantenimiento está activo para máquinas agrupadas y dedicadas.
- Todas las máquinas de los catálogos de máquinas que usa la conexión están apagadas.

Un catálogo de máquinas se vuelve inutilizable cuando se elimina una conexión a la que se hace referencia en ese catálogo. Si se hace referencia a esta conexión en un catálogo, tiene la opción de eliminar el catálogo. Antes de eliminar un catálogo, compruebe que no haya otras conexiones que lo estén utilizando.

1. Seleccione **Configuración > Alojamiento** en el panel de navegación de **Studio**.
2. Seleccione la conexión y, a continuación, seleccione **Eliminar conexión** en el panel **Acciones**.
3. Si esta conexión contiene máquinas almacenadas, se le preguntará si las máquinas deben eliminarse. Si debieran eliminarse, especifique qué medidas deben tomarse con las cuentas de equipo de Active Directory asociadas.

## Cambiar de nombre o probar una conexión

1. Seleccione **Configuración > Alojamiento** en el panel de navegación de **Studio**.
2. Seleccione la conexión y, a continuación, seleccione **Cambiar nombre de la conexión** o **Probar conexión** en el panel **Acciones**.

## Ver detalles de máquinas en una conexión

1. Seleccione **Configuración > Alojamiento** en el panel de navegación de **Studio**.
2. Seleccione la conexión y, a continuación, seleccione **Ver máquinas** en el panel **Acciones**.

El panel superior ofrece una lista de las máquinas a las que se accede a través de la conexión. Seleccione una máquina para ver información detallada sobre ella en el panel inferior. También se proporcionan detalles de sesión para las sesiones abiertas.

Utilice la función de búsqueda para encontrar máquinas rápidamente. Seleccione una búsqueda guardada en la lista que aparece en la parte superior de la ventana o cree una búsqueda. Puede realizar la búsqueda con todo o parte del nombre de la máquina o puede crear una expresión y usarla para una búsqueda avanzada. Para crear una expresión, haga clic en **Expandir** y, a continuación, seleccione los elementos de las listas de propiedades y operadores.

## Administrar máquinas en una conexión

1. Seleccione **Configuración > Alojamiento** en el panel de navegación de **Studio**.
2. Seleccione una conexión y, a continuación, seleccione **Ver máquinas** en el panel **Acción**.
3. Seleccione una de las siguientes opciones en el panel **Acciones**. Algunas acciones no están disponibles según el estado de la máquina y el tipo de host de la conexión.

---

Acción	Descripción
Iniciar	Inicia la máquina si está apagada o suspendida.
Suspender	Pausa la máquina sin apagarla y actualiza la lista de máquinas.
Apagar	Solicita al sistema operativo que se apague.
Forzar apagado	Obliga a la máquina a apagarse y actualiza la lista de máquinas.
Reiniciar	Solicita al sistema operativo que se apague y que, a continuación, vuelva a iniciar la máquina. Si el sistema operativo no puede hacerlo, el escritorio se mantiene en su estado actual.

Acción	Descripción
Habilitar modo de mantenimiento	Detiene temporalmente las conexiones a una máquina. Los usuarios no pueden conectarse a una máquina en este estado. Si los usuarios están conectados, los cambios del modo de mantenimiento se efectúan cuando se cierra la sesión (también puede activar o desactivar el modo de mantenimiento en todas las máquinas a las que se accede a través de una conexión, como se describió anteriormente).
Quitar del grupo de entrega	Al quitar una máquina de un grupo de entrega no se eliminará del catálogo de máquinas que el grupo de entrega utiliza. Puede quitar una máquina solamente cuando no haya ningún usuario conectado a ella. Active el modo de mantenimiento para evitar temporalmente la conexión de usuarios mientras la quita.
Eliminar	Cuando se elimina una máquina, los usuarios dejan de tener acceso a ella y esta se elimina del catálogo de máquinas. Antes de eliminar una máquina, asegúrese de contar con una copia de seguridad de todos los datos del usuario o de que esos datos ya no sean necesarios. Puede eliminar una máquina solamente cuando no haya ningún usuario conectado a ella. Active el modo de mantenimiento para impedir temporalmente la conexión de usuarios mientras la elimina.

---

Para acciones que implican el apagado de una máquina, si la máquina no se apaga en 10 minutos, se desconecta. Si Windows intenta instalar actualizaciones durante el cierre, existe el riesgo de que el equipo se apague antes de que se completen las actualizaciones.

### **Modificar la opción de almacenamiento**

Puede mostrar el estado de los servidores que se usan para almacenar datos de sistema operativo, datos temporales y datos personales (PvD) para las VM que usan esa conexión. También puede especificar qué servidores usar para el almacenamiento de cada tipo de datos.

1. Seleccione **Configuración > Alojamiento** en el panel de navegación de **Studio**.
2. Seleccione la conexión y, a continuación, seleccione **Modificar almacenamiento** en el panel **Acciones**.
3. En el panel izquierdo, seleccione el tipo de datos: sistema operativo, Personal vDisk, o datos temporales.
4. Seleccione o deje sin seleccionar las casillas de los dispositivos de almacenamiento para el tipo de datos seleccionado.
5. Haga clic en **OK**.

Cada dispositivo de almacenamiento en la lista incluye su nombre y su estado. Los valores del estado de almacenamiento son:

- **En uso:** El almacenamiento se está utilizando para crear máquinas.
- **Reemplazado:** El almacenamiento se usa solo para máquinas existentes. No se agregan nuevas máquinas a este almacenamiento.
- **Sin usar:** El almacenamiento no se está utilizando para crear máquinas.

Si deja sin marcar la casilla de un dispositivo que está actualmente **En uso**, su estado cambia a **Reemplazado**. Las máquinas ya existentes seguirán usándolo (y pueden escribir datos en él) por lo que es posible que esa ubicación se llene incluso aunque haya dejado de usarse para crear máquinas.

## Eliminar, cambiar el nombre o probar recursos

1. Seleccione **Configuración > Alojamiento** en el panel de navegación de **Studio**.
2. Seleccione el recurso y, a continuación, seleccione la entrada correspondiente en el panel **Acciones: Eliminar recursos, Cambiar nombre de recursos o Probar recursos**.

## Temporizadores de conexión

Puede usar configuraciones de directiva para configurar tres temporizadores de conexión:

- **Temporizador de duración máxima de conexión:** Determina la duración máxima de una conexión sin interrupciones entre un dispositivo de usuario y un escritorio virtual. Use las configuraciones de directiva **Temporizador de conexión de sesión** e **Intervalo de temporizador de conexión de sesiones**.
- **Temporizador de conexión inactiva:** Este parámetro determina la cantidad de tiempo que se mantiene la conexión sin interrupciones entre un dispositivo de usuario y un escritorio virtual, si el usuario no realiza entradas. Use las configuraciones de directiva **Temporizador de sesión inactiva** e **Intervalo de temporizador de sesiones inactivas**.
- **Temporizador de desconexión:** Este parámetro determina la cantidad de tiempo que un escritorio virtual desconectado y bloqueado puede permanecer bloqueado antes de que se cierre

la sesión. Use las configuraciones de directiva **Temporizador de sesión desconectada** e **Intervalo de temporizador de sesiones desconectadas**.

Al actualizar estos parámetros, compruebe que son coherentes en toda la implementación.

Consulte la documentación de configuraciones de directivas para obtener más información.

## Solución de problemas

Utilice la información de esta sección para solucionar problemas relacionados con las conexiones de host.

### Error de clave de acceso al agregar la URL de EC2 de AWS al recurso de alojamiento

En la pantalla del **nodo Alojamiento** de Citrix Studio, el hecho de agregar EC2 de AWS como conexión de alojamiento y especificar la clave de **API**, la clave secreta y el nombre de conexión genera un error SSL. Aparece un mensaje que indica “Se ha producido un error en la combinación de la clave de **API** y la clave secreta. Asegúrese de introducirlos correctamente”.

Este problema se produce por:

- utilizar el servidor proxy para conectarse a la red externa.
- utilizar otra conexión EC2 que tenga una conexión URL distinta del [servidor Amazon AWS](#).

En la pantalla del **nodo Alojamiento** de Studio, la cadena de la dirección predeterminada para una conexión de EC2 está codificada de forma rígida como `https://ec2.amazonaws.com`, que es una URL global de punto final. Si el servicio AWS no puede enrutar la URL del punto final a la que usted especifique, no se pueden verificar las claves de acceso, incluidas la ID de la clave de acceso y la clave de acceso secreta.

Para resolver este problema, agregue la conexión de EC con otra dirección URL o conéctese a Internet mediante un servidor proxy. Aparte, cree manualmente una conexión de alojamiento de EC2 mediante PowerShell en lugar de hacerlo mediante Citrix Studio:

1. Inicie PowerShell desde el host de DDC y cargue todos los módulos de Citrix mediante el comando `asnp Citrix`.
2. Configure las variables de entorno del servidor proxy y del puerto:

```
1 $server = "<PROXY_SERVER>"
2 $port = "<PROXY_SERVER_PORT>"
3 $options = "ProxyHost=$server,ProxyPort=$port"
4 <!--NeedCopy-->
```

Ejecute los siguientes comandos para agregar la conexión de alojamiento de EC2:

```
1 $hyp= New-Item -Path xdhyp:\Connections -AdminAddress "localhost" -Name
   "AWSEC2" -ConnectionType "AWS" -HypervisorAddress @[AWS URL](
   https://<AWS_URL>) -UserName "APIkey" -Password "Secret key" -
   Metadata @{
2   "Citrix_MachineManagement_Options" = $options }
3   -Persist
4 <!--NeedCopy-->
```

```
1 New-BrokerHypervisorConnection -HypHypervisorConnectionUid $hyp.
   HypervisorConnectionUid
2 <!--NeedCopy-->
```

Inicie Citrix Studio y compruebe la conexión de host para verificar la generación del sitio de EC2 de AWS.

## Caché de host local

April 19, 2024

Para que la base de datos del sitio de Citrix Virtual Apps and Desktops esté siempre disponible, Citrix recomienda empezar con una implementación de SQL Server con tolerancia a fallos que resulta de las prácticas recomendadas para la alta disponibilidad de Microsoft (Para ver las funcionalidades de alta disponibilidad de SQL Server que se admiten, consulte [Bases de datos](#).) Sin embargo, las interrupciones y los problemas de red pueden tener como resultado que los usuarios no puedan conectarse a sus aplicaciones o escritorios.

La función Caché de host local (LHC) permite que las operaciones de intermediación (broker) de las conexiones en un sitio continúen cuando se produce una interrupción. Se produce una interrupción cuando se interrumpe la conexión entre un Delivery Controller y la base de datos del sitio en un entorno local de Citrix. La función Caché de host local se activa cuando no se puede acceder a la base de datos del sitio durante 90 segundos.

A partir XenApp y XenDesktop 7.16, la Concesión de conexiones (una función de alta disponibilidad en versiones anteriores) se eliminó de XenApp y XenDesktop, y ya no está disponible.

## Contenido de datos

La Caché de host local incluye la siguiente información, que es un subconjunto de la información contenida en la base de datos principal:

- Identidades de los usuarios y los grupos que tienen derechos específicamente asignados a recursos publicados en el sitio.

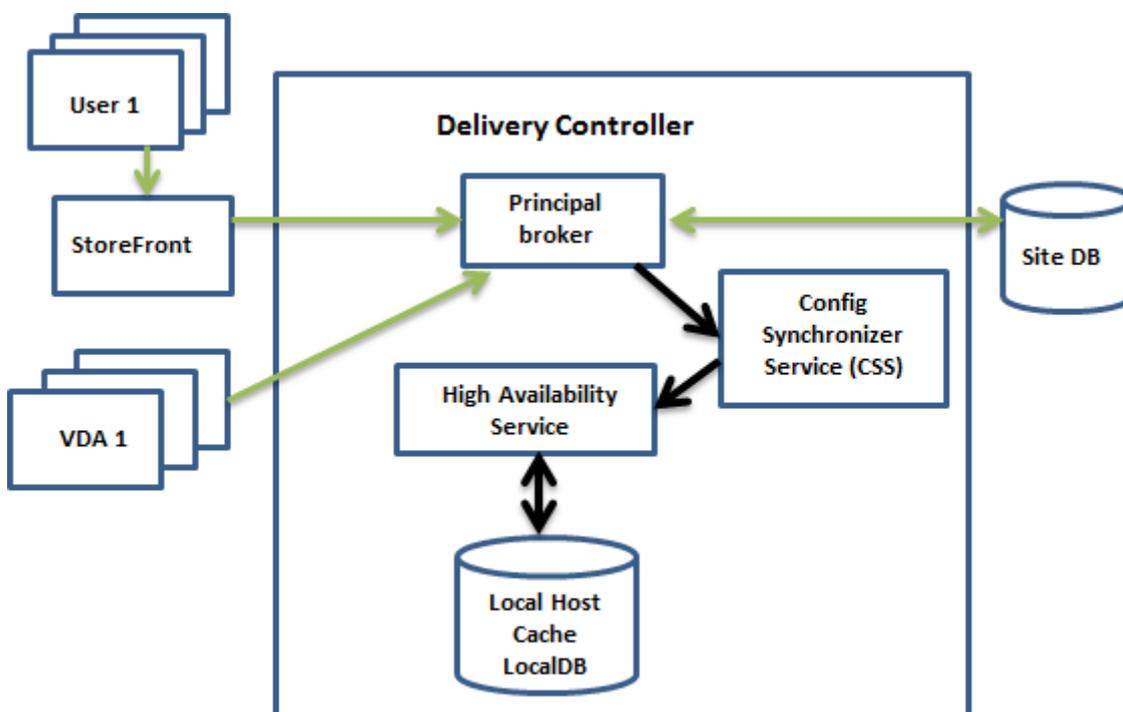
- Identidades de los usuarios que actualmente usan, o que han utilizado recientemente, recursos publicados en el sitio.
- Identidades de las máquinas VDA (incluidas las máquinas de acceso con Remote PC) configuradas en el sitio.
- Identidades (nombres y direcciones IP) de las máquinas cliente de Citrix Receiver que se utilizan activamente para conectarse a los recursos publicados.

También contiene información para las conexiones actualmente activas que se establecieron mientras la base de datos principal no estaba disponible:

- Resultados de todos los análisis de máquinas de punto final del cliente realizados por Citrix Receiver.
- Identidades de las máquinas de la infraestructura (tales como NetScaler Gateway y servidores de StoreFront) que intervienen en las operaciones del sitio.
- Fechas, horas y tipos de actividades recientes de los usuarios.

## Funcionamiento

En el siguiente gráfico, se muestran los componentes de Caché de host local y las rutas de comunicación que se establecen durante un funcionamiento normal.



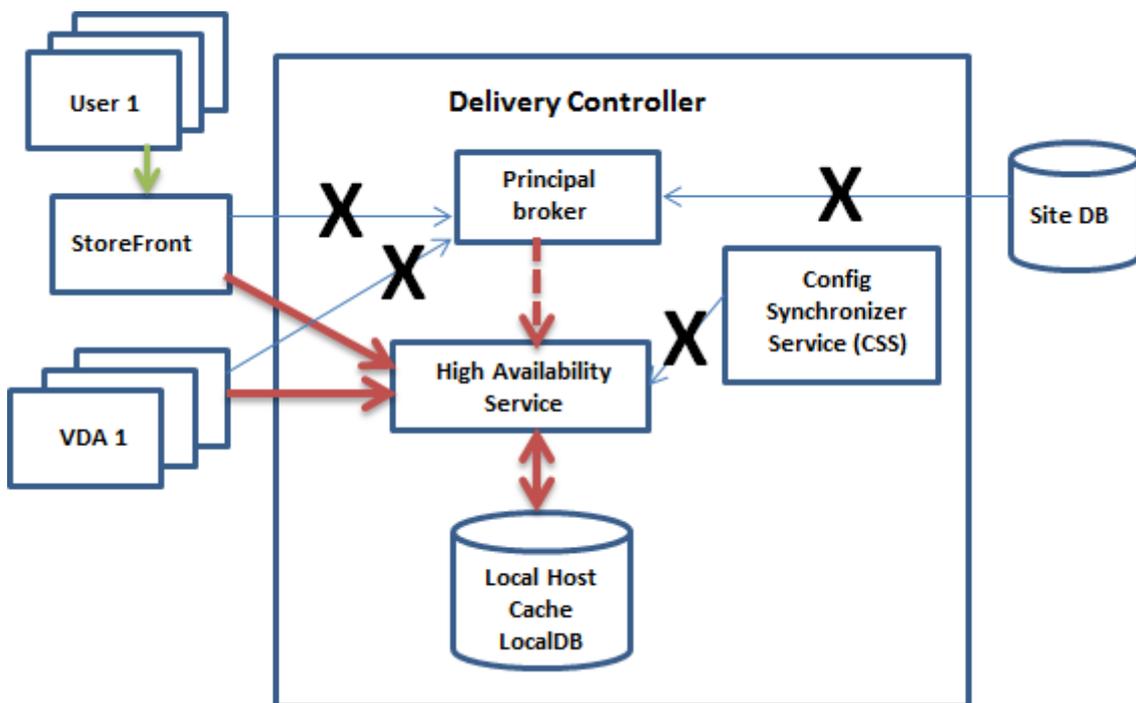
### Durante el funcionamiento habitual:

- El *broker principal* (Citrix Broker Service) en un Controller acepta las solicitudes de conexión provenientes de StoreFront, y se comunica con la base de datos del sitio para conectar usuarios

a los agentes VDA que están registrados en el Controller.

- Se comprueba periódicamente (un minuto después de la comprobación anterior) si se han realizado cambios en la configuración del broker principal. Esos cambios pueden haberse iniciado con acciones de PowerShell, de Studio (como modificar una propiedad del grupo de entrega) o del sistema (como las asignaciones de máquinas).
- Si se ha realizado algún cambio desde la última comprobación, el servicio Citrix Config Synchronizer Service (CSS) sincroniza (copia) información al servicio Citrix High Availability Service ubicado en el Controller (en parte de la documentación, el servicio High Availability Service se denomina broker secundario). Se copian todos los datos de configuración del broker, no solo los elementos que han cambiado desde la comprobación anterior. El servicio High Availability Service importa los datos en una base de datos LocalDB de Microsoft SQL Server Express ubicada en el Controller. El servicio CSS comprueba que la información de la base de datos LocalDB coincide con la información que hay en la base de datos del sitio. La base de datos LocalDB se crea con cada sincronización.
- Si no se han producido cambios desde la última comprobación, no se copian los datos.

En el siguiente gráfico, se muestran los cambios que se realizan en las rutas de comunicación si se interrumpe la conexión entre el broker principal y la base de datos del sitio:



#### Al principio de una interrupción del servicio:

- El broker principal ya no puede comunicarse con la base de datos del sitio y deja de escuchar para obtener información de StoreFront y VDA (marcado con una X en el gráfico). El broker principal indica al servicio High Availability Service que empiece a escuchar y a procesar solicitudes de conexión (marcado con una línea discontinua de color rojo en el gráfico). El servicio High

Availability Service descarta todas las llamadas provenientes del CSS.

- Cuando empieza la interrupción, el servicio High Availability Service no dispone de datos actuales de registro de agentes VDA, pero, en cuanto un VDA se comunica con él, comienza un proceso de rerregistro. Durante este proceso, el servicio High Availability Service también obtiene información de sesión actualizada acerca de ese VDA.
- Mientras el servicio High Availability Service gestiona las conexiones, el broker principal sigue supervisando la conexión a la base de datos del sitio. Cuando se restaura la conexión, el broker principal indica al High Availability Service que deje de escuchar para obtener la información de conexión. A continuación, el broker principal reanuda la intermediación. La próxima vez que el VDA se comunica con el broker principal, comienza un proceso de rerregistro. El servicio High Availability Service elimina toda información de registro de VDA que haya quedado de la interrupción anterior, y vuelve a actualizar la base de datos LocalDB con los cambios de configuración que ha recibido del servicio CSS.

La transición entre el modo normal y de interrupción no afecta a las sesiones existentes; solo afecta al inicio de sesiones nuevas.

En el caso improbable de que se inicie una interrupción durante una sincronización, la importación de ese momento se descarta y se utiliza la última configuración conocida.

El registro de eventos proporciona información sobre sincronizaciones e interrupciones del servicio. Consulte la siguiente sección “Supervisar” para obtener más información.

También puede empezar intencionadamente una interrupción; consulte la siguiente sección “Forzar una interrupción” para obtener más información sobre cómo y por qué hacerlo.

### **Sitios con varios Controllers**

Entre otras de sus tareas, CSS proporciona constantemente al servicio High Availability Service información sobre todos los Controllers de la zona (si su entorno no contiene varias zonas, esta acción afecta a todos los Controllers del sitio). Con esta información, cada High Availability Service obtiene datos de todos los demás servicios High Availability Service de su nivel.

Los servicios High Availability Service se comunican entre sí por un canal independiente. Utilizan una lista alfabética de nombres de dominio completo (FQDN) de las máquinas que están ejecutando para determinar (elegir) al High Availability Service que estará a cargo de intermediar las operaciones de la zona si se produce una interrupción. Durante la interrupción, todos los VDA vuelven a registrarse en el High Availability Service que se haya elegido. Los servicios High Availability Service de la zona que no hayan sido elegidos rechazarán las solicitudes entrantes de conexión y de registro que les envíen los agentes VDA.

Si un High Availability Service falla durante una interrupción, se elige otro High Availability Service para tomar el control, y los VDA se volverán a registrar en el High Availability Service recién elegido.

Durante una interrupción, si se reinicia un Controller:

- Si ese Controller no es el broker principal elegido, el reinicio no tiene repercusión.
- Si ese Controller es el broker principal elegido, se elegirá otro Controller, por lo que los VDA deberán volver a registrarse. Después de que el Controller reiniciado se encienda, se hace cargo automáticamente de la intermediación, por lo que los VDA deben volver a registrarse. En este caso, el rendimiento puede verse afectado durante los nuevos registros.

Si apaga un Controller durante las operaciones normales y lo enciende durante una interrupción, la función Caché de host local no se puede utilizar en ese Controller si este se elige como broker principal.

El registro de eventos proporciona información sobre las opciones elegidas. Consulte la sección siguiente “Supervisión”.

## **Requisitos y consideraciones de diseño**

No hay límites de tiempo impuestos para el funcionamiento en modo de interrupción. Sin embargo, debe restaurar el sitio a su funcionamiento normal lo más rápidamente posible.

## **Lo que no está disponible durante una interrupción y otras diferencias**

- No puede usar Studio ni ejecutar cmdlets de PowerShell.
- Host Service no puede proporcionar credenciales de hipervisor. Todas las máquinas están en el estado de energía desconocido (unknown) y no se pueden emitir operaciones de administración de energía. No obstante, las máquinas virtuales del host que estén encendidas se pueden utilizar para las solicitudes de conexión.
- Una máquina asignada solo se puede usar si la asignación se dio durante el funcionamiento normal. No se pueden realizar asignaciones nuevas durante una interrupción del servicio.
- No se puede configurar ni inscribir automáticamente las máquinas de acceso con Remote PC. En cambio, las máquinas que se inscribieron y configuraron durante el funcionamiento normal se pueden usar.
- Si los recursos están en zonas diferentes, es posible que los usuarios de aplicaciones y escritorios alojados en servidor superen la cantidad de sesiones indicadas en el límite configurado de sesiones.
- Los usuarios solo pueden iniciar aplicaciones y escritorios desde los VDA registrados en la zona que contiene el High Availability Service actualmente activo o elegido. Durante una interrupción, no se admiten inicios entre zonas (desde un High Availability Service de una zona en un VDA de otra zona).

- Si se produce una interrupción de la base de datos del sitio antes de que comience un reinicio programado para los agentes VDA de un grupo de entrega, los reinicios comienzan cuando finaliza la interrupción del servicio. Esto puede provocar resultados inesperados. Para obtener más información, consulte [Reinicios programados que se retrasan por una interrupción de la base de datos](#).
- Las [restricciones por etiquetas](#) en las que se utilizan etiquetas para designar zonas no se admiten para el inicio de sesiones. Cuando se configuran tales restricciones por etiquetas y la opción de [comprobación avanzada de estado](#) de un almacén de StoreFront está habilitada, es posible que las sesiones no consigan iniciarse de forma intermitente.

La función “Caché de host local” se admite para aplicaciones y escritorios alojados en servidores y escritorios estáticos (asignados).

De forma predeterminada, los VDA de escritorio con administración de energía en grupos de entrega agrupados (creados por MCS o Citrix Provisioning) que tienen la propiedad `ShutdownDesktopsAfterUse` habilitada no están disponibles para nuevas conexiones durante eventos de caché de host local. Puede cambiar este valor predeterminado para permitir que esos escritorios se usen durante la caché de host local. Sin embargo, no podrá confiar en la administración de energía durante la interrupción (la administración de energía se reanuda una vez reanudadas las operaciones normales). Además, esos escritorios podrían contener datos del usuario anterior, porque no se han reiniciado.

Para reemplazar el comportamiento predeterminado, debe habilitarlo en todo el sitio y para cada grupo de entrega afectado. Ejecute los siguientes cmdlets de PowerShell.

```
Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true Set-BrokerDesktopGroup -Name "name"-ReuseMachinesWithoutShutdownInOutage $true
```

Habilitar esta función en el sitio y los grupos de entrega no afecta al funcionamiento de la propiedad configurada “ShutdownDesktopsAfterUse” durante las operaciones normales. Cuando esta función está habilitada, los VDA no se reinician automáticamente una vez finalizado el evento del LHC. Los VDA de escritorio con administración de energía de los grupos de entrega agrupados pueden retener los datos de las sesiones anteriores hasta que se reinicie el VDA. Esto puede ocurrir cuando un usuario cierra sesión en el VDA durante operaciones ajenas al LHC o cuando el reinicio se desencadena manualmente.

**Importante:**

Si no se habilitan `ReuseMachinesWithoutShutdownInOutageAllowed` al nivel del sitio ni `ReuseMachinesWithoutShutdownInOutage` al nivel del grupo de entrega, no se podrán iniciar sesiones en los VDA de escritorio con administración de energía desde grupos de entrega agrupados durante eventos de caché de host local.

### **Consideraciones sobre tamaño de RAM**

El servicio LocalDB puede usar aproximadamente 1,2 GB de RAM (1 GB máximo para la caché de la base de datos, más 200 MB para ejecutar LocalDB de SQL Server Express). El servicio High Availability Service puede usar hasta 1 GB de RAM si la interrupción es duradera y se producen muchos inicios de sesión (por ejemplo, 12 horas con 10 000 usuarios). Estos requisitos de memoria son adicionales a los requisitos de memoria RAM habituales para el Controller. Por lo tanto, es posible que necesite aumentar la cantidad total de RAM.

Tenga en cuenta que, si usa una base de datos de SQL Server Express como la base de datos del sitio, el servidor tendrá dos procesos sqlserver.exe.

### **Consideraciones sobre la configuración de sockets y núcleo de CPU**

La configuración de la CPU de un Controller, especialmente la cantidad de núcleos disponibles para la base de datos LocalDB de SQL Server Express, afecta directamente al rendimiento que tendrá la Caché de host local, incluso más que la asignación de memoria. Este consumo de recursos de CPU solo se ha observado durante el periodo de interrupción cuando la base de datos no está disponible y el servicio High Availability Service está activo.

A pesar de que LocalDB pueda usar varios núcleos (hasta 4), está limitada a solamente un socket. Agregar más sockets no mejorará el rendimiento (por ejemplo, tener 4 sockets con 1 núcleo cada uno). En vez de ello, Citrix recomienda usar varios sockets con varios núcleos. En las pruebas llevadas a cabo por Citrix, una configuración de 2x3 (2 sockets, 3 núcleos) proporciona un mejor rendimiento que las configuraciones 4x1 y 6x1.

### **Consideraciones sobre almacenamiento**

LocalDB aumenta de tamaño a medida que los usuarios acceden a los recursos durante una interrupción. Por ejemplo, durante una prueba de inicio y cierre de sesión en la que se ejecutan 10 inicios de sesión por segundo, la base de datos aumentó de tamaño 1 MB cada 2 o 3 minutos. Cuando se reanuda el funcionamiento normal, la base de datos local se vuelve a crear y el espacio se devuelve. No obstante, debe haber suficiente espacio en la unidad donde está instalada LocalDB para permitir el aumento del tamaño de la base de datos durante una interrupción. La Caché de host local también conlleva E/S adicional durante una interrupción: aproximadamente 3 MB de escrituras por segundo, con varios cientos de miles de lecturas.

### **Consideraciones sobre rendimiento**

Durante una interrupción, un solo High Availability Service se encarga de todas las conexiones, por lo que, en los sitios (o las zonas) con carga equilibrada entre varios Controllers durante el

funcionamiento normal, es posible que el High Availability Service elegido deba gestionar muchas más solicitudes durante una interrupción que en una situación normal. Por lo tanto, la necesidad de CPU será mucho mayor. Cada High Availability Service del sitio (zona) debe ser capaz de gestionar la carga adicional que impone LocalDB y todos los VDA afectados porque el High Availability Service elegido durante una interrupción podría cambiar.

Límites de VDI:

- En una implementación de VDI de zona única, se puede controlar hasta 10 000 agentes VDA durante una interrupción.
- En una implementación de VDI de varias zonas, se puede controlar hasta 10 000 agentes VDA por zona durante una interrupción, hasta un máximo de 40 000 agentes VDA en el sitio. Por ejemplo: cada uno de los siguientes sitios puede controlarse de forma eficaz durante una interrupción:
  - Un sitio de cuatro zonas, cada zona con 10 000 agentes VDA.
  - Un sitio con siete zonas, una zona con 10 000 agentes VDA y seis zonas con 5000 agentes VDA.

Durante una interrupción, la administración de carga dentro del sitio puede verse afectada. Es posible que se superen los patrones de carga (especialmente, las reglas de recuento de sesiones).

Mientras todos los VDA vuelven a registrarse en un High Availability Service, este puede no disponer de información completa sobre las sesiones actuales. Por lo tanto, si un usuario solicita conectarse durante ese intervalo, puede que se inicie otra sesión, aunque la reconexión a una sesión existente fuera posible. Este intervalo (mientras el “nuevo” High Availability Service obtiene la información de sesión de todos los VDA durante el proceso de rerregistro) no se puede evitar. Tenga en cuenta que las sesiones que están conectadas cuando se inicia una interrupción no se verán afectadas durante ese intervalo de transición, pero las sesiones nuevas y las reconexiones sí pueden verse afectadas.

Este intervalo se da siempre que los VDA deben volver a registrarse:

- Comienza una interrupción: Al migrar desde un broker principal a un High Availability Service.
- Fallo del servicio High Availability Service durante una interrupción: Al migrar desde un servicio High Availability Service que falló al servicio High Availability Service recién elegido.
- Recuperación de una interrupción: Cuando se reanudan las operaciones normales y el broker principal retoma el control.

Puede reducir el intervalo si disminuye el valor de Registro HeartbeatPeriodMs del protocolo del broker de Citrix (el valor predeterminado es 600 000 ms, que equivale a 10 minutos). Este valor de latido es el doble del intervalo que usa el VDA para los pings, por lo que el valor predeterminado da como resultado un ping cada 5 minutos.

Por ejemplo: este comando cambia el latido a cinco minutos (300 000 milisegundos), lo que resulta en un ping cada 2 minutos y medio:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name  
HeartbeatPeriodMs -PropertyType DWORD -Value 300000
```

Tenga cuidado al cambiar el valor de latido. Aumentar la frecuencia resulta en una mayor carga en los Controllers durante los modos de funcionamiento normal y el de interrupción.

El intervalo no se puede eliminar por completo, independientemente de lo rápido que se registren los VDA.

El tiempo que tarda la sincronización entre servicios High Availability Service aumenta con la cantidad de objetos (como agentes VDA, aplicaciones, grupos). Por ejemplo, sincronizar 5000 VDA podría llevar diez minutos o más. Consulte Supervisión para obtener información sobre las entradas de sincronización en el registro de eventos.

### **Diferencias con versiones de XenApp 6.x**

Aunque esta implementación de Caché de host local comparte el nombre con la funcionalidad Caché de host local de XenApp 6.x y versiones anteriores de XenApp, existen entre ellas diferencias importantes. Esta implementación es más sólida e inmune al daño. Los requisitos de mantenimiento se han minimizado; por ejemplo, se ha eliminado la necesidad de comandos dsmaint periódicos. Técnicamente, esta implementación de Caché de host local es completamente diferente.

### **Administrar la Caché de host local**

Para que la “Caché de host local” funcione correctamente, la directiva de ejecución de PowerShell en cada Controller debe establecerse en RemoteSigned, Unrestricted o Bypass.

### **LocalDB de SQL Server Express**

La base de datos LocalDB de Microsoft SQL Server Express que usa la Caché de host local se instala automáticamente al instalar un Controller o actualizarlo desde una versión anterior a 7.9. No se necesita mantenimiento de administrador para la LocalDB. Only the High Availability Service communicates with this database. No puede usar cmdlets de PowerShell para realizar ningún cambio en esta base de datos. La LocalDB no se puede compartir entre los Controllers.

La base de datos LocalDB de SQL Server Express se instala independientemente de si la Caché de host local está habilitada.

Para impedir la instalación, instale o actualice el Controller con el comando XenDesktopServer-Setup.exe e incluya la opción `/exclude "Local Host Cache Storage (LocalDB)"`. No obstante, tenga en cuenta que la función “Caché de host local” no funcionará sin la base de datos, y no se puede usar otra base de datos con el servicio High Availability Service.

Instalar esta base de datos LocalDB no influye en si instala SQL Server Express para usarla como la base de datos del sitio.

Para obtener información sobre cómo reemplazar una versión anterior de SQL Server Express LocalDB por una versión más reciente, consulte [Reemplazar SQL Server Express LocalDB](#).

### **Parámetros predeterminados después de la instalación y la actualización de los productos**

La Caché de host local se habilita durante una nueva instalación de Citrix Virtual Apps and Desktops (7.16 como versión mínima). Después de una actualización (a la versión 7.16 o posterior), la Caché de host local se habilita si hay menos de 10 000 agentes VDA en toda la implementación.

### **Habilitar o inhabilitar la Caché de host local**

- Para habilitar la Caché de host local, escriba:

```
Set-BrokerSite -LocalHostCacheEnabled $true
```

Para saber si la Caché de host local está habilitada, escriba:

```
Get-BrokerSite
```

Compruebe que la propiedad LocalHostCacheEnabled es True.

- Para inhabilitar la Caché de host local, escriba:

```
Set-BrokerSite -LocalHostCacheEnabled $false
```

Recuerde: A partir de XenApp y XenDesktop 7.16, la concesión de conexiones (la función que precedió a la Caché de host local desde la versión 7.6) se ha eliminado del producto y ya no está disponible.

### **Verificar que la Caché de host local está funcionando**

Para verificar que la Caché de host local está configurada y funciona correctamente:

- Compruebe que las importaciones de sincronización se completan correctamente. Verifique los registros de eventos.
- Asegúrese de que la base de datos LocalDB de SQL Server Express se ha creado en cada Delivery Controller. Eso confirma que el servicio de alta disponibilidad High Availability Service puede tomar el control, si fuera necesario.
- En el servidor de Delivery Controller, vaya a C:\Windows\ServiceProfiles\NetworkService.
- Verifique que se hayan creado HaDatabaseName.mdf y HaDatabaseName\_log.ldf.

- Fuerce una interrupción en los Delivery Controllers. Una vez que haya verificado que la Caché de host local funciona, recuerde volver a colocar todos los Controllers de nuevo en el modo normal. Este proceso puede tardar aproximadamente 15 minutos y, gracias a él, se evitan avalanchas de registros de VDA.

## Forzar una interrupción del servicio

Puede que le convenga forzar una interrupción de la base de datos.

- Si la red tiene altibajos repetidos. Forzar una interrupción hasta que se resuelvan los problemas de red impide una transición fluida entre los modos normal y de interrupción.
- Para probar un plan de recuperación ante desastres.
- Al cambiar o mantener el servidor de la base de datos del sitio.

Para forzar una interrupción, modifique el Registro de cada servidor que contiene un Delivery Controller. En `HKLM\Software\Citrix\DesktopServer\LHC`, establezca `OutageModeForced` como `REG_DWORD` en 1. Esto indica al broker que introduzca el modo de interrupción independientemente del estado de la base de datos. Establecer este valor en 0 saca al servidor del modo de interrupción.

## Supervisar

Los registros de eventos indican cuándo tienen lugar las sincronizaciones y las interrupciones.

### Config Synchronizer Service:

Durante el funcionamiento normal, pueden ocurrir los siguientes eventos cuando CSS copia, exporta la configuración del broker y la importa a la LocalDB mediante High Availability Service.

- 503: Se ha encontrado un cambio en la configuración del broker principal, por lo que se inicia un proceso de importación.
- 504: La configuración del broker se ha copiado, exportado y, a continuación, importado a la LocalDB.
- 505: Ha fallado una importación a la LocalDB; consulte más adelante para obtener más información.
- 507: Se ha abandonado una importación debido a una interrupción pendiente. Si se inicia una interrupción durante una sincronización, la importación de ese momento se descarta y se utiliza la última configuración conocida.
- 510: No se recibieron datos de configuración del servicio de configuración procedentes del servicio de configuración principal.
- 517: Hubo un problema de comunicación con el broker principal.

- 518: Se ha abortado el script de Config Sync porque el Broker secundario (High Availability Service) no se está ejecutando.

#### **High Availability Service (Servicio de alta disponibilidad):**

- 3502: Se ha producido una interrupción y el servicio High Availability Service está llevando a cabo operaciones de intermediación.
- 3503: Se ha resuelto una interrupción y se ha reanudado el funcionamiento normal.
- 3504: Indica el servicio High Availability Service elegido, además de otros servicios que hayan participado en la elección.

### **Solucionar problemas técnicos**

Existen varias herramientas de solución de problemas disponibles cuando falla una importación de sincronización a la LocalDB y se publica un evento 505.

**Rastreo CDF:** Contiene opciones para los módulos ConfigSyncServer y BrokerLHC. Esas opciones, junto con otros módulos de broker, identificarán probablemente el problema.

**Informe:** Puede generar y proporcionar un informe que detalle el punto del error. Esta funcionalidad de informe afecta a la velocidad de sincronización, por lo que Citrix recomienda inhabilitarla cuando no se use.

Para habilitar y generar un informe de rastreo de CSS, escriba:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -PropertyType DWORD -Value 1
```

El informe HTML se publica en C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerCon

Una vez generado el informe, inhabilite la funcionalidad de informes:

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -Value 0
```

**Exportar la configuración de broker:** Proporciona la configuración exacta con fines de depuración.

```
Export-BrokerConfiguration | Out-File <file-pathname>
```

Por ejemplo, `Export-BrokerConfiguration | Out-File C:\\BrokerConfig.xml`.

### **Administrar las claves de seguridad**

June 27, 2024

**Nota:**

Debe utilizar esta función en combinación con StoreFront 1912 LTSR CU2 o una versión posterior.

Esta función permite especificar que solo las máquinas StoreFront y Citrix Gateway aprobadas se comuniquen con los Delivery Controllers de Citrix. Después de habilitar esta función, se bloquearán todas las solicitudes que no contengan la clave. Utilice esta función para agregar una capa adicional de seguridad y protegerse contra ataques que se originen en la red interna.

He aquí un flujo de trabajo general para utilizar esta función:

1. Habilite Studio para mostrar los parámetros de las funciones.
2. Configure los parámetros de su sitio (use la consola de Studio o PowerShell).
3. Configure los parámetros en StoreFront (use PowerShell).
4. Configure los parámetros en Citrix ADC (use PowerShell).

## Habilitar Studio para mostrar los parámetros de las funciones

De forma predeterminada, los parámetros de las claves de seguridad están ocultos en Studio. Para permitir que Studio los muestre, utilice el SDK de PowerShell de esta manera:

Para habilitarlo, siga estos pasos:

1. Ejecute el SDK de PowerShell remoto de Citrix Virtual Apps and Desktops
2. En una ventana de comandos, ejecute los siguientes comandos:
  - `Add-PSSnapIn Citrix*`. Este comando agrega los complementos de Citrix.
  - `Set-ConfigSiteMetadata -Name "Citrix_DesktopStudio_SecurityKeyManagemem" -Value "True"`

Para obtener más información sobre el SDK de PowerShell remoto, consulte [SDK](#) y [API](#).

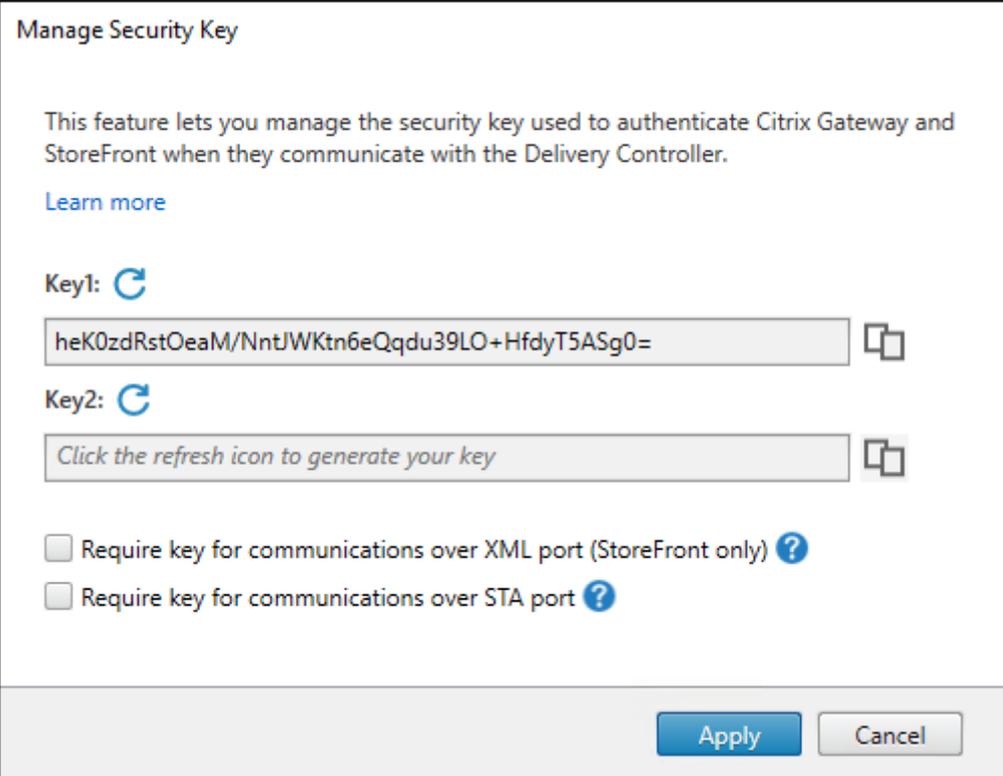
## Configurar los parámetros de su sitio

Puede configurar los parámetros en Studio mediante la consola de Studio o PowerShell.

### Usar la consola de Studio

Después de habilitar Studio para que muestre los parámetros de las funciones, vaya a **Studio > Configuración > Administrar clave de seguridad**. Es posible que deba hacer clic en **Actualizar** para que aparezca la opción **Administrar clave de seguridad**.

La ventana **Administrar clave de seguridad** aparece después de hacer clic en **Administrar clave de seguridad**.



Manage Security Key

This feature lets you manage the security key used to authenticate Citrix Gateway and StoreFront when they communicate with the Delivery Controller.

[Learn more](#)

Key1: 

heK0zdRstOeaM/NntJWKtn6eQqdu39LO+HfdyT5ASg0= 

Key2: 

Click the refresh icon to generate your key 

Require key for communications over XML port (StoreFront only) 

Require key for communications over STA port 

**Apply** **Cancel**

**Importante:**

- Hay dos claves disponibles para uso. Puede utilizar la misma clave o claves diferentes para las comunicaciones a través de los puertos XML y STA. Le recomendamos usar solo una tecla a la vez. La clave no utilizada solo se utiliza para la rotación de claves.
- No haga clic en el icono de actualización para actualizar la clave que ya está en uso. Si lo hace, se producirá una interrupción del servicio.

Haga clic en el icono de actualización para generar nuevas claves.

**Requerir clave para las comunicaciones a través del puerto XML (solo para StoreFront).** Si se selecciona, se necesita una clave para autenticar las comunicaciones a través del puerto XML. StoreFront se comunica con Citrix Cloud a través de este puerto. Para obtener información acerca de cómo cambiar el puerto XML, consulte el artículo [CTX127945](#) de Knowledge Center.

**Requerir clave para las comunicaciones a través del puerto STA.** Si se selecciona, se necesita una clave para autenticar las comunicaciones a través del puerto STA. Citrix Gateway y StoreFront se comunican con Citrix Cloud a través de este puerto. Para obtener información sobre cómo cambiar el puerto STA, consulte el artículo [CTX101988](#) de Knowledge Center.

Después de aplicar los cambios, haga clic en **Cerrar** para salir de la ventana **Administrar clave de seguridad**.

## Usar PowerShell

Estos son los pasos en PowerShell equivalentes a las operaciones en Studio.

1. Ejecute el SDK de PowerShell remoto de Citrix Virtual Apps and Desktops
2. En una ventana de comandos, ejecute el siguiente comando:
  - `Add-PSSnapIn Citrix*`
3. Ejecute los siguientes comandos para generar una clave y configurar Key1:
  - `New-BrokerXmlServiceKey`
  - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`
4. Ejecute los siguientes comandos para generar una clave y configurar Key2:
  - `New-BrokerXmlServiceKey`
  - `Set-BrokerSite -XmlServiceKey2 <the key you generated>`
5. Ejecute uno o estos dos comandos para habilitar el uso de una clave en la autenticación de comunicaciones:
  - Para autenticar las comunicaciones a través del puerto XML:
    - `Set-BrokerSite -RequireXmlServiceKeyForNFuse $true`
  - Para autenticar las comunicaciones a través del puerto STA:
    - `Set-BrokerSite -RequireXmlServiceKeyForSta $true`

Consulte la ayuda de los comandos de PowerShell para ver instrucciones y sintaxis.

## Configurar los parámetros en StoreFront

Una vez completada la configuración en Studio, debe configurar los parámetros relevantes en StoreFront mediante PowerShell.

En el servidor de StoreFront, ejecute estos comandos de PowerShell:

---

Para configurar la clave para las comunicaciones a través del puerto XML, utilice el comando	<a href="https://developer-docs.citrix.com/es-es/storefront-powershell-sdk/current-release/Set-STFStoreFarm.html">https://developer-docs.citrix.com/es-es/storefront-powershell-sdk/current-release/Set-STFStoreFarm.html</a> . Por ejemplo
--	---

---

```
1 $store = Get-STFStoreService -VirtualPath [Path to store]
2 $farm = Get-STFStoreFarm -StoreService $store -FarmName [Resource feed name]
```

```
3 Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true -  
  XMLValidationSecret [secret]  
4 <!--NeedCopy-->
```

Introduzca los valores adecuados para los siguientes parámetros:

- Path to store
- Resource feed name
- secret

Para configurar la clave para las comunicaciones a través del puerto STA, utilice los comandos `New-STFSecureTicketAuthority` y `Set-STFRoamingGateway`. Por ejemplo:

```
1 $gateway = Get-STFRoamingGateway -Name [Gateway name]  
2 $sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL] -  
  StaValidationEnabled $true -StaValidationSecret [secret]  
3 $sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL] -  
  StaValidationEnabled $true -StaValidationSecret [secret]  
4 Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs  
  $sta1,$sta2  
5 <!--NeedCopy-->
```

Introduzca los valores adecuados para los siguientes parámetros:

- Gateway name
- STA URL
- Secret

Consulte la ayuda de los comandos de PowerShell para ver instrucciones y sintaxis.

## Configurar los parámetros en Citrix ADC

### Nota:

No es necesario configurar esta función en Citrix ADC, a no ser que utilice Citrix ADC como puerta de enlace. Si utiliza Citrix ADC, siga los pasos que se indican a continuación.

1. Asegúrese de que ya está implementada la siguiente configuración de requisitos previos:

- Se configuran las siguientes direcciones IP relacionadas con Citrix ADC.
  - Dirección IP de administración (NSIP) de Citrix ADC para acceder a la consola de Citrix ADC. Para obtener más información, consulte [Configurar la dirección IP de NetScaler](#).



### Citrix ADC IP Address

If you change the Citrix ADC IP address and subnet mask, click **Reboot** for the changes to become effective. Citrix recommends that you change the default administrator (nsroot) password.

Citrix ADC IP Address\*

Netmask\*

Change Administrator Password

**Done** Back

- Dirección IP de subred (SNIP) para permitir la comunicación entre el dispositivo Citrix ADC y los servidores back-end. Para obtener más información, consulte [Configurar direcciones IP de subred](#).
- Dirección IP virtual de Citrix Gateway y dirección IP virtual del equilibrador de carga para iniciar sesión en el dispositivo ADC para el lanzamiento de sesiones. Para obtener más información, consulte [Crear un servidor virtual](#).



### Subnet IP Address

A subnet IP address is used by the Citrix ADC to communicate with the backend servers. Citrix ADC uses this subnet IP address as a source IP address to proxy the client connections as well as to send monitor probes to check the health of the backend servers.

The infographic shows the usage of SNIP in client server communication.

Depending on your network topology, you might have to configure additional subnet IP addresses.

For more information about subnet IP addresses, [click here](#).

The screenshot shows a configuration form with two input fields. The first field is labeled 'Subnet IP Address\*' and is empty, with a red error message 'Please enter value' to its right. The second field is labeled 'Netmask\*' and contains the value '255 . 255 . 255 . 0'. At the bottom of the form are two buttons: 'Done' and 'Back'.

- Los modos y las funciones requeridos en el dispositivo Citrix ADC están habilitados.
  - Para habilitar los modos, en la GUI de Citrix ADC vaya a **System > Settings > Configure Mode**.
  - Para habilitar las funciones, en la GUI de Citrix ADC vaya a **System > Settings > Configure Basic Features**.
- Se han completado las configuraciones relacionadas con los certificados.
  - Se crea la solicitud de firma de certificado (CSR). Para obtener más información, consulte [Crear un certificado](#).

## ← Create RSA Key

Key Filename\*

Choose File ▾ SSLTest ⓘ

Key Size(bits)\*

2048 ▾

Public Exponent Value\*

F4 ▾

Key Format\*

PEM ▾

PEM Encoding Algorithm

▾

PEM Passphrase

▾

Confirm PEM Passphrase

▾

PKCS8

Create Close

- Los certificados de CA y del servidor y los certificados raíz están instalados. Para obtener más información, consulte [Instalación, enlace y actualizaciones](#).

## ← Install Server Certificate

Certificate-Key Pair Name\*  
 ⓘ

Certificate File Name\*  
 CSR\_DER ⓘ

Key File Name  
 ns-server.key ⓘ

Notify When Expires

---

2 SNMP Trap destination found.

Notification Period

## ← Install CA Certificate

Certificate-Key Pair Name\*  
 ⓘ

Certificate File Name\*  
 ns-server.cert ⓘ

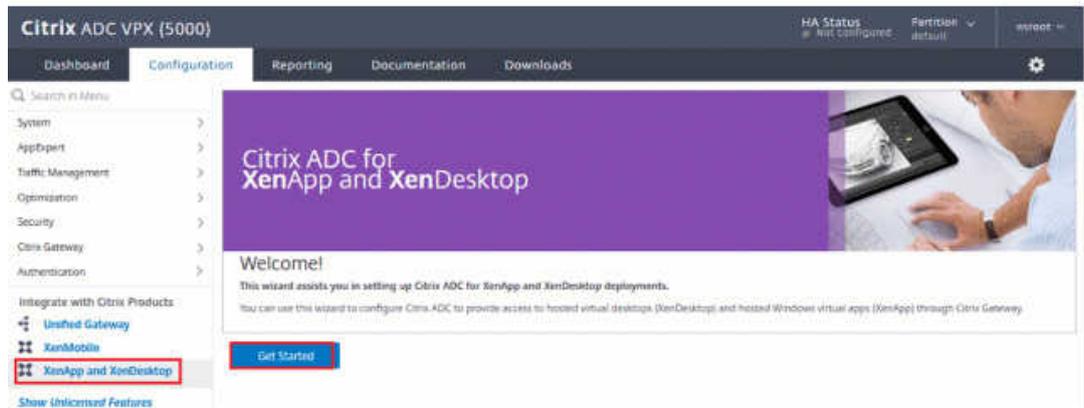
Notify When Expires

---

2 SNMP Trap destination found.

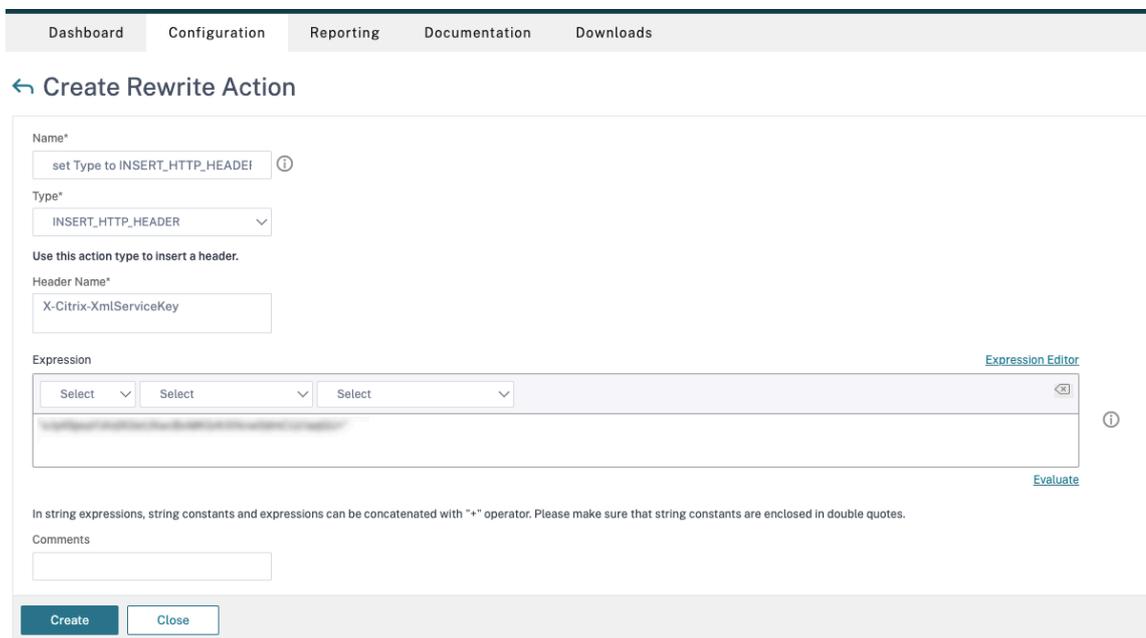
Notification Period

- Se ha creado una conexión de Citrix Gateway para Citrix Virtual Desktops. Pruebe la conectividad. Para ello, haga clic en el botón **Test STA Connectivity** para confirmar que los servidores virtuales están conectados. Para obtener más información, consulte [Configurar Citrix ADC para Citrix Virtual Apps and Desktops](#).



2. Agregue una acción de reescritura. Para obtener más información, consulte [Configurar una acción de reescritura](#).

- a) Vaya a **AppExpert > Reescribir > Acciones**.
- b) Haga clic en **Add** para agregar una acción de reescritura. Puede asignar a la acción el nombre “set Type to INSERT\_HTTP\_HEADER”.



- a) En **Type**, seleccione **INSERT\_HTTP\_HEADER**.
- b) En **Header Name**, escriba X-Citrix-XmlServiceKey.
- c) En **Expression**, agregue `<XmlServiceKey1 value>` con las comillas. Puede copiar el valor XmlServiceKey1 desde la configuración de Desktop Delivery Controller.

```
PS C:\Users\tyadmin> Get-BrokerSite
BaseOU :
BrokerServiceGroupUid :
ColorDepth :
ConfigLastChangeTime :
ConfigurationServiceGroupUid :
ConnectionLeasingEnabled :
DefaultMinimumFunctionalLevel :
DesktopGroupIconUid :
DnsResolutionEnabled :
IsSecondaryBroker :
LicenseEdition :
LicenseGraceSessionsRemaining :
LicenseModel :
LicenseServerName :
LicenseServerPort :
LicensedSessionsActive :
LicensingBurnIn :
LicensingBurnInDate :
LicensingGraceHoursLeft :
LicensingGracePeriodActive :
LicensingOutOfBoxGracePeriodActive :
LocalHostCacheEnabled :
MetadataMap :
Name :
PeakConcurrentLicenseUsers :
RequireXmlServiceKeyForNFuse :
RequireXmlServiceKeyForSta :
ReuseMachinesWithoutShutdownInOutageAllowed :
SecureIcaRequired :
TotalUniqueLicenseUsers :
TrustManagedAnonymousXmlServiceRequests :
TrustRequestsSentToTheXmlServicePort :
UseVerticalScalingForRdsLaunches :
XmlServiceKey1 :
XmlServiceKey2 :
```

3. Agregue una directiva de reescritura. Para obtener más información, consulte [Configurar una directiva de reescritura](#).
  - a) Vaya a **AppExpert > Reescribir > Directivas**.
  - b) Haga clic en **Agregar** para agregar una directiva.

Dashboard Configuration Reporting Documentation Downloads

### ← Create Rewrite Policy

Name\*  
DDCPolicy ⓘ

Action\*  
set Type to INSERT\_HTTP\_HEADER ⓘ

Configure Assignments  
Configure Rewrite Actions

Log Action  
Add Edit ⓘ

Undefined-Result Action\*  
-Global-undefined-result-action-

Expression\* ⓘ  
Expression Editor  
Select Select Select  
HTTP.REQ.IS\_VALID  
Evaluate

Comments ⓘ

Create Close

- a) En **Action**, seleccione la acción creada en el paso anterior.
  - b) En **Expression**, agregue HTTP.REQ.IS\_VALID.
  - c) Haga clic en **Aceptar**.
4. Configure el equilibrio de carga. Debe configurar un servidor virtual de equilibrio de carga por cada servidor STA. En caso contrario, no se iniciarán las sesiones.

Para obtener más información, consulte [Configurar el equilibrio de carga básico](#).

- a) Cree un servidor virtual de equilibrio de carga.
  - Vaya a **Traffic Management > Load Balancing > Servers**.
  - En la página **Virtual Servers**, haga clic en **Add**.

← Load Balancing Virtual Server

**Basic Settings**

Create a virtual server by specifying a name, an IP address, a port, and a protocol type. If an application is accessible from the Internet, the virtual server IP (VIP) address is a public IP address; if the application is accessible only from the local area network (LAN) or wide area network (WAN), the VIP is usually a private (RFC 1918) IP address. You can configure multiple virtual servers to receive client requests, thereby increasing the availability of resources to process client requests.

Name\*  
 ⓘ

Protocol\*

IP Address Type\*  
 ⓘ

IP Address\*  
 ⓘ

Port\*

▶ More

- En **Protocol**, seleccione **HTTP**.
- Agregue la dirección IP virtual de equilibrio de carga y, en **Port**, seleccione **80**.
- Haga clic en **Aceptar**.

b) Cree un servicio de equilibrio de carga.

- Vaya a **Traffic Management > Load Balancing > Services**.

← Load Balancing Service

**Basic Settings**

Service Name\*  
 ⓘ

New Server  Existing Server

Server\*

Protocol\*

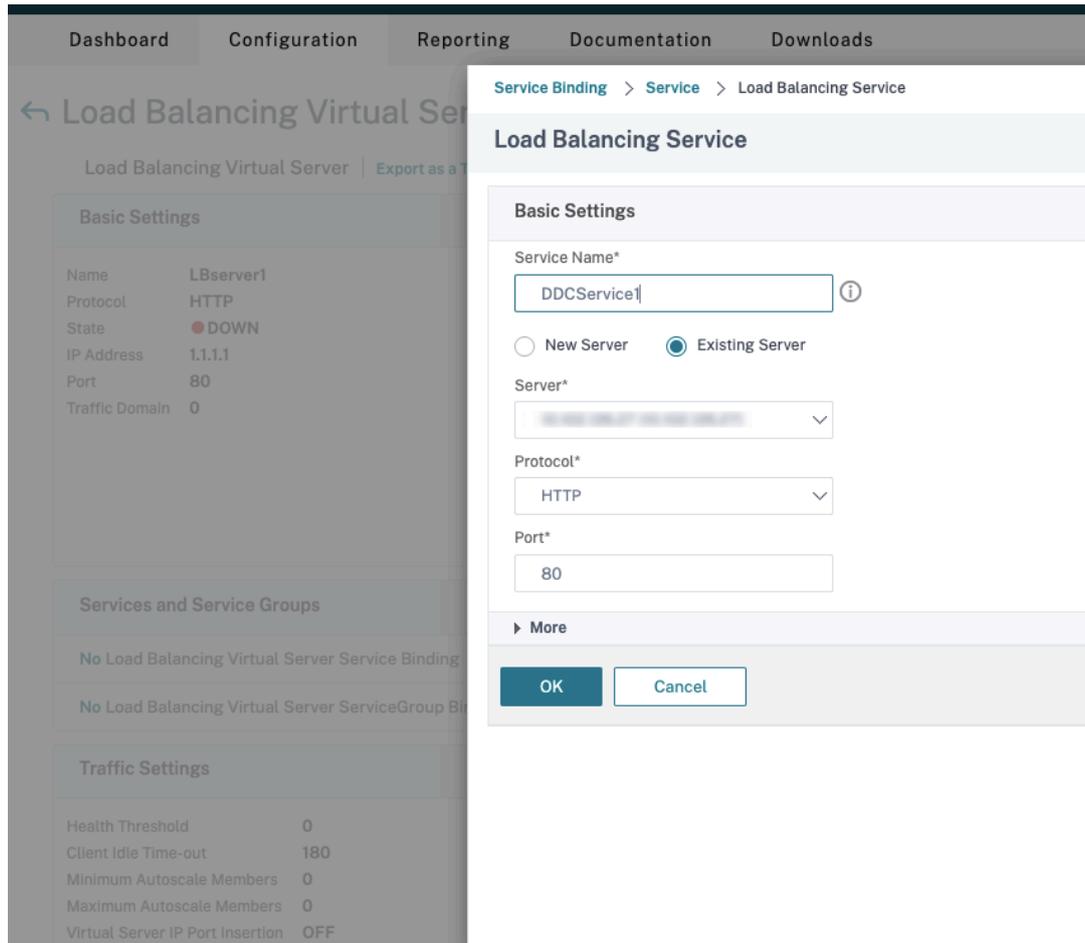
Port\*

▶ More

- En **Existing Server**, seleccione el servidor virtual creado en el paso anterior.
- En **Protocol**, seleccione **HTTP** y, en **Port**, seleccione **80**.
- Haga clic en **OK** y, a continuación, en **Done**.

c) Enlace el servicio al servidor virtual.

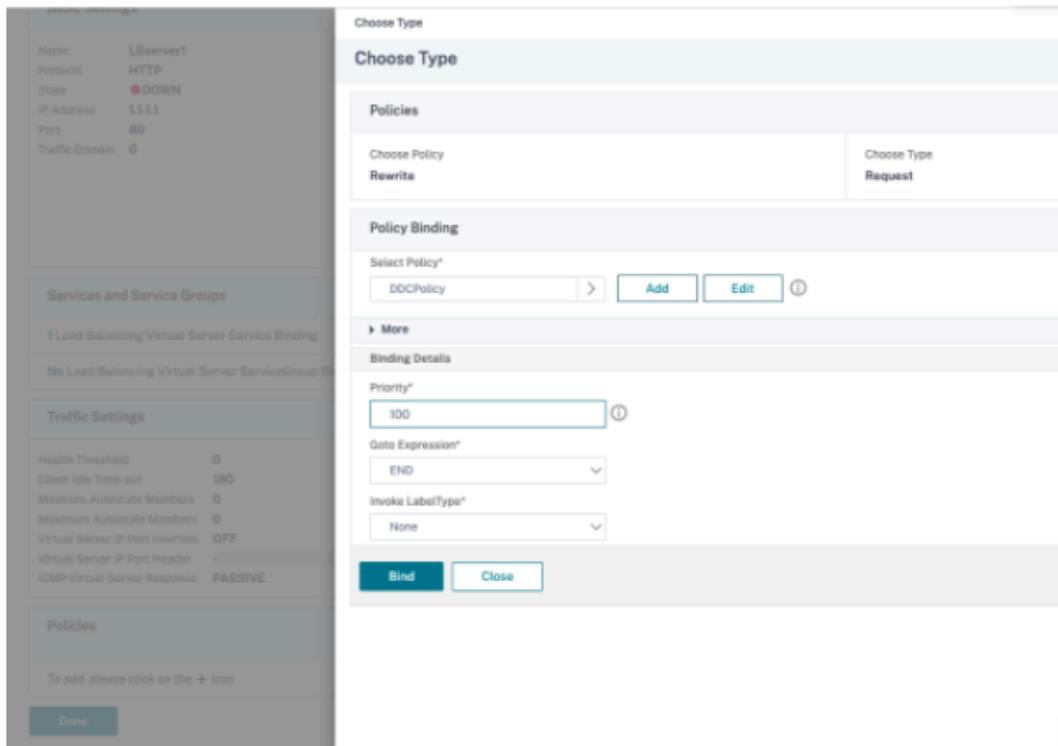
- Seleccione el servidor virtual creado anteriormente y haga clic en **Edit**.
- En **Services and Service Groups**, haga clic en **No Load Balancing Virtual Server Service Binding**.



- En **Service Binding**, seleccione el servicio creado anteriormente.
- Haga clic en **Bind**.

d) Vincule la directiva de reescritura creada anteriormente al servidor virtual.

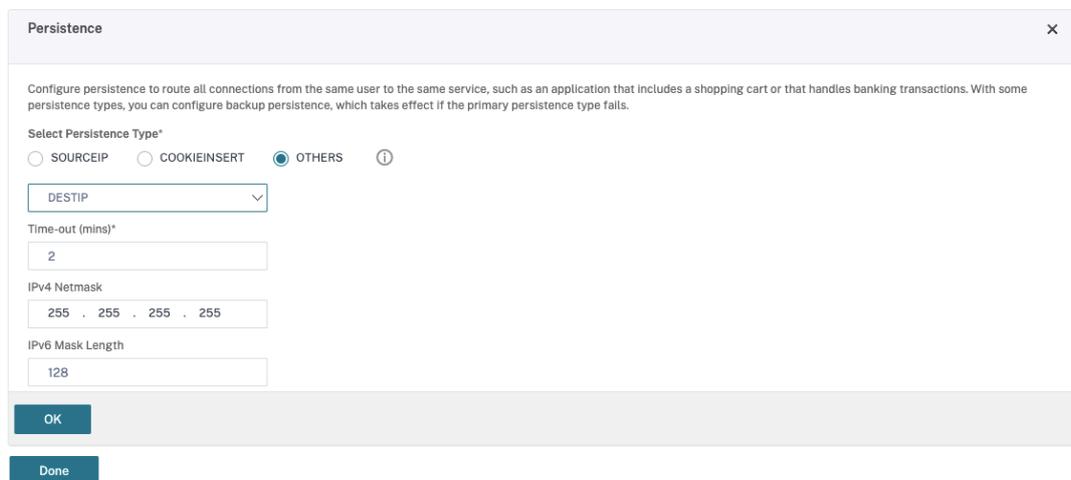
- Seleccione el servidor virtual creado anteriormente y haga clic en **Edit**.
- En **Advanced Settings**, haga clic en **Policies**, y, a continuación, en la sección **Policies** haga clic en **+**.



- En **Choose Policy**, seleccione **Rewrite** y, en **Choose Type**, seleccione **Request**.
- Haga clic en **Continuar**.
- En **Select Policy**, seleccione la directiva de reescritura creada anteriormente.
- Haga clic en **Bind**.
- Haga clic en **Listo**.

e) Configure la persistencia para el servidor virtual, si es necesario.

- Seleccione el servidor virtual creado anteriormente y haga clic en **Edit**.
- En **Advanced Settings**, haga clic en **Persistence**.



- Seleccione el tipo de persistencia **Others**.

- Seleccione **DESTIP** para crear sesiones de persistencia basadas en la dirección IP del servicio seleccionado por el servidor virtual (la dirección IP de destino)
- En **IPv4 Netmask**, agregue una máscara de red igual que la del Desktop Delivery Controller.
- Haga clic en **Aceptar**.

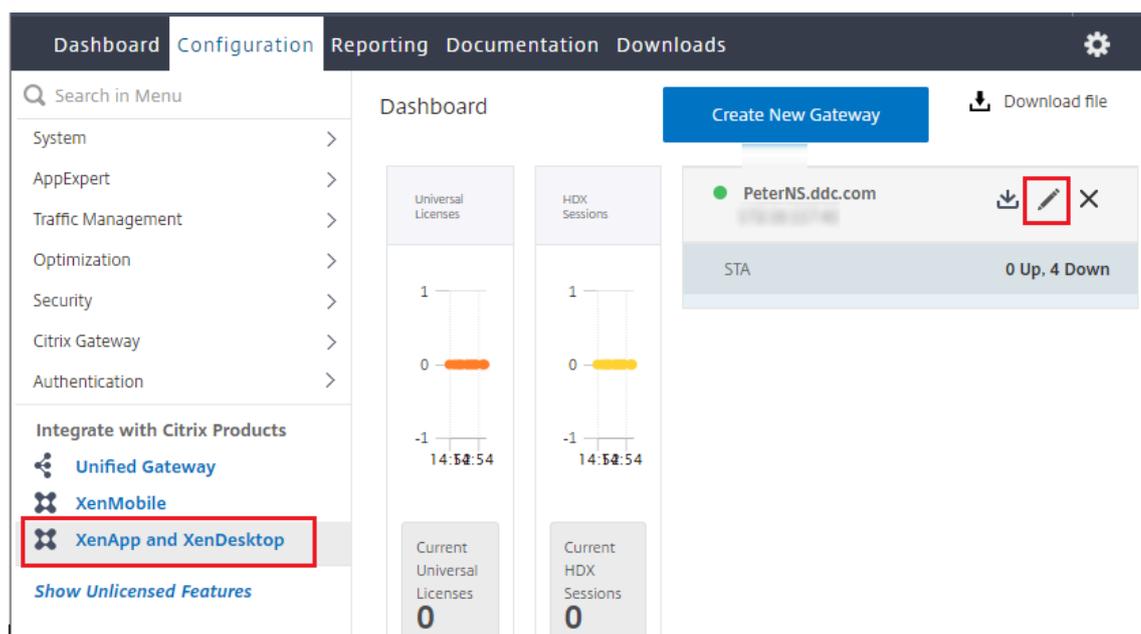
f) Repita estos pasos para el otro servidor virtual.

## La configuración cambia si el dispositivo Citrix ADC ya está configurado con Citrix Virtual Desktops

Si ya ha configurado el dispositivo Citrix ADC con Citrix Virtual Desktops, para utilizar la funcionalidad Secure XML, debe realizar los siguientes cambios de configuración.

- Antes de iniciar la sesión, cambie la **URL de Secure Ticket Authority (STA)** de la puerta de enlace para que utilice utilizar los nombres de dominio completos (FQDN) de los servidores virtuales de equilibrio de carga.
- Compruebe que el parámetro `TrustRequestsSentToTheXmlServicePort` esté establecido en False. De forma predeterminada, el parámetro `TrustRequestsSentToTheXmlServicePort` se establece en False. Sin embargo, si el cliente ya ha configurado Citrix ADC para Citrix Virtual Desktops, `TrustRequestsSentToTheXmlServicePort` se establece en True.

1. En la GUI de Citrix ADC, vaya a **Configuration > Integrate with Citrix Products** y haga clic en **XenApp and XenDesktop**.
2. Seleccione la instancia de puerta de enlace y haga clic en el icono de modificación.



3. En el panel StoreFront, haga clic en el icono de modificación.

StoreFront	
StoreFront URL	https://yj-en2016-1.ddc.com
Storefront Status	
Receiver for Web Path	/Citrix/StoreWeb
Default Active Directory Domain	ddc.com
List of Secure Ticket Authority URL(s) with status	
http://[redacted].com	● DOWN

4. Agregue la **URL de Secure Ticket Authority**

- Si la funcionalidad Secure XML está habilitada, la URL de STA debe ser la URL del servicio de equilibrio de carga.
- Si la funcionalidad Secure XML está inhabilitada, la URL de STA debe ser la URL de STA (la dirección del Desktop Delivery Controller) y el parámetro TrustRequestsSentToTheXmlServicePort del Desktop Delivery Controller debe establecerse en True.

**StoreFront**

StoreFront URL\*

ⓘ

**Retrieve Stores**

Receiver for Web Path\*

Default Active Directory Domain\*

Secure Ticket Authority URL\*

<input type="text" value="http://[redacted].com"/>	×

**Test STA Connectivity**

Use this StoreFront for Authentication

## IP virtual y bucle invertido virtual

September 22, 2021

**Importante:**

La multisesión de Windows 10 Enterprise no admite virtualización de IP de Escritorio remoto (IP virtual) y nosotros no admitimos IP virtual ni bucle invertido virtual en multisesión con Windows 10 Enterprise.

Las funciones de IP virtual y bucle invertido virtual se admiten en máquinas con Windows Server 2016. Sin embargo, no se aplican a las máquinas con SO de escritorio Windows.

La función de dirección IP virtual de Microsoft proporciona una dirección IP exclusiva a una aplicación publicada, asignada dinámicamente para cada sesión. La función de bucle invertido virtual de Citrix permite configurar aplicaciones que dependen de la comunicación con el host local (127.0.0.1 de forma predeterminada) para utilizar una dirección de bucle invertido virtual exclusiva en el intervalo de host local (127.\*).

Algunas aplicaciones, como CRM y Computer Telephony Integration (CTI), utilizan una dirección IP para el direccionamiento, las licencias, la identificación y otros fines, y, por lo tanto, requieren una dirección IP exclusiva o una dirección de bucle invertido en las sesiones. Otras aplicaciones pueden enlazar con un puerto estático, por lo que, al intentar iniciar instancias adicionales de una aplicación en un entorno multiusuario, se producirá un error porque el puerto ya está en uso. Para que estas aplicaciones funcionen correctamente en un entorno Citrix Virtual Apps, se necesita una dirección IP exclusiva para cada dispositivo.

Las funciones de IP virtual y bucle invertido virtual son funciones independientes. Puede usar solo una de ellas o ambas.

Sinopsis de acciones de administrador:

- Para utilizar la dirección IP virtual de Microsoft, habilite y configure esta función en el servidor Windows. (No se necesitan configuraciones de directivas de Citrix).
- Para usar el bucle virtual de Citrix, configure dos parámetros en una directiva de Citrix.

## **IP virtual**

Cuando la función IP virtual está habilitada y configurada en el servidor Windows, cada una de las aplicaciones configuradas que se ejecutan en una sesión parece tener una dirección exclusiva. Los usuarios acceden a dichas aplicaciones en un servidor de Citrix Virtual Apps del mismo modo que acceden a cualquier otra aplicación publicada. Un proceso requiere IP virtual en cualquiera de los siguientes casos:

- El proceso utiliza un número de puerto TCP integrado en el código.
- El proceso utiliza Windows Sockets y requiere una dirección IP exclusiva o un número de puerto TCP específico.

Para determinar si una aplicación necesita utilizar direcciones IP virtuales:

1. Obtenga la herramienta TCPView de Microsoft. Esta herramienta muestra todas las aplicaciones que enlazan puertos y direcciones IP específicas.
2. Inhabilite la función de resolución de direcciones IP de forma que vea las direcciones en lugar de los nombres de host.
3. Ejecute la aplicación y con ayuda de TCPView consulte qué direcciones IP y puertos abre la aplicación y qué nombres de proceso abren estos puertos.
4. Configure los procesos que abren la dirección IP del servidor, 0.0.0.0 ó 127.0.0.1.
5. Para asegurarse de que la aplicación no abre la misma dirección IP en otro puerto, ejecute otra instancia de la aplicación.

### **Funcionamiento de la virtualización de IP de Escritorio remoto (RD) de Microsoft**

- El uso de direcciones IP virtuales debe estar habilitado en el servidor de Microsoft.

Por ejemplo, en un entorno de Windows Server 2016, desde el Administrador del servidor, expanda **Servicios de Escritorio remoto > Conexiones de host de sesión de Escritorio remoto** para activar la función Virtualización de IP de Escritorio remoto y configure los parámetros para asignar direcciones IP dinámicamente mediante el servidor DHCP (Dynamic Host Configuration Protocol) para cada sesión o cada programa. Consulte la documentación de Microsoft para obtener instrucciones.

- Después de habilitar la función, al comenzar una sesión, el servidor solicita al servidor DHCP las direcciones IP asignadas dinámicamente.
- La función de Virtualización de IP de Escritorio remoto asigna direcciones IP a las conexiones a escritorios remotos por sesión y por programa. Si se asignan direcciones IP para varios programas, éstos comparten una dirección IP por sesión.
- Después de asignar una dirección a una sesión, la sesión utiliza la dirección virtual en lugar de la dirección IP principal del sistema, siempre que se efectúan las siguientes llamadas: `bind`, `closesocket`, `connect`, `WSAConnect`, `WSAAccept`, `getpeername`, `getsockname`, `sendto`, `WSASendTo`, `WSASocketW`, `gethostbyaddr`, `getnameinfo`, `getaddrinfo`.

Con la función de virtualización de IP de Microsoft en la configuración de host de sesiones de Escritorio remoto, las aplicaciones se vinculan con direcciones IP específicas mediante la introducción de un componente de “filtro” entre la aplicación y las llamadas de función de Winsock. La aplicación solo ve entonces la dirección IP que debe usar. Cualquier intento de la aplicación de escuchar comunicaciones TCP o UDP se vincula inmediatamente a su dirección IP virtual asignada (o dirección de bucle invertido) y cualquier conexión de origen abierta por la aplicación se origina desde la dirección IP vinculada a la aplicación.

En funciones que devuelven una dirección, tales como `GetAddrInfo()` (que está controlada por una directiva de Windows), si se solicita la dirección IP local del host, la IP virtual examina la dirección IP devuelta y la cambia a la dirección IP virtual de la sesión. Las aplicaciones que intentan obtener la dirección IP del servidor local a través de dichas funciones de nombre solo ven la dirección IP virtual exclusiva asignada a dicha sesión. Esta dirección IP se utiliza con frecuencia en las posteriores llamadas de socket (tales como `bind` o `connect`). Para obtener más información acerca de las directivas de Windows, consulte [Virtualización de IP de RDS en Windows Server](#).

A menudo una aplicación solicita vincularse a un puerto para escuchar en la dirección 0.0.0.0. En ese caso, si además la aplicación utiliza un puerto estático, no podrá ejecutar más de una instancia de la aplicación. La función de dirección IP virtual también busca 0.0.0.0 en estos tipos de llamada y cambia la llamada para escuchar en la dirección IP virtual específica, lo que permite que varias aplicaciones puedan escuchar en el mismo puerto en el mismo equipo, puesto que todas escuchan en diferentes direcciones. La llamada solo se cambia si se está en una sesión ICA y la función de dirección IP virtual está habilitada. Por ejemplo, si dos instancias de una aplicación que se ejecutan en distintas sesiones intentan vincularse a todas las interfaces (0.0.0.0) y un puerto específico, por ejemplo, el 9000, se vinculan a `VIPAddress1:9000` y `VIPAddress2:9000`, por lo que no existen conflictos.

## Bucle invertido virtual

La habilitación de la configuración de directiva de Bucle invertido de IP virtual de Citrix permite que cada sesión disponga de su propia dirección de bucle invertido para las comunicaciones. Cuando una aplicación usa la dirección de host local (predeterminada = 127.0.0.1) en una llamada de Winsock, la función de bucle invertido virtual sencillamente sustituye 127.0.0.1 por 127.X.X.X, donde X.X.X es una representación del ID de sesión + 1. Por ejemplo, un ID de sesión de 7 es 127.0.0.8. En el caso improbable de que un ID de sesión fuera superior al cuarto octeto (más de 255), la dirección pasaría al octeto siguiente (127.0.1.0) hasta el máximo de 127.255.255.255.

Un proceso requiere el bucle invertido virtual en los siguientes casos:

- El proceso usa la dirección de bucle invertido de Windows Sockets del host local (127.0.0.1)
- El proceso utiliza un número de puerto TCP integrado en el código.

Use la [configuración de directiva de bucle invertido](#) para aplicaciones que usan una dirección de bucle invertido para la comunicación entre procesos. No se requiere ninguna configuración adicional. La función de bucle invertido virtual no depende de la dirección IP virtual, de modo que no es necesario configurar el servidor de Microsoft.

- Funcionalidad de bucle invertido de IP virtual. Cuando está habilitada, esta configuración de directiva permite que cada sesión tenga su propia dirección virtual de bucle invertido. Este parámetro está inhabilitado de forma predeterminada. La función solo se aplica a las aplicaciones especificadas en la configuración de directiva lista de programas para bucle invertido de

IP virtual.

- Lista de programas para bucle invertido de IP virtual. Esta configuración de directiva especifica las aplicaciones que usan la función de bucle invertido de IP virtual. Esta configuración solo se aplica cuando está habilitada la configuración de directiva Funcionalidad de bucle invertido de IP virtual.

### Funciones relacionadas

Se pueden usar los siguientes parámetros del Registro del sistema para garantizar que se da preferencia al bucle invertido sobre la IP virtual; esto se denomina bucle invertido preferido. Sin embargo, hay que actuar con precaución:

- Utilice el bucle invertido preferido solo cuando tanto IP virtual como Bucle invertido virtual están habilitados; en caso contrario, podría obtener resultados inesperados.
- Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Ejecute regedit en los servidores donde residen las aplicaciones.

- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP
- Nombre: PreferLoopback, Tipo: REG\_DWORD, Datos: 1
- Nombre: PreferLoopbackProcesses, Tipo: REG\_MULTI\_SZ, Datos: <lista de procesos>

## Delivery Controllers

September 22, 2021

Delivery Controller es el componente de servidor que es responsable de la administración del acceso de los usuarios, además de la intermediación y optimización de las conexiones. Los Controllers también proporcionan los Machine Creation Services que crean imágenes de escritorio y servidor.

Un sitio debe tener al menos un Controller. Después de instalar el primer Controller, se pueden agregar más al crear un sitio o más adelante. Tener más de un Controller en un sitio ofrece dos ventajas principales.

- **Redundancia:** Se recomienda que un sitio de producción siempre tenga al menos dos Controllers en diferentes servidores físicos. De este modo, si falla un Controller, los demás pueden gestionar las conexiones y administrar el sitio.

- **Escalabilidad:** A medida que aumenta la actividad de un sitio, también aumenta el uso de CPU en el Controller y la actividad de la base de datos. Más Controllers ofrecen la capacidad de administrar más usuarios y más solicitudes de aplicaciones y escritorios, además de mejorar la capacidad general de respuesta.

Cada Controller se comunica directamente con la base de datos del sitio. En un sitio con más de una zona, los Controllers de cada zona se comunican con la base de datos del sitio de la zona principal.

**Importante:**

No cambie el nombre de equipo ni la pertenencia al dominio de un Controller una vez configurado el sitio.

## Cómo se registran los agentes VDA en Controllers

Para poder utilizar un VDA, este debe registrarse (establecer comunicación) con un Delivery Controller del sitio. Para obtener información sobre el registro de VDA, consulte [Registro de VDA en Controllers](#).

## Agregar, quitar o mover Controllers

Para agregar, quitar o mover un Controller, debe tener los permisos del rol de servidor y del rol de base de datos. Se ofrece una lista de esos permisos en el artículo [Bases de datos](#).

No se admite la instalación de Controller en un nodo de clúster de SQL o de instalación duplicada (mirroring) de SQL.

Si la implementación usa la creación de reflejo de la base de datos:

- Antes de agregar, quitar o mover un Controller, compruebe que la base de datos principal y la reflejada se estén ejecutando. Además, si está utilizando scripts con SQL Server Management Studio, habilite el modo SQLCMD antes de ejecutar los scripts.
- Para verificar el reflejo después de agregar, quitar o mover un Controller, ejecute el cmdlet `Get-ConfigDbConnection` de PowerShell para asegurarse de que el socio de conmutación por error se haya definido en la cadena de conexión con la base de datos reflejada.

Después de agregar, quitar o mover un Controller:

- Si la actualización automática está habilitada, los VDA reciben una lista actualizada de los Controllers en los 90 minutos siguientes.
- Si la actualización automática no está habilitada, asegúrese de que la configuración de directiva o la clave del Registro ListOfDDCs están actualizadas para todos los VDA. Después de mover un Controller a otro sitio, actualice la configuración de directiva o la clave del Registro en ambos sitios.

## Agregar un Controller

Puede agregar Controllers al crear un sitio o más adelante. No puede agregar Controllers instalados con una versión anterior de este software a un sitio que se haya creado con esta versión.

1. Ejecute el instalador en un servidor con un sistema operativo compatible. Instale el componente Delivery Controller y los demás componentes principales que quiera. Complete el asistente de instalación.
2. Si aún no ha creado ningún sitio, inicie Studio. Se le pedirá que cree un sitio. En la página Bases de datos del asistente para la creación de sitios, haga clic en el botón Seleccionar y, a continuación, agregue la dirección del servidor donde instaló el Controller adicional.

Si va a generar scripts para inicializar bases de datos, agregue los Controllers antes de generarlos.

3. Si ya ha creado un sitio, indique en Studio el servidor donde instaló el Controller adicional. Haga clic en **Ampliar la implementación** e introduzca la dirección del sitio.

## Quitar un Controller

Al quitar un Controller de un sitio, no se desinstala el software Citrix ni ningún otro componente. Con esa acción, se quita el Controller de la base de datos, de forma que ya no se pueda usar para hacer de intermediario (broker) de conexiones ni realizar otras tareas. Si quita un Controller, es posible volver a agregarlo al mismo sitio o a otro posteriormente. Un sitio requiere como mínimo un Controller; esto significa que no puede quitar el último de la lista de Studio.

Aunque quite un Controller de un sitio, no se quita el inicio de sesión del Controller en el servidor de la base de datos. Esto evita el peligro potencial provocado por la acción de quitar un inicio de sesión que utilizan otros servicios de producto en la misma máquina. Si ya no es necesario, el inicio de sesión debe quitarse manualmente. Para hacerlo, se necesita el permiso del rol de servidor `securityadmin`.

### Importante:

No quite el Controller de Active Directory hasta que lo haya quitado del sitio.

1. Compruebe que el Controller está ejecutándose de forma que Studio se cargue en menos de una hora. Una vez que Studio carga el Controller que quiere quitar, apague el Controller cuando lo pida el sistema.
2. Seleccione **Configuración > Controllers** en el panel de navegación de Studio. A continuación, seleccione el Controller que quiere quitar.
3. Seleccione **Quitar Controller** en el panel Acciones. Si no dispone de los roles y permisos adecuados para la base de datos, se le ofrece la opción de generar un script que permita al administrador de bases de datos quitar el Controller por usted.

4. Es posible que necesite quitar la cuenta de la máquina del Controller del servidor de la base de datos. Antes de hacerlo, compruebe que no hay ningún otro servicio que esté utilizando la cuenta.

Después de usar Studio para quitar un Controller, el tráfico hacia ese Controller puede permanecer activo durante un corto período de tiempo para garantizar la correcta finalización de las tareas actuales. Si quiere forzar la retirada de un Controller en un período de tiempo corto, Citrix recomienda apagar el servidor donde se instaló o quitar ese servidor de Active Directory. A continuación, reinicie el resto de Controllers del sitio para asegurarse de que no hay más comunicaciones con el Controller que ha quitado.

### **Mover un Controller a otra zona**

Si el sitio contiene más de una zona, puede mover un Controller a otra zona. Consulte el artículo *Zonas* para obtener información sobre cómo puede esto afectar al registro de VDA y otras operaciones.

1. Seleccione **Configuración > Controllers** en el panel de navegación de Studio. A continuación, seleccione el Controller que quiere mover.
2. Seleccione **Mover** en el panel Acciones.
3. Especifique la zona a la que quiere mover el Controller.

### **Mover un Controller a otro sitio**

No puede mover un Controller a un sitio creado con una versión anterior del software.

1. En el sitio donde el Controller se encuentra actualmente (el que será el sitio antiguo), seleccione **Configuración > Controllers** en el panel de navegación de Studio y, a continuación, seleccione el Controller que quiera mover.
2. Seleccione **Quitar Controller** en el panel Acciones. Si no dispone de los permisos adecuados para la base de datos, puede generar un script que permita a alguien con esos permisos (como un administrador de bases de datos) quitar el Controller. Un sitio requiere como mínimo un Controller; esto significa que no puede quitar el último de la lista de Studio.
3. En el Controller que está moviendo, abra Studio, restablezca los servicios cuando el sistema se lo solicite, seleccione **Incorporarse a un sitio existente** e introduzca la dirección del sitio nuevo.

### **Mover un VDA a otro sitio**

Si un VDA se aprovisionó mediante Citrix Provisioning o es una imagen existente, puede moverlo a otro sitio (del sitio 1 al sitio 2) al actualizar. También puede mover una imagen VDA creada en un sitio de

prueba a un sitio de producción. Los VDA provisionados mediante Machine Creation Services (MCS) no se pueden mover de un sitio a otro porque MCS no admite el cambio de ListOfDDCs que el VDA comprueba para registrarse en un Controller. Los VDA provisionados con MCS siempre consultan la lista ListOfDDCs asociada al sitio donde se crearon.

Hay dos formas de mover un VDA a otro sitio: mediante el instalador o mediante directivas de Citrix.

**Instalador** Ejecute el instalador y agregue un Controller, especificando el FQDN (entrada DNS) de un Controller en el sitio 2.

Especifique los Controllers en el instalador solo si la configuración de directiva de Controllers no se utiliza.

**Editor de directivas de grupo** En el siguiente ejemplo se mueven varios VDA entre sitios.

1. Cree una directiva en el Sitio 1 que contenga la siguiente configuración y, a continuación, filtre la directiva al nivel de grupo de entrega para iniciar una migración de VDA entre sitios, por fases.
  - Contiene los nombres de dominio completo o FQDN (entradas de DNS) de uno o más Controllers del sitio 2.
  - Habilitar actualización automática de Controller: defínala como inhabilitada.
2. Cada VDA en el grupo de entrega recibe un aviso sobre la nueva directiva en los siguientes 90 minutos. El VDA ignora la lista de Controllers que recibe (porque la actualización automática está inhabilitada). El VDA selecciona uno de los Controllers especificados en la directiva, que enumera los Controllers en el sitio 2.
3. Cuando el VDA se registra correctamente con un Controller del sitio 2, recibe la ListOfDDC y la información de directivas del sitio 2, que tiene la actualización automática habilitada de forma predeterminada. Puesto que el Controller con el que se registró el VDA en el sitio 1 no está en la lista enviada por el Controller del sitio 2, el VDA vuelve a registrarse y selecciona un Controller de la lista de Controllers del sitio 2. A partir de entonces, el VDA se actualiza automáticamente con la información del sitio 2.

## Registro de VDA

June 27, 2024

## Introducción

Para poder utilizar un VDA, este debe registrarse en (o establecer comunicación con) uno o varios Controllers o Cloud Connectors del sitio. (En una implementación local de Citrix Virtual Apps and Desktops, los VDA se registran en los Controllers. En una implementación de Citrix Virtual Apps and Desktops Service, los VDA se registran en Cloud Connectors.) El VDA busca un Controller o un Connector en una lista llamada `ListOfDDCs`. En un VDA, la lista `ListOfDDCs` consta de entradas DNS que le indican los Controllers o Cloud Connectors del sitio. Para conseguir un equilibrio de carga, el VDA distribuye automáticamente las conexiones entre todos los Controllers o Cloud Connectors de la lista.

¿Por qué es tan importante que el VDA se registre?

- Desde el punto de vista de la seguridad, el registro es una operación confidencial. Se establece una conexión entre el Controller o Cloud Connector y el VDA. Para una operación confidencial, el comportamiento esperado es rechazar la conexión si algo no se cumple a la perfección. Se establecen dos canales independientes de comunicación: del VDA al Controller o Cloud Connector y del Controller o Cloud Connector al VDA. La conexión utiliza Kerberos, de modo que los problemas de sincronización horaria y los problemas de pertenencia a dominios son obstáculos que impiden la conexión. Kerberos utiliza nombres principales de servicio (SPN), por lo que no se puede usar IP ni nombre de host con carga equilibrada.
- Si un VDA no tiene información precisa y actual acerca de los Controllers (o Cloud Connector), la cual se actualiza a medida que se agregan o quitan Controllers de un sitio, ese VDA podría rechazar inicios de sesión si interviene como intermediario un Controller que no conste en la información. Las entradas no válidas pueden retrasar el inicio del software del sistema de escritorios virtuales. Un VDA no puede aceptar una conexión desde un Controller o Cloud Connector desconocido con el que no haya una relación de confianza.

Además de `ListOfDDCs`, la lista `ListOfSIDs` (identificadores de seguridad) indica las máquinas de `ListOfDDCs` que son de confianza. La lista `ListOfSIDs` se puede utilizar para reducir la carga de Active Directory o para evitar las posibles amenazas de seguridad que presente un servidor DNS interceptado. Para obtener más información, consulte `ListOfSIDs`.

Si en una `ListOfDDCs` se especifica más de un Controller o Cloud Connector, el VDA intenta conectarse a ellos aleatoriamente. En una implementación local, la lista `ListOfDDCs` también puede contener grupos de Controllers. El VDA intenta conectarse a cada Controller del grupo antes de pasar a otras entradas de la `ListOfDDCs`.

Citrix Virtual Apps and Desktops comprueban automáticamente la conectividad a los Controllers o Cloud Connectors configurados durante la instalación de VDA. Si no se puede establecer conexión con un Controller o Cloud Connector, se muestran errores. Si ignora el mensaje de advertencia que indica que no se puede conectar a un Controller o Cloud Connector (o si no especifica direcciones de Controller ni Cloud Connector durante la instalación de VDA), los mensajes se lo recuerdan.

## Métodos para configurar direcciones de Controller o Cloud Connector

El administrador es quien selecciona el método de configuración a utilizar cuando el VDA se registra por primera vez. Esto se denomina registro inicial. Durante ese registro inicial, se crea una memoria caché persistente en el VDA. Durante los registros subsiguientes, el VDA obtiene la lista de Controllers o Cloud Connectors desde esa memoria caché local, a menos que se detecte un cambio de configuración.

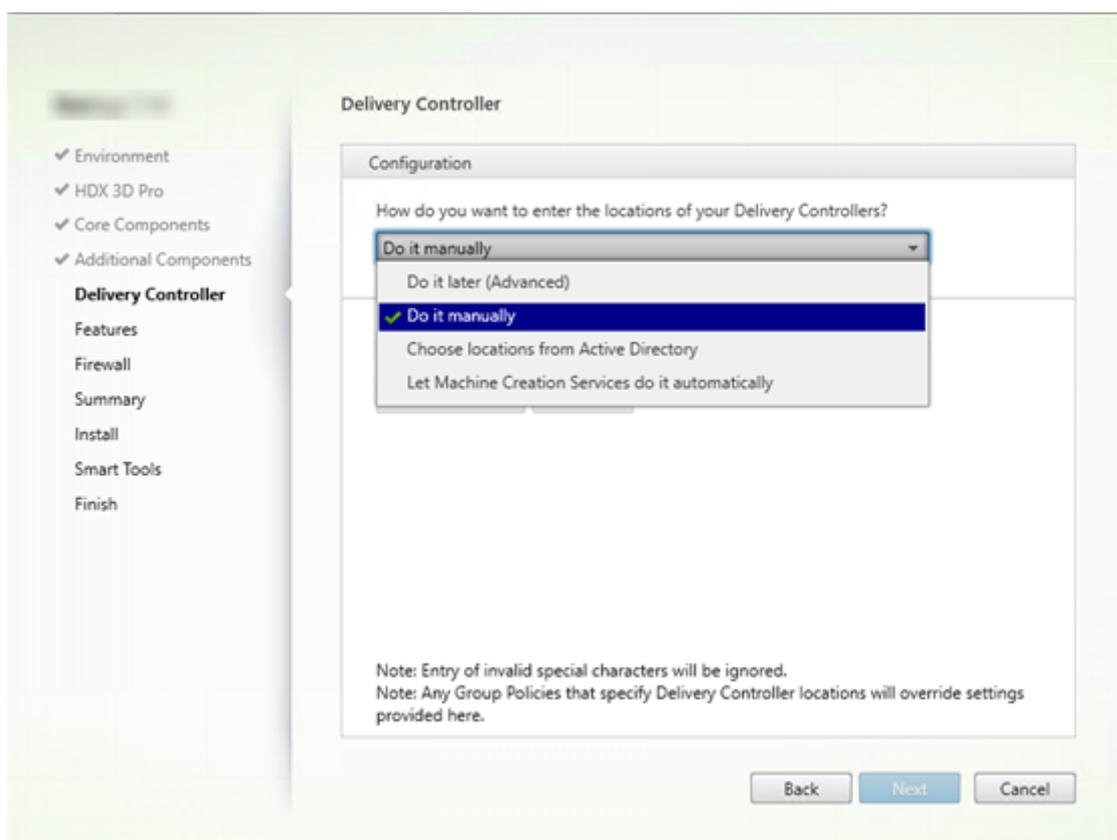
La forma más fácil de recuperar esa lista en los registros subsiguientes es mediante la función de actualización automática. De forma predeterminada, la actualización automática está habilitada. Para obtener más información, consulte Actualización automática.

Existen varios métodos para configurar direcciones de Controller o Cloud Connector en un VDA.

- Método basado en directivas (LGPO o GPO)
- Método basado en el Registro (manual, GPP, direcciones especificadas durante la instalación de VDA)
- Método basado en unidades organizativas de Active Directory (detección de OU antiguas)
- Método basado en MCS (personality.ini)

El método de registro inicial se indica cuando se instala un VDA. (Si se inhabilita la actualización automática, el método seleccionado durante la instalación del VDA también se utilizará para los registros posteriores.)

En la siguiente imagen, se muestra la página **Delivery Controller** del Asistente de instalación de VDA.



### Método basado en directivas (LGPO o GPO)

Citrix recomienda usar GPO para el registro inicial del VDA. Tiene la prioridad más alta (Aunque la actualización automática se haya indicado como la máxima prioridad, solo se usa después del registro inicial.) El registro basado en directivas ofrece las ventajas de las directivas de grupo centralizadas para la configuración.

Para especificar este método, complete los dos siguientes pasos:

- En la página **Delivery Controller** del Asistente de instalación de VDA, seleccione **Hacerlo más tarde (Avanzado)**. El asistente le recordará varias veces que indique direcciones de Controller, incluso aunque no las indique durante la instalación del VDA. (Se lo recuerda porque el registro del VDA es sumamente importante.)
- Habilite o inhabilite el registro del VDA basado en directivas mediante la directiva de Citrix desde [Virtual Delivery Agent Settings > Controllers](#). (Si la seguridad es su prioridad principal, utilice el parámetro [Virtual Delivery Agent Settings > Controller SIDs](#).)

Esta configuración se almacena en `HKLM\Software\Policies\Citrix\VirtualDesktopAgent (ListOfDDCs)`.

## Método basado en el Registro

Para especificar este método, complete uno de los siguientes pasos:

- En la página **Delivery Controller** del Asistente de instalación de VDA, seleccione **Hacerlo manualmente**. Introduzca el nombre de dominio completo (FQDN) de un Controller instalado y, a continuación, haga clic en **Agregar**. Si ha instalado más Controllers, agregue sus direcciones respectivas.
- Para una instalación de VDA desde la línea de comandos, use la opción `/controllers` y especifique los FQDN de los Controllers o Cloud Connectors instalados.

Esta información se almacena en el valor de Registro `ListOfDDCs` en la clave de Registro `HKLM\Software\Citrix\VirtualDesktopAgent` o `HKLM\Software\Wow6432Node\Citrix\VirtualDesktopAgent`.

También puede configurar esta clave de Registro de forma manual o utilizar las preferencias de directiva de grupo (GPP). Este método puede ser preferible al método basado en las directivas (por ejemplo, si quiere condicionar el procesamiento de Controllers o Cloud Connectors diferentes, como usar XDC-001 para nombres de equipo que empiezan por XDW-001-).

Actualice la clave de Registro de `ListOfDDCs`, que contiene los FQDN de todos los Controllers o Cloud Connectors del sitio. (esta clave es el equivalente de la OU del sitio de Active Directory).

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfDDCs` (REG\_SZ)

Si la ubicación `HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent` del Registro contiene ambas claves, `ListOfDDCs` y `FarmGUID`, `ListOfDDCs` se utiliza para la detección del Controller o Cloud Connector. `FarmGUID` está presente si se especificó una unidad organizativa del sitio durante la instalación del VDA (puede usarlo en implementaciones antiguas).

Si lo prefiere, puede actualizar la clave de Registro `ListOfSIDs`. Para obtener más información, consulte `ListOfSIDs`:

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs` (REG\_SZ)

Recuerde: Si habilita también el registro de VDA basado en directivas mediante la directiva de Citrix, esta configuración sobrescribe los parámetros especificados durante la instalación de VDA, porque es un método de mayor prioridad.

## Método basado en unidades organizativas de Active Directory (antiguo)

Este no es el método recomendado; se admite principalmente para la compatibilidad con versiones anteriores. Si aún lo utiliza, Citrix recomienda cambiar a otro método.

Para especificar este método, complete los dos siguientes pasos:

- En la página **Delivery Controller** del Asistente de instalación de VDA, seleccione **Elegir ubicaciones desde Active Directory**.
- Use el script `Set-ADControllerDiscovery.ps1` (disponible en cada Controller). Además, configure la entrada del Registro `FarmGuid` en cada VDA para que apunte a la OU correspondiente. Esta configuración puede configurarse mediante la directiva de grupo.

Para obtener más información, consulte [Detección basada en unidades organizativas de Active Directory](#).

### Método basado en MCS

Si usa MCS para aprovisionar máquinas virtuales, MCS configura la lista de controladores o Cloud Connector. Esta función funciona con la actualización automática. Al crear el catálogo, MCS inserta la lista de Controllers o Cloud Connectors en el archivo `Personality.ini` durante el aprovisionamiento inicial. La actualización automática mantiene la lista al día.

Para especificar este método, en la página **Delivery Controller** del Asistente de instalación de VDA, seleccione **Dejar que Machine Creation Services lo haga**.

### Recomendaciones

Recomendaciones:

- Use el método del registro basado en la directiva de grupo para el registro inicial.
- Use la actualización automática (habilitada de forma predeterminada) para mantener actualizada su lista de Controllers.
- En una implementación de varias zonas, use la directiva de grupo para la configuración inicial (con al menos dos Controllers o Cloud Connectors). Apunte los agentes VDA a los Controllers o Cloud Connectors locales de la zona. Utilice la actualización automática para mantenerlos actualizados. La actualización automática optimiza automáticamente la lista `ListOfDDCs` para agentes VDA en las zonas satélite.
- Incluya más de un Controller en la clave de Registro `ListOfDDCs`, separados por un espacio para evitar problemas de Registro si un Controller no está disponible.

Ejemplo:

```
DDC7x.xd.local DDC7xHA.xd.local
```

```
HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\ListOfDDCs  
(32 bits)
```

HKEY\_LOCAL\_MACHINE \Software\Citrix\VirtualDesktopAgent\ListOfDDCs  
(REG\_SZ)

- Compruebe que todos los valores indicados en la lista `ListOfDDCs` se asignen a un nombre de dominio completo y válido para evitar retrasos en el registro de inicios.

## Actualización automática

Introducida desde XenApp y XenDesktop 7.6, la actualización automática está habilitada de forma predeterminada. Es el método más eficaz para mantener actualizados los registros de VDA. A pesar de que la actualización automática no se utilice para el registro inicial, el software de la actualización automática descarga y almacena la lista `ListOfDDCs` en una caché persistente en el VDA cuando se produce el registro inicial. Esto se lleva a cabo para cada VDA (esta memoria caché también contiene información de directivas de máquina que garantizan que las configuraciones de directiva se conserven después de reiniciar).

Se admite la actualización automática cuando se utiliza MCS o Citrix Provisioning para aprovisionar las máquinas, salvo para la caché del servidor Citrix Provisioning (que no es un caso frecuente porque no hay almacenamiento persistente para la caché de actualización automática).

Para especificar este método:

- Habilite o inhabilite la actualización automática a través de una directiva de Citrix que contenga la configuración: `Virtual Delivery Agent Settings > Enable auto update of Controllers`. Esta configuración está habilitada de forma predeterminada.

Funcionamiento:

- La memoria caché se actualiza cada vez que el VDA se registra (por ejemplo, después de un reinicio de máquina). Todos los Controllers o Cloud Connectors consultan a su vez la base de datos del sitio cada 90 minutos. Si se ha agregado o quitado un Controller desde la última comprobación, o bien si se ha producido un cambio de directiva que afecte al registro de VDA, el Controller envía una lista actualizada a sus VDA registrados y la memoria caché se actualiza. El VDA acepta conexiones provenientes de todos los Controllers de la lista más reciente que contenga en su memoria caché.
- Si un VDA recibe una lista que no incluye el Controller (o el Cloud Connector) en el que está registrado (en otras palabras, el Controller se quitó del sitio), el VDA vuelve a registrarse en algún Controller que sí conste en la lista `ListOfDDCs`.

Ejemplo:

- Una implementación contiene tres Controllers: A, B y C. Un VDA se registra en el Controller B (el cual se especificó durante la instalación del VDA).

- Más tarde, dos Controllers (D y E) se agregan al sitio. En los 90 minutos siguientes, los VDA reciben listas actualizadas y aceptan conexiones provenientes de los Controllers A, B, C, D y E (la carga no se reparte equitativamente entre todos los Controllers hasta que se reinicien los VDA).
- Posteriormente, se traslada al Controller B a otro sitio. En los 90 minutos siguientes, los VDA del sitio original reciben listas actualizadas porque se ha producido un cambio de Controllers desde la última comprobación. El VDA que se registró en su momento en el Controller B (que ya no está en la lista) vuelve a registrarse y elige entre los Controllers de la lista actual (A, C, D y E).

En una implementación de varias zonas, la actualización automática de una zona satélite almacena automáticamente en caché primero todos los Controllers locales. Todos los Controllers de la zona principal se almacenan en caché en un grupo de seguridad. Si no hay disponible ningún Controller local de la zona satélite, el VDA intenta registrarse en un Controller de la zona principal.

Como se muestra en el siguiente ejemplo, el archivo de memoria caché contiene nombres de host y una lista de identificadores de seguridad (ListOfSIDs). El VDA no consulta identificadores SID, lo que reduce la carga de Active Directory.

```
<?xml version="1.0"?>
<ListOfDDcsListfSids xmlns="http://schemas.datacontract.org/2004/07/Citrix.Cds.BrokerAgent" xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
  - <_x003C_GroupsOfDDcs_x003E_k__BackingField xmlns:d2p1="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
    - <d2p1:ArrayOfstring>
      <d2p1:string>CTX-XDC-002.zugec.lan</d2p1:string>
      <d2p1:string>CTX-XDC-001.zugec.lan</d2p1:string>
    </d2p1:ArrayOfstring>
  </_x003C_GroupsOfDDcs_x003E_k__BackingField>
  - <_x003C_ListOfDDcs_x003E_k__BackingField xmlns:d2p1="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
    <d2p1:string>CTX-XDC-002.zugec.lan</d2p1:string>
    <d2p1:string>CTX-XDC-001.zugec.lan</d2p1:string>
  </_x003C_ListOfDDcs_x003E_k__BackingField>
  - <_x003C_ListOfSids_x003E_k__BackingField xmlns:d2p1="http://schemas.microsoft.com/2003/10/Serialization/Arrays">
    <d2p1:string>S-1-5-21-726903571-3621260514-849154371-1119</d2p1:string>
    <d2p1:string>S-1-5-21-726903571-3621260514-849154371-1126</d2p1:string>
  </_x003C_ListOfSids_x003E_k__BackingField>
  <_x003C_NonAutoListofDDcsMethod_x003E_k__BackingField>RegistryBasedFarm</_x003C_NonAutoListofDDcsMethod_x003E_k__BackingField>
  <_x003C_NonAutoListofDDcsOrOu_x003E_k__BackingField>CTX-XDC-002.zugec.lan</_x003C_NonAutoListofDDcsOrOu_x003E_k__BackingField>
</ListOfDDcsListfSids>
```

Puede obtener el archivo de caché con una llamada WMI. No obstante, ese archivo se guarda en una ubicación que solo puede leer la cuenta de sistema.

#### Importante:

Esta información se ofrece únicamente para fines informativos. NO MODIFIQUE ESTE ARCHIVO. Cualquier modificación en este archivo o carpeta resulta en una configuración no compatible.

```
Get-WmiObject -Namespace "Root\Citrix\DesktopInformation" -Class "Citrix_VirtualDesktopInfo" -Property "PersistentDataLocation"
```

Si necesita configurar manualmente la lista `ListofSIDs` por razones de seguridad (a diferencia de motivos como la reducción de carga de Active Directory), no puede usar la función de actualización automática. Para obtener más información, consulte `ListofSIDs`.

## Excepción a la prioridad de actualización automática

Aunque normalmente la actualización automática tiene la prioridad más alta de todos los métodos de registro de VDA y anula la configuración de los demás métodos, existe una excepción. Los elementos `NonAutoListOfDDCs` en la memoria caché especifican el método inicial de configuración de VDA. La actualización automática supervisa esta información. Si cambia el método de registro inicial, el proceso de registro omite la actualización automática y usa el siguiente método de configuración de prioridad más alta. Esto puede ser útil cuando se mueve un VDA a otro sitio (por ejemplo, durante la recuperación ante desastres).

## Consideraciones sobre la configuración

Tenga en cuenta lo siguiente al configurar los elementos que pueden afectar el registro de VDA.

### Direcciones de Controller o Cloud Connector

Independientemente del método que utilice para especificar Controllers o Cloud Connectors, Citrix recomienda usar una dirección FQDN. Una dirección IP no se considera una configuración de confianza, porque es más fácil interceptar una IP que un registro DNS. Si rellena manualmente la lista `ListOfSIDs`, puede usar una IP en una lista `ListOfDDCs`. Aun así, se recomienda el FQDN.

### Equilibrio de carga

Como se ha indicado anteriormente, el VDA distribuye automáticamente las conexiones entre todos los Controllers o Cloud Connectors de la lista `ListOfDDCs`. La funcionalidad de equilibrio de carga y conmutación por error se ha integrado en el protocolo Citrix Brokering Protocol (CBP). Si especifica varios Controllers o Cloud Connectors en la configuración, el registro conmuta por error automáticamente entre ellos, si fuera necesario. Con la actualización automática, la conmutación por error automática se produce automáticamente para todos los VDA.

Por motivos de seguridad, no puede usar ningún equilibrador de carga de red, como Citrix ADC. En el registro del VDA, se utiliza la autenticación mutua de Kerberos, donde el cliente (VDA) debe demostrar su identidad al servicio (Controller). No obstante, el Controller o Cloud Connector también debe demostrar su identidad al VDA. Eso significa que el VDA y el Controller o Cloud Connector actúan como cliente y servidor al mismo tiempo. Como se ha indicado al principio de este artículo, hay dos canales de comunicación: VDA a Controller o Cloud Connector y Controller o Cloud Connector a VDA.

Existe un componente en este proceso que se denomina Service Principal Name (nombre principal de servicio o SPN), que se almacena como una propiedad en un objeto de equipo de Active Directory. Cuando el VDA intenta conectarse a un Controller o Cloud Connector, debe especificar “con quién”

quiere comunicarse. Esta dirección es un nombre SPN. Si utiliza una dirección IP con carga equilibrada, la autenticación mutua de Kerberos reconoce correctamente que la dirección IP no pertenece al Controller o Cloud Connector que debería.

Para obtener más información, consulte:

- [Introducción a Kerberos](#)
- [Autenticación mutua mediante Kerberos](#)

### **La actualización automática reemplaza CNAME**

La función de actualización automática sustituye a la función CNAME (alias de DNS) desde versiones de XenApp y XenDesktop anteriores a 7.x. La función CNAME se inhabilitó a partir de XenApp y XenDesktop 7. Utilice la actualización automática en lugar de CNAME. (Si le es necesario usar CNAME, consulte [CTX137960](#). Para que el alias de DNS funcione de manera coherente, no use la actualización automática y CNAME al mismo tiempo.)

### **Grupos de Controllers o Cloud Connectors**

En ciertos casos, puede que le interese procesar a los Controllers o Cloud Connectors por grupos, donde un grupo es el preferente y el otro se utiliza para una conmutación por error si fallan todos los Controllers o Cloud Connectors del primer grupo. Recuerde que los Controllers o Cloud Connectors se seleccionan aleatoriamente de la lista; por tanto, agruparlos puede fomentar la preferencia de un grupo sobre otro.

Estos grupos están diseñados para ser utilizados dentro de un único sitio (no en múltiples sitios).

Use paréntesis para especificar grupos de Controllers o Cloud Connectors. Por ejemplo, con cuatro Controllers (dos primarios y dos de seguridad), puede tener la siguiente agrupación:

`(XDC-001.cdz.lan XDC-002.cdz.lan) (XDC-003.cdz.lan XDC-004.cdz.lan)`

En este ejemplo, los Controllers del primer grupo (001 y 002) se procesan primero. Si ambos fallan, se procesan los Controllers del segundo grupo (003 y 004).

Para XenDesktop 7.0 o versiones posteriores, existe un paso adicional que debe seguir para usar la función **Grupos de registro**. Debe prohibir la directiva de Citrix Studio **Habilitar la actualización automática de Controller**

### **ListOfSIDs**

La lista de Controllers con los que un VDA puede contactar para el registro se llama [ListOfDDCs](#). Un VDA también debe saber con qué Controllers existe una relación de confianza. Los VDA no confían

automáticamente en los Controllers que haya en la lista `ListOfDDCs`. La lista `ListOfSIDs` (identificadores de seguridad) identifica a los Controllers de confianza. Los agentes VDA solo intentarán registrarse en los Controllers de confianza.

En la mayoría de los entornos, la lista `ListOfSIDs` se genera automáticamente a partir de la lista `ListOfDDCs`. Puede utilizar un rastreo CDF para leer la lista `ListOfSIDs`.

Por lo general, no es necesario modificar manualmente la lista `ListOfSIDs`. Sin embargo, existen varias excepciones a ello. Las dos primeras excepciones ya no son válidas, porque están disponibles tecnologías más recientes.

- **Separar roles para los Controllers:** Antes de que se introdujeran las zonas en XenApp y XenDesktop 7.7, la lista `ListOfSIDs` se configuraba manualmente cuando solo se utilizaba un subconjunto de los Controllers para el registro. Por ejemplo: si se utilizaba XDC-001 y XDC-002 como brokers XML, y XDC-003 y XDC-004 para el registro de VDA, se especificaban todos los Controllers en la lista `ListOfSIDs`, y XDC-003 y XDC-004 se indicaban en la lista `ListOfDDCs`. Ésta no es una configuración típica ni recomendada para entornos más recientes. En su lugar, use las zonas.
- **Reducir la carga de Active Directory:** Antes de que se introdujera la función de actualización automática en XenApp y XenDesktop 7.6, la lista `ListOfSIDs` se utilizaba para reducir la carga de los controladores de dominio. Al rellenarse previamente la lista `ListOfSIDs`, no se puede omitir la resolución de nombres DNS a identificadores SID. No obstante, la función de actualización automática elimina la necesidad de esta tarea, porque la memoria caché persistente contiene los identificadores SID. Citrix recomienda mantener habilitada la función de actualización automática.
- **Seguridad:** En algunos entornos muy protegidos, los SID de los Controllers de confianza se configuraban manualmente para evitar las posibles amenazas a la seguridad que podía representar un servidor DNS interceptado. Sin embargo, si hace esto, también debe desactivar la función de actualización automática. De lo contrario, se utiliza la configuración de caché persistente.

Por lo tanto, a menos que tenga un motivo concreto, no modifique la lista `ListOfSIDs`.

Si debe modificar `ListOfSIDs`, cree una clave de Registro llamada `ListOfSIDs (REG_SZ)` en `HKLM\Software\Citrix\VirtualDesktopAgent`. El valor es una lista de los SID de confianza, separados por espacios, si tiene más de uno.

En el siguiente ejemplo, se usa un Controller para el registro de VDA (`ListOfDDCs`), pero se utilizan dos Controllers para la intermediación (`List OfSIDs`).

Name	Type	Data
(Default)	REG_SZ	(value not set)
ControllerRegist...	REG_DWORD	0x00000050 (80)
HaModeCompu...	REG_SZ	
HaModeTimeEnd	REG_SZ	0
ListOfDDCs	REG_SZ	CTX-XDC-001.cdz.lan
ListOfSIDs	REG_SZ	S-1-5-21-2905519506-1074916935-2191873980-1121 S-1-5-21-2905519506-1074916935-2191873980-1118
ProductInstalled	REG_DWORD	0x00000008 (8)
RegistryOverride...	REG_DWORD	0x00000001 (1)
ResyncTimeOnF...	REG_DWORD	0x00000001 (1)
StartMenuScanE...	REG_SZ	C:\Program Files\Citrix\Virtual Desktop Agent\StartMenuScan.exe

## Búsqueda del Controller durante el registro de VDA

Cuando un VDA intenta registrarse, Broker Agent realiza primero una búsqueda DNS en el dominio local para asegurarse de que se puede acceder al Controller especificado.

Si en esa búsqueda inicial no se encuentra el Controller, Broker Agent puede iniciar una consulta de reserva de arriba hacia abajo en AD. Esa consulta examina todos los dominios y se repite con frecuencia. Si la dirección del Controller no es válida (por ejemplo, el administrador introdujo un FQDN incorrecto al instalar el VDA), la actividad de esa consulta puede provocar una condición de denegación de servicio distribuido (DDoS) en el controlador de dominio.

La siguiente clave del Registro controla si Broker Agent utiliza la consulta de reserva de arriba hacia abajo cuando no puede encontrar un Controller durante la búsqueda inicial.

`HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`

- Nombre: `DisableDdcWildcardNameLookup`
- Tipo: `DWORD`
- Valor: `1` (predeterminado) o `0`

Cuando se establece en `1`, la búsqueda de reserva está inhabilitada. Si la búsqueda inicial del Controller falla, Broker Agent deja de buscar. Esta es la opción predeterminada.

Cuando se establece en `0`, la búsqueda de reserva está habilitada. Si la búsqueda inicial del Controller falla, se inicia la búsqueda de reserva de arriba hacia abajo.

## Solucionar problemas en el registro de VDA

Como se ha indicado anteriormente, un VDA debe registrarse en un Delivery Controller para que se le tenga en cuenta al iniciar sesiones con broker. Los VDA no registrados pueden derivar en una infrutilización de los recursos disponibles. Existen diversos motivos por los que un VDA puede no registrarse, y un administrador puede solucionar muchos de ellos. Studio ofrece información para solucionar problemas en el Asistente para la creación de catálogos, después de que cree un grupo de entrega.

- **Identificación de problemas durante la creación del catálogo de máquinas:** En el Asistente para la creación de catálogos de máquinas, después de agregar las máquinas existentes, la lista de nombres de cuenta de equipo indicará si cada máquina es adecuada para agregarla al catálogo. Pase el puntero sobre el icono situado junto a cada máquina para ver un mensaje informativo sobre esa máquina.

Si el mensaje indica una máquina problemática, puede quitarla (mediante el botón **Quitar**) o agregarla. Por ejemplo, si un mensaje indica que no se ha podido obtener información acerca de una máquina (posiblemente porque nunca se registró en un Delivery Controller), puede optar por agregarla de todos modos.

Con el nivel funcional de un catálogo, decide qué funciones de producto están disponibles para las máquinas del catálogo. Para poder usar las funciones introducidas en las nuevas versiones de producto, es posible que necesite un nuevo VDA. Establecer un nivel funcional permite que todas las funcionalidades introducidas en esa versión (y versiones posteriores, si el nivel funcional no cambia) estén disponibles para las máquinas del catálogo. Sin embargo, las máquinas de ese catálogo que tengan una versión anterior de VDA no podrán registrarse.

- **Identificación de problemas después de crear los grupos de entrega:** Después de crear un grupo de entrega, Studio muestra información sobre las máquinas asociadas a ese grupo. El panel de detalles de un grupo de entrega indica la cantidad de máquinas que deberían estar registradas, pero no se han registrado. En otras palabras, una o varias máquinas que están activadas y no están en modo de mantenimiento, pero no están actualmente registradas en el Controller. Al ver una máquina que “no está registrada pero debería estarlo”, consulte el panel de detalles de la ficha Solución de problemas para buscar las posibles causas y las acciones correctivas recomendadas.

### Más información sobre la solución de problemas de registro de VDA

- Para obtener más información acerca de niveles funcionales, consulte la sección [Versiones de VDA y niveles funcionales](#).
- Para obtener más información sobre la solución de problemas de registro de VDA, consulte [CTX136668](#).
- También puede usar Citrix Health Assistant para solucionar problemas de inicio de sesiones y registro de VDA. Para obtener más información, consulte [CTX207624](#).

## Sesiones

March 21, 2023

El mantenimiento de la actividad de las sesiones es fundamental para ofrecer la mejor experiencia de uso. La pérdida de conectividad debido a redes poco fiables, a una latencia de red muy variable y a limitaciones del alcance de los dispositivos inalámbricos puede provocar frustración en el usuario. Poder cambiar rápidamente de una estación de trabajo a otra y acceder al mismo conjunto de aplicaciones cada vez que se inicie sesión es prioritario para muchos empleados móviles, como sería el caso de los empleados de un hospital.

Las funciones que se describen en este artículo optimizan la fiabilidad de las sesiones y reducen las molestias, los períodos de inactividad y la pérdida de productividad; con estas funciones, los usuarios móviles pueden trasladarse de unos equipos a otros fácil y rápidamente.

Además, puede cerrar la sesión o desconectar a un usuario, así como configurar el preinicio y la persistencia de sesiones. Para obtener más información, consulte [Administrar grupos de entrega](#).

## Fiabilidad de la sesión

La fiabilidad de la sesión mantiene las sesiones activas y en la pantalla de los usuarios cuando se interrumpe la conexión de red. Los usuarios siguen viendo la aplicación que están utilizando hasta que vuelve la conexión.

Esta función es especialmente útil para usuarios móviles con conexiones inalámbricas. Pensemos, por ejemplo, en un usuario con una conexión inalámbrica que se encuentra viajando en un tren y entra en un túnel, y pierde por un momento la conectividad. Por lo general, la sesión se desconecta y desaparece de la pantalla del usuario y después debe volver a conectarse. Con la función Fiabilidad de la sesión, la sesión permanece activa en la máquina. Para indicar que se ha perdido la conectividad, la pantalla del usuario se congela y el cursor se convierte en un reloj de arena giratorio hasta que se recupera la conectividad al salir del túnel. El usuario sigue teniendo acceso a la presentación en pantalla durante la interrupción y puede reanudar la interacción con la aplicación después de restablecerse la conexión de red. La función Fiabilidad de la sesión vuelve a conectar a los usuarios sin pedirles que repitan la autenticación.

Los usuarios de la aplicación Citrix Workspace no pueden anular la configuración de Controller.

Puede usar la función de fiabilidad de la sesión con Transport Layer Security (TLS). TLS cifra solo los datos enviados entre el dispositivo de usuario y Citrix Gateway.

Habilite y configure la fiabilidad de la sesión con las siguientes configuraciones de directiva:

- La configuración de directiva Conexiones de fiabilidad de la sesión permite o impide la fiabilidad de la sesión.
- La configuración de directiva Tiempo de espera de fiabilidad de la sesión tiene un tiempo predefinido de 180 segundos, o tres minutos. Aunque puede ampliar la cantidad de tiempo que Fiabilidad de la sesión mantiene abierta una sesión, esta función está diseñada para la comodidad del usuario, por lo que no pedirá a este que repita la autenticación. Si se alarga la cantidad

de tiempo que una sesión se mantiene abierta, se incrementa el riesgo de que un usuario se distraiga, se aleje del dispositivo y con ello facilite a usuarios no autorizados el acceso a la sesión.

- Las conexiones entrantes de fiabilidad de la sesión utilizan el puerto 2598 a menos que usted cambie el número de puerto definido en la configuración de directiva Número de puerto para fiabilidad de la sesión.
- Si no desea que los usuarios se reconecten con sesiones interrumpidas sin tener que repetir la autenticación, use la función Reconexión automática de clientes. Puede definir la configuración de la directiva Autenticación para Reconexión automática de clientes de manera que solicite a los usuarios que repitan la autenticación cuando vuelvan a conectarse a las sesiones interrumpidas.

Si usa tanto la fiabilidad de la sesión como la reconexión automática de clientes, las dos actúan de manera secuencial. La fiabilidad de la sesión cierra o desconecta la sesión de usuario después de transcurrido el tiempo que se especifica en la configuración de directiva Tiempo de espera de fiabilidad de la sesión. A continuación, se aplicará la configuración de directiva de Reconexión automática de clientes y se intentará reconectar al usuario con la sesión desconectada.

## Reconexión automática de clientes

Con la función de reconexión automática de clientes, la aplicación Citrix Workspace puede detectar desconexiones accidentales de las sesiones ICA y volver a conectar automáticamente a los usuarios de las sesiones afectadas. Cuando esta función está habilitada en el servidor, los usuarios no tienen que volver a conectarse de forma manual para continuar trabajando.

En sesiones de aplicación, la aplicación Citrix Workspace trata de reconectarse a la sesión hasta que lo logra o el usuario cancela el intento de reconexión.

En sesiones de escritorio, la aplicación Citrix Workspace intenta reconectarse a la sesión durante un período de tiempo especificado a menos que lo logre o el usuario cancele el intento de reconexión. De forma predeterminada, este período es de cinco minutos. Para cambiar este período de tiempo, modifique el Registro en el dispositivo de usuario:

HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;<seconds>

donde <seconds> es la cantidad de segundos después de los que no hay más intentos para volver a conectarse a la sesión.

Habilite y configure la Reconexión automática de clientes con las siguientes configuraciones de directiva:

- **Reconexión automática de clientes:** Habilita o inhabilita la reconexión automática de la aplicación Citrix Workspace cuando una sesión se ve interrumpida.
- **Autenticación para Reconexión automática de clientes:** Habilita o inhabilita el requisito de autenticación del usuario después de la reconexión automática.

- **Registro de Reconexión automática de clientes:** Habilita o inhabilita el registro de sucesos de reconexión en el registro de sucesos. El registro de sucesos está inhabilitado de forma predefinida. Si está habilitado, los registros de sistema del servidor capturan información sobre sucesos de reconexión automática correctos y fallidos. Cada servidor almacena información sobre los sucesos de reconexión en su propio registro de sistema; el sitio no proporciona los registros combinados de sucesos de reconexión en todos los servidores.

Reconexión automática de clientes incorpora un mecanismo de autenticación basado en credenciales de usuario cifradas. Cuando un usuario inicia una primera sesión, el servidor cifra y guarda en memoria las credenciales de usuario, y crea y envía a la aplicación Citrix Workspace una cookie que contiene la clave de cifrado. La aplicación Citrix Workspace envía la clave al servidor para la reconexión. El servidor descifra las credenciales y las envía al inicio de sesión de Windows para su autenticación. Cuando caducan las cookies, los usuarios deben repetir la autenticación para volver a conectarse a las sesiones.

Las cookies no se usan si se habilita la configuración Autenticación para Reconexión automática de clientes. En este caso, en su lugar, los usuarios ven un cuadro de diálogo que les solicita sus credenciales cuando la aplicación Citrix Workspace intenta reconectarse automáticamente.

Para lograr la máxima protección de las credenciales y las sesiones del usuario, utilice el cifrado para todas las comunicaciones entre los clientes y el sitio.

Inhabilite la función Reconexión automática de clientes en la aplicación Citrix Workspace para Windows mediante el archivo icaclient.adm. Para obtener más información, consulte la documentación correspondiente a su versión de la aplicación Citrix Workspace para Windows.

Las configuraciones de las conexiones también influyen en la función de reconexión automática de clientes:

- De forma predeterminada, la reconexión automática de clientes se habilita a través de las configuraciones de directiva en el nivel del sitio, como se describe anteriormente. No es necesario repetir la autenticación de los usuarios. Sin embargo, si la conexión ICA TCP del servidor está configurada para restablecer sesiones con un vínculo de comunicación interrumpido, la reconexión automática no se produce. La reconexión automática de clientes solo funciona si el servidor desconecta sesiones cuando existe alguna conexión interrumpida o que ha superado el tiempo de espera. En este contexto, la conexión ICA TCP hace referencia a un puerto virtual del servidor (en lugar de una conexión de red real) que se utiliza para las sesiones en redes TCP/IP.
- De manera predeterminada, la conexión ICA TCP de un servidor está configurada para desconectar sesiones cuya conexión se haya interrumpido o haya superado el tiempo de espera. Las sesiones desconectadas permanecen intactas en la memoria del sistema y la aplicación Citrix Workspace puede volver a conectarse a ellas.
- La conexión se puede configurar para restablecer o cerrar sesiones cuya conexión se haya interrumpido o haya superado el tiempo de espera. Si una sesión se restablece, los intentos de

reconexión inician una nueva sesión; es decir, en lugar de restaurar al usuario a la posición en que se encontraba la aplicación que estaba mediante, la aplicación se reinicia.

- Si el servidor está configurado para restablecer sesiones, la reconexión automática de clientes crea otra sesión. En este proceso, el usuario debe introducir sus credenciales para iniciar sesión en el servidor.
- Es posible que la reconexión automática no se lleve a cabo si la aplicación Citrix Workspace o el plugin envían una información de autenticación incorrecta; por ejemplo, durante un ataque o si el servidor determina que ha transcurrido demasiado tiempo desde que se detectó la interrupción de la conexión.

## ICA Keep-Alive

La habilitación de ICA Keep-Alive impide que las conexiones interrumpidas se desconecten. Cuando esta función está habilitada, si el servidor detecta que no hay actividad (por ejemplo, no hay cambios en el reloj, no hay movimientos del puntero ni actualizaciones de pantalla), esta función impide que Servicios de Escritorio remoto desconecte la sesión. El servidor envía paquetes de Keep-Alive cada pocos segundos a fin de detectar si la sesión está activa. Si la sesión ya no está activa, el servidor la marca como desconectada.

### Importante:

La función ICA Keep-Alive solo funciona si no se usa la función Fiabilidad de la sesión. Fiabilidad de la sesión tiene su propio mecanismo para impedir que las conexiones interrumpidas se desconecten. Configure ICA Keep-Alive únicamente para las conexiones que no usen Fiabilidad de la sesión.

Los parámetros de ICA Keep-Alive sobrescriben los parámetros de Keep-Alive configurados en la directiva de grupo de Microsoft Windows.

Habilite y configure ICA Keep-Alive con las siguientes configuraciones de directiva:

- **Tiempo de espera de ICA Keep Alive:** Especifica el intervalo de envío de mensajes de ICA Keep-Alive (de 1 a 3600 segundos). No seleccione esta opción si desea que su software de supervisión de red cierre las conexiones inactivas en los entornos en los que las conexiones interrumpidas son tan poco frecuentes que permitir que los usuarios se vuelvan a conectar a las sesiones no es relevante.

El intervalo predeterminado es 60 segundos: los paquetes de ICA Keep-Alive se envían a los dispositivos de usuario cada 60 segundos. Si un dispositivo del usuario no responde en 60 segundos, el estado de las sesiones ICA cambia a “Desconectado”.

- **ICA Keep Alive:** Envía o impide el envío de mensajes de ICA Keep-Alive.

## Control del espacio de trabajo

Con el control del espacio de trabajo, los escritorios y las aplicaciones permanecen disponibles para el usuario cuando éste pasa de un dispositivo a otro. Esta capacidad para moverse entre dispositivos permite que un usuario pueda acceder a todos sus escritorios o aplicaciones abiertas, desde cualquier lugar, simplemente iniciando una sesión, sin tener que reiniciar dichos escritorios y aplicaciones cuando cambia de dispositivo. Por ejemplo, el control del espacio de trabajo puede ser muy útil para los trabajadores de un hospital, que se desplazan rápidamente entre estaciones de trabajo y necesitan acceder al mismo conjunto de aplicaciones cada vez que inician una sesión. Si configura las opciones de control del espacio de trabajo con este propósito, estos trabajadores pueden desconectarse de varias aplicaciones en un dispositivo cliente y reconectarse a las mismas en un dispositivo cliente distinto.

El control del espacio de trabajo afecta a las siguientes actividades:

- **Inicio de sesión:** De manera predeterminada, el control del espacio de trabajo permite a los usuarios reconectarse automáticamente a todos los escritorios y las aplicaciones que estén ejecutándose simplemente iniciando una sesión, sin tener que volver a abrirlos manualmente. Mediante el control del espacio de trabajo, los usuarios pueden abrir aplicaciones y escritorios desconectados, así como otros que estén activos en otro dispositivo cliente. Cuando el usuario se desconecta de una aplicación o de un escritorio, estos siguen ejecutándose en el servidor. Si hay usuarios móviles que necesitan mantener en ejecución ciertas aplicaciones o escritorios en un dispositivo cliente, mientras se reconectan con un subconjunto de sus aplicaciones y escritorios en otro dispositivo cliente distinto, puede configurar el comportamiento de reconexión durante el inicio de sesión para que se abran solo los escritorios y aplicaciones de los que se haya desconectado el usuario anteriormente.
- **Reconexión:** Después de iniciar una sesión en el servidor, los usuarios pueden reconectarse a todos sus escritorios o aplicaciones en cualquier momento haciendo clic en Reconectar. De manera predeterminada, la función Reconectar abre los escritorios y aplicaciones desconectados, además de los que estén ejecutándose en ese momento en otro dispositivo cliente. Puede configurar la función Reconectar para que abra solo los escritorios y aplicaciones de los que se desconectó el usuario anteriormente.
- **Cierre de sesión:** En el caso de usuarios que abren aplicaciones o escritorios mediante StoreFront, puede configurar el comando Cerrar sesión para que el usuario cierre su sesión en StoreFront y en todas las sesiones activas conjuntamente, o bien para que solo cierre la sesión en StoreFront.
- **Desconexión:** Los usuarios se pueden desconectar de todos los escritorios y aplicaciones a la vez, sin necesidad de desconectarse de cada uno de ellos individualmente.

El control del espacio de trabajo solamente está disponible para los usuarios de la aplicación Citrix Workspace que acceden a escritorios y aplicaciones a través de una conexión de Citrix StoreFront. De

manera predeterminada, el control del espacio de trabajo está inhabilitado para las sesiones de escritorio virtual, pero está habilitado para las aplicaciones alojadas en servidores. El uso compartido de sesiones no se produce de manera predeterminada entre los escritorios publicados y las aplicaciones publicadas que se ejecutan en esos escritorios.

Las directivas de usuario, asignaciones de unidad cliente y configuraciones de impresora cambian según sea necesario al cambiar el usuario de dispositivo cliente. Las directivas y asignaciones se aplican según el dispositivo cliente donde el usuario haya iniciado sesión. Por ejemplo, si un trabajador cierra sesión en un dispositivo cliente en el área de Urgencias del hospital y luego inicia una sesión en una estación de trabajo del Laboratorio de rayos X, las directivas, las asignaciones de impresora y las asignaciones de unidades del cliente adecuadas para la sesión en el Laboratorio de rayos X entran en efecto en el momento en que se inicia esa nueva sesión.

Puede personalizar qué impresoras se muestran a los usuarios cuando éstos cambian de ubicación. También puede controlar si los usuarios pueden imprimir en impresoras locales, cuánto ancho de banda pueden consumir cuando se conectan de forma remota, así como otros aspectos de la impresión.

Si desea más información sobre cómo habilitar y configurar el control del espacio de trabajo para los usuarios, consulte la documentación de StoreFront.

## **Itinerancia de sesiones**

De forma predeterminada, las sesiones se mueven con el usuario entre los diferentes dispositivos cliente. Cuando el usuario inicia una sesión y, más tarde, cambia de dispositivo, se utiliza la misma sesión y las aplicaciones están disponibles en ambos dispositivos. Las aplicaciones se mueven, independientemente del dispositivo o de si las sesiones actuales existen. En muchos casos, las impresoras y otros recursos asignados a la aplicación también se mueven.

Aunque este comportamiento predeterminado ofrece muchas ventajas, es posible que no sea el mejor para todos los casos. Puede impedir la movilidad de sesión mediante el SDK de PowerShell.

Ejemplo 1. Un miembro del personal médico usa dos dispositivos: uno para completar un formulario del seguro en un equipo de escritorio y otro para consultar información sobre un paciente en una tableta.

- Si la movilidad de sesión está habilitada, ambas aplicaciones aparecerán en ambos dispositivos (una aplicación iniciada en un dispositivo es visible en todos los dispositivos en uso). Es posible que este comportamiento no cumpla los requisitos de seguridad.
- Si se inhabilita la movilidad de sesión, el registro del paciente no aparecerá en el equipo de escritorio y el formulario del seguro no aparecerá en la tableta.

Ejemplo 2. Un director de producción inicia una aplicación en su equipo de oficina. La ubicación y el nombre del dispositivo determinan qué impresoras y otros recursos están disponibles para esa sesión.

Más tarde en la misma jornada laboral, el director va a una oficina situada en el edificio contiguo con el objetivo de asistir a una reunión para la que necesitará usar una impresora.

- Si la movilidad de sesión está habilitada, posiblemente el director de producción no podrá acceder a las impresoras de la sala de la reunión porque las aplicaciones que inició antes, en su oficina, resultaron en la asignación de impresoras y otros recursos cercanos a esa ubicación.
- Si la movilidad de sesión está inhabilitada, cuando inicie sesión en otra máquina (con las mismas credenciales), se iniciará una nueva sesión y las impresoras y los recursos cercanos estarán disponibles.

### Configurar la itinerancia de sesiones

Para configurar la movilidad de sesión, use los siguientes cmdlets de la regla de directiva de derechos con la propiedad “SessionReconnection”. Opcionalmente, también puede especificar la propiedad “LeasingBehavior”.

Para sesiones de escritorio:

```
Set-BrokerEntitlementPolicyRule \<Delivery-Group-name> -SessionReconnection  
 \<value> -LeasingBehavior Allowed|Disallowed
```

Para sesiones de aplicación:

```
Set-BrokerAppEntitlementPolicyRule \<Delivery-Group-name> -SessionReconnection  
 \<value> -LeasingBehavior Allowed|Disallowed
```

Donde <value> puede ser una de las siguientes opciones:

- **Always:** Las sesiones siempre se mueven, independientemente del dispositivo cliente y si la sesión está conectada o desconectada. Este es el valor predeterminado.
- **DisconnectedOnly:** Reconnectarse solo a sesiones que ya se han desconectado; de lo contrario, iniciar una nueva sesión. (Las sesiones pueden moverse entre dispositivos cliente primero desconectándolos, o bien mediante el control del espacio de trabajo para moverlas explícitamente.) Una sesión activa conectada desde otro dispositivo cliente no se utiliza nunca; en su lugar, se inicia una nueva sesión.
- **SameEndpointOnly:** El usuario obtiene una sesión única para cada dispositivo que use. Esto inhabilita completamente la movilidad. Los usuarios solo pueden volver a conectarse al mismo dispositivo que usaron anteriormente en la sesión.

La propiedad “LeasingBehavior” se describe más adelante.

### Efectos de otras opciones de configuración:

La inhabilitación de la movilidad de sesión se ve afectada por el límite para aplicaciones “Permitir una sola instancia de aplicación por usuario” en las propiedades de aplicación, en el grupo de entrega.

- Si inhabilita la movilidad de sesión, inhabilite el límite para aplicaciones “Permitir una sola instancia de aplicación por usuario”.
- Si habilita el límite para aplicaciones “Permitir una sola instancia de aplicación por usuario”, no configure uno de los dos valores que permiten sesiones nuevas en dispositivos nuevos.

## Intervalo de inicio de sesión

Si una máquina virtual que contiene un escritorio VDA se cierra antes de que se complete el proceso de inicio de sesión, se puede asignar más tiempo al proceso. El valor predeterminado para 7.6 y versiones posteriores es de 180 segundos, mientras que el predeterminado para versiones de 7.0 a 7.5 es de 90 segundos.

En la máquina (o la imagen maestra utilizada en un catálogo de máquinas), defina la siguiente clave de Registro:

Clave: HKLM\SOFTWARE\Citrix\PortICA

- Valor: AutoLogonTimeout
- Tipo: DWORD
- Especifique un número decimal en segundos que vaya de 0 a 3600.

Si cambia una imagen maestra, actualice el catálogo.

Esta configuración se aplica solo a las máquinas virtuales con agentes VDA de escritorio (estaciones de trabajo). Microsoft controla el tiempo de espera de inicio de sesión en las máquinas con servidores VDA.

## Usar búsquedas en Studio

February 6, 2020

Utilice la función de búsqueda para ver información sobre máquinas, sesiones, catálogos de máquinas, aplicaciones o grupos de entrega específicos.

1. Seleccione **Buscar** en el panel de navegación de Studio.

No se puede buscar dentro de las fichas Catálogos de máquinas o Grupos de entrega desde el cuadro de búsqueda. Use el nodo Buscar en el panel de navegación.

Para mostrar criterios de búsqueda adicionales en la pantalla, haga clic en el signo más, junto a los campos desplegados de búsqueda. Quite criterios de búsqueda haciendo clic en el botón de menos.

2. Escriba el nombre o use la lista desplegable para seleccionar otra opción de búsqueda para el elemento que quiere buscar.
3. También puede guardar la búsqueda si selecciona **Guardar como**. La búsqueda aparece en la lista **Búsquedas guardadas**.

Si lo prefiere, también puede hacer clic en el icono **Expandir búsqueda** (doble corchete angular hacia abajo) para mostrar un menú de propiedades de búsqueda. Puede realizar una búsqueda avanzada creando una expresión a partir de las propiedades del menú.

Sugerencias para mejorar la búsqueda:

- Para mostrar las funciones adicionales a incluir en la pantalla en la que puede buscar y ordenar, haga clic con el botón secundario en cualquier columna y seleccione **Seleccionar columnas**.
- Para buscar un dispositivo de usuario conectado a una máquina, use **Cliente (IP)** y **Es** y escriba la dirección IP del dispositivo.
- Para buscar sesiones activas, use **Estado de la sesión, Es y Conectado**.
- Para enumerar todas las máquinas de un grupo de entrega, seleccione **Grupos de entrega** en el panel de navegación, seleccione el grupo pertinente y, a continuación, seleccione **Ver máquinas** en el panel Acciones.

## Etiquetas

September 22, 2021

### Introducción

Las etiquetas son cadenas que identifican elementos como, por ejemplo, máquinas, aplicaciones, escritorios, grupos de entrega, grupos de aplicaciones y directivas. Después de crear una etiqueta y agregarla a un elemento, puede adaptar determinadas operaciones para que solo se apliquen a los elementos que tengan esa etiqueta concreta.

- Personalizar las pantallas de búsquedas en Studio.  
Por ejemplo, si quiere que solo se muestren las aplicaciones que se hayan optimizado de cara a evaluadores, cree una etiqueta llamada “evaluar” y agréguela (aplíquela) a esas aplicaciones. Entonces, podrá filtrar la búsqueda de Studio con la etiqueta “evaluar”.
- Publicar aplicaciones de un grupo de aplicaciones o escritorios concretos de un grupo de entrega, teniendo en cuenta solo un subconjunto de las máquinas en los grupos de entrega seleccionados. Esto se denomina una *restricción por etiquetas*.

Con una restricción por etiquetas, puede usar las máquinas existentes para más de una tarea de publicación, con lo que se ahorran los costes asociados a la implementación y la administración de más máquinas. La restricción de etiqueta puede entenderse como una subdivisión (o partición) de las máquinas de un grupo de entrega. Su funcionalidad es similar (pero no idéntica) a los grupos de trabajo en las versiones de XenApp anteriores a 7.x.

Usar un grupo de aplicaciones o escritorios con una restricción de etiqueta puede ser útil para aislar un subconjunto de las máquinas de un grupo de entrega y solucionar los problemas que presentan.

- Programar reinicios periódicos para un subconjunto de las máquinas de un grupo de entrega.

Una restricción de etiqueta en las máquinas permite utilizar los nuevos cmdlets de PowerShell para configurar varias programaciones de reinicios para subconjuntos de máquinas en un grupo de entrega. Para obtener más información, consulte [Administrar grupos de entrega](#).

- Personalizar la aplicación (asignación) de las directivas de Citrix a máquinas de los grupos de entrega, tipos de grupos de entrega o unidades organizativas que contienen (o no) una etiqueta especificada.

Por ejemplo, si quiere aplicar una directiva de Citrix solo a las estaciones de trabajo más potentes, agregue una etiqueta llamada “potencia alta” a esas máquinas. A continuación, en la página **Asignar directiva**, seleccione esa etiqueta y la casilla **Habilitar**. También puede agregar una etiqueta a un grupo de entrega y, a continuación, aplicar una directiva de Citrix a ese grupo. Para obtener más información, consulte [Crear directivas](#).

Puede aplicar etiquetas a:

- Máquinas
- Aplicaciones
- Catálogos de máquinas (solo para PowerShell; consulte Etiquetas en catálogos de máquinas)
- Grupos de entrega
- Grupos de aplicaciones

Puede configurar una restricción de etiqueta al crear o modificar lo siguiente en Studio:

- Un escritorio en un grupo de entrega compartido
- Un grupo de aplicaciones

## Restricciones de etiqueta para un grupo de escritorios o aplicaciones

Una restricción por etiquetas implica varios pasos:

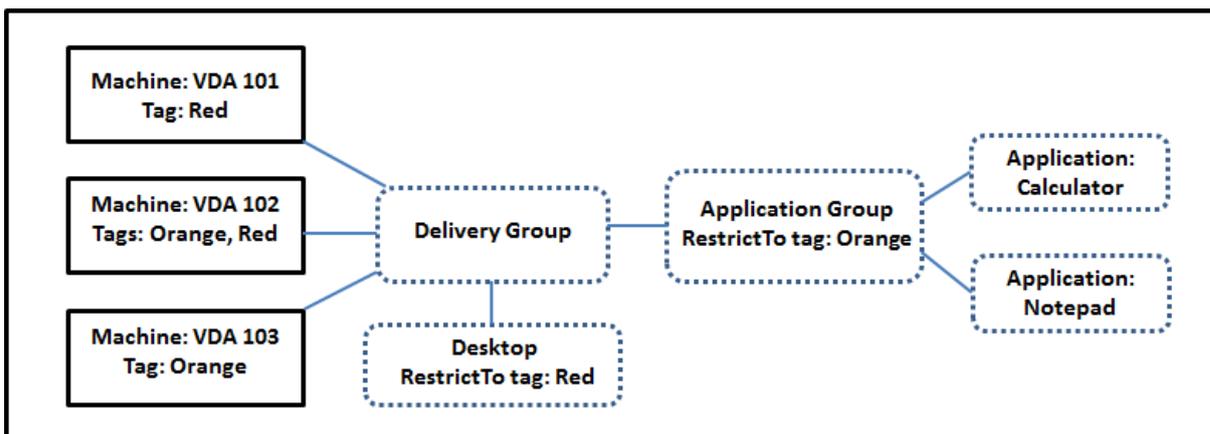
- Crear la etiqueta y, a continuación, agregarla (aplicarla) a las máquinas.

- Crear o modificar un grupo con la restricción de etiqueta (en otras palabras, “restringir inicios a máquinas con la etiqueta x”).

La restricción por etiquetas amplía el proceso de selección de máquinas del intermediario. El broker selecciona una máquina de un grupo de entrega asociado al que se aplican: la directiva de acceso, las listas de usuarios configurados, la preferencia de zonas, la disponibilidad de inicio y la restricción de etiqueta (si existe). Para las aplicaciones, el broker recurre a otros grupos de entrega por orden de prioridad, aplica las mismas reglas de selección de máquinas para cada grupo de entrega que se tiene en cuenta.

### Ejemplo 1: Distribución sencilla

En este ejemplo, se presenta una distribución sencilla que usa restricciones por etiqueta para limitar las máquinas que se tienen en cuenta para ciertos inicios de aplicaciones y escritorios. El sitio tiene un grupo de entrega compartido, un escritorio publicado, y un grupo de aplicaciones configurado con dos aplicaciones.



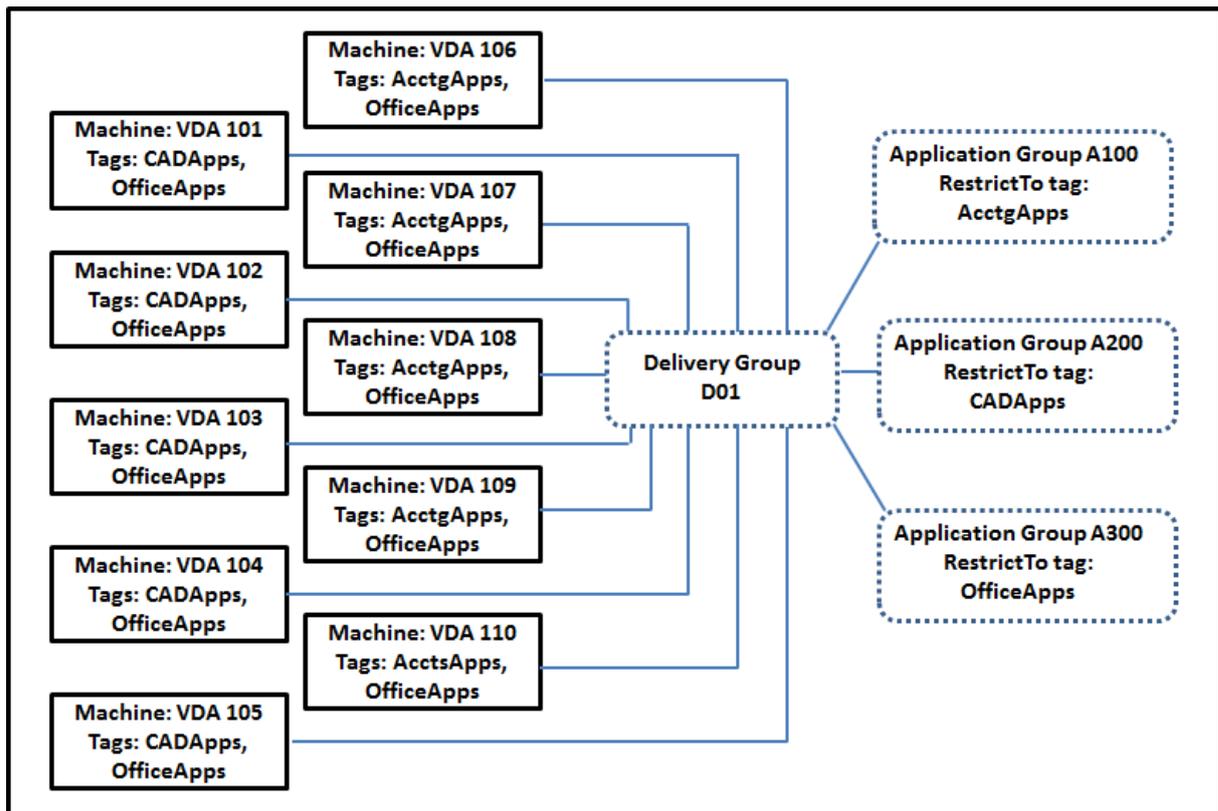
- Se han agregado etiquetas a cada una de las tres máquinas (VDA 101, 102 y 103).
- El escritorio del grupo de entrega compartido se creó con una restricción de etiqueta llamada **Red**, por lo que ese escritorio solo se puede iniciar en las máquinas de ese grupo de entrega que tengan la etiqueta **Red**: VDA 101 y 102.
- El grupo de aplicaciones se creó con la restricción de etiqueta **Orange**, por lo que cada una de sus aplicaciones (Calculadora y Bloc de notas) solo se pueden iniciar en las máquinas de ese grupo de entrega que tengan la etiqueta **Orange**: VDA 102 y 103.

La máquina VDA 102 tiene ambas etiquetas (**Red** y **Orange**); por lo tanto, puede considerarse para iniciar las aplicaciones y el escritorio.

## Ejemplo 2: Distribución más compleja

En este ejemplo, existen varios grupos de aplicaciones que se han creado con restricciones de etiqueta. Por eso, se pueden entregar más aplicaciones con menos máquinas de las que se necesitarían si solo se usaran grupos de entrega.

En Ejemplo 2: Cómo configurar, se describen los pasos que hay que seguir para crear, aplicar las etiquetas y configurar las restricciones de etiqueta de este ejemplo.



En este ejemplo, se utilizan 10 máquinas (VDA 101-110), un grupo de entrega (D01) y tres grupos de aplicaciones (A100, A200 y A300). Si aplica etiquetas a cada máquina y especifica las restricciones de etiqueta cuando cree cada grupo de aplicaciones:

- Los usuarios de Contabilidad del grupo pueden acceder a las aplicaciones que necesitan en cinco máquinas (VDA de 101 a 105)
- Los diseñadores de CAD del grupo pueden acceder a las aplicaciones que necesitan en cinco máquinas (VDA de 106 a 110)
- Los usuarios del grupo que necesitan las aplicaciones de Office pueden acceder a las aplicaciones Office en 10 máquinas (VDA de 101 a 110)

Solo se utilizan 10 máquinas, con un solo grupo de entrega. Usar solo grupos de entrega (sin grupos de aplicaciones) requeriría el doble de máquinas, porque una máquina solo puede pertenecer a un grupo de entrega.

## Administrar etiquetas y restricciones por etiqueta

Las etiquetas se crean y se agregan (se aplican), se modifican y se eliminan de los elementos seleccionados mediante la acción **Administrar etiquetas** en Studio.

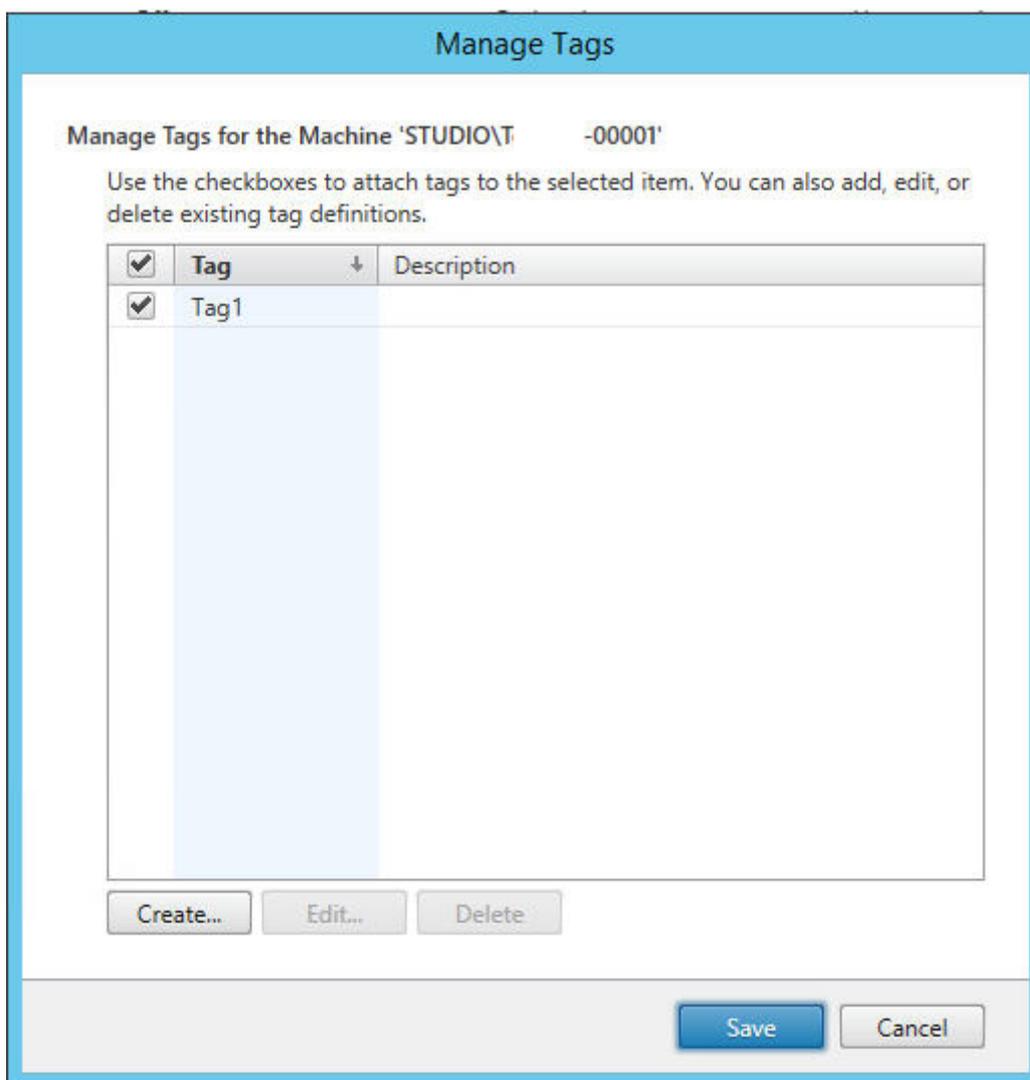
(Excepción: Las etiquetas que se utilizan para las asignaciones de directiva se crean, se modifican y se eliminan mediante la acción **Administrar etiquetas** en Studio. Sin embargo, las etiquetas se aplican (se asignan) en el momento de crear la directiva. Consulte [Crear directivas](#) para obtener más detalles.)

Las restricciones de etiqueta se configuran cuando crea o modifica los escritorios de los grupos de entrega, y cuando crea y modifica grupos de aplicaciones.

### Uso del cuadro de diálogo Administrar etiquetas en Studio

En Studio, seleccione los elementos a los que quiere aplicar una etiqueta (máquinas, aplicaciones, un escritorio, un grupo de entrega o un grupo de aplicaciones) y, a continuación, seleccione **Administrar etiquetas** en el panel Acciones. El cuadro de diálogo **Administrar etiquetas** muestra todas las etiquetas que se han creado en el sitio, no solo las correspondientes a los elementos seleccionados.

- La casilla de verificación que contiene una marca indica que la etiqueta ya se ha agregado a los elementos seleccionados. (En la captura de pantalla siguiente, la etiqueta llamada `Tag1` se aplica a la máquina seleccionada.)
- Si ha seleccionado más de un elemento, una casilla de verificación que contiene un guión indica que algunos elementos seleccionados (pero no todos) tienen agregada esa etiqueta.



Puede llevar a cabo estas acciones desde el cuadro de diálogo **Administrar etiquetas**. Revise Precauciones al trabajar con etiquetas.

- **Para crear una etiqueta:**

Haga clic en **Crear**. Escriba un nombre y una descripción. Los nombres de etiqueta deben ser únicos; en ellos, no se distingue entre mayúsculas y minúsculas. Luego haga clic en **Aceptar**. (Crear una etiqueta no la aplica automáticamente a los elementos que haya seleccionado. Utilice las casillas de verificación para aplicar la etiqueta.)

- **Para agregar (aplicar) una o varias etiquetas:**

Marque la casilla de verificación situada junto al nombre de la etiqueta. Si marca varios elementos y la casilla ubicada junto a una etiqueta contiene un guión (para indicar que algunos pero no todos los elementos seleccionados ya tienen aplicada la etiqueta), cambiar ese guión a una marca de verificación afectará a todas las máquinas seleccionadas.

Si intenta agregar una etiqueta a las máquinas y resulta que esa etiqueta se usa como restricción en un grupo de aplicaciones, Studio advierte que la acción puede provocar que esas máquinas estén disponibles para el inicio. Si es lo que quería hacer, continúe.

- **Para quitar una o varias etiquetas:**

Desmarque la casilla de verificación situada junto al nombre de la etiqueta. Un guión en la casilla de verificación indica que algunos elementos seleccionados (pero no todos) ya tienen aplicada la etiqueta. Si ha seleccionado varios elementos y la casilla situada junto a una etiqueta contiene un guión, al desmarcar esa casilla, se quitará la etiqueta de todas las máquinas seleccionadas.

Si intenta quitar una etiqueta desde una máquina que la utiliza como una restricción, Studio le advertirá de que su acción podría afectar a las máquinas que se tienen en cuenta para el inicio. Si es lo que quería hacer, continúe.

- **Para modificar una etiqueta:**

Seleccione una etiqueta y, a continuación, haga clic en **Modificar**. Introduzca un nuevo nombre, descripción o ambos. Solo puede modificar una etiqueta a la vez.

- **Para eliminar una o varias etiquetas:**

Seleccione las etiquetas y, a continuación, haga clic en **Eliminar**. El cuadro de diálogo **Eliminar etiqueta** indica la cantidad de elementos que usan en ese momento las etiquetas seleccionadas (por ejemplo, “2 máquinas”). Haga clic en un elemento para ver más información. Por ejemplo, hacer clic en “2 máquinas” mostrará los nombres de las dos máquinas que tienen aplicada la etiqueta. Confirme si quiere eliminar las etiquetas.

No puede usar Studio para eliminar una etiqueta que se usa como una restricción. Primero, debe modificar el grupo de aplicaciones y quitar la restricción de etiqueta o seleccionar otra etiqueta.

Cuando haya terminado en el cuadro de diálogo **Administrar etiquetas**, haga clic en **Guardar**.

Para ver si una máquina tiene etiquetas aplicadas: Seleccione **Grupos de entrega** en el panel de navegación. Seleccione un grupo de entrega en el panel central y, a continuación, seleccione **Ver máquinas** en el panel Acciones. Seleccione una máquina en el panel central y, a continuación, seleccione la ficha Etiquetas en el panel Detalles.

## **Administrar restricciones por etiqueta**

Configurar una restricción de etiqueta es un proceso de varios pasos: Primero, debe crear la etiqueta y agregarla o aplicarla a las máquinas. A continuación, debe agregar la restricción al grupo de aplicaciones o al escritorio.

- **Para crear y aplicar la etiqueta:**

Cree la etiqueta y, a continuación, agréguela (aplíquela) a las máquinas afectadas por la restricción de etiqueta mediante las acciones de **Administrar etiquetas** descritas anteriormente.

- **Para agregar una restricción de etiqueta a un grupo de aplicaciones:**

Cree o modifique el grupo de aplicaciones. En la página Grupos de entrega, seleccione **Restringir inicios a máquinas con la etiqueta** y, a continuación, seleccione la etiqueta en la lista.

- **Para cambiar o quitar una restricción de etiqueta de un grupo de aplicaciones:**

Modifique el grupo. En la página Grupos de entrega, seleccione otra etiqueta en la lista o quite la restricción de etiqueta por completo desmarcando **Restringir inicios a máquinas con la etiqueta**.

- **Para agregar una restricción por etiquetas a un escritorio:**

Cree o modifique un grupo de entrega. Haga clic en **Agregar** o **Modificar** en la página **Escritorios**. En el cuadro de diálogo Agregar escritorio, marque **Restringir inicios a máquinas con la etiqueta** y, a continuación, seleccione la etiqueta en el menú.

- **Para cambiar o quitar la restricción de etiqueta de un grupo de entrega:**

Modifique el grupo. En la página **Escritorios**, haga clic en **Modificar**. En el cuadro de diálogo, seleccione otra etiqueta en la lista o quite la restricción de etiqueta por completo desmarcando **Restringir inicios a máquinas con la etiqueta**.

## **Precauciones al trabajar con etiquetas**

Una etiqueta que se aplica a un elemento se puede usar para distintos fines, por lo tanto, tenga en cuenta que agregar, quitar y eliminar una etiqueta puede tener efectos no deseados. Puede utilizar una etiqueta para ordenar máquinas en el campo de búsqueda de Studio. Puede utilizar la misma etiqueta como restricción en un grupo de aplicaciones o un escritorio. Así, hará que solo se tengan en cuenta para inicio las máquinas de los grupos de entrega especificados que tengan esa etiqueta.

Si intenta agregar una etiqueta a máquinas cuando esa etiqueta ya se utiliza como restricción de etiqueta para un escritorio o un grupo de aplicaciones, Studio mostrará una advertencia. Agregar esa etiqueta puede hacer que las máquinas estén disponibles para iniciar otras aplicaciones o escritorios. Si es su objetivo, continúe. Si no, cancele la operación.

Por ejemplo, supongamos que crea un grupo de aplicaciones con la restricción de etiqueta **Red**". Posteriormente, agrega otras máquinas a los mismos grupos de entrega que utiliza ese grupo de aplicaciones. Si, a continuación, intenta agregar la etiqueta **Red** a esas máquinas, Studio mostrará un mensaje similar a: "La etiqueta 'Red' se utiliza como restricción en los siguientes grupos de aplicaciones. Agregar esta etiqueta puede hacer que las máquinas seleccionadas estén disponibles para

iniciar las aplicaciones de este grupo de aplicaciones”. Puede confirmar o cancelar la operación de agregar esa etiqueta a esas máquinas adicionales.

Del mismo modo, si se utiliza una etiqueta en un grupo de aplicaciones para restringir inicios, Studio le advierte que no puede eliminar la etiqueta hasta que modifique el grupo y la quite como restricción. (Si pudiera eliminar una etiqueta que se usa como una restricción en un grupo de aplicaciones, podría provocar que se permita iniciar las aplicaciones en todas las máquinas de los grupos de entrega asociados al grupo de aplicaciones.) La misma prohibición de eliminar una etiqueta se aplica si esta se utiliza como una restricción para inicios de escritorio. Después de modificar el grupo de aplicaciones o escritorios en el grupo de entrega para quitar la restricción de etiqueta, puede eliminar la etiqueta.

Es posible que no todas las máquinas tengan el mismo conjunto de aplicaciones. Un usuario puede pertenecer a más de un grupo de aplicaciones, cada uno con una restricción de etiqueta diferente y conjuntos de máquinas diferentes o iguales en los grupos de entrega. En la tabla siguiente, se ofrece una lista de cómo se tienen en cuenta las máquinas.

<b>Cuando una aplicación se ha agregado a</b>	<b>Estas máquinas de los grupos de entrega seleccionados se tienen en cuenta para el inicio</b>
Un grupo de aplicaciones sin restricción de etiqueta	Cualquier máquina
Un grupo de aplicaciones con una restricción de etiqueta A	Máquinas que tienen aplicada la etiqueta A
Dos grupos de aplicaciones: uno con una restricción de etiqueta A y otro con una restricción de etiqueta B	Máquinas que tienen las etiquetas A y B; si no hay ninguna disponible, máquinas que tienen la etiqueta A o B
Dos grupos de aplicaciones: uno con una restricción de etiqueta A y otro sin restricción de etiqueta	Máquinas que tienen la etiqueta A. Si no hay ninguna disponible, cualquier máquina

Si ha utilizado una restricción por etiquetas en una programación de reinicios, los cambios que realice que afecten a las aplicaciones o las restricciones por etiqueta afectarán al próximo ciclo de reinicios. Lo que no afecta a los ciclos de reinicios en vigor mientras se realizan los cambios.

### **Ejemplo 2: Cómo configurar**

En la siguiente secuencia, se muestran los pasos a seguir para crear y aplicar las etiquetas, así como para configurar las restricciones de etiqueta para los grupos de aplicaciones representados en el segundo ejemplo.

Los agentes VDA y las aplicaciones ya se han instalado en las máquinas y el grupo de entrega se ha creado.

Crear etiquetas y aplicarlas a las máquinas:

1. En Studio, seleccione el grupo de entrega **D01** y, a continuación, seleccione **Ver máquinas** en el panel Acciones.
2. Seleccione las máquinas VDA de la 101 a la 105 y, a continuación, seleccione **Administrar etiquetas** en el panel Acciones.
3. En el cuadro de diálogo **Administrar etiquetas**, haga clic en **Crear**. Cree una etiqueta llamada **CADApps**. Haga clic en **OK**.
4. Haga clic de nuevo en **Crear** y cree una etiqueta llamada **OfficeApps**. Haga clic en **OK**.
5. Mientras esté todavía en el cuadro de diálogo **Administrar etiquetas**, agregue (aplique) las etiquetas recién creadas a las máquinas seleccionadas marcando las casillas de verificación situadas junto al nombre de cada etiqueta (**CADApps** y **OfficeApps**). Cierre el cuadro de diálogo.
6. Seleccione el grupo de entrega **D01** y, a continuación, seleccione **Ver máquinas** en el panel Acciones.
7. Seleccione las máquinas VDA de la 106 a la 110 y, a continuación, seleccione **Administrar etiquetas** en el panel Acciones.
8. En el cuadro de diálogo **Administrar etiquetas**, haga clic en **Crear**. Cree una etiqueta llamada **AcctgApps**. Haga clic en **OK**.
9. Aplique la etiqueta recién creada **AcctgApps** y la etiqueta **OfficeApps** a las máquinas seleccionadas marcando las casillas de verificación situadas junto al nombre de cada etiqueta. Cierre el cuadro de diálogo.

Cree los grupos de aplicaciones con restricciones de etiqueta.

1. En Studio, seleccione **Aplicaciones** en el panel de navegación y, a continuación, seleccione **Crear grupo de aplicaciones** en el panel Acciones.
2. En la página **Grupos de entrega**, seleccione el grupo de entrega **D01**. Seleccione **Restringir inicios a máquinas con la etiqueta**. A continuación, seleccione la etiqueta **AcctgApps** de la lista.
3. Para completar el asistente, especifique los usuarios y las aplicaciones de contabilidad (al agregar la aplicación, seleccione el origen **Desde el menú Inicio**, que busca la aplicación en las máquinas que tienen la etiqueta **AcctgApps**). En la página **Resumen**, especifique un nombre para el grupo **A100**.
4. Repita los pasos anteriores para crear el grupo de aplicaciones **A200**, en que especifique las máquinas que tienen la etiqueta **CADApps**, además de sus usuarios y aplicaciones pertinentes.
5. Repita estos pasos para crear el grupo de aplicaciones **A300**, en que especifique las máquinas que tienen la etiqueta **OfficeApps**, además de sus usuarios y aplicaciones pertinentes.

## Etiquetas en catálogos de máquinas

Puede utilizar etiquetas en catálogos de máquinas. La secuencia general de creación de etiquetas y, a continuación, aplicarla a un catálogo es la misma que la descrita anteriormente. Sin embargo, la aplicación de etiquetas a catálogos solo se puede hacer a través de la interfaz de PowerShell. No se puede utilizar Studio para aplicar ni quitar etiquetas de catálogos. Las pantallas de los catálogos en Studio no indican si se han aplicado etiquetas.

Resumen: Puede utilizar Studio o PowerShell para crear o eliminar etiquetas para su uso en catálogos. Utilice PowerShell para aplicarlas a los catálogos.

He aquí algunos ejemplos de uso de etiquetas con catálogos:

- Un grupo de entrega tiene máquinas de varios catálogos, pero en este caso es mejor una operación (como, por ejemplo, una programación de reinicios) que afecte solamente a las máquinas de un catálogo específico. Aplicar una etiqueta a ese catálogo cumple dicho objetivo.
- En un grupo de aplicaciones, digamos que quiere limitar las sesiones de aplicación a las máquinas de un catálogo específico. Aplicar una etiqueta a ese catálogo cumple dicho objetivo.

Cmdlets de PowerShell afectados:

- Puede pasar objetos de catálogo a cmdlets como `Add-BrokerTag` y `Remove-BrokerTag`.
- `Get-BrokerTagUsage` muestra cuántos catálogos contienen etiquetas.
- `Get-BrokerCatalog` tiene una propiedad llamada `Tags`.

Por ejemplo, los siguientes cmdlets agregan una etiqueta denominada `fy2018` al catálogo `acctg`: `Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018` (la etiqueta se ha creado previamente con Studio o PowerShell).

Consulte la ayuda de los cmdlets de PowerShell para ver instrucciones y sintaxis.

## Más información

Entrada de blog: [How to assign desktops to specific servers.](#)

## Compatibilidad con IPv4/IPv6

January 4, 2021

Esta versión es compatible con solo IPv4, con solo IPv6, así como con implementaciones de doble pila que usan redes IPv4 e IPv6 superpuestas.

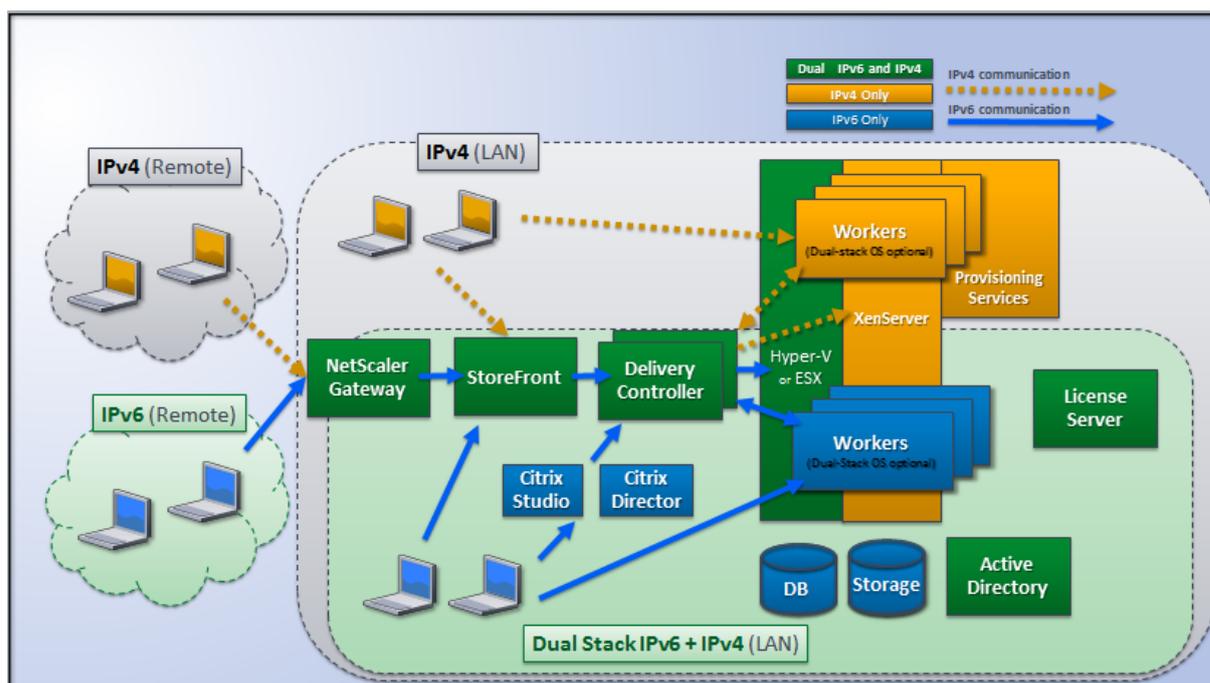
Las comunicaciones de IPv6 se controlan con dos configuraciones de directiva de Citrix relacionadas con las conexiones del Virtual Delivery Agent (VDA):

- Una configuración principal que aplica el uso de IPv6: Usar solo registro de Controller con IPv6.
- Una configuración dependiente que define una máscara de red IPv6: Máscara de red IPv6 para registro de Controller.

Cuando la configuración de directiva Usar solo registro de Controller con IPv6 está habilitada, el VDA se registra con un Delivery Controller para las conexiones entrantes mediante una dirección IPv6.

## Implementación de doble pila IPv4/IPv6

La siguiente figura ilustra una implementación de doble pila de IPv4/IPv6. En este caso, un trabajador es un VDA instalado en un hipervisor o en un sistema físico, y se utiliza principalmente para habilitar las conexiones de aplicaciones y escritorios. Los componentes compatibles con ambos protocolos, IPv4 y IPv6, se ejecutan en los sistemas operativos que usan software de tunelización o protocolo doble.



Estos productos, componentes y funciones de Citrix solo son compatibles con IPv4:

- Citrix Provisioning
- XenServer
- Los VDA no controlados por la configuración de directiva **Usar solo registro de Controller con IPv6**
- Versiones de XenApp anteriores a 7.5, versiones de XenDesktop anteriores a 7 y Director

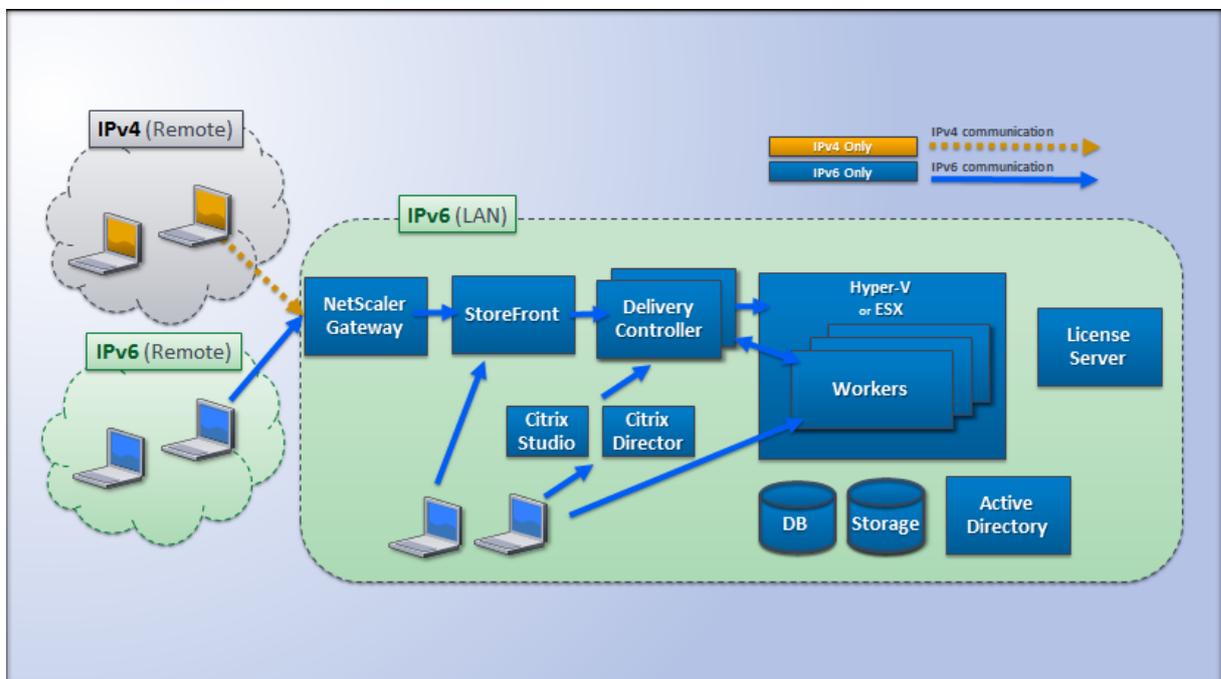
En esta implementación:

- Si un grupo de usuarios usa una red IPv6 de manera habitual y el administrador desea que use el tráfico IPv6, publicará escritorios y aplicaciones con IPv6 para esos usuarios a partir de una imagen de trabajo o de una unidad organizativa (OU) que tiene la configuración de directiva principal de IPv6 habilitada (es decir, la configuración Usar solo registro de Controller con IPv6 está habilitada).
- Si un grupo de usuarios usa una red IPv4 de manera habitual, el administrador publicará los escritorios y las aplicaciones con IPv4 para esos usuarios a partir de una imagen de trabajo o unidad organizativa que tiene la configuración de directiva de IPv6 inhabilitada (es decir, Usar solo registro de Controller con IPv6 está inhabilitada), que es el valor predeterminado.

### Implementación de solo IPv6

En la siguiente imagen se ilustra una implementación de solo IPv6. En este caso:

- Los componentes se están ejecutando en sistemas operativos configurados para admitir una red IPv6.
- La configuración de directiva principal de Citrix (Usar solo registro de Controller con IPv6) está habilitada para todos los VDA, por lo que deben registrarse con el Controller mediante una dirección IPv6.



## Configuraciones de directiva para IPv6

Hay dos configuraciones de directiva de Citrix que afectan a la compatibilidad con implementaciones puras de IPv6 o implementaciones de doble pila IPv4/IPv6. Defina las siguientes configuraciones de directiva relacionadas con las conexiones:

- **Usar solo registro de Controller con IPv6:** Controla el formato de dirección que utiliza Virtual Delivery Agent (VDA) para registrarse en el Delivery Controller. Valor predeterminado = inhabilitado
  - Cuando el VDA se comunica con el Controller, utiliza una sola dirección IPv6 seleccionada según las siguientes prioridades: dirección IP global, Unique Local Address (ULA), dirección local de enlace (solo si no hay otras direcciones IPv6 disponibles).
  - Cuando está inhabilitada, el VDA se registra y se comunica con el Controller mediante la dirección IPv4 de la máquina.
- **Máscara de red IPv6 para registro de Controller:** Una máquina puede tener varias direcciones IPv6; esta configuración de directiva permite a los administradores restringir el VDA a una sola subred preferida (en lugar de una dirección IP global, si hay alguna registrada). Esta configuración especifica la red en la que se registrará VDA. El VDA se registra solo en la primera dirección que coincide con la máscara de red. Esta configuración solo es válida si la configuración de directiva Usar solo registro de Controller con IPv6 está habilitada. Valor predeterminado = Cadena vacía

El uso de IPv4 o IPv6 por parte de un VDA está determinado únicamente por estas configuraciones de directiva. En otras palabras, para usar direcciones IPv6, el VDA debe estar controlado por una directiva de Citrix que contenga la configuración **Usar solo registro de Controller con IPv6** habilitada.

## Consideraciones sobre la implementación

Si el entorno contiene redes IPv4 e IPv6, necesitará configuraciones diferentes de grupos de entrega, uno para los clientes que solo pueden acceder a IPv4 y otro para los clientes que pueden acceder a la red IPv6. Considere la posibilidad de usar nombres, asignaciones de grupo de Active Directory o filtros de SmartAccess para diferenciar a los usuarios.

Es posible que la reconexión a una sesión falle si la conexión se inicia en una red IPv6 y, a continuación, se intenta la reconexión a partir de un cliente interno que solo tiene acceso de IPv4.

## Perfiles de usuario

April 29, 2022

De forma predeterminada, Citrix Profile Management se instala de forma silenciosa en las imágenes maestras al instalar el Virtual Delivery Agent, pero no tiene que utilizar Profile Management necesariamente como solución de administración de perfiles.

Para responder a las distintas necesidades de los usuarios, puede aplicar, mediante las directivas de Citrix Virtual Apps and Desktops, un comportamiento de perfil diferente a las máquinas de cada grupo de entrega. Por ejemplo, un grupo de entrega puede requerir perfiles obligatorios de Citrix, cuya plantilla está almacenada en una ubicación de red, mientras que otro grupo de entrega puede requerir perfiles móviles de Citrix almacenados en otra ubicación con varias carpetas redirigidas.

- Si otros administradores de su organización son responsables de las directivas de Citrix Virtual Apps and Desktops, colabore con ellos para asegurarse de que establecen directivas relacionadas con los perfiles en todos los grupos de entrega.
- Las directivas de Profile Management también se pueden establecer en las Directivas de grupo, en el archivo INI de Profile Management, y localmente, en máquinas virtuales individuales. Todas estas formas de definir el comportamiento de perfil se leen en el orden siguiente:
  1. Directiva de grupo (archivos .adm o .admx)
  2. Directivas de Citrix Virtual Apps and Desktops en el nodo Directiva
  3. Directivas locales en la máquina virtual a la que el usuario se conecta
  4. Archivo INI de Profile Management

Por ejemplo, si configura la misma directiva en la Directiva de grupo y en el nodo Directiva, el sistema lee la configuración de directiva en la Directiva de grupo y omite la configuración de directiva de Citrix Virtual Apps and Desktops.

Independientemente de la solución de administración de perfiles que elija, los administradores de Director pueden acceder a la información de diagnóstico y solucionar problemas de perfiles de usuario. Para obtener más información, consulte la documentación de [Director](#).

Si usa la función Personal vDisk, los perfiles de usuario de Citrix se almacenan en los discos Personal vDisk de los escritorios virtuales de forma predeterminada. No borre la copia de ningún perfil en el almacén de usuarios mientras aún quede una copia en el disco Personal vDisk. Si lo hace, se producirá un error de Profile Management y provocará el uso de un perfil temporal para los inicios de sesión en el escritorio virtual.

## Configuración automática

Este tipo de escritorio se detecta automáticamente en función de la instalación de Virtual Delivery Agent y, además de las opciones de configuración seleccionadas en Studio, configura los parámetros predeterminados de Profile Management según corresponda.

En la tabla siguiente se muestran las directivas que ajusta Profile Management. Esta función conserva las configuraciones de directiva no predeterminadas, no las sobrescribe. Consulte la documentación de Profile Management para obtener información sobre cada directiva. Los tipos de máquinas que crean perfiles afectan a las directivas que se ajustan. Los factores principales son si las máquinas son persistentes o aprovisionadas y si están compartidas por varios usuarios o son máquinas dedicadas a un solo usuario.

Los sistemas persistentes tienen un tipo de almacenamiento local, cuyo contenido se conserva (persiste) cuando el sistema se apaga. Los sistemas persistentes pueden emplear tecnología de almacenamiento como las redes de área de almacenamiento SAN (Storage Area Network) para proveer de imitaciones de discos locales. En cambio, los sistemas aprovisionados se crean “en el momento” a partir de un disco base y algún tipo de disco de identidad. El almacenamiento local es imitado por un disco RAM o disco de red, y éste último es normalmente suministrado por una red SAN con un enlace de alta velocidad. La tecnología de aprovisionamiento suele ser Citrix Provisioning o Machine Creation Services (o un producto equivalente de terceros). Algunas veces los sistemas aprovisionados tienen un almacenamiento local persistente, que puede consistir en discos virtuales personales (Personal vDisk); estos se clasifican como persistentes.

Juntos, estos dos factores definen los siguientes tipos de máquinas:

- **Persistentes y dedicadas.** Por ejemplo, máquinas con SO de sesión única con una asignación estática y un disco Personal vDisk, creadas con Machine Creation Services; escritorios con discos Personal vDisk creados con VDI-in-a-Box; estaciones de trabajo físicas y equipos portátiles.
- **Persistentes y compartidas.** Por ejemplo, máquinas con SO multisesión creadas con los servicios Machine Creation Services.
- **Aprovisionadas y dedicadas.** Por ejemplo, máquinas de SO de sesión única con una asignación estática pero sin Personal vDisk, creadas con Citrix Provisioning.
- **Aprovisionadas y compartidas.** Por ejemplo, máquinas de SO de sesión única con una asignación aleatoria, creadas con Citrix Provisioning; escritorios sin discos Personal vDisk creados con VDI-in-a-Box.

Se sugieren las siguientes configuraciones de directiva de Profile Management para los distintos tipos de máquina. En la mayoría de los casos funcionan correctamente, aunque puede cambiarlas según sea necesario en su entorno.

**Importante:**

Eliminar perfiles guardados en caché local al cerrar la sesión, Streaming de perfiles y Guardar siempre en caché se aplican obligatoriamente mediante la función de configuración automática. Ajuste el resto de las directivas manualmente.

## Máquinas persistentes

Directiva	Persistentes y dedicadas	Persistentes y compartidas
Eliminar perfiles guardados en caché local al cerrar la sesión	Inhabilitado	Habilitado
Streaming de perfiles	Inhabilitado	Habilitado
Guardar siempre en caché	Habilitada (nota 1)	Inhabilitada (nota 2)
Reescritura activa	Inhabilitado	Inhabilitada (nota 3)
Procesar inicios de sesión de administradores locales	Habilitado	Inhabilitada (nota 4)

### Máquinas aprovisionadas

Directiva	Aprovisionadas y dedicadas	Aprovisionadas y compartidas
Eliminar perfiles guardados en caché local al cerrar la sesión	Inhabilitada (nota 5)	Habilitado
Streaming de perfiles	Habilitado	Habilitado
Guardar siempre en caché	Inhabilitada (nota 6)	Inhabilitado
Reescritura activa	Habilitado	Habilitado
Procesar inicios de sesión de administradores locales	Habilitado	Habilitada (nota 7)

1. Puesto que Streaming de perfiles está inhabilitado para este tipo de máquina, el parámetro Guardar siempre en caché se omite siempre.
2. Inhabilite Guardar siempre en caché. No obstante, para asegurarse de que los archivos de gran tamaño se cargan en los perfiles tan pronto como sea posible después de iniciar la sesión, puede habilitar esta directiva y usarla para definir un límite de tamaño de archivo (en MB). Todos los archivos de este tamaño o más grandes se almacenarán en el caché local tan pronto como sea posible.
3. Inhabilite Reescritura activa excepto para guardar cambios en los perfiles de los usuarios que se mueven entre servidores de Citrix Virtual Apps. En ese caso, habilite esta directiva.
4. Inhabilite Procesar inicios de sesión de administradores locales excepto para escritorios alojados compartidos. En ese caso, habilite esta directiva.
5. Inhabilite Eliminar perfiles guardados en caché local al cerrar la sesión. Esto conserva los perfiles guardados en caché local. Puesto que las máquinas se restablecen al cerrar la sesión pero están asignadas a usuarios individuales, los inicios de sesión son más rápidos si sus perfiles se guardan en caché.

6. Inhabilite Guardar siempre en caché. No obstante, para asegurarse de que los archivos de gran tamaño se cargan en los perfiles tan pronto como sea posible después de iniciar la sesión, puede habilitar esta directiva y usarla para definir un límite de tamaño de archivo (en MB). Todos los archivos de este tamaño o más grandes se almacenarán en el caché local tan pronto como sea posible.
7. Habilite Procesar inicios de sesión de administradores locales excepto para perfiles de usuarios que se mueven entre servidores de Citrix Virtual Apps and Desktops. En ese caso, inhabilite esta directiva.

## Redirección de carpetas

La redirección de carpetas permite almacenar datos de usuario en recursos compartidos de red, distintos de la ubicación donde se guardan los perfiles. Esto reduce el tamaño y el tiempo de carga del perfil pero podría afectar al ancho de banda de la red. Para la redirección de carpetas no se requiere el empleo de perfiles de usuario de Citrix. Puede optar por administrar los perfiles de usuario usted mismo y aplicar la redirección de carpetas.

Configure la redirección de carpetas con las directivas de Citrix en Studio.

- Asegúrese de que las ubicaciones de red usadas para almacenar el contenido de las carpetas redirigidas estén disponibles y tengan los permisos correctos. Se validan las propiedades de ubicación.
- Las carpetas redirigidas se configuran en la red y su contenido se crea desde los escritorios virtuales de los usuarios al iniciar sesión.

Configure la redirección de carpetas con las directivas de Citrix o con los objetos de directiva de grupo de Active Directory, pero no ambos a la vez. Si configura la redirección de carpetas mediante ambos motores de directivas, puede que obtenga resultados impredecibles.

## Redirección de carpetas avanzada

En las implementaciones con varios sistemas operativos (SO), puede ser conveniente que una porción de un perfil de usuario esté compartida por cada SO. El resto del perfil no está compartido y solo lo utiliza un sistema operativo. Para garantizar una experiencia de usuario consistente en todos los sistemas operativos, necesita una configuración diferente para cada sistema operativo. En esto consiste la redirección de carpetas avanzada. Por ejemplo, es posible que haya diferentes versiones de una aplicación que se ejecuta en dos sistemas operativos que necesiten leer o modificar un archivo compartido. En este caso, puede decidir redirigir dicho archivo a una única ubicación de red donde ambas versiones de la aplicación puedan acceder a él. Si no, debido a que el contenido de la carpeta Menú Inicio está organizado de manera diferente en dos sistemas operativos, puede optar por rediri-

gir solo una carpeta, en lugar de ambas. Esto separa la carpeta Menú Inicio y su contenido en cada sistema operativo, lo que garantiza una experiencia consistente para los usuarios.

Si la implementación requiere una redirección de carpetas avanzada, es necesario comprender la estructura de los datos de perfil de los usuarios y determinar qué partes de ella se pueden compartir entre distintos sistemas operativos. Esto es importante porque si la redirección de carpetas no se aplica correctamente, su comportamiento puede ser impredecible.

Para redirigir las carpetas en implementaciones avanzadas:

- Use un grupo de entrega distinto para cada sistema operativo.
- Es necesario conocer dónde guardan las aplicaciones virtuales, incluidas las ejecutadas en escritorios virtuales, los datos y los parámetros del usuario, y conocer cómo están organizados esos datos.
- En el caso de datos de perfil compartidos que se pueden mover de manera segura (porque están organizados idénticamente en cada SO), redirija las carpetas contenedoras en cada grupo de entrega.
- En el caso de datos de perfil no compartidos que no se pueden mover, redirija la carpeta contenedora solo en uno de los grupos de entrega, normalmente el grupo correspondiente al SO utilizado con más frecuencia, o el grupo donde los datos sean más importantes. De manera alternativa, en el caso de datos no compartidos que no se pueden mover entre sistemas operativos, puede redirigir las carpetas contenedoras de ambos sistemas a ubicaciones de red distintas.

### **Ejemplo de implementación avanzada**

Esta implementación contiene aplicaciones (incluidas las versiones de Microsoft Outlook y de Internet Explorer) que se ejecutan en escritorios Windows 8, así como aplicaciones (incluidas otras versiones de Outlook y de Internet Explorer) entregadas por Windows Server 2008. Para lograr esto, se han configurado dos grupos de entrega, uno para cada sistema operativo. Los usuarios quieren acceder al mismo conjunto de Contactos y Favoritos en ambas versiones de esas dos aplicaciones.

Importante: Las decisiones y las sugerencias siguientes son válidas para los sistemas operativos y la implementación descritos. En una organización, la elección de carpetas para redirigir y si se decide compartirlas, dependen de una serie de factores que son específicos de la implementación en cuestión.

- Mediante el uso de directivas aplicadas a los grupos de entrega, se eligen las siguientes carpetas a redirigir.

Carpeta	¿Redirigida en Windows 8?	¿Redirigida en Windows Server 2008?
Mis documentos	Sí	Sí
Datos de programa	No	No
Contactos	Sí	Sí
Escritorio	Sí	No
Descargas	No	No
Favoritos	Sí	Sí
Enlaces	Sí	No
Mi música	Sí	Sí
Mis imágenes	Sí	Sí
Mis vídeos	Sí	Sí
Búsquedas	Sí	No
Partidas guardadas	No	No
Menú Inicio	Sí	No

- Para las carpetas redirigidas compartidas:
  - Después de analizar la estructura de los datos guardados por las distintas versiones de Outlook y de Internet Explorer, se decide que es posible compartir las carpetas Contactos y Favoritos
  - Se sabe que las carpetas Mis documentos, Mi música, Mis imágenes y Mis vídeos tienen una estructura estándar en todos los sistemas operativos, por lo tanto se pueden guardar en la misma ubicación de red para cada grupo de entrega
- Para las carpetas redirigidas no compartidas:
  - Se decide no redirigir las carpetas Escritorio, Vínculos, Búsquedas ni Menú Inicio del grupo de entrega de Windows Server porque los datos incluidos en estas carpetas están organizados de manera diferente en cada sistema operativo. Por lo tanto, no se pueden compartir.
  - Para garantizar un comportamiento predecible de estos datos no compartidos, se decide aplicar la redirección solamente en el grupo de entrega de Windows 8. Se elige éste, en lugar del grupo de entrega de Windows Server, porque los usuarios utilizarán Windows 8 con más frecuencia en su trabajo del día a día, mientras que solo ocasionalmente necesitarán acceder a las aplicaciones entregadas por el servidor. Además, en este caso, los datos no compartidos son más relevantes para el entorno de escritorio que para un en-

torno de aplicaciones. Por ejemplo, los accesos directos de escritorio se guardan en la carpeta Escritorio y pueden ser útiles si se originan desde una máquina Windows 8, pero no desde una máquina Windows Server.

- Para las carpetas no redirigidas:
  - No conviene que los servidores se llenen de archivos descargados por los usuarios, por lo que se decide no redirigir la carpeta Descargas
  - Los datos de las distintas aplicaciones pueden provocar problemas de compatibilidad y de rendimiento, por lo que se decide no redirigir la carpeta Datos de programa

Para obtener más información sobre la redirección de carpetas, consulte [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-vista/cc766489\(v=ws.10\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-vista/cc766489(v=ws.10)?redirectedfrom=MSDN).

## Redirección de carpetas y exclusiones

En Citrix Profile Management (pero no en Studio), hay una mejora del rendimiento que permite impedir que las carpetas se procesen, aplicando exclusiones. Si usa esta función, no excluya ninguna de las carpetas redirigidas. Las funciones de redirección de carpetas y exclusión funcionan juntas, de modo que si se asegura de que ninguna de las carpetas redirigidas está excluida, Profile Management puede moverlas de vuelta a la estructura de carpetas del perfil, conservando la integridad de los datos, si más adelante decide no redirigir dichas carpetas. Para obtener más información acerca de las exclusiones, consulte [Para incluir y excluir elementos](#).

## Recopilar rastreos de Citrix Diagnostic Facility (CDF) durante el inicio del sistema

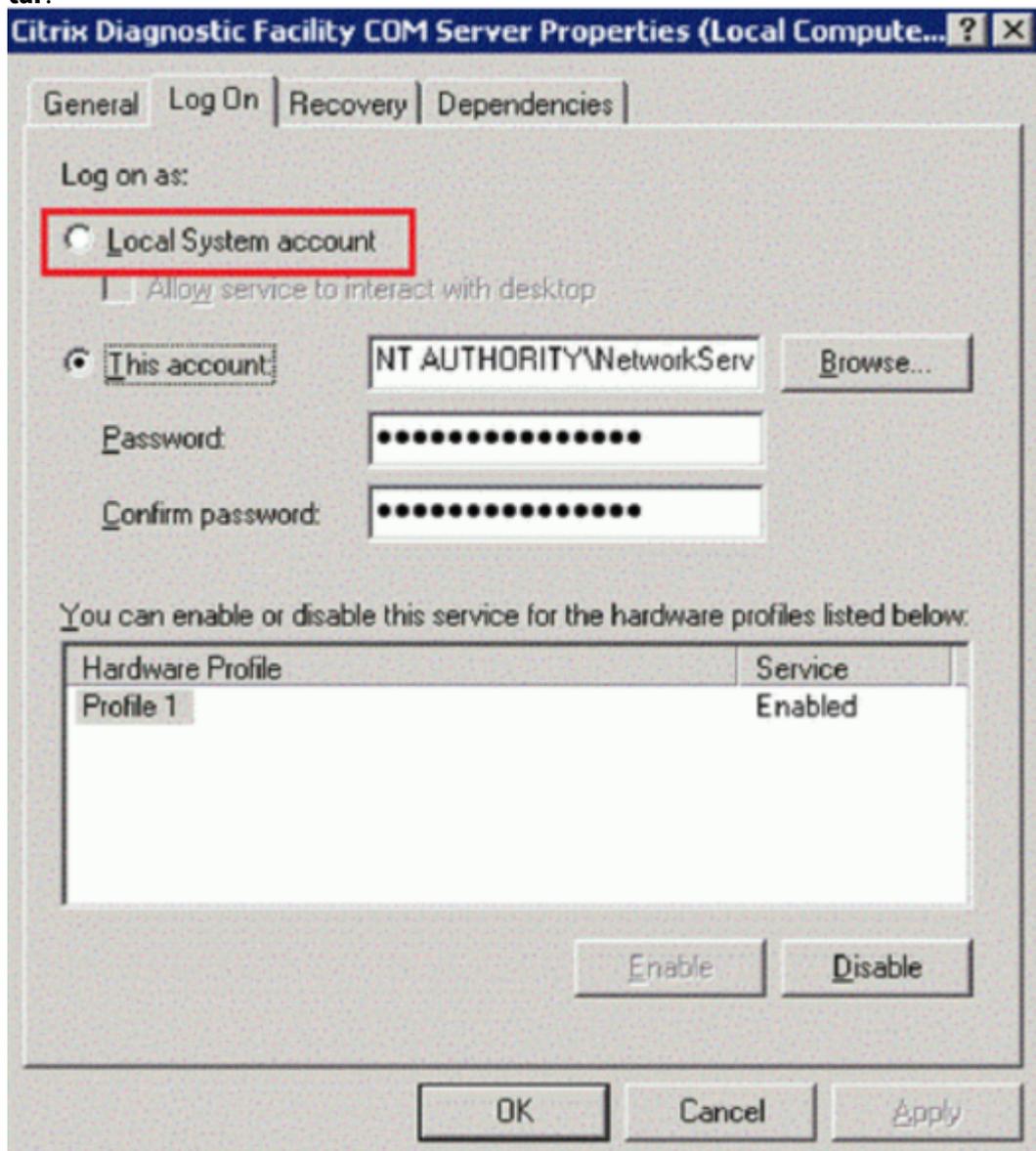
January 4, 2021

La utilidad CDFControl es un controlador o consumidor de rastreo de eventos que sirve para capturar los mensajes de rastreo de Citrix Diagnostic Facility (CDF) mostrados por varios proveedores de rastreo de Citrix. Está diseñado para solucionar problemas complejos relacionados con Citrix, analizar la compatibilidad de filtros y recopilar datos de rendimiento. Para descargar la utilidad CDFControl, consulte [CTX111961](#).

## Use la cuenta del sistema local

Para usar la cuenta del sistema local para el servicio del servidor COM de Citrix Diagnostic Facility, complete los siguientes pasos:

1. Haga clic en **Ejecutar** desde el menú **Inicio**.
2. Introduzca `services.msc` en el cuadro de diálogo y haga clic en **Aceptar**.
3. Seleccione el servicio **Servidor COM de Citrix Diagnostics Facility** y elija **Propiedades**.
4. Haga clic en la ficha **Iniciar sesión** y habilite la cuenta **Sistema local**. Luego haga clic en **Aceptar**.

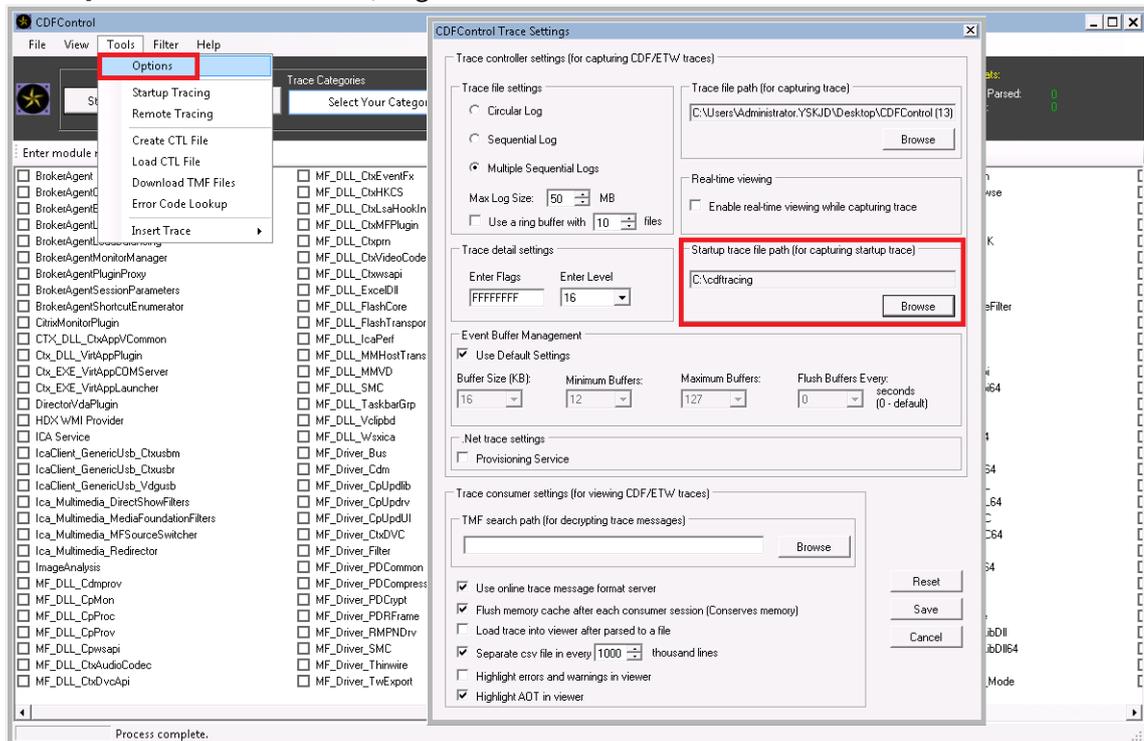


5. Reinicie el servicio.

## Recopilar un rastreo al iniciar el sistema

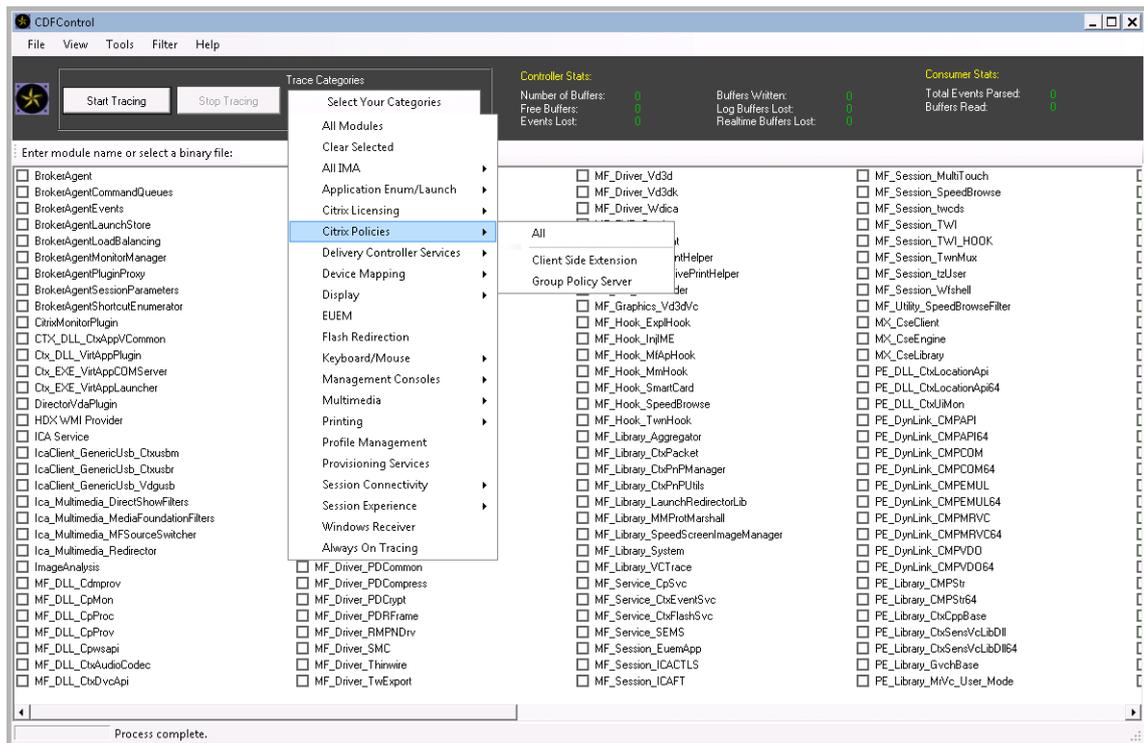
Para recopilar un rastreo CDF al iniciar del sistema, consulte el procedimiento:

1. Inicie **CDFControl** y seleccione **Options** del menú **Tools**.
2. Especifique la ruta del archivo de rastreo en la sección **Startup trace file path for capturing startup trace**. A continuación, haga clic en **Guardar**.



3. Seleccione las **Trace Categories** según las recomendaciones del servicio de asistencia técnica de Citrix. En este ejemplo, se selecciona **Citrix Policies**.

La selección de **Citrix Policies** que figura a continuación se muestra únicamente como ejemplo de rastreo de inicio. Le recomendamos habilitar los proveedores para el problema específico que solucione.



4. Con privilegios de administrador, seleccione **Startup Tracing** y haga clic en **Enable** desde el menú **Tools**.

Después de seleccionar **Enable**, la barra animada comienza a desplazarse. Esto no afecta al procedimiento. Continúe en el paso 5.

5. Cierre la **utilidad CDFControl** y reinicie el sistema después de habilitar **Startup Tracing**.
6. Inicie la utilidad **CDFControl**. Después de que el sistema se reinicie y aparezca el error, inhabilite la opción **Startup Tracing** con el botón **Disable**.

Para inhabilitar la opción **Startup Tracing**, seleccione Startup Tracing en el menú **Tools** y haga clic en **Disable**, como se describe en los pasos 4 y 5.

7. Interrumpa el servicio del servidor de **Citrix Diagnostics Facility COM**.
8. Recopile el archivo de registros de rastreo (.etl) para analizarlo en la ruta del archivo especificado con los pasos 1 y 2.
9. Inicie el servicio del servidor de **Citrix Diagnostics Facility COM**.

## Citrix Insight Services

May 24, 2024

Citrix Insight Services (CIS) es una plataforma de Citrix para instrumentación, telemetría y generación de información empresarial. Sus capacidades de instrumentación y telemetría permiten a los usuarios técnicos (clientes, socios e ingenieros) emitir ellos mismos diagnósticos de los problemas y corregirlos, optimizando así sus entornos de trabajo. Para obtener la información más reciente y detallada sobre CIS y saber cómo funciona, consulte <https://cis.citrix.com> (se necesitan credenciales de cuenta de Citrix).

Toda la información que se carga en Citrix se usa para la solución de problemas y para diagnósticos, además de mejorar la calidad, la confiabilidad y el rendimiento de los productos, y está sujeta a estas directivas:

- Directiva de Citrix Insight Services en <https://cis.citrix.com/legal>
- Directiva de privacidad de Citrix en <https://www.cloud.com/privacy-policy>

Esta versión de Citrix Virtual Apps and Desktops admite las siguientes tecnologías.

- Análisis sobre la instalación y la actualización de Citrix Virtual Apps and Desktops
- Customer Experience Improvement Program (CEIP) de Citrix
- Citrix Call Home
- [Citrix Scout](#)

Además (e independientemente) de CIS y Citrix Analytics: Los datos de Google Analytics se recopilan (y luego se cargan) automáticamente cuando se instala (o se actualiza) Studio. Después de instalar Studio, puede cambiar este parámetro con la clave de Registro HKLM\Software\Citrix\DesktopStudio\GAEnabled. El valor 1 habilita la recopilación y la carga, mientras que el valor 0 las inhabilita.

## Datos de análisis de instalación y actualización

Cuando se usa el instalador del producto completo para implementar o actualizar los componentes de Citrix Virtual Apps and Desktops, se recopila información anónima sobre el proceso de instalación y se guarda en la máquina donde se está realizando la instalación o actualización del componente. Esta información se utiliza para ayudar a Citrix a mejorar la experiencia de instalación de sus clientes.

La información se almacena localmente en %ProgramData%\Citrix\CTQs.

La carga automática de estos datos está habilitada de forma predeterminada en ambas interfaces, la gráfica y la de línea de comandos, del programa de instalación de producto completo.

- Puede cambiar el valor predeterminado en un parámetro de Registro. Si cambia el parámetro de Registro antes de instalar o actualizar, ese valor se usará cuando use el programa de instalación de producto completo.
- Puede anular la configuración predeterminada si instala o actualiza con la interfaz de línea de comandos y especifica esa opción con el comando.

### Controlar las cargas automáticas:

- El parámetro de Registro que controla la carga automática de los datos de análisis de instalación o actualización (predeterminado = 1):
  - Ubicación: HKLM:\Software\Citrix\MetaInstall
  - Nombre: SendExperienceMetrics
  - Valor: 0 = inhabilitado, 1 = habilitado
- Mediante PowerShell, el cmdlet siguiente inhabilita la carga automática de los datos de análisis de instalación o actualización:

```
1 New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name
   SendExperienceMetrics -PropertyType DWORD -Value 0
2 <!--NeedCopy-->
```

- Para inhabilitar las cargas automáticas con el comando XenDesktopServerSetup.exe o XenDesktopVDASetup.exe, incluya la opción `/disableexperiencemetrics`.  
Para habilitar las cargas automáticas con el comando XenDesktopServerSetup.exe o XenDesktopVDASetup.exe, incluya la opción `/sendexperiencemetrics`.

### Customer Experience Improvement Program (CEIP) de Citrix

Cuando se participa en el programa CEIP de mejora de la experiencia del usuario (Customer Experience Improvement Program), se envían estadísticas e información de uso anónimos a Citrix para ayudar a Citrix a mejorar la calidad y el rendimiento de sus productos. Para obtener más información, consulte <https://more.citrix.com/XD-CEIP>.

#### Inscripción durante la creación o actualización de un sitio

Se inscribe automáticamente en el programa CEIP al crear un sitio (después de instalar el primer Delivery Controller). La primera carga de datos tiene lugar aproximadamente siete días después de crear el sitio. Puede dejar de participar en cualquier momento después de crear el sitio. Seleccione el nodo **Configuración** en el panel de navegación de Studio. A continuación, seleccione la ficha **Asistencia para productos** y siga las instrucciones.

Cuando se actualiza una implementación de Citrix Virtual Apps and Desktops:

- Si actualiza una versión desde otra no compatible con CEIP, se le preguntará si quiere participar.
- Si actualiza una versión desde otra compatible con CEIP y la participación en el programa ya estaba habilitada, CEIP se habilitará en el sitio actualizado.
- Si actualiza una versión desde otra compatible con CEIP y la participación en el programa no estaba habilitada, CEIP se inhabilitará en el sitio actualizado.

- Si actualiza una versión desde otra compatible con CEIP, pero no se sabe si la participación estaba o no habilitada, se le preguntará si quiere participar.

La información recopilada es anónima, por lo que no se puede ver una vez cargada en Citrix Insight Services.

### Inscripción al instalar un VDA

De forma predeterminada, se inscribe automáticamente en el programa CEIP cuando instala un Windows VDA. Puede cambiar esta opción predeterminada en el parámetro de Registro del sistema. Si cambia el parámetro de Registro del sistema antes de instalar el VDA, se usará ese valor.

El parámetro de Registro que controla la inscripción automática en CEIP (predeterminado = 1):

Ubicación: HKLM:\Software\Citrix\Telemetry\CEIP

Name: Enabled

Value: 0 = disabled, 1 = enabled

De forma predeterminada, la propiedad `Enabled` está oculta en el Registro del sistema. Si no se especifica, significa que la funcionalidad de carga automática está habilitada.

Con PowerShell, el cmdlet siguiente inhabilita la inscripción en el programa CEIP:

```
1 New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name
   Enabled -PropertyType DWORD -Value 0
2 <!--NeedCopy-->
```

Los puntos de datos sobre el tiempo de ejecución recopilados se escriben periódicamente como archivos en una carpeta de salida (ubicación predeterminada: %programdata%\Citrix\VdaCeip).

La primera carga de datos tiene lugar aproximadamente siete días después de instalar el VDA.

### Inscripción al instalar otros productos y componentes

También puede participar en CEIP al instalar tecnologías, productos y componentes relacionados de Citrix, tales como Citrix Provisioning, AppDNA, Citrix License Server, la aplicación Citrix Workspace para Windows, Universal Print Server y Grabación de sesiones. Consulte la documentación para obtener más detalles sobre los valores predeterminados de instalación y participación en el programa.

### Citrix Call Home

Al instalar determinados componentes y funciones de Citrix Virtual Apps and Desktops, se le ofrece la oportunidad de participar en Citrix Call Home. Call Home recopila datos de diagnóstico y carga

periódicamente paquetes de telemetría con esos datos directamente en Citrix Insight Services (por HTTPS a través del puerto predeterminado 443) para el análisis y la solución de problemas.

En Citrix Virtual Apps and Desktops, Call Home se ejecuta como un servicio en segundo plano con el nombre de Citrix Telemetry Service. Para obtener más información, consulte <https://more.citrix.com/XD-CALLHOME>.

La funcionalidad de programación de Call Home también está disponible en Citrix Scout. Para obtener más información, consulte [Citrix Scout](#).

### Qué datos se recopilan

Citrix Diagnostic Facility (CDF) recopila información que puede ser útil para solucionar problemas. Call Home recopila un subconjunto de rastros CDF que pueden ser útiles para solucionar errores comunes como, por ejemplo, los registros de VDA e inicios de aplicaciones o escritorios. Esta tecnología se conoce como rastreo permanente (Always-On Tracing o AOT). Los registros AOT se guardan en el disco en C:\Users\CitrixTelemetryService\AppData\Local\CitrixAOT.

Call Home no recopilará ningún otro rastreo de eventos de Windows (Event Tracing for Windows, ETW), ni tampoco se puede configurar para hacerlo.

Call Home también recopila información adicional, como:

- Registros creados por Citrix Virtual Apps and Desktops en `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`.
- Información de WMI (Instrumental de administración de Windows) en el espacio de nombres de Citrix.
- Lista de procesos en ejecución.
- Volcados de errores de procesos de Citrix que están almacenados en `%PROGRAM DATA%\Citrix\CDF`
- Información sobre instalaciones y actualizaciones. Esto puede incluir el registro completo del metainstalador del producto, los registros MSI con errores, los resultados del analizador de registros MSI, los registros de StoreFront, los registros de comprobación de compatibilidad de licencias y los resultados de las pruebas preliminares de actualización de versión del sitio.

La información de rastreo se comprime tras recopilarse. Citrix Telemetry Service conserva un máximo de 10 MB de la información de rastreo más reciente comprimida, con un tiempo límite máximo de ocho días.

- La compresión de los datos permite que Call Home ocupe muy poco espacio del VDA.
- Los rastreos se guardan en memoria a fin de evitar operaciones E/S en las máquinas aprovisionadas.
- El búfer de rastreo utiliza un mecanismo circular para conservar los rastreos en memoria.

Call Home recopila los puntos de datos clave: [Puntos de datos clave para Call Home](#).

## Resumen de configuración y administración

Puede inscribirse en Call Home cuando use el asistente de instalación del producto completo, o más adelante, mediante cmdlets de PowerShell. Cuando se inscribe, de forma predeterminada, los diagnósticos se recopilan y se cargan en Citrix cada domingo aproximadamente a las 3:00, hora local. La hora de carga es aleatoria en un máximo de dos horas respecto a la hora especificada. Esto significa que una carga programada de forma predeterminada se realiza entre 3:00 y 5:00 de la mañana.

Si no quiere cargar la información de diagnóstico siguiendo la programación (o si quiere cambiar la programación existente), puede usar los cmdlets de PowerShell para recopilar y cargar manualmente los diagnósticos o guardarlos localmente.

Cuando se inscriba en cargas programadas de Call Home y cuando cargue manualmente información de diagnóstico en Citrix, deberá proporcionar las credenciales de su cuenta de Citrix o de Citrix Cloud. Citrix intercambia las credenciales por un token de carga que se utiliza para identificar al cliente y cargar los datos. Las credenciales no se guardan.

Cuando tiene lugar una operación de carga, se envía una notificación por correo electrónico a la dirección asociada a la cuenta de Citrix.

Si habilita Call Home al instalar un componente, puede inhabilitarlo más tarde.

## Requisitos previos

- La máquina debe estar ejecutando PowerShell 3.0 o posterior.
- La máquina debe estar ejecutando Citrix Telemetry Service.
- La variable del sistema `PSModulePath` debe establecerse en la ruta de instalación de Telemetry; por ejemplo: `C:\Archivos de programa\Citrix\Telemetry Service\`.

## Habilitar Call Home durante la instalación de componentes

**Durante la instalación o la actualización del VDA:** Cuando instala o actualiza un Virtual Delivery Agent desde la interfaz gráfica del instalador del producto completo, se le pregunta si quiere participar en Call Home. Existen dos opciones:

- Participar en Call Home.
- No participar en Call Home.

Si actualiza un VDA y se había inscrito antes en Call Home, esa página del asistente no aparece.

**Durante la instalación o la actualización de versión del Controller:** Cuando instala o actualiza la versión de un Delivery Controller desde la interfaz gráfica, se le pregunta si quiere participar en Call Home. Existen tres opciones:

Cuando instale un Controller, no podrá configurar información en la página Call Home del asistente de instalación si el servidor tiene aplicado un objeto de directiva de grupo de Active Directory con la configuración de directiva “Iniciar sesión como un servicio”. Para obtener más información, consulte [CTX218094](#).

Si actualiza un Controller y se había inscrito antes en Call Home, no se le preguntará sobre la participación.

## Cmdlets de PowerShell

La ayuda de PowerShell proporciona la sintaxis completa, incluidas las descripciones de cmdlets y parámetros que no se utilizan en estos casos de uso más comunes.

Si quiere usar un servidor proxy para las cargas, consulte [Configurar un servidor proxy](#).

- **Puntos de datos clave para Call Home:** Las recopilaciones de diagnósticos se cargan automáticamente en Citrix. Si no introduce más cmdlets para una programación personalizada, se usa la programación predeterminada.

```
1 $cred = Get-Credential
2 Enable-CitrixCallHome -Credential $cred
3 <!--NeedCopy-->
```

Para confirmar que las cargas programadas se han habilitado, escriba `Get-CitrixCallHomeGet -CitrixCallHome`. Si se han habilitado, se devuelve `IsEnabled=True` y `IsMasterImage=False`.

- **Habilitación de cargas programadas para máquinas creadas a partir de una imagen maestra:** Si habilita cargas programadas en una imagen maestra, no tendrá que configurar esto en cada una de las máquinas que se creen en el catálogo de máquinas.

```
Enable-CitrixCallHome -Credential $cred -MasterImage
```

Para confirmar que las cargas programadas se han habilitado, escriba `Get-CitrixCallHome`. Si se han habilitado, se devuelve `IsEnabled=True` y `IsMasterImage=True`.

- **Creación de una programación personalizada:** Cree una programación semanal o diaria para recopilaciones y cargas de diagnósticos.

```
1 $timespan = New-TimeSpan -Hours hours -Minutes minutes
2 Set-CitrixCallHomeSchedule -TimeOfDay $timespan -DayOfWeek day
3   -UploadFrequency {
4     Daily|Weekly }
5 <!--NeedCopy-->
```

## Ejemplos:

El cmdlet siguiente crea una programación para crear un paquete con los datos y cargarlos a las 22:20 todas las noches. El parámetro de horas se usa un reloj de 24 horas. Cuando el valor del parámetro `UploadFrequency` es `Daily`, el parámetro `DayOfWeek` se ignora aunque se haya especificado.

```
1 $timespan - New-TimeSpan -Hours 22 -Minutes 20
2 Set-CitrixCallHomeSchedule -TimeOfDay $timespan -UploadFrequency Daily
3 <!--NeedCopy-->
```

Para confirmar la programación, introduzca `Get-CitrixCallHomeSchedule`. En el ejemplo anterior, la acción devuelve `StartTime=22:20:00`, `DayOfWeek=Sunday (ignored)`, `Upload Frequency=Daily`.

El cmdlet siguiente crea una programación para crear un paquete con los datos y cargarlos a las 22:20 los miércoles.

```
1 $timespan - New-TimeSpan -Hours 22 -Minutes 20
2 Set-CitrixCallHomeSchedule -TimeOfDay $timespan -DayOfWeek Wed -
  UploadFrequency Weekly
3 <!--NeedCopy-->
```

Para confirmar la programación, introduzca `Get-CitrixCallHomeSchedule`. En el ejemplo anterior, la acción devuelve `StartTime=22:20:00`, `DayOfWeek=Wednesday`, `Upload Frequency=Weekly`.

## Inhabilitar Call Home

Puede inhabilitar Call Home mediante un cmdlet de PowerShell o a través de Citrix Scout.

Los registros AOT se recopilan y guardan en el disco, incluso cuando se inhabilitan las cargas programadas de Call Home. (Cuando se inhabilitan las cargas programadas, los registros AOT no se cargan automáticamente en Citrix). Puede inhabilitar la recopilación y el almacenamiento local de los registros AOT.

**Inhabilitar Call Home con PowerShell** Después de ejecutar el siguiente cmdlet, los datos de diagnóstico no se cargarán automáticamente en Citrix (puede seguir cargando datos de diagnóstico mediante Citrix Scout o cmdlets de telemetría de PowerShell).

### `Disable-CitrixCallHome`

Para confirmar que Call Home está inhabilitado, introduzca `Get-CitrixCallHome`. Si se ha inhabilitado, el retorno es `IsEnabled=False` y `IsMasterImage=False`.

**Inhabilitar una programación de recopilación mediante Citrix Scout** Para inhabilitar una programación de recopilación de diagnóstico mediante Citrix Scout, siga las instrucciones de [Programar](#)

**recopilaciones.** En el paso 3, haga clic en **No** para cancelar la programación de las máquinas seleccionadas.

**Inhabilitar la recopilación de registros AOT** Después de ejecutar el siguiente cmdlet (con el campo **Enabled** establecido en **false**), no se recopilarán los registros AOT.

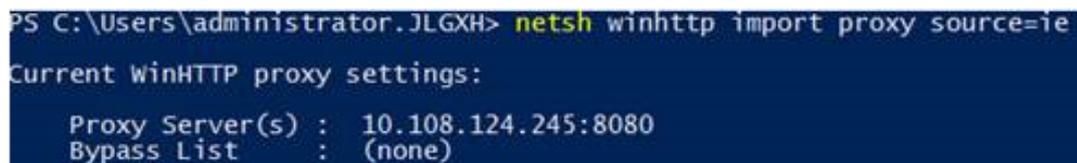
```
Enable-CitrixTrace -Listen '{ "trace": { "enabled": false, "persistDirectory": "C:\Users\Public", "maxSizeBytes": 1000000, "sliceDurationSeconds": 300 } } '
```

El parámetro `Listen` contiene argumentos en formato JSON.

### Configurar un servidor proxy para cargas de Call Home

Complete las siguientes tareas en la máquina donde esté habilitado Call Home. Los diagramas de ejemplo en el siguiente procedimiento contienen el puerto y la dirección del servidor 10.158.139.37:3128. Su información será diferente.

1. Agregue información del servidor proxy a su explorador web. En Internet Explorer, seleccione **Opciones de Internet > Conexiones > Configuración de LAN**. Seleccione **Usar un servidor proxy para la LAN** e introduzca el número de puerto y la dirección del servidor proxy.
2. En PowerShell, ejecute `netsh winhttp import proxy source=ie`.



```
PS C:\Users\administrator.JLGXH> netsh winhttp import proxy source=ie
Current WinHTTP proxy settings:
Proxy Server(s) : 10.108.124.245:8080
Bypass List    : (none)
```

3. Con un editor de texto, modifique el archivo de configuración `TelemetryService.exe`, que se encuentra en `C:\Archivos de programa\Citrix\Telemetry Service`. Agregue la información que aparece en el cuadro rojo.



```
TelemetryService.exe - Notepad
File Edit Format View Help
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1" />
  </startup>
  <runtime>
    <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
      <dependentAssembly>
        <assemblyIdentity name="Newtonsoft.Json" culture="neutral" publicKeyToken="30ad4fe6b2a6aeed" />
        <bindingRedirect oldVersion="0.0.0.0-9.0.0.0" newVersion="9.0.0.0" />
      </dependentAssembly>
      <probing privatePath="TelemetryModule" />
    </assemblyBinding>
  </runtime>
  <system.net>
    <defaultProxy>
      <proxy bypassonlocal="false" usesystemdefault="true" proxyaddress="http://10.108.124.245:8080" />
    </defaultProxy>
  </system.net>
</configuration>
```

#### 4. Reinicie Telemetry Service.

Ejecute los cmdlets de Call Home en PowerShell.

### Recopilar y cargar manualmente la información de diagnóstico

Puede usar el sitio web de CIS para cargar un paquete de información de diagnóstico en CIS. También puede usar cmdlets de PowerShell para recopilar y cargar la información de diagnóstico en CIS.

Para cargar un paquete mediante el sitio web de CIS:

1. Inicie una sesión en Citrix Insight Services mediante las credenciales de su cuenta de Citrix.
2. Seleccione **My Workspace**.
3. Seleccione **Healthcheck** y vaya a la ubicación de sus datos.

CIS admite varios cmdlets de PowerShell para administrar la carga de datos. Esta documentación cubre los cmdlets de los dos casos de uso más frecuentes:

- Use el cmdlet `Start-CitrixCallHomeUpload` para recopilar y cargar manualmente un paquete de información de diagnóstico en CIS. (El paquete no se guarda localmente.)
- Use el cmdlet `Start-CitrixCallHomeUpload` para recopilar manualmente un paquete de información de diagnóstico y guardarlo localmente. Esto le permite obtener una vista previa de los datos. Luego, use el cmdlet `Send-CitrixCallHomeBundle` para cargar manualmente una copia del paquete en CIS (los datos permanecen guardados localmente).

La ayuda de PowerShell proporciona la sintaxis completa, incluidas las descripciones de cmdlets y parámetros que no se utilizan en estos casos de uso más comunes.

Al introducir un cmdlet para cargar datos en CIS, se le pedirá que confirme la carga. Si el cmdlet excede el tiempo de espera de la operación antes de que se complete la carga, compruebe el estado de la

carga en el registro de eventos del sistema. La solicitud de carga puede rechazarse si el servicio ya está realizando una carga.

### Recopilar datos y cargar paquetes en CIS:

```
1 Start-CitrixCallHomeUpload [-Credential] PSCredential [-InputPath
  string] [-Description string] [-IncidentTime string] [-SRNumber
  string] [-Name string] [-UploadHeader string] [-AppendHeaders string
  ] [-Collect string] [<CommonParameters>]
2 <!--NeedCopy-->
```

### Recopilar datos para guardarlos localmente:

```
1 Start-CitrixCallHomeUpload -OutputPath <String> [-InputPath string] [-
  Description string] [-IncidentTime string] [-SRNumber string] [-Name
  string] [-UploaderHeader string] [-AppendHeaders string] [-Collect
  strings] [<CommonParameters>]
2 <!--NeedCopy-->
```

Los siguientes parámetros son válidos:

- **Credential:** Dirige la carga a CIS.
- **InputPath:** Ubicación del archivo zip que desea incluir en el paquete. Esto puede ser algún archivo adicional que le pida Citrix Support. Asegúrese de incluir la extensión .zip.
- **OutputPath:** Ubicación donde se guarda la información de diagnóstico. Este parámetro es necesario cuando se guardan los datos de Call Home localmente.
- **Descripción y tiempo de incidente:** información de forma gratuita sobre la carga.
- **SRNumber:** Número de incidente de Citrix Technical Support.
- **Nombre:** Nombre que identifica el paquete.
- **UploadHeader:** Cadena en formato JSON que especifica los encabezados cargados en CIS.
- **AppendHeaders:** Cadena en formato JSON que especifica los encabezados anexados cargados en CIS.
- **Collect:** Cadena en formato JSON que especifica qué datos hay que recopilar u omitir, con el formato {'collector':{'enabled':Boolean}}, donde Boolean es True o False.

Los valores válidos de recopilador para el parámetro 'collector'son:

- 'wmi'
- 'process'
- 'registry'
- 'crashreport'
- 'trace'
- 'file'

- 'msi'
- 'localdata'
- 'sitedata'
- 'sfb'

De forma predeterminada, están habilitados todos los recopiladores salvo "sfb".

El recopilador "sfb" está diseñado para utilizarse a petición para diagnosticar problemas de Skype Empresarial. Además del parámetro "enabled", el recopilador 'sfb' admite los parámetros "account" y "accounts" para especificar usuarios de destino. Utilice uno de los formatos:

- "-Collect "{sfb':{'account':'domain\\user1'}}"
- "-Collect "{sfb':{'accounts':['domain\\user1','domain\\user2']}}"

- **Parámetros comunes:** consulte la ayuda de PowerShell.

### Cargar datos previamente guardados localmente:

```
Send-CitrixCallHomeBundle -Credential <PSCredential> -Path string [<CommonParameters>]
```

El parámetro `Path` especifica la ubicación del paquete que fue guardado previamente.

### Ejemplos:

El cmdlet siguiente solicita una carga de datos de Call Home (excluyendo los datos del recopilador de WMI) en CIS. Estos datos están relacionados con los fallos de registros de los VDA de Citrix Provisioning, notificados a las 14:30 para el caso de asistencia técnica de Citrix Support número 123456. Además de los datos de Call Home, se incorpora el archivo "c:\Diagnostics\ExtraData.zip" al paquete que se carga.

```
1 C:\PS>Start-CitrixCallHomeUpload -InputPath "c:\Diagnostics\ExtraData.zip" -Description "Registration failures with Citrix Provisioning VDAs" -IncidentTime "14:30" -SRNumber 123456 -Name "RegistrationFailure-021812016" -Collect "{
2   'wmi':{
3     'enabled':false }
4   }
5   " -UploadHeader "{
6     'key1':'value1' }
7   " -AppendHeaders "{
8     'key2':'value2' }
9   "
10  <!--NeedCopy-->
```

El siguiente cmdlet guarda los datos de Call Home relacionados con el caso de asistencia técnica de Citrix Support número 223344, notificado a las 8:15 de la mañana. Los datos se guardan en el archivo mydata.zip en un recurso compartido de red. Además de los datos de Call Home, se incorporará el archivo "c:\Diagnostics\ExtraData.zip" al paquete guardado.

```
1 C:\PS>Start-CitrixCallHomeUpload -OutputPath \mynetwork\myshare\mydata.zip -InputPath "c:\Diagnostics\ExtraData.zip" -Description "Diagnostics for incident number 223344" -IncidentTime "8:15" -SRNumber 223344
2 <!--NeedCopy-->
```

El cmdlet siguiente carga el paquete de los datos que guardó previamente.

```
1 $cred=Get-Credential
2 C:\PS>Send-CitrixCallHomeBundle -Credential $cred -Path \mynetwork\myshare\mydata.zip
3 <!--NeedCopy-->
```

## Citrix Scout

January 19, 2023

### Introducción

Citrix Scout recopila diagnósticos y realiza comprobaciones de estado. Puede utilizar los resultados para el mantenimiento proactivo en su implementación de Citrix Virtual Apps and Desktops. Citrix ofrece el análisis integral y automatizado de las recopilaciones de diagnósticos a través de Citrix Insight Services. También puede usar Citrix Scout para solucionar problemas, ya sea por su cuenta o con las instrucciones de Citrix Support.

Puede cargar en Citrix los archivos de recopilaciones para que la Asistencia de Citrix los analice y le facilite instrucciones para solucionar los problemas. O bien, puede guardar localmente una recopilación para revisarlo más adelante y, más tarde, cargar el archivo de la recopilación en Citrix para que éste lo analice.

Scout ofrece los siguientes procedimientos:

- **Recopilar:** Se recopilan diagnósticos una vez en las máquinas que seleccione en el sitio. A continuación, puede cargar el archivo en Citrix o guardarlo localmente.
- **Rastrear y reproducir:** Se inicia un rastreo manual en las máquinas que seleccione. A continuación, puede reproducir los problemas en esas máquinas. Después de reproducir el problema, se detiene el rastreo. Scout recopila otros diagnósticos y carga el archivo en Citrix o lo guarda localmente.
- **Programar:** Se programan recopilaciones diarias o semanales de diagnósticos en un tiempo especificado y en las máquinas que seleccione. El archivo se carga automáticamente en Citrix.

- **Comprobación de estado:** Realiza comprobaciones que evalúan el estado y la disponibilidad del sitio y de sus componentes. Puede realizar comprobaciones de estado para Delivery Controllers, VDA, servidores de StoreFront y servidores de licencias de Citrix. Si se encuentran problemas durante las comprobaciones, Scout proporciona un informe detallado. Cada vez que Scout se inicia, comprueba si hay scripts actualizados de comprobación de estado. Si hay nuevas versiones disponibles, Scout las descarga automáticamente para usarlas la próxima vez que se realicen las comprobaciones de estado.

La interfaz gráfica que se describe en este artículo es la forma principal de usar Citrix Scout. También puede utilizar PowerShell para configurar recopilaciones puntuales de diagnósticos, programarlas o cargarlas. Consulte [Call Home](#).

Dónde ejecutar Scout:

- En una implementación local, ejecute Scout desde un Delivery Controller para capturar diagnósticos o realizar comprobaciones en agentes Virtual Delivery Agent (VDA), Delivery Controllers, servidores de StoreFront y servidores de licencias. También puede ejecutar Scout desde un VDA para recopilar diagnósticos locales.
- En un entorno de Citrix Cloud donde se usa el servicio Citrix Virtual Apps and Desktops, ejecute Citrix Scout desde un VDA para recopilar datos de diagnóstico local.

El registro de la aplicación Scout se almacena en `C:\ProgramData\Citrix\TelemetryService\ScoutUI.log`. Este archivo se puede usar para solucionar problemas.

## Qué datos se recopilan

El diagnóstico recopilado por Scout incluye archivos de registro de rastreos de Citrix Diagnostic Facility (CDF). También se incluye un subconjunto de rastros CDF llamado Always-on Tracing (AOT). La información de AOT puede ser útil para solucionar problemas comunes, como los registros de VDA e inicios de aplicaciones o escritorios. No se recopila ninguna otra información de rastreo de eventos para Windows (ETW).

La colección incluye:

- Entradas de Registro creadas por Citrix Virtual Apps and Desktops en `HKEY\LOCAL_MACHINE\SOFTWARE\CITRIX`.
- Información de WMI (Instrumental de administración de Windows) en el **espacio de nombres de Citrix**.
- Procesos que se están ejecutando.
- Volcados de errores de procesos de Citrix que están almacenados en `%PROGRAM DATA%\Citrix\CDF`
- Información sobre directivas de Citrix en formato CSV.

- Información sobre instalaciones y actualizaciones. Esta colección puede incluir el registro completo del metainstalador del producto, los registros MSI con errores, los resultados del analizador de registros MSI, los registros de StoreFront, los registros de comprobación de compatibilidad de licencias y los resultados de las pruebas preliminares de actualización de versión del sitio.

Acerca de la información rastreada:

- La información rastreada se comprime a medida que se recopila, por lo que ocupa poco espacio en la máquina.
- En cada máquina, Citrix Telemetry Service conserva durante un máximo de ocho días la información de rastreo más reciente comprimida.
- A partir de Citrix Virtual Apps and Desktops 7 1808, los rastros AOT se guardan en el disco local de forma predeterminada (en versiones anteriores, los rastreos se conservaban en la memoria). Ruta predeterminada = `C:\Users\CitrixTelemetryService\AppData\Local\CitrixAOT`.
- A partir de Citrix Virtual Apps and Desktops 7 1811, los rastros AOT guardados en los recursos compartidos de red se recopilan junto con otros diagnósticos.
- Puede modificar el tamaño máximo (predeterminado = 10 MB) y la duración del corte mediante el cmdlet `Enable-CitrixTrace` o la cadena de Registro `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Telemetry DefaultListen`.
- Los rastreos se adjuntan al archivo hasta que este alcanza el 10% de `MaxSize`.

Para ver una lista de los puntos de datos que recopila Scout, consulte [Puntos de datos clave para Call Home](#).

## Acerca de las comprobaciones de estado

Los datos de las comprobaciones de estado se almacenan en carpetas dentro de `C:\ProgramData\Citrix\TelemetryService\`.

### Comprobaciones de estado del sitio

Las comprobaciones de estado del sitio se incluyen en Environment Test Service, que proporciona una evaluación completa de los servicios de FlexCast Management Architecture (FMA). Además de comprobar la disponibilidad del servicio, estas comprobaciones buscan otros indicadores de estado, como las conexiones de las bases de datos.

Las comprobaciones de estado del sitio se realicen en los Delivery Controllers. En función del tamaño del sitio, estas comprobaciones pueden tardar hasta una hora en completarse.

**Comprobaciones de configuración de los Delivery Controllers** Como parte de las comprobaciones de estado del sitio. Las comprobaciones de configuración de los Delivery Controllers verifican la existencia de los siguientes problemas según las recomendaciones de Citrix para sitios de Virtual Apps and Desktops:

- Uno o más Delivery Controllers se encuentran en un estado fallido.
- Solo hay un Delivery Controller en el sitio.
- Los Delivery Controllers tienen versiones diferentes.

Además de cumplir con los permisos y requisitos de las comprobaciones de estado, las comprobaciones de la configuración de los Delivery Controllers requieren:

- Al menos un Controller encendido.
- Broker Service activo en un Controller.
- Una conexión activa del Controller a la base de datos del sitio.

### **Comprobaciones de estado en el VDA**

Las comprobaciones de estado de los VDA identifican posibles causas de problemas comunes con el registro, el inicio de sesión y la redirección de zona horaria de los VDA.

Para el registro en los VDA, Scout comprueba:

- Instalación del software en el VDA
- Pertenencia al dominio de máquinas en el VDA
- Disponibilidad del puerto de comunicación en el VDA
- Estado del servicio en el VDA
- Configuración del firewall de Windows
- Comunicación con el Controller
- Sincronización de tiempo con el Controller
- Estado de registro de VDA

Para el inicio de sesión en VDA, Scout comprueba:

- Disponibilidad del puerto de comunicación en el inicio de sesión
- Estado de los servicios en el inicio de sesión
- Configuración del firewall de Windows en el inicio de sesión
- Licencias de acceso de cliente a Servicios de Escritorio remoto en VDA
- Ruta de inicio de aplicaciones en VDA

Para la redirección de zona horaria en VDA, Scout comprueba:

- Instalación de parches rápidos de Windows
- Instalación de parches rápidos de Citrix

- Configuración de directivas de grupo de Microsoft
- Configuración de directivas de grupo de Citrix

### **Comprobaciones de estado de StoreFront**

Las comprobaciones de StoreFront verifican:

- Citrix Default Domain Service no está activo
- Citrix Credential Wallet Service no está activo
- Conexión desde el servidor de StoreFront al puerto 88 de Active Directory
- Conexión desde el servidor de StoreFront al puerto 389 de Active Directory
- La URL base tiene un nombre FQDN válido
- La dirección IP correcta de la URL base se puede obtener
- El grupo de aplicaciones de IIS utiliza .NET 4.0
- Si el certificado está enlazado al puerto SSL para la URL del host
- Si la cadena de certificados está completa
- Si los certificados han caducado
- Si un certificado caduca pronto (en un plazo de 30 días)

### **Comprobaciones del servidor de licencias**

Las comprobaciones del servidor de licencias verifican:

- Conexión del servidor de licencias desde el Delivery Controller
- Estado del acceso remoto del firewall del servidor de licencias
- Estado del servicio Citrix Licensing
- Estado del período de gracia del servidor de licencias
- Conexión de puertos del servidor de licencias
- Si el demonio de proveedor de Citrix (CITRIX) está activo
- Si los relojes del sistema están sincronizados
- Si Citrix Licensing Service no está activo en la cuenta de servicio local
- Presencia del archivo `CITRIX.opt`
- Fecha válida para Customer Success Services
- Actualización de Citrix License Server
- Si el certificado del servidor de licencias se encuentra en el almacén raíz de confianza del Delivery Controller

Además de cumplir con los permisos y requisitos de las comprobaciones de estado, el servidor de licencias debe estar unido a un dominio. De lo contrario, el servidor de licencias no se detectará.

## Permisos y requisitos

Permisos:

- Para recopilar diagnósticos:
  - Debe ser un administrador local y un usuario de dominio en cada máquina donde recopila datos de diagnóstico.
  - Debe tener permiso para escribir en el directorio LocalAppData de cada máquina.
- Para realizar comprobaciones de estado:
  - Debe ser miembro del grupo de usuarios del dominio.
  - Debe ser administrador total o tener un rol personalizado con permisos de solo lectura y de **ejecución de pruebas de entorno** para el sitio.
- Use **Ejecutar como administrador** al iniciar Citrix Scout.

Para cada máquina desde la que recopile diagnósticos o realice comprobaciones de estado:

- Scout debe poder comunicarse con la máquina.
- La posibilidad de compartir archivos e impresoras debe estar activada.
- PSRemoting y WinRM deben estar habilitados. La máquina también debe ejecutar PowerShell 3.0 o posterior.
- La máquina debe estar ejecutando Citrix Telemetry Service.
- El acceso a Windows Management Infrastructure (WMI) debe estar habilitado en la máquina.
- Para establecer una programación de la recopilación de diagnósticos, la máquina debe contar con una versión compatible de Scout.

No use el signo de dólar (\$) en los nombres de usuario especificados en las rutas de acceso. Impide la recopilación de información de diagnóstico.

Scout ejecuta pruebas de verificación en las máquinas que seleccione para garantizar que se cumplen estos requisitos.

## Pruebas de verificación

Antes del inicio de una recopilación de diagnóstico o una comprobación de estado, se ejecutan automáticamente pruebas de verificación en cada máquina seleccionada. Estas pruebas tienen por finalidad comprobar que se cumplen los requisitos. Si la prueba de una máquina falla, Scout muestra un mensaje con acciones correctivas sugeridas.

- **Scout no puede acceder a esta máquina:** Compruebe que:
  - La máquina está encendida.

- La conexión de red funciona correctamente (es posible que esto implique verificar que el firewall está configurado correctamente).
- Se pueden compartir archivos e impresoras. Consulte la documentación de Microsoft para obtener instrucciones.
- **Habilitar PSRemoting y WinRM:** Puede habilitar la comunicación remota de PowerShell y WinRM al mismo tiempo. Con la opción **Ejecutar como administrador**, ejecute el cmdlet `Enable-PSRemoting`. Para obtener más información, consulte la Ayuda de Microsoft para el cmdlet.
- **Scout requiere PowerShell 3.0 (como mínimo):** Instale PowerShell 3.0 (o una versión posterior) en la máquina y habilite la comunicación remota de PowerShell.
- **No se puede acceder al directorio LocalAppData en esta máquina:** Compruebe que su cuenta tiene permiso para escribir en el directorio LocalAppData de la máquina.
- **No se encuentra Citrix Telemetry Service:** Asegúrese de que Citrix Telemetry Service está instalado e iniciado en la máquina.
- **No se puede obtener la programación:** Actualice la versión de XenApp y XenDesktop de la máquina a 7.14 (mínimo).
- **WMI no se está ejecutando en la máquina:** Compruebe que el acceso del Instrumental de administración de Windows (WMI) está habilitado.
- **Conexiones de WMI bloqueadas:** Habilite WMI en el servicio Firewall de Windows.
- **Se requiere una versión más reciente de Citrix Telemetry Service** (la versión solo se comprueba para recopilar y rastrear y reproducir). Actualice la versión de Telemetry Service en la máquina (consulte Instalación y actualización). Si no actualiza la versión del servicio, esa máquina no participará en las acciones **Recopilar** ni **Rastrear y reproducir**.

## Compatibilidad de versiones

Esta versión de Scout (3.x) está diseñada para ejecutarse en Controllers y agentes VDA de Citrix Virtual Apps and Desktops (o XenApp y XenDesktop 7.14 como mínimo).

Se proporciona una versión anterior de Scout con las versiones anteriores de XenApp y XenDesktop 7.14. Para obtener información sobre esa versión anterior, consulte [CTX130147](#).

Si actualiza un Controller o VDA anteriores a 7.14 a la versión 7.14 (o una versión posterior compatible), la versión anterior de Scout se reemplaza por la versión actual.

Función	Scout 2.23	Scout 3.0
Compatibilidad con Citrix Virtual Apps and Desktops (además de XenApp y XenDesktop de 7.14 a 7.18)	Sí	Sí
Compatibilidad con XenDesktop 5.x, de 7.1 a 7.13	Sí	No
Compatibilidad con XenApp 6.x y de 7.5 a 7.13	Sí	No
Entregado con el producto	7.1 a 7.13	A partir de 7.14
Se puede descargar desde un artículo CTX	Sí	No
Capturar rastros CDF	Sí	Sí
Capturar rastreos permanentes (AOT)	No	Sí
Permitir recopilación de diagnósticos	Un máximo de 10 máquinas a la vez (de forma predeterminada)	Sin límite (sujeto a la disponibilidad de recursos)
Permitir que los datos de diagnóstico se envíen a Citrix	Sí	Sí
Permitir que los datos de diagnóstico se guarden localmente	Sí	Sí
Funcionalidad para credenciales de Citrix Cloud	No	Sí
Funcionalidad para credenciales de Citrix	Sí	Sí
Funcionalidad para servidores proxy de carga	Sí	Sí
Ajustar programaciones	N/D	Sí
Funcionalidad para scripts	Línea de comandos (solo para el Controller local)	PowerShell mediante los cmdlets de Call Home (es decir, cualquier máquina con Telemetry Service instalado)
Comprobaciones de estado	No	Sí
Enmascaramiento de datos	No	A partir de 3.17

## Instalación y actualización

De forma predeterminada, Scout se instala o se actualiza automáticamente como parte de Citrix Telemetry Service cuando se instala o actualiza un VDA o un Controller.

Si omite Citrix Telemetry Service cuando instala un VDA o elimina el servicio más adelante, ejecute `TelemetryServiceInstaller_xx.msi` desde la carpeta `x64\Virtual Desktop Components` o `x86\Virtual Desktop Components` en los medios de instalación de Citrix Virtual Apps and Desktops.

Al seleccionar las acciones **Recopilar** o **Rastrear y reproducir**, se le notificará si una máquina utiliza una versión anterior de Citrix Telemetry Service. Citrix recomienda utilizar la versión más reciente admitida. Si no actualiza Telemetry Service en esa máquina, no participará en las acciones **Recopilar** ni **Rastrear y reproducir**. Para actualizar Telemetry Service, utilice el mismo procedimiento el de su instalación.

## Autorización de carga

Si va a cargar las recopilaciones de diagnósticos en Citrix, debe tener una cuenta de Citrix o Citrix Cloud. (Estas son las credenciales que debe utilizar para acceder a las descargas de Citrix o para acceder a la central de control de Citrix Cloud.) Una vez validadas las credenciales de cuenta, se emite un token.

- Si se autentica con una cuenta de Citrix, el proceso de emisión de token no se ve. Simplemente, introduce sus credenciales de cuenta. Una vez que Citrix haya validado las credenciales, puede continuar en el asistente de Scout.
- Si se autentica con una cuenta de Citrix Cloud, debe hacer clic en un enlace para acceder a Citrix Cloud mediante HTTPS con su explorador web predeterminado. Después de introducir sus credenciales de Citrix Cloud, se muestra el token. Copie el token y luego péguelo en Citrix Scout. A continuación, puede seguir en el asistente de Scout.

El token se almacena localmente en la máquina que ejecuta Citrix Scout. Para habilitar el uso de este token la próxima vez que ejecute **Recopilar** o **Rastrear y reproducir**, marque la casilla **Guardar el token y omitir este paso en el futuro**.

Debe volver a autorizar cada vez que seleccione **Programar** en la página de inicio de Citrix Scout. No puede usar un token almacenado al crear o cambiar una programación.

## Usar un proxy para cargas

Si quiere utilizar un proxy para cargar recopilaciones en Citrix, puede configurar Scout para que use los parámetros de proxy configurados para las propiedades de Internet del explorador. Si no, también puede especificar la dirección IP y el número de puerto del servidor proxy.

## Agregar máquinas manualmente

Después de que Scout indique los Controllers y los agentes VDA que haya detectado, puede agregar manualmente otras máquinas de la implementación, como, por ejemplo, servidores de StoreFront, servidores de licencias y servidores de Citrix Provisioning.

Al realizar comprobaciones de estado:

- Los servidores de licencias de Citrix del dominio se detectan automáticamente. No puede agregar servidores de licencias manualmente.
- Por ahora, las comprobaciones de estado no se admiten en los servidores de Citrix Provisioning.

En una página de Scout que ofrece la lista de las máquinas detectadas, haga clic en **+ Agregar máquina**. Introduzca el nombre FQDN de la máquina que quiera agregar y, a continuación, haga clic en **Continuar**. Repita los pasos para agregar otras máquinas si fuera necesario (aunque introducir un alias DNS en lugar de un nombre FQDN pueda parecer válido, es posible que las comprobaciones de estado fallen).

Las máquinas agregadas manualmente siempre aparecen en la parte superior de la lista de máquinas, encima de las máquinas detectadas.

Una manera sencilla de identificar una máquina agregada manualmente es el botón rojo “Eliminar” situado en el extremo derecho de la fila. Solo las máquinas agregadas manualmente tienen ese botón. Las máquinas detectadas, no.

Para quitar una máquina agregada manualmente, haga clic en el botón de color rojo en el final derecho de la fila. Confirme la eliminación. Repita los pasos para eliminar otras máquinas que se hayan agregado manualmente.

Scout recuerda las máquinas agregadas manualmente hasta que las elimine. Al cerrar y volver a abrir Scout, las máquinas agregadas manualmente siguen figurando en la parte superior de la lista.

Los rastreos CDF no se recopilan cuando se usa **Rastrear y reproducir** en los servidores de StoreFront. Sin embargo, se recopila toda la información restante de rastreo.

## Recopilar diagnósticos

El procedimiento **Recopilar** comprende la selección de máquinas, el inicio de la recopilación de datos de diagnóstico y la carga del archivo que contiene la recopilación en Citrix (también se puede guardar localmente).

1. Inicie Scout. Desde el menú **Inicio** de la máquina, seleccione **Citrix > Citrix Scout**. En la página de inicio, haga clic en **Recopilar**.
2. Seleccione las máquinas. La página **Seleccionar máquinas** ofrece una lista de todos los agentes VDA y los Controllers del sitio. Puede filtrar la lista por el nombre de la máquina.

Marque la casilla de verificación situada junto a cada máquina de la que quiera recopilar datos de diagnóstico y, a continuación, haga clic en **Continuar**.

Para agregar manualmente otras máquinas, por ejemplo, servidores Citrix Provisioning o Store-Front, consulte Agregar máquinas manualmente.

Scout inicia automáticamente pruebas en cada máquina seleccionada para verificar que cumple los criterios que figuran en Pruebas de verificación. Si se produce un error en la verificación, aparece un mensaje en la columna **Estado** y la casilla de verificación de la máquina se desmarca. Puede:

- Resolver el problema y, a continuación, volver a marcar la casilla de verificación de la máquina. Esto provoca un reintento de las pruebas de verificación.
- Omitir esa máquina (dejar la casilla de verificación desmarcada). No se recopilarán datos de diagnóstico en esa máquina.

Cuando finalicen las pruebas de verificación, haga clic en **Continuar**.

3. Recopile diagnósticos. En el resumen, se ofrece una lista de todas las máquinas desde donde se recopilarán los diagnósticos (las máquinas seleccionadas que han superado las pruebas de verificación). Haga clic en **Iniciar recopilación**.

Durante la recopilación:

- La columna **Estado** indica el estado actual de la recopilación de una máquina.
- Para detener una recopilación en curso en una sola máquina, haga clic en **Cancelar** en la columna **Acción** perteneciente a esa máquina.
- Para detener todas las recopilaciones en curso, haga clic en **Detener recopilación** en la esquina inferior derecha de la página. Se conservan los diagnósticos de las máquinas cuya recopilación se haya acabado. Para reanudar la recopilación, haga clic en **Reintentar** en la columna **Acción** de cada máquina.
- Cuando se completa la recopilación de todas las máquinas seleccionadas, el botón **Detener recopilación** de la esquina inferior derecha cambia a **Continuar**.
- Para volver a recopilar diagnósticos, haga clic en **Repetir**, en la columna **Acción** de la máquina. La recopilación más reciente sobrescribe la anterior.
- Si se produce un error en una recopilación, puede hacer clic en **Reintentar** en la columna **Acción**. Solo se cargan o se guardan las recopilaciones correctas.
- Una vez completada la recopilación de todas las máquinas seleccionadas, no haga clic en **Atrás** (si hace clic, la recopilación se pierde).

Cuando la recopilación se complete, haga clic en **Continuar**.

4. Guarde la recopilación o cárguela. Elija si quiere cargar el archivo en Citrix o guardarlo en la máquina local.

Si elige cargar el archivo ahora, continúe en el paso 5.

Si opta por guardar localmente el archivo:

- Aparecerá el cuadro de diálogo **Guardar** de Windows. Vaya a la ubicación pertinente.
- Cuando se complete la operación de guardado local, aparecerá el nombre de ruta del archivo y se vinculará. Puede ver el archivo. Puede cargar el archivo en Citrix más tarde. Véase [CTX136396](#).

Haga clic en **Listo** para volver a la página de inicio de Citrix Scout. No es necesario completar más pasos en este procedimiento.

5. Auténtiquese para cargar archivos y, si quiere, especifique un proxy. Para obtener información más detallada, consulte Autorización de carga.

- Si no se ha autenticado por Scout, continúe en este paso.
- Si se ha autenticado por Scout, se utiliza el token de autorización almacenado de forma predeterminada. Si esto es lo que quiere hacer, seleccione esta opción y haga clic en **Continuar**. No se le solicitan credenciales para esta recopilación. Continúe en el paso 6.
- Si se ha autenticado antes, pero quiere volver a autorizar la carga y obtener un nuevo token, haga clic en **Cambiar / volver a autorizar** y continúe con este paso.

Elija si quiere usar credenciales de Citrix Cloud o las credenciales de Citrix para autenticar la carga. Haga clic en **Continuar**. Aparecerá la página de credenciales solo si no usa un token almacenado.

En la página de credenciales:

- Si quiere utilizar un servidor proxy para la carga de archivos, haga clic en **Configurar proxy**. Puede configurar Scout para que use los parámetros de proxy configurados para las propiedades de Internet de su explorador web. Si no, también puede introducir la dirección IP y el número de puerto del servidor proxy. Cierre el cuadro de diálogo del proxy.
- Para una cuenta de Citrix Cloud, haga clic en **Generar token** en Citrix Cloud. Su explorador web predeterminado se inicia con una página de Citrix Cloud donde se muestra el token. Copie el token y luego péguelo en la página de Citrix Scout.
- Para una cuenta de Citrix, introduzca las credenciales.

Cuando haya terminado, haga clic en **Continuar**.

6. Introduzca información sobre la carga.

- El campo de nombre contiene el nombre predeterminado del archivo de los diagnósticos recopilados. Este nombre es suficiente para la mayoría de las recopilaciones, aunque puede cambiarlo (si elimina el nombre predeterminado y deja vacío el campo de nombre, se usará el nombre predeterminado).
- Si lo prefiere, puede especificar un número de caso de asistencia de Citrix de 8 dígitos.

- En el campo opcional **Descripción**, describa el problema e indique cuándo ocurrió, si corresponde.

Cuando haya terminado, haga clic en **Iniciar carga**.

Durante la carga, la parte inferior izquierda de la página muestra el porcentaje aproximado de la carga que se ha completado. Para cancelar una carga en curso, haga clic en **Detener carga**.

Cuando se complete la carga, se muestra y se vincula la URL de su ubicación. Siga el enlace a la ubicación de Citrix para ver el análisis de la carga; también puede copiar el enlace.

Haga clic en **Listo** para volver a la página de inicio de Citrix Scout.

## Rastrear y reproducir

El procedimiento de **rastreo y reproducción** comprende la selección de máquinas, el inicio del rastreo, la reproducción de problemas, la recopilación de diagnósticos y la carga del archivo en Citrix o su almacenamiento local.

Este procedimiento es similar al procedimiento estándar **Recopilar**. No obstante, permite iniciar un rastreo en las máquinas y, a continuación, recrear los problemas ocurridos en esas máquinas. Todas las recopilaciones de diagnósticos incluyen información de rastros AOT. Este procedimiento agrega rastros CDF para ayudar a solucionar problemas.

1. Inicie Scout. Desde el menú **Inicio** de la máquina, seleccione **Citrix > Citrix Scout**. En la página de inicio, haga clic en **Rastrear y reproducir**.
2. Seleccione las máquinas. La página **Seleccionar máquinas** ofrece una lista de todos los agentes VDA y los Controllers del sitio. Puede filtrar la lista por el nombre de la máquina. Marque la casilla de verificación situada junto a cada máquina de la que quiera recopilar datos de rastreo y diagnóstico. Luego haga clic en **Continuar**.

Para agregar manualmente otras máquinas, por ejemplo, servidores Citrix Provisioning o StoreFront, consulte Agregar máquinas manualmente.

Scout inicia automáticamente pruebas en cada máquina seleccionada para verificar que cumple los criterios que figuran en Pruebas de verificación. Si se produce un error en la verificación de una máquina, aparece un mensaje en la columna **Estado** y la casilla de verificación de la máquina se desmarca. Puede:

- Resolver el problema y, a continuación, volver a marcar la casilla de verificación de la máquina. Esto provoca un reintento de las pruebas de verificación.
- Omitir esa máquina (dejar la casilla de verificación desmarcada). No se recopilarán datos de diagnóstico ni de rastreo en esa máquina.

Cuando finalicen las pruebas de verificación, haga clic en **Continuar**.

3. Inicie el rastreo. En el resumen, se ofrece una lista de todas las máquinas desde donde se recopilarán rastreos. Haga clic en **Iniciar rastreo**.

En una o varias de las máquinas seleccionadas, reproduzca los problemas que tuvo. La recopilación de rastreo continúa mientras recrea los problemas. Cuando haya terminado de recrear el problema, haga clic en **Continuar** en Citrix Scout. Eso detiene el rastreo.

Una vez detenido el rastreo, indique si reprodujo el problema durante el rastreo.

4. Recopile diagnósticos de máquinas. Haga clic en **Iniciar recopilación**. Durante la recopilación:

- La columna **Estado** indica el estado actual de la recopilación de una máquina.
- Para detener una recopilación en curso en una sola máquina, haga clic en **Cancelar** en la columna **Acción** perteneciente a esa máquina.
- Para detener todas las recopilaciones en curso, haga clic en **Detener recopilación** en la esquina inferior derecha de la página. Se conservan los diagnósticos de las máquinas cuya recopilación se haya acabado. Para reanudar la recopilación, haga clic en **Reintentar** en la columna **Acción** de cada máquina.
- Cuando se completa la recopilación de todas las máquinas seleccionadas, el botón **Detener recopilación** de la esquina inferior derecha cambia a **Continuar**.
- Para volver a recopilar diagnósticos de una máquina, haga clic en **Repetir**, en la columna **Acción** de la máquina. La recopilación más reciente sobrescribe la anterior.
- Si se produce un error en una recopilación, puede hacer clic en **Reintentar** en la columna **Acción**. Solo se cargan o se guardan las recopilaciones correctas.
- Una vez completada la recopilación de todas las máquinas seleccionadas, no haga clic en **Atrás** (si hace clic, la recopilación se pierde).

Cuando la recopilación se complete, haga clic en **Continuar**.

5. Guarde la recopilación o cárguela. Elija si quiere cargar el archivo en Citrix o guardarlo localmente.

Si elige cargar el archivo ahora, continúe en el paso 6.

Si opta por guardar localmente el archivo:

- Aparecerá el cuadro de diálogo Guardar de Windows. Seleccione la ubicación pertinente.
- Cuando se complete la operación de guardado local, aparecerá el nombre de ruta del archivo y se vinculará. Puede ver el archivo. Recuerde: Puede cargar el archivo más adelante en Citrix; consulte [CTX136396](#) para Citrix Insight Services.

Haga clic en **Listo** para volver a la página de inicio de Citrix Scout. No es necesario completar más pasos en este procedimiento.

6. Auténtíquese para cargar archivos y, si quiere, especifique un proxy. Revise Autorización de carga para obtener más información de este proceso.

- Si no se ha autenticado por Scout, continúe en este paso.
- Si se ha autenticado por Scout, se utiliza el token de autorización almacenado de forma predeterminada. Si esto es lo que quiere hacer, elija esta opción y haga clic en **Continuar**. No se le solicitan credenciales para esta recopilación. Continúe en el paso 7.
- Si se ha autenticado antes, pero quiere volver a autorizar la carga y obtener un nuevo token, haga clic en **Cambiar / volver a autorizar** y continúe con este paso.

Elija si quiere usar credenciales de Citrix Cloud o las credenciales de Citrix para autenticar la carga. Haga clic en **Continuar**. Aparecerá la página de credenciales solo si no usa un token almacenado.

En la página de credenciales:

- Si quiere utilizar un servidor proxy para la carga de archivos, haga clic en **Configurar proxy**. Puede configurar Scout para que use los parámetros de proxy configurados para las propiedades de Internet de su explorador web. Si no, también puede introducir la dirección IP y el número de puerto del servidor proxy. Cierre el cuadro de diálogo del proxy.
- Para una cuenta de Citrix Cloud, haga clic en **Generar token** en Citrix Cloud. Su explorador web predeterminado se inicia con una página de Citrix Cloud donde se muestra el token. Copie el token y luego péguelo en la página de Citrix Scout.
- Para una cuenta de Citrix, introduzca las credenciales.

Cuando haya terminado, haga clic en **Continuar**.

## 7. Facilite información sobre la carga.

Introduzca los datos de carga:

- El campo de nombre contiene el nombre predeterminado del archivo de los diagnósticos recopilados. Este nombre es suficiente para la mayoría de las recopilaciones, aunque puede cambiarlo (si elimina el nombre predeterminado y deja vacío el campo de nombre, se usará el nombre predeterminado).
- Si lo prefiere, puede especificar un número de caso de asistencia de Citrix de 8 dígitos.
- En el campo opcional Descripción, describa el problema e indique cuándo ocurrió, si corresponde.

Cuando haya terminado, haga clic en **Iniciar carga**.

Durante la carga, la parte inferior izquierda de la página muestra el porcentaje aproximado de la carga que se ha completado. Para cancelar una carga en curso, haga clic en **Detener carga**.

Cuando se complete la carga, se muestra y se vincula la URL de su ubicación. Siga el enlace a la ubicación de Citrix para ver el análisis de la carga; también puede copiar el enlace.

Haga clic en **Listo** para volver a la página de inicio de Citrix Scout.

## Programar recopilaciones

Nota:

En la actualidad, puede programar colecciones, pero no comprobaciones de estado.

El procedimiento de programación incluye la selección de las máquinas y el establecimiento o la cancelación de la programación. Las recopilaciones programadas se cargan automáticamente en Citrix (puede guardar localmente las recopilaciones programadas mediante la interfaz de PowerShell; Consulte [Citrix Call Home](#).)

1. Inicie Scout. Desde el menú Inicio de la máquina, seleccione **Citrix > Citrix Scout**. En la página de inicio, haga clic en **Programar**.
2. Seleccione las máquinas. Se muestran todos los VDA y Controllers del sitio. Puede filtrar la lista por el nombre de la máquina.

Al instalar los VDA y los Controllers mediante la interfaz gráfica, si establece una programación de Call Home (consulte [Citrix Call Home](#)), Scout muestra esa configuración de forma predeterminada. Puede usar esta versión de Scout para iniciar recopilaciones programadas por primera vez, o bien para cambiar una programación previamente configurada.

Aunque haya habilitado o inhabilitado Call Home por máquina durante la instalación de componentes, una programación configurada en Scout afecta a todas las máquinas seleccionadas.

Marque la casilla de verificación situada junto a cada máquina de la que quiera recopilar datos de diagnóstico y, a continuación, haga clic en **Continuar**.

Para agregar manualmente otras máquinas, por ejemplo, servidores Citrix Provisioning o StoreFront, consulte [Agregar máquinas manualmente](#).

Scout inicia automáticamente pruebas en cada una de las máquinas seleccionadas para verificar que cumple los criterios que figuran en Pruebas de verificación. Si se produce un error en la verificación de una máquina, aparece un mensaje en la columna **Estado** y la casilla de verificación de la máquina se desmarca. Puede:

- Resolver el problema y, a continuación, volver a marcar la casilla de verificación de la máquina. Esto provoca un reintento de las pruebas de verificación.
- Omitir esa máquina (dejar la casilla de verificación desmarcada). No se recopilarán datos de diagnóstico (ni de rastreo) en esa máquina.

Cuando finalicen las pruebas de verificación, haga clic en **Continuar**.

En la página de resumen, se ofrece una lista de las máquinas a las que se aplicarán las programaciones. Haga clic en **Continuar**.

3. Configure la programación. Indique si quiere que se recopilen datos de diagnóstico. Recuerde: La programación afecta a todas las máquinas seleccionadas.

- Para configurar una programación semanal para las máquinas seleccionadas, haga clic en **Semanalmente**. Elija el día de la semana. Elija la hora del día (reloj de 24 horas) en que debe comenzar la recopilación de datos.
- Para configurar una programación diaria para las máquinas seleccionadas, haga clic en **Diariamente**. Elija la hora del día (reloj de 24 horas) en que debe comenzar la recopilación de datos.
- Para cancelar una programación existente para las máquinas seleccionadas (y no sustituirla por otra), **desactívela**. Eso cancelará cualquier programación que se haya configurado previamente para esas máquinas.

Haga clic en **Continuar**.

4. Auténtíquese para cargar archivos y, si quiere, especifique un proxy. Revise Autorización de carga para obtener más información de este proceso. Recuerde: No puede usar un token almacenado para autenticarse cuando utiliza una programación de Citrix Scout.

Elija si quiere usar credenciales de Citrix Cloud o las credenciales de Citrix para autenticar la carga. Haga clic en **Continuar**.

En la página de credenciales:

- Si quiere utilizar un servidor proxy para la carga de archivos, haga clic en **Configurar proxy**. Puede configurar Scout para que use los parámetros de proxy configurados para las propiedades de Internet de su explorador web. Si no, también puede introducir la dirección IP y el número de puerto del servidor proxy. Cierre el cuadro de diálogo del proxy.
- Para una cuenta de Citrix Cloud, haga clic en **Generar token** en Citrix Cloud. Su explorador web predeterminado se inicia con una página de Citrix Cloud donde se muestra el token. Copie el token y luego péguelo en la página de Citrix Scout.
- Para una cuenta de Citrix, introduzca las credenciales.

Cuando haya terminado, haga clic en **Continuar**.

Revise la programación configurada. Haga clic en **Listo** para volver a la página de inicio de Citrix Scout.

Durante una recopilación, el registro de aplicaciones de Windows de cada máquina seleccionada contiene entradas sobre la recopilación y la carga.

## Realizar comprobaciones de estado

El procedimiento de comprobación de estado comprende la selección de máquinas, el inicio de la comprobación y, a continuación, la revisión del informe de resultados.

1. Inicie Scout. Desde el menú **Inicio** de la máquina, seleccione **Citrix > Citrix Scout**. En la página de inicio, haga clic en **Comprobación de estado**.
2. Seleccione las máquinas. La página **Seleccionar máquinas** ofrece una lista de todos los agentes VDA, los Delivery Controllers y los servidores de licencias detectados en el sitio. Puede filtrar la lista por el nombre de la máquina. Marque la casilla de verificación situada junto a cada máquina de la que quiera recopilar datos de diagnóstico y, a continuación, haga clic en **Continuar**.

Para agregar otros tipos de componentes (como, por ejemplo, los servidores de StoreFront), consulte Agregar máquinas manualmente. No puede agregar manualmente servidores de Citrix Provisioning Server o servidores de licencias.

Scout inicia automáticamente pruebas en cada máquina seleccionada para verificar que cumple los criterios que figuran en Pruebas de verificación. Si se produce un error en la verificación, aparece un mensaje en la columna **Estado** y la casilla de verificación de la máquina se desmarca. Puede:

- Resolver el problema y, a continuación, volver a marcar la casilla de verificación de la máquina. Esto provoca un reintento de las pruebas de verificación.
- Omitir esa máquina (dejar la casilla de verificación desmarcada). No se realizarán comprobaciones de estado para esa máquina.

Cuando finalicen las pruebas de verificación, haga clic en **Continuar**.

3. Realice las comprobaciones de estado en las máquinas seleccionadas. En el resumen, se ofrece una lista de las máquinas en que se realizarán las pruebas (las máquinas seleccionadas que han superado las pruebas de verificación). Haga clic en **Iniciar la comprobación**.

Durante y después de la comprobación:

- La columna **Estado** indica el estado actual de la comprobación de una máquina.
- Para detener todas las comprobaciones en curso, haga clic en **Detener comprobación** en la esquina inferior derecha de la página (no puede cancelar la comprobación de estado de una sola máquina; solamente puede hacerlo para todas las máquinas seleccionadas). Se mantiene la información de las máquinas que han completado las comprobaciones.
- Cuando se completa la comprobación de todas las máquinas seleccionadas, el botón **Detener comprobación** de la esquina inferior derecha cambia a **Listo**.
- Si se produce un error en una comprobación, haga clic en **Reintentar** en la columna **Acción**.
- Si se completa una comprobación sin que se haya encontrado ningún problema, la columna **Acción** estará vacía.
- Si una comprobación encuentra problemas, haga clic en **Ver detalles** para mostrar los resultados.

- Una vez completada la comprobación de todas las máquinas seleccionadas, no haga clic en **Atrás** (si hace clic, se pierden los resultados de la comprobación).
4. Cuando finalicen las comprobaciones, haga clic en **Listo** para volver a la página de inicio de Scout.

### **Resultados de la comprobación de estado**

Para las comprobaciones de Citrix en la generación de informes, estos contienen:

- Hora y fecha en que se generó el informe de resultados
- Máquinas comprobadas
- Condiciones que la comprobación buscó en las máquinas correspondientes

## **Supervisar**

September 22, 2021

Los administradores y el personal de asistencia técnica pueden supervisar los sitios de Citrix Virtual Apps and Desktops con la ayuda de una gran variedad de funciones y herramientas. Con estas herramientas, puede supervisar:

- Sesiones de usuario y uso de sesiones
- Rendimiento de los inicios de sesión
- Conexiones y máquinas, incluidos los errores
- Patrones de carga
- Tendencias históricas
- Infraestructura

### **Citrix Director**

Director es una herramienta web en tiempo real que permite supervisar, solucionar problemas y realizar tareas de asistencia a los usuarios finales.

Para obtener más información, consulte los artículos de [Director](#).

### **Registro de configuraciones**

El registro de configuración (Configuration Logging) es una función que permite a los administradores realizar un rastreo de los cambios administrativos hechos en un sitio. El registro de configuración

puede ayudar a los administradores a diagnosticar y solucionar problemas después de realizar cambios de configuración, también puede ayudar en la administración de cambios y el rastreo de configuraciones, y notificar sobre actividades administrativas.

Puede ver y generar informes sobre la información registrada de Studio. También puede ver los elementos registrados en Director desde la vista Tendencias para ofrecer notificaciones acerca de los cambios de configuración. Esta función es útil para los administradores que no tienen acceso a Studio.

La vista Tendencias ofrece datos históricos de cambios de configuración realizados a lo largo de un período de tiempo, de forma que los administradores puedan ver qué cambios se hicieron en el sitio, quién los hizo y cuándo tuvieron lugar, para averiguar la causa de algún problema. Esta vista ordena la información de configuración en tres categorías:

- Fallos de conexión
- Máquinas de sesión única fallidas
- Máquinas de multisesión fallidas

Para obtener más información sobre cómo habilitar y configurar la función Registro de configuración, consulte el artículo [Registro de configuración](#). Los artículos de [Director](#) describen cómo ver la información registrada de esa herramienta.

## Registros de eventos

Los servicios dentro de Citrix Virtual Apps and Desktops registran los eventos que ocurren. Los registros de eventos se pueden usar para supervisar y solucionar problemas de las operaciones.

Para obtener más información, consulte [Registros de eventos](#). Los artículos referidos a funcionalidades individuales también pueden contener información de eventos.

## Registro de configuraciones

September 22, 2021

La función Registros de configuración (Configuration Logging) captura, en una base de datos, los cambios de configuración y las actividades de administración realizados en un sitio. Puede usar el contenido registrado para:

- Diagnosticar y solucionar problemas después de realizar cambios de configuración; el registro proporciona un trazado de los pasos seguidos.
- Ayudar en la administración de cambios y en el rastreo de las configuraciones

- Realizar informes de actividades administrativas

Puede establecer las preferencias de la captura de registros, mostrar los registros de configuración y generar informes HTML y CSV desde Citrix Studio. Puede filtrar la presentación en pantalla de los registros por intervalos de fechas y por resultados de búsqueda de texto. Cuando está habilitado, el registro obligatorio impide que se hagan cambios de configuración a menos que sea posible registrarlos. Con los permisos adecuados, puede eliminar entradas de los registros de configuración. No se puede utilizar la función Registros de configuración para modificar su contenido.

La función Registros de configuración usa un SDK de PowerShell y el servicio Configuration Logging Service. El servicio Configuration Logging Service se ejecuta en todos los Controllers del sitio. Si un Controller falla, el servicio instalado en otro Controller pasa automáticamente a gestionar las solicitudes de captura de registros.

De forma predeterminada, la función Registros de configuración está habilitada y usa la base de datos que se crea en el momento de crear un sitio (la base de datos de configuración del sitio). Puede especificar otra ubicación para la base de datos. La base de datos de registros de configuración admite las mismas funciones de alta disponibilidad que la base de datos de configuración del sitio.

El acceso a los datos de los registros de configuración se controla mediante la administración delegada, con los permisos Modificar preferencias de registros y Ver registros de configuración.

Los registros de configuración toman el idioma cuando se crean. Por ejemplo, un registro creado en inglés se lee en inglés, independientemente de la configuración regional del lector.

## Qué se registra

Se registran cambios de configuración y actividades de tipo administrativo iniciadas desde Studio, Director y scripts de PowerShell. Los ejemplos de cambios de configuración registrados incluyen trabajar con (crear, modificar, eliminar y asignar):

- Catálogos de máquinas
- Grupos de entrega (incluido cambiar la configuración de la administración de energía)
- Roles y ámbitos de administrador
- Recursos y conexiones de host
- Directivas de Citrix a través de Studio

Algunos ejemplos de actividades de tipo administrativo que se registran:

- Administrar energía de una máquina virtual o un escritorio de usuario
- Cuando Studio o Director envían un mensaje a un usuario

Las siguientes operaciones no se registran:

- Operaciones autónomas, como el encendido de máquinas virtuales mediante la administración de agrupaciones.
- Acciones de directivas implementadas mediante la Consola de administración de directivas de grupo (GPMC); puede utilizar herramientas de Microsoft para ver los registros de estas acciones.
- Los cambios realizados en el Registro, los accesos realizados directamente en la base de datos o desde otros orígenes distintos de Studio, Director o PowerShell.
- Cuando se inicializa la implementación, los registros de configuración están disponibles cuando la primera instancia del servicio Configuration Logging Service se registra con el servicio de configuración (Configuration Service). Por lo tanto, las primeras fases de la configuración no se registran (por ejemplo, cuando el esquema de la base de datos se obtiene y se aplica o cuando un hipervisor se inicializa).

## Administrar Registros de configuración

De forma predeterminada, Registros de configuración utiliza la base de datos que se crea al crear un sitio (también conocida como base de datos de configuración del sitio). Citrix recomienda usar otra ubicación para la base de datos de registros de configuración (y la base de datos de supervisión) por los siguientes motivos:

- Es probable que la estrategia de copia de seguridad para la base de datos de Registros de configuración sea distinta de la estrategia para la base de datos de configuración del sitio.
- El volumen de datos recopilados por los servicios de Registros de configuración (Configuration Logging) y de supervisión (Monitoring) puede afectar negativamente al espacio disponible en la base de datos de configuración del sitio.
- Elimina el punto de fallo único para las tres bases de datos.

Las ediciones del producto que no admiten los registros de configuración no tienen ningún nodo Registros en Studio.

## Habilitar o inhabilitar los Registros de configuración y el registro obligatorio

De forma predeterminada, Registros de configuración (Configuration Logging) está habilitado, pero la captura obligatoria está inhabilitada.

1. Seleccione **Registros** en el panel de navegación de Studio.
2. Seleccione **Preferencias** en el panel Acciones. El cuadro de diálogo Registros de configuración contiene información sobre las bases de datos e indica si los registros de configuración y el registro obligatorio están habilitados o inhabilitados.
3. Seleccione la acción pertinente:

Para habilitar Registros de configuración, seleccione **Habilitar**. Esta es la opción predeterminada. Si no se puede escribir en la base de datos, los datos de registros se descartan, aunque la operación sigue teniendo lugar.

Para inhabilitar Registros de configuración, seleccione **Inhabilitar**. Si la captura de registros estuvo habilitada previamente, los registros existentes se conservan y se pueden seguir consultando con el SDK de PowerShell.

Para habilitar la captura obligatoria de registros, seleccione **Impedir cambios en la configuración si la base de datos no está disponible**. No se permitirá ningún cambio de configuración o de tipo administrativo que normalmente se registraría, a menos que pueda registrarse en la base de datos de registros de configuración. Puede habilitar el registro obligatorio solo cuando Registros de configuración está habilitado; es decir, cuando **Habilitar** está seleccionado. Si el servicio de registros de configuración (Configuration Logging Service) falla y no se usa la alta disponibilidad, se asume que se aplica el registro obligatorio. En tales casos, las operaciones que normalmente se registrarían no se llevan a cabo.

Para inhabilitar la captura obligatoria de registros, seleccione **Permitir cambios en la configuración si la base de datos no está disponible**. Se permiten cambios de configuración y actividades de tipo administrativo incluso aunque no se pueda acceder a la base de datos de registros de configuración. Esta es la opción predeterminada.

## Cambiar la ubicación de la base de datos de Registros de configuración

No se puede cambiar la ubicación de la base de datos cuando está habilitado el registro obligatorio, ya que el cambio de ubicación implica un breve intervalo de desconexión que no se puede registrar.

1. Cree un servidor de base de datos mediante una versión compatible de SQL Server.
2. Seleccione **Registros** en el panel de navegación de Studio.
3. Seleccione **Preferencias** en el panel Acciones.
4. En el cuadro de diálogo “Preferencias de registros”, seleccione **Cambiar base de datos de registros**.
5. En el cuadro de diálogo Cambiar base de datos de registros, especifique la ubicación del servidor que contiene el nuevo servidor de base de datos. Consulte [Formatos de direcciones de bases de datos](#) para conocer los formatos válidos.
6. Para permitir que Studio cree la base de datos, haga clic en **Aceptar**. Cuando se le solicite, haga clic en **Aceptar** y la base de datos se creará automáticamente. Studio intenta acceder a la base de datos mediante las credenciales del usuario actual de Studio. Si no puede, el sistema pedirá las credenciales del usuario de la base de datos. Studio carga el esquema de base de datos en la base de datos. (Las credenciales se conservan solo durante la creación de la base de datos.)
7. Para crear la base de datos manualmente, haga clic en **Generar script de base de datos**. El script generado incluye instrucciones para crear manualmente la base de datos. Asegúrese de

que la base de datos está vacía y de que al menos un usuario tiene permiso para acceder y cambiar la base de datos antes de cargar el esquema.

Los datos de registros de configuración de la base de datos anterior no se importarán en la nueva base de datos. Los registros no pueden combinarse desde ambas bases de datos al consultarlos. La primera entrada del registro en la nueva base de datos de registros de configuración indica que se ha producido un cambio en la base de datos, pero no identifica la base de datos anterior.

## Mostrar el contenido de los registros de configuración

Cuando se inician cambios de configuración y actividades de tipo administrativo, las operaciones de alto nivel creadas con Studio y Director se muestran en el panel central superior de Studio. Una operación de alto nivel tiene como resultado la llamada a uno o varios servicios y SDK, que son operaciones de bajo nivel. Cuando se selecciona una operación de alto nivel en el panel superior, el panel inferior muestra las operaciones de bajo nivel.

Si la operación falla antes de completarse, la operación de registro puede no completarse en la base de datos. Por ejemplo, puede que una entrada inicial no tenga una entrada final. En estos casos, el registro indica que hay información que falta. Cuando se muestran registros correspondientes a intervalos de tiempo, los registros incompletos se muestran si los datos cumplen los requisitos. Por ejemplo, si se solicitan todos los registros de los últimos cinco días y hay un registro con una hora de inicio dentro de esos cinco días, pero no tiene hora de fin, será incluido de todos modos.

Cuando se utiliza un script que llama a los cmdlets de PowerShell, si se crea una operación de bajo nivel sin especificar su correspondiente operación de alto nivel, el servicio de registros de configuración (Configuration Logging) creará una operación de alto nivel suplente.

Para ver el contenido de los registros de configuración, seleccione **Registros** en el panel de navegación de Studio. De forma predeterminada, el panel central muestra el contenido de las entradas de los registros por orden cronológico (primero las entradas más recientes), separadas por su fecha. Puede hacer lo siguiente:

- Ordenar los elementos en pantalla por el encabezado de la columna.
- Filtrar los elementos en pantalla mediante un intervalo de un día o texto en el cuadro **Buscar**. Para volver a la versión estándar de la presentación de los registros, borre el texto del cuadro **Buscar**.

## Generar informes

Puede generar informes CSV y HTML que contengan los datos de los registros de configuración.

- El informe CSV es un volcado de todos los datos de registros correspondientes a un intervalo de tiempo específico. Los datos jerárquicos en la base de datos se vuelcan sin estructura en

una sola tabla CSV. Ningún aspecto de los datos tiene prioridad en la tabla. No se utiliza ningún tipo de formato y no se supone ningún tipo de legibilidad humana. El archivo (denominado MyReport) contiene datos en formato universalmente consumible. Los archivos CSV se usan a menudo para archivos históricos o como fuentes de datos para alguna herramienta de gestión de datos o de creación de informes como Microsoft Excel.

- El informe HTML presenta los datos de registros correspondientes a un intervalo de tiempo, en un formato legible para las personas. Proporciona una vista estructurada y explorable donde se pueden consultar los cambios. Un informe HTML consta de dos archivos, llamados Resumen y Detalles. El archivo de Resumen consiste en una lista de las operaciones de alto nivel: cuándo ocurrió cada operación, quién la realizó y el resultado de esta. Cuando se hace clic en el enlace Detalles junto a cada operación, se abre el archivo de Detalles con las operaciones de bajo nivel asociadas, que ofrecen información adicional sobre la operación.

Para generar un informe de registros de configuración, seleccione **Registros** en el panel de navegación de Studio y, a continuación, seleccione **Crear informe personalizado** en el panel Acciones.

- Seleccione el intervalo de fechas del informe.
- Seleccione el formato del informe: CSV, HTML o ambos.
- Busque la ubicación donde quiere guardar el informe.

## Eliminar contenido de los registros de configuración

Para eliminar el registro de configuración, debe tener ciertos permisos de Administración delegada y permisos para la base de datos de SQL Server.

- **Administración delegada:** Debe tener un rol de administración delegada que le permita leer la configuración de la implementación. El rol Administrador total tiene ese permiso. Si se trata de un rol personalizado, éste debe tener seleccionados Solo lectura o Administrar en la categoría Otros permisos.

Para crear una copia de seguridad de los datos de registros de configuración antes de eliminarlos, el rol personalizado también debe tener seleccionados Solo lectura o Administrar en la categoría de Permisos para registros.

- **Base de datos SQL Server:** Debe tener unas credenciales de inicio de sesión de SQL Server con permiso para eliminar registros de la base de datos. Hay dos formas de hacerlo:
  - Usar unas credenciales para la base de datos SQL Server con un rol sysadmin de servidor, que permite realizar cualquier actividad en el servidor de la base de datos. De forma alternativa, los roles serveradmin o setupadmin de servidor permiten realizar operaciones de eliminación.

- Si la implementación requiere seguridad adicional, use unas credenciales de base de datos que no sean de sysadmin asignadas a un usuario de la base de datos que tenga permisos para eliminar registros de esta.
  1. En SQL Server Management Studio, cree unas credenciales de inicio de sesión de SQL Server con un rol de servidor que no sea 'sysadmin'.
  2. Asigne esas credenciales de inicio de sesión a un usuario de la base de datos. SQL Server crea automáticamente un usuario en la base de datos con el mismo nombre que esas credenciales.
  3. En Pertenencia al rol de la base de datos, especifique al menos uno de los miembros de rol para el usuario de la base de datos: ConfigurationLoggingSchema\_ROLE o dbowner.

Para obtener información adicional, consulte la documentación sobre SQL Server Management Studio.

Para eliminar los registros de configuración:

1. Seleccione **Registros** en el panel de navegación de Studio.
2. Seleccione **Eliminar registros** en el panel Acciones.
3. Verá la opción para crear una copia de seguridad de los registros antes de eliminarlos. Si decide crear una copia de seguridad, vaya a la ubicación donde se guarda la copia archivada. La copia de seguridad se crea como un archivo CSV.

Una vez eliminados los registros de configuración, la eliminación de los registros es la primera actividad que se anotará en el nuevo registro vacío. Esa entrada proporciona información acerca de quién y cuándo eliminó los registros.

## Registros de eventos

March 31, 2021

Los siguientes artículos contienen listas y descripciones de los eventos que registran los servicios de Citrix Virtual Apps and Desktops.

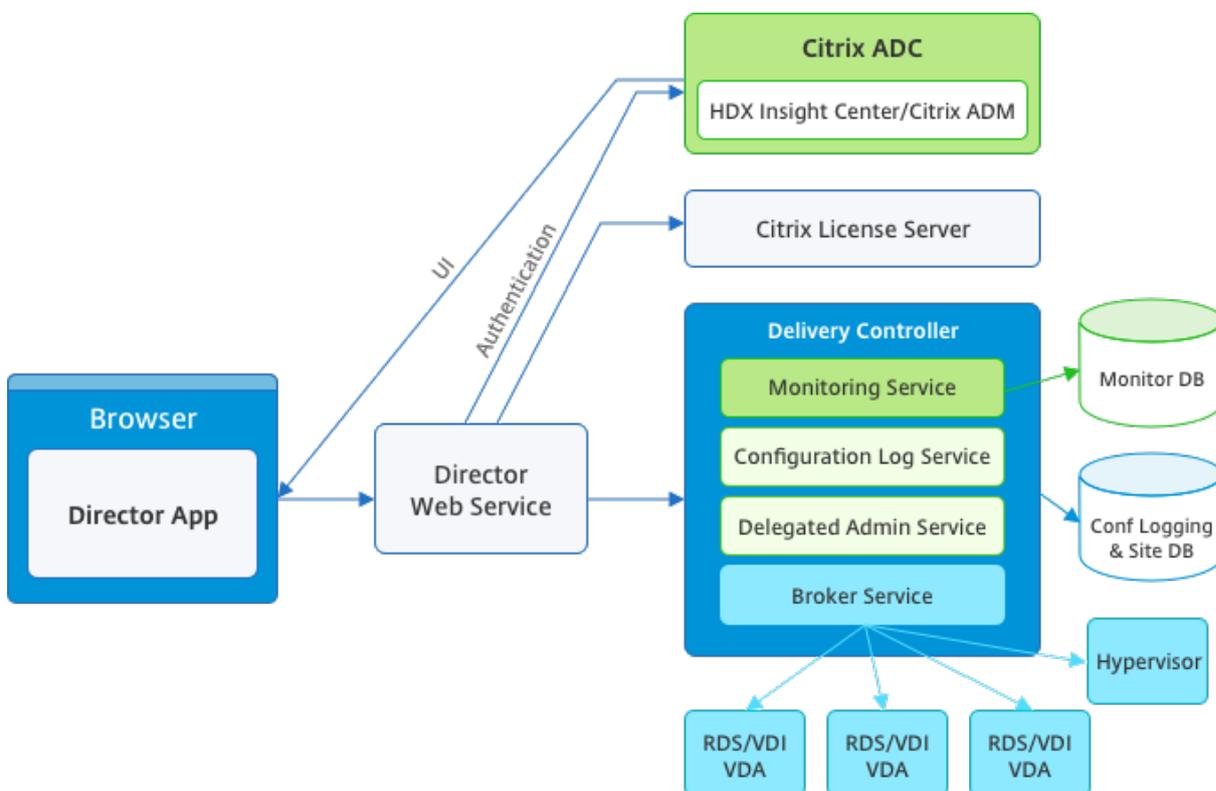
Esta información es general. Debe consultar los artículos de las funciones concretas para obtener más información sobre los eventos.

- [Eventos de Citrix Broker Service](#)
- [Eventos del Citrix FMA Service SDK](#)
- [Eventos de Citrix Configuration Service](#)
- [Eventos de Citrix Delegated Administration Service](#)

## Director

May 24, 2024

Director es una consola para supervisar y solucionar problemas de Citrix Virtual Apps and Desktops.



Director puede acceder a:

- Datos en tiempo real de Broker Agent, mediante una consola unificada integrada con las funciones de Analytics, Performance Manager y Network Inspector.
  - Las funciones de Analytics incluyen la administración de rendimiento para garantizar el estado y la capacidad de la implementación y el análisis de red y tendencias históricas, con tecnología de Citrix ADM, con el fin de identificar posibles cuellos de botella debido a problemas de red en el entorno de Citrix Virtual Apps and Desktops.
- Datos históricos almacenados en la base de datos de Supervisar para acceder a la base de datos de registros de configuración.
- Datos ICA de Citrix Gateway mediante Citrix ADM.
  - Consiga visibilidad de la experiencia que tiene el usuario final en aplicaciones y escritorios virtuales y usuarios de Citrix Virtual Apps o Desktops.
  - Correlacione datos de red con datos de aplicaciones y métricas en tiempo real para solucionar problemas más eficazmente.

- Integre la herramienta de supervisión de Director de Citrix Virtual Desktop 7.

Director utiliza un panel de mandos de solución de problemas que permite una supervisión histórica y en tiempo real del estado del sitio de Citrix Virtual Apps o Desktops. Esta función permite ver los fallos en tiempo real, lo que proporciona una mejor idea de la experiencia del usuario final.

Para obtener más información acerca de la compatibilidad de las funciones de Director con Delivery Controller (DC), VDA y cualquier otro componente dependiente, consulte [Tabla de compatibilidad de funciones](#).

Nota:

Con la divulgación sobre las vulnerabilidades del canal lateral de ejecución especulativa Meltdown y Spectre, Citrix recomienda que instale las revisiones de mitigación relevantes. Tenga en cuenta que esas revisiones pueden afectar al rendimiento de SQL Server. Para obtener más información, consulte el artículo de asistencia de Microsoft: [Protect SQL Server from attacks on Spectre and Meltdown side-channel vulnerabilities](#). Citrix recomienda probar la escalabilidad y planificar las cargas de trabajo antes de implementar esas revisiones en sus entornos de producción.

Director se instala de forma predeterminada como un sitio web en el Delivery Controller. Para obtener información sobre requisitos previos y otros datos, consulte la documentación de [Requisitos del sistema](#) para esta versión. Para obtener información específica sobre la instalación y la configuración de Director, consulte [Instalar y configurar Director](#).

## Iniciar sesión en Director

El sitio web de Director está ubicado en `https` o `http://<Server FQDN>/Director`.

Si uno de los sitios en la implementación de varios sitios está inactivo, el inicio de sesión de Director tarda un poco más porque intenta conectarse con el sitio que está inactivo.

## Usar Director con la autenticación con tarjetas inteligentes PIV

Ahora Director admite la autenticación con tarjetas inteligentes basadas en PIV (Personal Identity Verification) para iniciar sesión. Esta función es útil para organizaciones y agencias gubernamentales que usan la autenticación basada en tarjetas inteligentes para controlar el acceso.

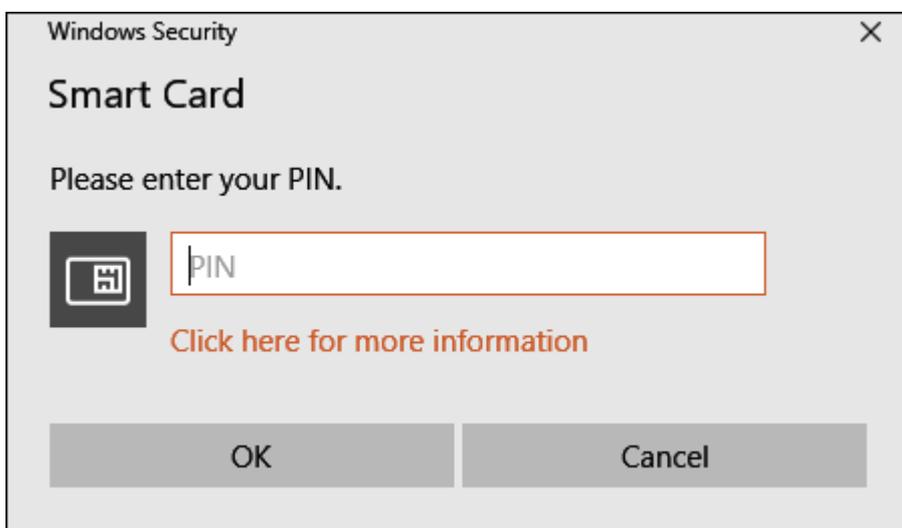
La autenticación con tarjeta inteligente requiere una configuración específica en el servidor de Director y en Active Directory. Los pasos de configuración se detallan en [Configurar la autenticación con tarjeta inteligente PIV](#).

Nota:

La autenticación con tarjetas inteligentes solo se admite para usuarios del mismo dominio de Active Directory.

Después de realizar la configuración requerida, puede iniciar sesión en Director mediante una tarjeta inteligente:

1. Inserte su tarjeta inteligente en el lector de tarjetas inteligentes.
2. Abra un explorador web y vaya a la URL de Director, <https://<directorfqdn>/Director>.
3. Seleccione un certificado de usuario válido de la lista que se muestra.
4. Escriba su token de tarjeta inteligente.



5. Después de autenticarse, puede acceder a Director sin tener que suministrar credenciales adicionales en la página de inicio de sesión de Director.

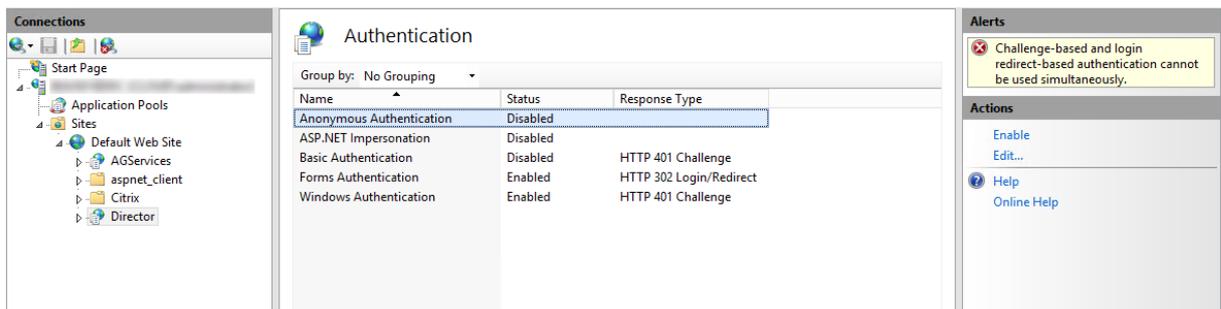
## Usar Director con la autenticación integrada de Windows

Con la autenticación de Windows integrada (IWA), los usuarios unidos a un dominio obtienen acceso directo a Director sin tener que volver a escribir sus credenciales en la página de inicio de sesión de Director. A continuación, se presentan los requisitos previos para utilizar Director y la autenticación integrada de Windows:

- Habilite la autenticación de Windows integrada en el sitio web de IIS que aloja Director. Al instalar Director, se habilitan formularios de autenticación anónima. Para combinar Director con

la autenticación integrada de Windows, inhabilite la autenticación anónima y habilite la autenticación de Windows. Los formularios de autenticación deben permanecer establecidos en Habilitados para la autenticación de usuarios sin dominio.

1. Inicie el Administrador de IIS.
2. Vaya a **Sitios > Sitio web predeterminado > Director**.
3. Seleccione **Autenticación**.
4. Haga clic con el botón secundario en **Autenticación anónima** y seleccione **Inhabilitar**.
5. Haga clic con el botón secundario en **Autenticación de Windows** y seleccione **Habilitar**.



- Configure el permiso de delegación de Active Directory para la máquina de Director. Esto solo es necesario si Director y el Delivery Controller están instalados en máquinas independientes.
  1. En la máquina de Active Directory, abra la consola de administración de Active Directory.
  2. Una vez abierta la consola de administración de Active Directory, vaya a **Nombre de dominio > Equipos**. Seleccione la máquina de Director.
  3. Haga clic con el botón secundario y seleccione **Propiedades**.
  4. En Propiedades, seleccione la ficha **Delegación**.
  5. Seleccione la opción **Confiar en este equipo para delegar en cualquier servicio (solo Kerberos)**.
- El explorador web que se utilice para acceder a Director debe admitir la autenticación de Windows integrada. Esto puede requerir pasos de configuración adicionales en Firefox y Chrome. Para obtener más información, consulte la documentación del explorador.
- El servicio Monitoring Service debe ejecutar Microsoft .NET Framework 4.5.1 o una versión posterior admitida que conste en los Requisitos del sistema para Director. Para obtener más información, consulte [Requisitos del sistema](#).

En Director, si un usuario cierra sesión o se agota el tiempo de espera de esa sesión, aparece la página de inicio de sesión. Desde la página de inicio de sesión, el usuario puede establecer el tipo de autenticación en **Inicio de sesión automático** o **Credenciales del usuario**.

## Vistas de interfaz

Director proporciona diferentes vistas de la interfaz que se adaptan a administradores específicos. Los permisos del producto definen lo que se muestra y los comandos disponibles.

Por ejemplo: los administradores de asistencia técnica ven una interfaz adaptada a las tareas de asistencia técnica. Director permite a los administradores de asistencia técnica buscar al usuario que informa de un problema y muestra las actividades asociadas al usuario, tales como el estado de las aplicaciones y los procesos de ese usuario. Pueden resolver problemas rápidamente al realizar acciones como finalizar una aplicación o un proceso que no responden, las operaciones de remedo en la máquina del usuario, reiniciar la máquina o restablecer el perfil de usuario.

En cambio, los administradores totales pueden ver y administrar todo el sitio, y pueden ejecutar comandos para varios usuarios y máquinas. El panel de mandos ofrece información general de los aspectos clave de la implementación, tales como el estado de las sesiones, los inicios de sesión de los usuarios y la infraestructura del sitio. La información se actualiza cada minuto. En caso de problemas, aparecen automáticamente los detalles sobre la cantidad y el tipo de fallos que se han producido.

Para obtener más información sobre los diversos roles y sus permisos en Director, consulte [Administración delegada y Director](#)

## Recopilación de datos de uso por parte de Google Analytics

Después de instalar Director, el servicio de Director usa Google Analytics para recopilar datos de uso anónimos. Se recopilan estadísticas e información sobre el uso de las páginas “Tendencias” y los análisis sobre las llamadas de la API de OData. La recopilación de datos de análisis cumple con la [directiva de privacidad de Citrix](#). La recopilación de datos se habilita de forma predeterminada cuando se instala Director.

Para dejar de participar en la recopilación de datos de Google Analytics, modifique la clave de Registro como se describe a continuación en la máquina donde está instalado Director. Si la clave de Registro aún no existe, créela y establézcala en el valor pertinente. Actualice la instancia de Director después de cambiar el valor de la clave de Registro.

**Precaución:** El uso incorrecto del Editor del Registro puede causar problemas graves que pueden requerir la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si usa el Editor del Registro, será bajo su propia responsabilidad. Citrix recomienda hacer una copia de seguridad del Registro de Windows antes de modificarlo.

Ubicación: HKEY\_LOCAL\_MACHINE\Software\Citrix\Director

Nombre: DisableGoogleAnalytics

Valor: 0 = habilitado (de forma predeterminada), 1 = inhabilitado

Puede usar el siguiente cmdlet de PowerShell para inhabilitar la recopilación de datos por parte de Google Analytics:

```
1 New-Item HKLM:\SOFTWARE\Citrix -Name Director
2 New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name
   DisableGoogleAnalytics -PropertyType DWORD -Value 1
```

## Guía de nuevas funciones

Director cuenta con una guía de producto que usa [Pendo](#) para ofrecer información sobre las nuevas funciones publicadas en la versión actual de Director. El breve resumen y los correspondientes mensajes en el producto le ayudan a comprender las novedades del producto.

Para dejar de participar en esta función, modifique la clave de Registro como se describe a continuación en la máquina donde está instalado Director. Si la clave de Registro aún no existe, créela y establézcala en el valor pertinente. Actualice la instancia de Director después de cambiar el valor de la clave de Registro.

**Precaución:** El uso incorrecto del Editor del Registro puede causar problemas graves que pueden requerir la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si usa el Editor del Registro, será bajo su propia responsabilidad. Citrix recomienda hacer una copia de seguridad del Registro de Windows antes de modificarlo.

Ubicación: HKEY\_LOCAL\_MACHINE\Software\Citrix\Director

Nombre: DisableGuidedHelp

Valor: 0 = habilitado (de forma predeterminada), 1 = inhabilitado

Puede usar el siguiente cmdlet de PowerShell para inhabilitar la guía incluida en el producto:

```
1 New-Item HKLM:\SOFTWARE\Citrix -Name Director
2 New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name DisableGuidedHelp
   -PropertyType DWORD -Value 1
```

## Instalación y configuración

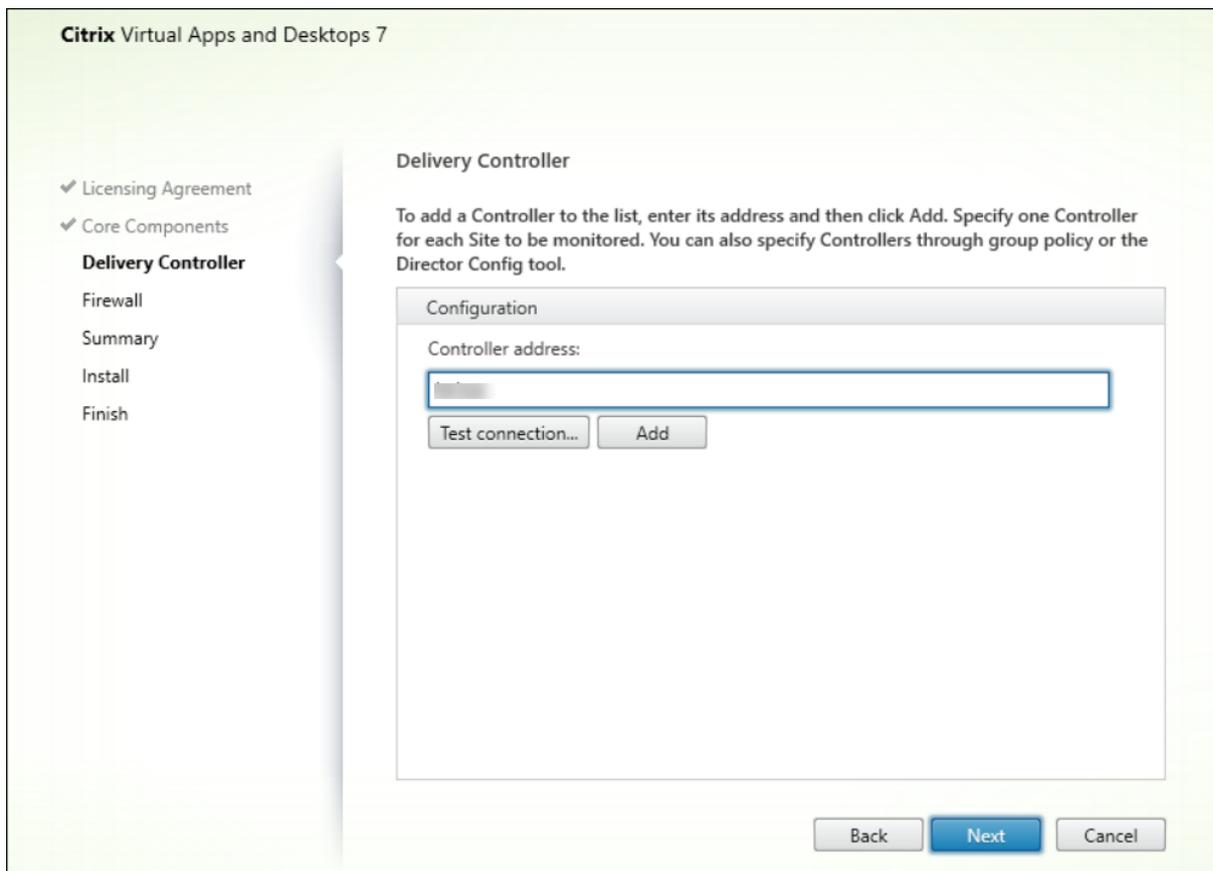
March 10, 2022

## Instalar Director

Instale Director desde la ISO del instalador de producto completo de Citrix Virtual Apps and Desktops, que verifica los requisitos previos, instala los componentes que faltan, configura el sitio web de Director y realiza la configuración básica. Para obtener información sobre requisitos previos y otros datos, consulte la documentación de [Requisitos del sistema](#) para esta versión. Esta versión de Director no es compatible ni con las implementaciones de Virtual Apps anteriores a 6.5 ni con las implementaciones de Virtual Desktops anteriores a la versión 7.

La configuración predeterminada que ofrece el instalador de la ISO administra implementaciones habituales. Si Director no se incluyó durante la instalación, use la ISO del instalador para agregarlo. Para agregar componentes adicionales, vuelva a ejecutar la ISO del instalador y seleccione los componentes a instalar. Para obtener información acerca del uso del instalador ISO, consulte [Instalar componentes principales](#) en la documentación de instalación. Citrix recomienda la instalación mediante la ISO del instalador del producto completo, no el archivo MSI.

Cuando Director se instala en el Controller, se configura automáticamente con localhost como la dirección del servidor, y Director se comunica con el Controller local de forma predeterminada. Para instalar Director en un servidor dedicado que es remoto desde un Controller, se le solicitará que introduzca el FQDN o la dirección IP de un Controller.



**Nota:**

Haga clic en **Agregar** para agregar el Controller que quiera supervisar.

Director se comunica con el Controller especificado de forma predeterminada. Especifique la dirección de un solo Controller para cada sitio que quiera supervisar. Director detecta automáticamente todos los demás Controllers en el mismo sitio y opta por utilizar los demás Controllers si en el Controller especificado se produce un error.

**Nota:**

Director no equilibra la carga entre los Controllers.

Para proteger la comunicación entre el explorador y el servidor web, Citrix recomienda implementar TLS en el sitio web de IIS que aloja Director. Consulte la documentación de Microsoft IIS para obtener instrucciones. No se requiere ninguna configuración de Director para habilitar TLS.

## Implementar y configurar Director

Cuando Director se usa en un entorno que contiene más de un sitio, se deben sincronizar los relojes del sistema en todos los servidores donde estén instalados los Controllers, Director y otros componentes principales. De lo contrario, los sitios podrían no mostrarse correctamente en Director.

Importante:

Para proteger los nombres de usuario y las contraseñas enviados como texto sin formato a través de la red, Citrix recomienda permitir las conexiones de Director solo con HTTPS (no con HTTP). Algunas herramientas pueden leer nombres y contraseñas de texto sin formato en paquetes de red HTTP (sin cifrar), lo que puede crear un riesgo de seguridad para los usuarios.

## Configurar permisos

Para iniciar sesión en Director, los administradores con permisos para Director deben ser usuarios del dominio de Active Directory y deben contar con los siguientes derechos:

- Derechos de lectura en todos los bosques de AD en los que se realizarán búsquedas (consulte [Configuración avanzada](#)).
- Roles configurados de administrador delegado (consulte [Administración delegada y Director](#)).
- Para remedar usuarios, los administradores deben configurarse mediante una directiva de grupo de Microsoft para la Asistencia remota de Windows. Además:
  - Durante la instalación de VDA, compruebe que la función Asistencia remota de Windows está habilitada en todos los dispositivos de usuario (seleccionada de forma predeterminada).

- Al instalar Director en un servidor, asegúrese de que la Asistencia remota de Windows está instalada (seleccionada de forma predeterminada). Sin embargo, en el servidor está inhabilitada de forma predeterminada. La función no necesita estar habilitada para que Director proporcione asistencia a los usuarios finales. Citrix recomienda dejar la función inhabilitada para mejorar la seguridad en el servidor.
- Para permitir que otros usuarios inicien la Asistencia remota de Windows, debe concederles los permisos requeridos desde las configuraciones de directiva de grupo de Microsoft adecuadas para la Asistencia remota. Para obtener más información, consulte [CTX127388: How to Enable Remote Assistance for Desktop Director](#).

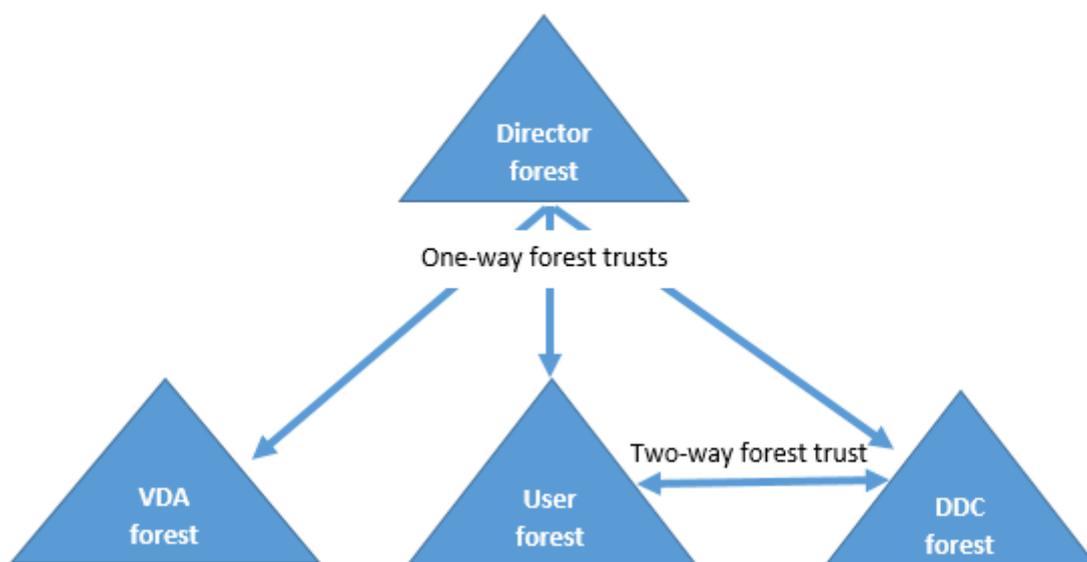
## Configuración avanzada

March 10, 2022

Director puede trabajar con entornos que abarcan varios bosques en que usuarios, Delivery Controllers, agentes VDA y Directores se encuentran en bosques distintos. Esto requiere una configuración adecuada de las relaciones de confianza entre los bosques y los parámetros de configuración.

### Configuración recomendada para un entorno multibosque

La configuración recomendada requiere crear relaciones de confianza entrantes y salientes entre bosques con una autenticación que sirva para todo el dominio.



La relación de confianza desde Director permite solucionar problemas en sesiones de usuario, agentes VDA y Delivery Controllers ubicados en varios bosques.

La configuración avanzada necesaria para que Director admita varios bosques se controla a través de parámetros definidos en el Administrador de Internet Information Services (IIS).

**Importante:**

Cuando cambie un parámetro en IIS, el servicio de Director se reiniciará automáticamente y cerrará las sesiones de los usuarios.

Para configurar parámetros avanzados mediante IIS:

1. Abra la consola del Administrador de Internet Information Services (IIS).
2. Vaya al sitio web de Director en el sitio web predeterminado.
3. Haga doble clic en **Configuración de aplicaciones**.
4. Haga doble clic en un parámetro para modificarlo.
5. Haga clic en **Agregar** para agregar un parámetro nuevo.

Director utiliza Active Directory para buscar usuarios y para consultar información adicional sobre usuarios y máquinas. De forma predeterminada, Director busca el dominio o el bosque en el que:

- La cuenta del administrador es miembro.
- El servidor web de Director es miembro (en caso de que sea diferente).

Director intenta realizar búsquedas en el nivel del bosque mediante el catálogo global de Active Directory. Si no tiene permisos para realizar búsquedas en los bosques, la búsqueda se realiza en el dominio solamente.

Para buscar datos en otros dominios o bosques de Active Directory, debe establecer explícitamente los dominios o bosques en los que realizar las búsquedas. Configure este parámetro Aplicaciones para el sitio web de Director en el Administrador de IIS:

```
1 Connector.ActiveDirectory.Domains = (user),(server)
```

Los atributos de valor user y server representan los dominios del usuario de Director (el administrador) y el servidor de Director respectivamente.

Para habilitar búsquedas desde un dominio o bosque adicionales, agregue el nombre del dominio a la lista, tal y como se muestra en el ejemplo:

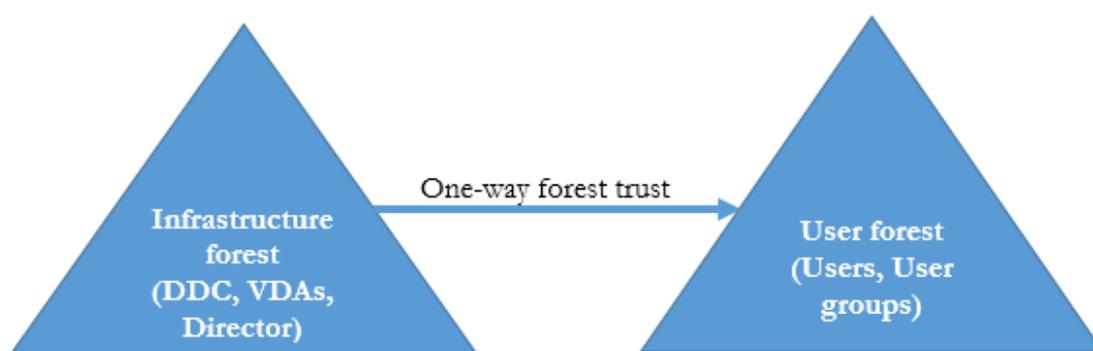
```
1 Connector.ActiveDirectory.Domains = (user),(server),\<domain1\>,\<domain2\>
```

Para cada dominio de la lista, Director intenta realizar búsquedas en el nivel del bosque. Si no tiene permisos para realizar búsquedas en los bosques, la búsqueda se realiza en el dominio solamente.

## Configuración de grupos locales de dominio

La mayoría de los proveedores de servicios Citrix (Citrix Service Providers) tienen configuraciones similares de entornos, compuestos de agentes VDA, Delivery Controllers y Director en lo que se llama el “bosque de infraestructura”, mientras que los registros de usuarios o grupos pertenecen al “bosque del cliente”. Existe una relación de confianza saliente unidireccional que se extiende desde el bosque de infraestructura al bosque del cliente.

Por regla general, los administradores CSP crean un grupo local de dominio en el bosque de infraestructura, y agregan a los usuarios o los grupos de usuarios que haya en el bosque del cliente a este grupo local de dominio.



Director puede emplear configuraciones multibosque como esta, y supervisa las sesiones de los usuarios configurados mediante grupos locales de dominio.

1. Configure estos parámetros Aplicaciones para el sitio web de Director en el Administrador de IIS:

```
1 Connector.ActiveDirectory.DomainLocalGroupSearch= true Connector.  
ActiveDirectory  
2  
3 DomainLocalGroupSearchDomains= \<domain1\>,\<domain2\>
```

Donde <domain1><domain2> son los nombres de los bosques donde reside el grupo local de dominio.

2. Asigne el grupo local de dominio a los grupos de entrega en Citrix Studio.
3. Reinicie IIS y vuelva a iniciar sesión en Director para que los cambios surtan efecto. Ahora, Director puede supervisar y mostrar las sesiones de estos usuarios.

## Agregar sitios a Director

Si Director ya está instalado, configúrelo para que funcione con varios sitios. Para ello, utilice la consola del Administrador de IIS en cada servidor de Director para actualizar la lista de direcciones de

servidor en la configuración de la aplicación.

Agregue la dirección de un Controller de cada sitio al siguiente parámetro:

```
1 Service.AutoDiscoveryAddresses = SiteAController,SiteBController
2 <!--NeedCopy-->
```

donde SiteAController y SiteBController son las direcciones de los Delivery Controllers de dos sitios diferentes.

## Inhabilitar la visibilidad de las aplicaciones en ejecución en el Administrador de actividades

De forma predeterminada, el Administrador de actividades de Director muestra una lista de todas las aplicaciones que haya en ejecución en la sesión del usuario. Esta información pueden verla todos los administradores que tengan acceso a la función del Administrador de actividades de Director. Para los roles de administrador delegado, esto incluye los roles de administrador total, administrador de grupos de entrega y administrador de asistencia técnica.

Para proteger la privacidad de los usuarios y las aplicaciones que estos ejecutan, puede configurar que la ficha Aplicaciones no muestre las aplicaciones en ejecución.

### Advertencia:

Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

1. En el VDA, modifique la clave de Registro ubicada en HKEY\_LOCAL\_MACHINE\Software\Citrix\Director\TaskM. De forma predeterminada, el valor de la clave es 1. Cambie el valor a 0 para que la información no se recopile del VDA y, por tanto, no se muestre en el Administrador de actividades.
2. En el servidor que tiene Director instalado, modifique el parámetro que controla la visibilidad de las aplicaciones en ejecución. De forma predeterminada, el valor es true, lo que permite la visibilidad de las aplicaciones en ejecución en la ficha Aplicaciones. Cambie el valor a false, lo que inhabilita la visibilidad. Esta opción solo afecta al Administrador de actividades de Director, no al VDA.

Modifique el valor del parámetro siguiente:

```
UI.TaskManager.EnableApplications = false
```

### Importante:

Para inhabilitar la vista de las aplicaciones en ejecución, Citrix recomienda realizar ambos cam-

bios para que los datos no se muestren en el Administrador de actividades.

## Configurar la autenticación con tarjetas inteligentes PIV

November 4, 2021

Este artículo contiene la configuración requerida en el servidor de Director y en Active Directory para habilitar la función de la autenticación con tarjetas inteligentes.

Nota:

La autenticación con tarjetas inteligentes solo se admite para usuarios del mismo dominio de Active Directory.

### Configurar el servidor de Director

Realice los siguientes pasos de configuración en el servidor de Director:

1. Instale y active la Autenticación de asignaciones de certificado de cliente. Siga las instrucciones indicadas en **Client Certificate Mapping authentication using Active Directory**, en el documento [Client Certificate Mapping Authentication](#) de Microsoft.

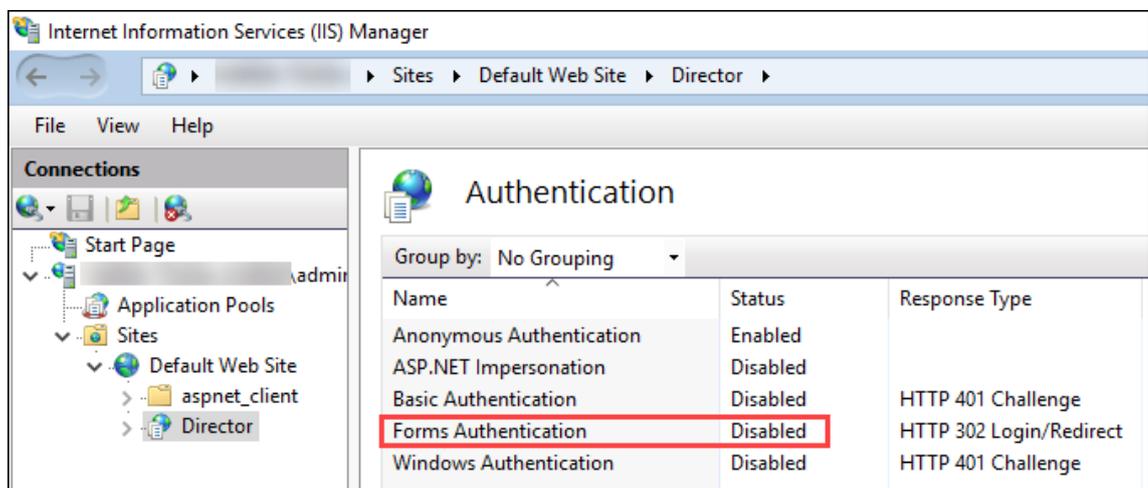
2. Inhabilite la autenticación mediante formularios en el sitio de Director.

Inicie el Administrador de IIS.

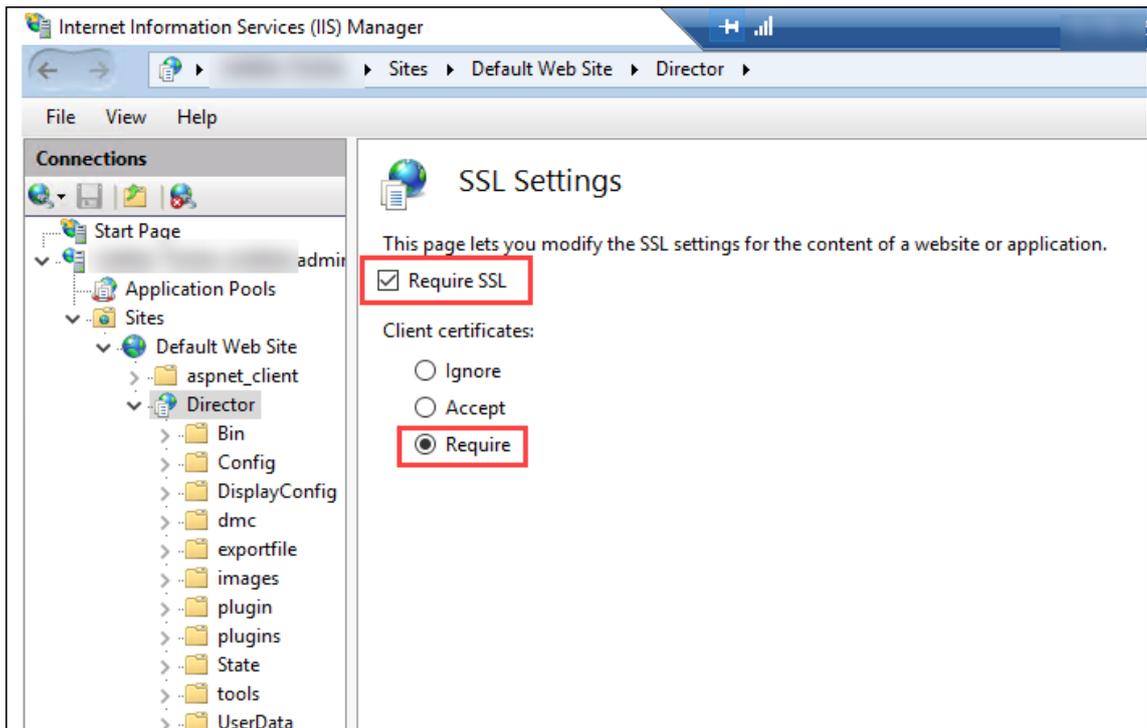
Vaya a **Sitios > Sitio web predeterminado > Director**.

Seleccione **Autenticación**.

Haga clic con el botón secundario en **Autenticación mediante formularios** y seleccione **Deshabilitar**.



3. Configure la URL de Director para el protocolo HTTPS (más seguro que HTTP) para la autenticación de certificados de cliente.
  - a) Inicie el Administrador de IIS.
  - b) Vaya a **Sitios > Sitio web predeterminado > Director**.
  - c) Seleccione **Configuración de SSL**.
  - d) Seleccione **Requerir SSL y Certificados de cliente > Requerir**.



4. Actualice web.config. Abra el archivo web.config (disponible en c:\inetpub\wwwroot\Director) mediante un editor de texto.

Debajo del elemento principal `<system.webServer>`, agregue el siguiente fragmento como primer elemento secundario:

```
1 <defaultDocument>
2   <files>
3     <add value="LogOn.aspx"/>
4   </files>
5 </defaultDocument>
```

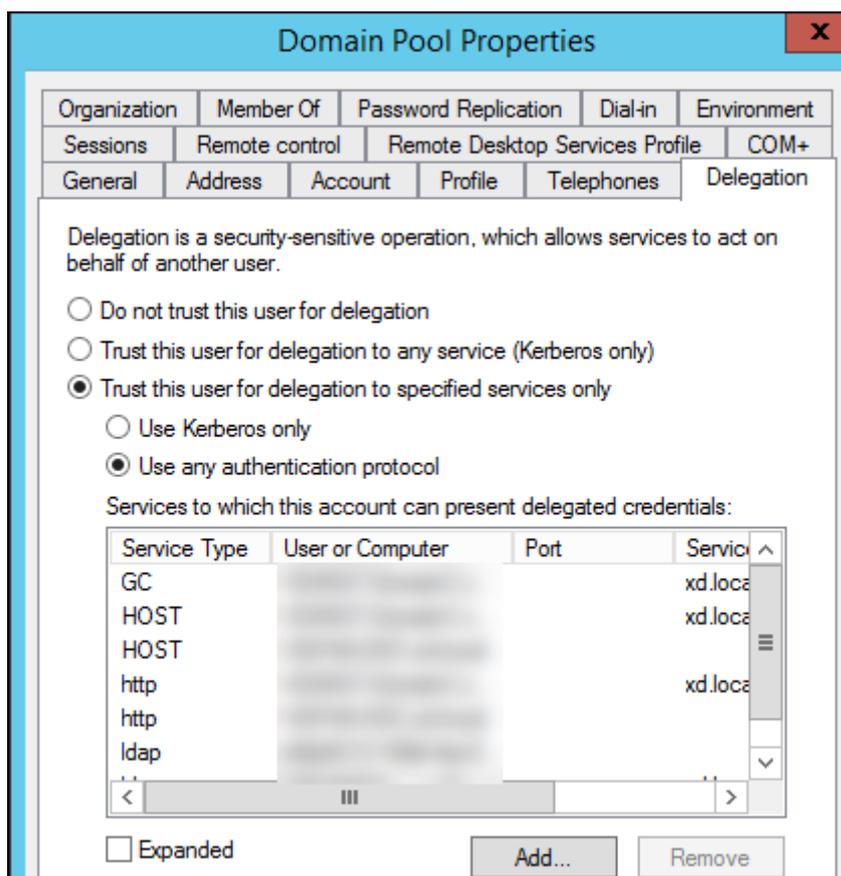
## Configurar Active Directory

De forma predeterminada, la aplicación Director se ejecuta con la propiedad de identidad **Grupo de aplicaciones**. La autenticación con tarjetas inteligentes requiere una delegación para la cual la iden-

tividad de la aplicación Director debe tener los privilegios “Base de computación de confianza”(TCB) en el host del servicio.

Citrix recomienda que cree una cuenta de servicio independiente para la identidad del grupo de aplicaciones. Cree la cuenta de servicio y asigne los privilegios TCB siguiendo las instrucciones del artículo [Protocol Transition with Constrained Delegation Technical Supplement](#) de Microsoft.

Asigne la cuenta de servicio recién creada al grupo de aplicaciones de Director. La siguiente imagen muestra el cuadro de diálogo de propiedades de una cuenta de servicio de ejemplo, Domain Pool.



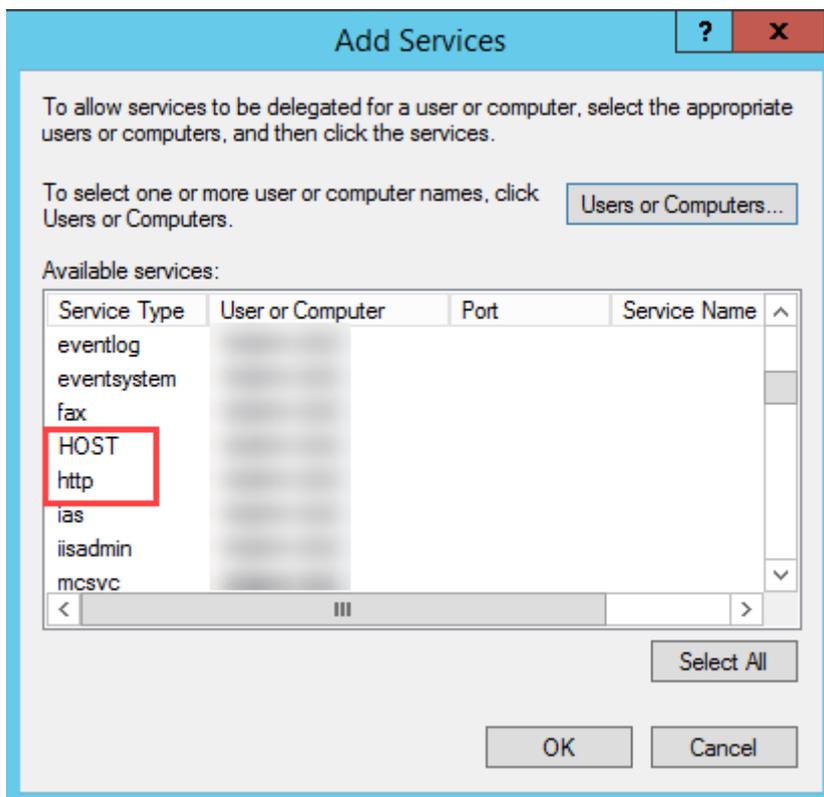
Configure los siguientes servicios para esta cuenta:

- Delivery Controller: HOST, http
- Director: HOST, http
- Active Directory: GC, LDAP

Para ello:

1. En el cuadro de diálogo de propiedades de la cuenta de usuario, haga clic en **Agregar**.
2. En el diálogo **Agregar servicios**, haga clic en “Usuarios o equipos”.
3. Seleccione el nombre de host del Delivery Controller.

4. En la lista **Servicios disponibles**, seleccione “HOST” y “http” en **Tipo de servicio**.



De forma similar, agregue “Tipos de servicio” para los hosts de **Director** y **Active Directory**.

## Configurar el explorador Firefox

Para usar el explorador Firefox, instale el controlador PIV disponible en [OpenSC 0.17.0](#). Para obtener instrucciones de instalación y configuración, consulte [Installing OpenSC PKCS#11 Module in Firefox, Step by Step](#).

Para obtener información sobre el uso de la función de autenticación basada en tarjetas inteligentes en Director, consulte el apartado [Usar Director con la autenticación por tarjeta inteligente basada en PIV](#) en el artículo “Director”.

## Configurar el análisis de red

March 4, 2024

### Nota:

La disponibilidad de esta función depende de la licencia de su organización y sus permisos de

administrador.

Director se integra en Citrix ADM para ofrecer análisis de la red y administración del rendimiento:

- El análisis de red utiliza informes de HDX Insight desde Citrix ADM para proporcionar una visión en contexto de los escritorios y las aplicaciones en la red. Con esta función, Director ofrece análisis avanzados del tráfico ICA en la implementación.
- La función de administración del rendimiento (Performance Management) proporciona la retención del historial y los informes de tendencias. Con la retención del historial de datos frente a la evaluación en tiempo real, puede crear informes de tendencias que incluyen las tendencias de capacidad y estado.

Después de habilitar esta función en Director, los informes de HDX Insight le proporcionan información adicional:

- La ficha Red en la página Tendencias muestra los efectos de la latencia y el ancho de banda para las aplicaciones, los escritorios y los usuarios de toda la implementación.
- La página Detalles del usuario muestra la información de latencia y ancho de banda específica de la sesión de un usuario en particular.

#### **Limitaciones:**

- En la vista Tendencias, los datos de inicio de sesión de conexiones HDX no se recopilan para los VDA anteriores a 7. Para los VDA anteriores, los datos gráficos se muestran como 0.

Para habilitar el análisis de red, debe instalar y configurar Citrix ADM en Director. Director requiere Citrix ADM 11.1 compilación 49.16 o posterior. MAS es un dispositivo virtual que se ejecuta en un servidor de Citrix XenServer. Con el análisis de red, Director se comunica con la implementación y recopila la información relacionada con ella.

Para obtener más información, consulte la documentación de [Citrix ADM](#).

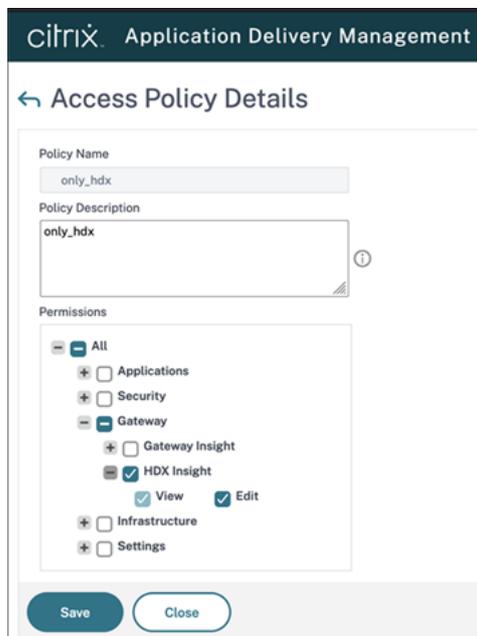
#### **Nota:**

Citrix NetScaler Insight Center ha alcanzado la fecha de su ciclo Fin de Mantenimiento el 15 de mayo de 2018. Consulte [Tabla de productos Citrix](#). Integre Director en Citrix ADM para el análisis de red. Para migrar NetScaler Insight Center a Citrix ADM, consulte [Migrar desde NetScaler Insight Center a Citrix ADM](#).

1. En el servidor donde está instalado Director, localice la herramienta de línea de comandos DirectorConfig en C:\inetpub\wwwroot\Director\tools y ejecútela con el parámetro /confignetscaler desde un símbolo del sistema.
2. Cuando se le solicite, introduzca el nombre de la máquina de Citrix ADM (el nombre de dominio completo o la dirección IP), el nombre de usuario, la contraseña, el tipo de conexión (se prefiere el tipo HTTPS al HTTP) y elija la integración en Citrix ADM.
3. Para comprobar los cambios, cierre la sesión y vuelva a iniciarla.

**Nota:**

Por motivos de seguridad, se recomienda crear un rol personalizado para la integración de ADM en Director con el permiso suficiente para acceder únicamente a HDX Insight.



Para obtener más información, consulte [Configurar directivas de acceso](#).

## Administración delegada y Director

September 22, 2021

La administración delegada utiliza tres conceptos: los administradores, los roles y los ámbitos. Los permisos se basan en un rol de administrador y en el ámbito de este rol. Por ejemplo, a un administrador se le puede asignar un rol de administrador de asistencia técnica en el que el ámbito implica la responsabilidad de usuarios finales en un único sitio.

Para obtener información sobre cómo crear administradores delegados, consulte el artículo principal de [Administración delegada](#).

Los permisos administrativos determinan la interfaz de Director que ven los administradores y las tareas que estos pueden realizar. Los permisos determinan:

- Las vistas a las que los administradores pueden acceder, denominadas conjuntamente como una vista.
- Los escritorios, las máquinas y las sesiones que el administrador puede ver y con las que puede interactuar.

- Los comandos que el administrador puede ejecutar, como el remedo de la sesión de un usuario o habilitar el modo de mantenimiento.

Los roles y permisos integrados también determinan cómo los administradores usan Director:

Rol de administrador	Los permisos en Director
Administrador total	Cuenta con acceso completo a todas las vistas y puede ejecutar todos los comandos, incluidos remedar la sesión de un usuario, habilitar el modo de mantenimiento y exportar los datos de tendencias.
Administrador de grupos de entrega	Cuenta con acceso completo a todas las vistas y puede ejecutar todos los comandos, incluidos remedar la sesión de un usuario, habilitar el modo de mantenimiento y exportar los datos de tendencias.
Administrador de solo lectura	Puede acceder a todas las vistas y ver todos los objetos en los ámbitos especificados, así como información global. Puede descargar informes de canales HDX y puede exportar datos de tendencias mediante la opción de exportación en la vista Tendencias. No puede ejecutar ningún otro comando ni cambiar nada en las vistas.
Administrador de asistencia técnica	Puede acceder únicamente a las vistas del Servicio de asistencia y de los Detalles del usuario y solo puede ver los objetos que le han sido delegados para que los administre. Puede remedar la sesión de un usuario y ejecutar comandos para ese usuario. Puede realizar operaciones en modo de mantenimiento. Puede utilizar las opciones de control de energía para las máquinas con sistema operativo de sesión única. No puede acceder a las vistas de Panel de mandos, Tendencias, Alertas ni Filtros. No puede utilizar las opciones de control de energía para las máquinas con sistema operativo multisesión.
Administrador de catálogos de máquinas	Solo puede acceder a la página “Detalles de la máquina”(búsqueda por máquinas).

Administrador de host

Sin acceso. Este administrador no es compatible en Director y no puede ver datos.

---

## Configurar roles personalizados para administradores de Director

En Studio, también puede configurar roles personalizados específicos para Director y coincidir mejor con los requisitos de su organización y delegar permisos con mayor flexibilidad. Por ejemplo, puede restringir el rol de administrador de asistencia técnico integrado para que el administrador no pueda cerrar sesiones.

Si crea un rol personalizada con permisos de Director, también debe dar a ese rol otros permisos genéricos:

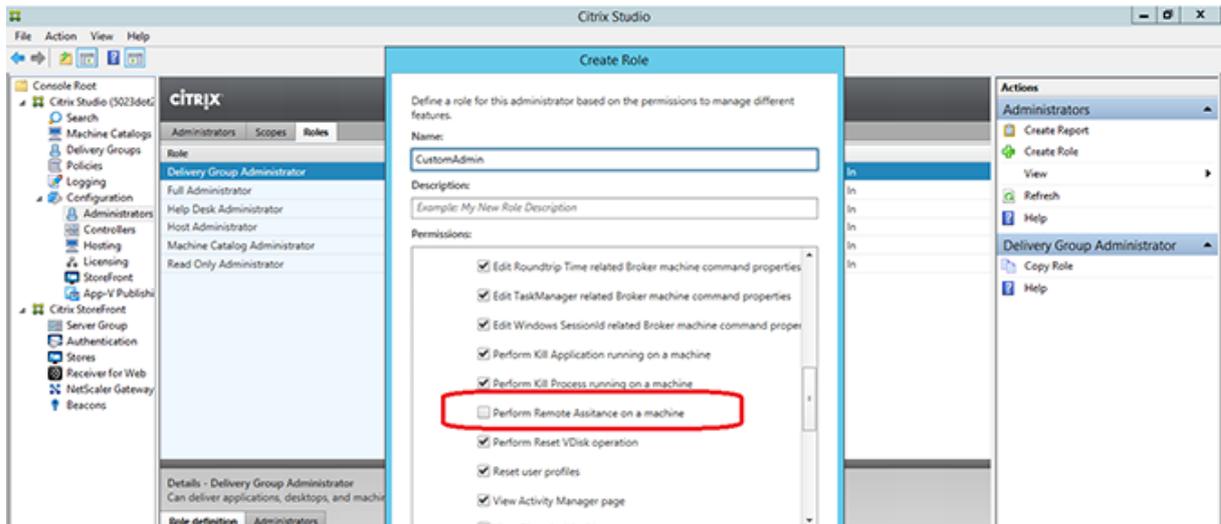
- Permiso de Delivery Controller para iniciar sesión en Director; al menos el acceso de solo lectura en el nodo Administrador
- Permisos para que los grupos de entrega vean los datos relacionados con esos grupos de entrega en Director; al menos el acceso de solo lectura

También puede crear un rol personalizado mediante la copia de un rol existente e incluir permisos adicionales para vistas diferentes. Por ejemplo, puede copiar el rol del servicio de asistencia e incluir permisos para ver las páginas Panel de mandos o Filtros.

Seleccione los permisos de Director para el rol personalizado, incluidos:

- Terminar aplicación ejecutada en una máquina
- Terminar proceso ejecutado en una máquina
- Asistencia remota en una máquina
- Restablecer disco virtual
- Restablecer perfiles de usuario
- Ver página Detalles de cliente
- Ver página Panel de mandos
- Ver página Filtros
- Ver página Detalles de la máquina
- Ver página Tendencias
- Ver página Detalles del usuario

En este ejemplo, el Remedo (Asistencia remota en una máquina) está desactivado.



Un permiso puede depender de otros para que se pueda aplicar en la interfaz de usuario. Por ejemplo, seleccionar el permiso **Terminar aplicación ejecutada en una máquina** habilita la funcionalidad **Finalizar aplicación** solo en aquellos paneles a los que tiene permiso el rol. Se pueden seleccionar los siguientes permisos de panel:

- Ver página Filtros
- Ver página Detalles del usuario
- Ver página Detalles de la máquina
- Ver página Detalles de cliente

Además, en la lista de permisos para otros componentes, tenga en cuenta estos permisos de grupos de entrega:

- Habilitar/inhabilitar el modo de mantenimiento de una máquina por su pertenencia a un grupo de entrega.
- Realizar operaciones de administración de energía en máquinas de escritorio Windows por su pertenencia a grupos de entrega.
- Administrar sesiones en máquinas por su pertenencia a un grupo de entrega.

## Implementación segura de Director

January 25, 2022

En este artículo se muestran las áreas que pueden afectar a la seguridad del sistema durante la implementación y la configuración de Director.

## **Configurar Microsoft Internet Information Services (IIS)**

Director puede configurarse con una configuración restringida de IIS. Esta no es la configuración predeterminada de IIS.

### **Límites de reciclaje de los grupos de aplicaciones**

Puede establecer estos límites de reciclaje de los grupos de aplicaciones:

- Límite de memoria virtual: 4 294 967 295
- Límite de memoria privada: El tamaño de la memoria física del servidor de StoreFront
- Límite de solicitudes: 4 000 000 000

### **Extensiones de nombre de archivo**

Puede prohibir extensiones de nombre de archivo no incluidas en la lista.

Director requiere estas extensiones de nombre de archivo en la opción Filtro de solicitudes:

- .aspx
- .css
- .html
- .js
- .png
- .svc
- .woff
- .woff2
- .png
- .eot
- .svg
- .ttf
- .json
- . (para redirecciones)

Director requiere los siguientes verbos de HTTP en Filtro de solicitudes. Puede prohibir los verbos que no se encuentren en la lista.

- GET
- POST
- HEAD

Director no requiere:

- Filtros de ISAPI
- Extensiones ISAPI
- Programas CGI
- Programas FastCGI

Importante:

- Director requiere Plena confianza. No configure el nivel de confianza de .NET con un nivel Alto o inferior.
- Director mantiene un grupo de aplicaciones separado. Para modificar los parámetros de Director, seleccione el sitio de Director y modifíquelos.

## Configurar derechos de usuario

Cuando se instala Director, sus grupos de aplicaciones reciben el derecho de Iniciar sesión como un servicio, y los privilegios siguientes: Ajustar las cuotas de la memoria para un proceso, Generar auditorías de seguridad y Reemplazar un símbolo (token) de nivel de proceso. Este es el comportamiento normal de instalación cuando se crean los grupos de aplicaciones.

No es necesario que cambie estos derechos de usuario. Estos privilegios no se usan en Director y están inhabilitados automáticamente.

## Comunicaciones de Director

En un entorno de producción, Citrix recomienda el uso del protocolo IPsec o los protocolos HTTPS para proteger la transferencia de los datos entre Director y los servidores. IPsec es un conjunto de extensiones estándar para el protocolo de Internet. Proporciona comunicaciones autenticadas y cifradas con integridad de datos y protección contra reproducción. Como IPsec es un conjunto de protocolos de capa de red, los protocolos con niveles más elevados pueden utilizarlo sin realizar ninguna modificación. HTTPS utiliza el protocolo Transport Layer Security (TLS) para brindar un cifrado de datos avanzado.

Nota:

- Citrix recomienda no habilitar conexiones a Director que no sean seguras en un entorno de producción.
- Para proteger las comunicaciones desde Director, se requiere una configuración aparte para cada conexión.
- No se recomienda usar el protocolo SSL. En su lugar, use el protocolo TLS, que es más seguro.
- Debe proteger las comunicaciones con Citrix ADC mediante TLS, no IPsec.

Para proteger las comunicaciones entre Director y los servidores Citrix Virtual Apps and Desktops (para supervisión e informes), consulte [Data Access Security](#).

Para proteger las comunicaciones entre Director y Citrix ADC (para Citrix Insight), consulte [Configurar el análisis de red](#).

Para proteger las comunicaciones entre Director y el servidor de licencias, consulte [Proteger License Administration Console](#).

## Separar la seguridad de Director

Si implementa aplicaciones web en el mismo dominio web (nombre de dominio y puerto) que Director, cualquier posible problema de seguridad de esas aplicaciones web podrían afectar a su vez a la seguridad de la implementación de Director. Cuando se necesita un mayor nivel de seguridad es necesario separarlos: Citrix recomienda implementar Director en un dominio web aparte.

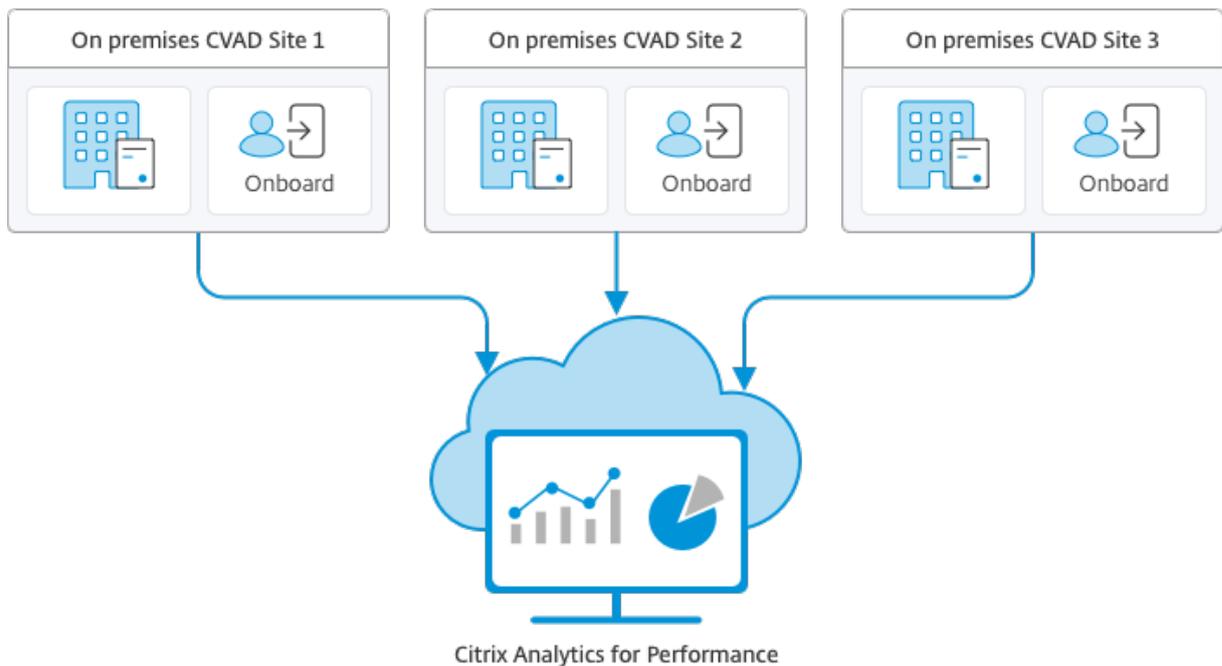
## Configurar sitios locales con Citrix Analytics for Performance

June 27, 2024

Citrix Analytics for Performance (análisis de rendimiento) es la solución integral de supervisión de rendimiento del servicio en la nube de Citrix Analytics. El análisis de rendimiento proporciona información avanzada y análisis basados en métricas de rendimiento. El análisis de rendimiento le ayuda a supervisar y consultar las métricas de uso y rendimiento de uno o más sitios de Citrix Virtual Apps and Desktops de su organización.

Para obtener más información, consulte el [artículo sobre el análisis de rendimiento](#).

Puede enviar datos de rendimiento desde su sitio a Citrix Analytics for Performance a Citrix Cloud para aprovechar sus funciones avanzadas de análisis de rendimiento. Para ver y usar el análisis de rendimiento, primero debe configurar sus sitios locales con Citrix Analytics for Performance desde la ficha **Analytics** de **Director**. Esta función requiere la versión 1909 de Director y Delivery Controller o una posterior, y la versión 1906 de VDA o una posterior.



El análisis de rendimiento accede a los datos de forma segura, y no se transfiere ningún dato desde Citrix Cloud al entorno local.

## Requisitos previos

Para configurar Citrix Analytics for Performance desde Director, no es necesario instalar componentes nuevos. Compruebe que se cumplen los siguientes requisitos:

- Su Delivery Controller y Director tienen la versión 1912 CU2 o una posterior. Para obtener más información, consulte la [tabla de compatibilidad de funciones](#).

### Nota:

- Es posible que no pueda configurar el sitio local con Citrix Analytics for Performance de Director si el Delivery Controller usa una versión de Microsoft .NET Framework anterior a 4.8. Como solución temporal, actualice la versión de .NET Framework del Delivery Controller a 4.8. [LCM-9255](#).
- Cuando se configura el sitio local que ejecuta Citrix Virtual Apps and Desktops versión 2012 con Citrix Analytics for Performance desde Director, la configuración puede fallar después de un par de horas o después de reiniciar Citrix Monitor Service en el Delivery Controller. La ficha Análisis muestra el estado No conectado en este caso. Como solución temporal, cree una carpeta Encryption en el Registro presente en el Delivery Controller, Ubicación: HKEY\_LOCAL\_MACHINE\Software\Citrix\XDservices\Monitor, Nombre de carpeta: Encryption. Compruebe que la cuenta CitrixMonitor tiene acceso de control total en la carpeta

Encryption. Reinicie Citrix Monitor Service.[DIR-14324](#).

- El acceso a la ficha **Analytics** para realizar esta configuración solo está disponible para administradores totales.
- Para que el análisis de rendimiento acceda a las métricas de rendimiento, el acceso saliente a Internet está disponible en todos los Delivery Controllers y en las máquinas en las que está instalado Director. Concretamente, garantice la posibilidad de acceso a las siguientes direcciones URL:

- Registro de claves de Citrix: [https://\\*.citrixnetworkapi.net/](https://*.citrixnetworkapi.net/)
- Citrix Cloud: [https://\\*.citrixworkspacesapi.net/](https://*.citrixworkspacesapi.net/)
- Citrix Analytics: [https://\\*.cloud.com/](https://*.cloud.com/)
- Microsoft Azure: [https://\\*.windows.net/](https://*.windows.net/)

Si las máquinas con Delivery Controllers y Director están dentro de una intranet y el acceso saliente a Internet pasa por un servidor proxy, asegúrese de lo siguiente:

- El servidor proxy debe permitir la lista anterior de direcciones URL.
- Agregue la configuración siguiente a los archivos web.config y citrix.monitor.exe.config de Director. Asegúrese de agregar esta configuración dentro de las etiquetas de **configuración**:

```

1 <system.net>
2   <defaultProxy>
3     <proxy usesystemdefault = "false" proxyaddress = "http
4       ://<your_proxyserver_address>:80" bypassonlocal = "
5         true" />
6   </defaultProxy>
7 </system.net>

```

- El archivo web.config de Director se encuentra en `C:\inetpub\wwwroot\Director\web.config` en la máquina donde está instalado Director. - El archivo citrix.monitor.exe.config se encuentra en `C:\Program Files\Citrix\Monitor\Service\Citrix.Monitor.exe.Config` en la máquina donde está instalado Delivery Controller.

Microsoft proporciona este parámetro en IIS. Para obtener más información, consulte <https://docs.microsoft.com/en-us/dotnet/framework/network-programming/proxy-configuration>.

El campo **defaultproxy** del archivo de configuración controla el acceso saliente de Director y Monitor Service. La configuración y la comunicación con Análisis de rendimiento requieren que el campo **defaultproxy** se establezca en **true**. Es posible que las directivas en vigor establezcan este campo en false. En ese caso, debe establecer manualmente el campo en true. Realice una copia de seguridad de los archivos de configuración antes de realizar los cambios. Reinicie Monitoring Service en el Delivery Controller para que los cambios surtan efecto.

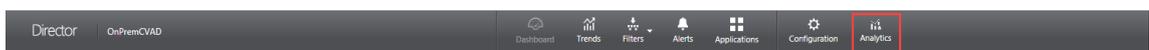
- Tiene un derecho activo de Citrix Cloud para Citrix Analytics for Performance.

- Su cuenta de Citrix Cloud es una cuenta de administrador con derechos sobre la experiencia de registro de productos. Para obtener más información sobre los permisos de administrador, consulte [Modificar permisos de administrador](#).

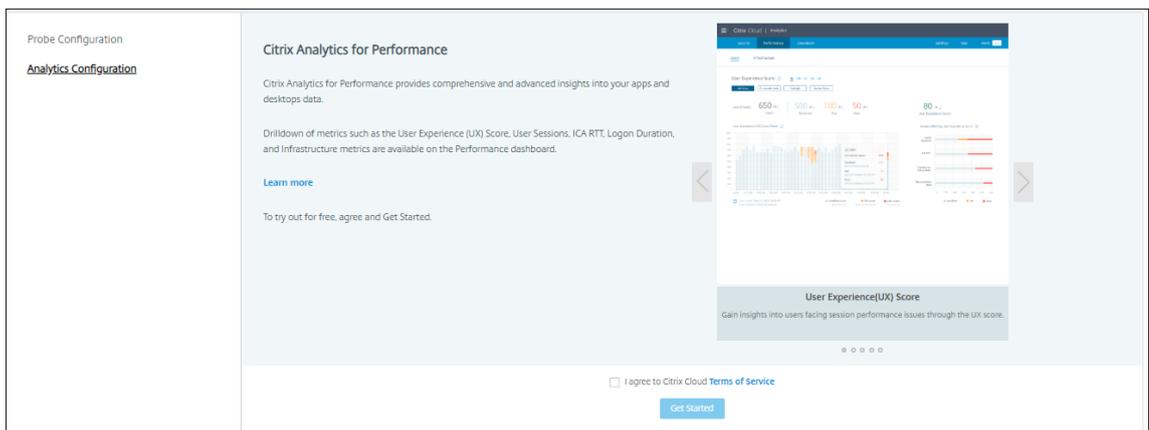
## Pasos de configuración

Después de verificar los requisitos previos, haga lo siguiente:

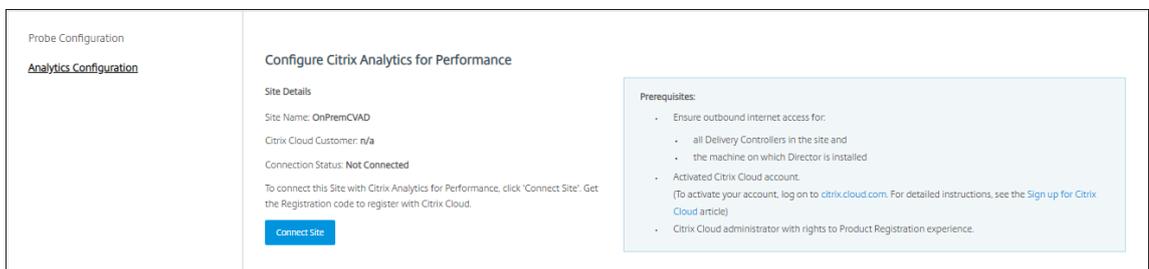
1. Inicie sesión en Director como administrador total y seleccione el sitio que quiere configurar con el análisis de rendimiento.
2. Haga clic en la ficha **Analytics**. Aparecerá la página **Configuración**.



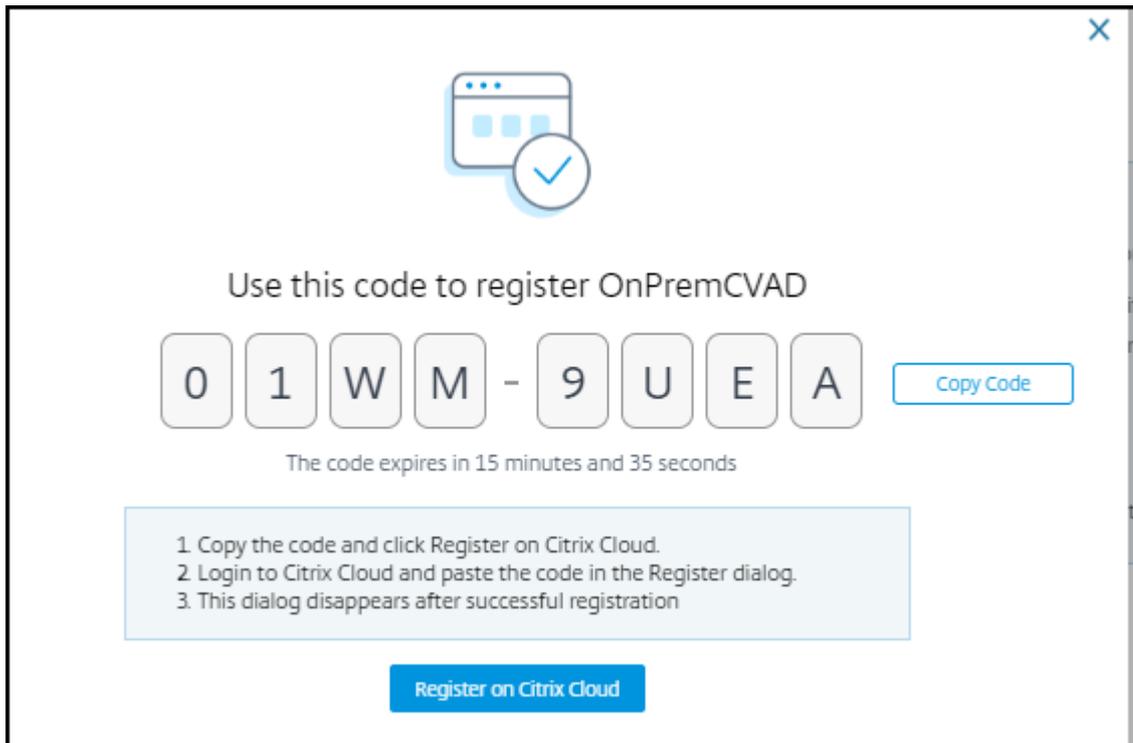
3. Revise los pasos, seleccione las condiciones de servicio y, a continuación, haga clic en **Comenzar**.



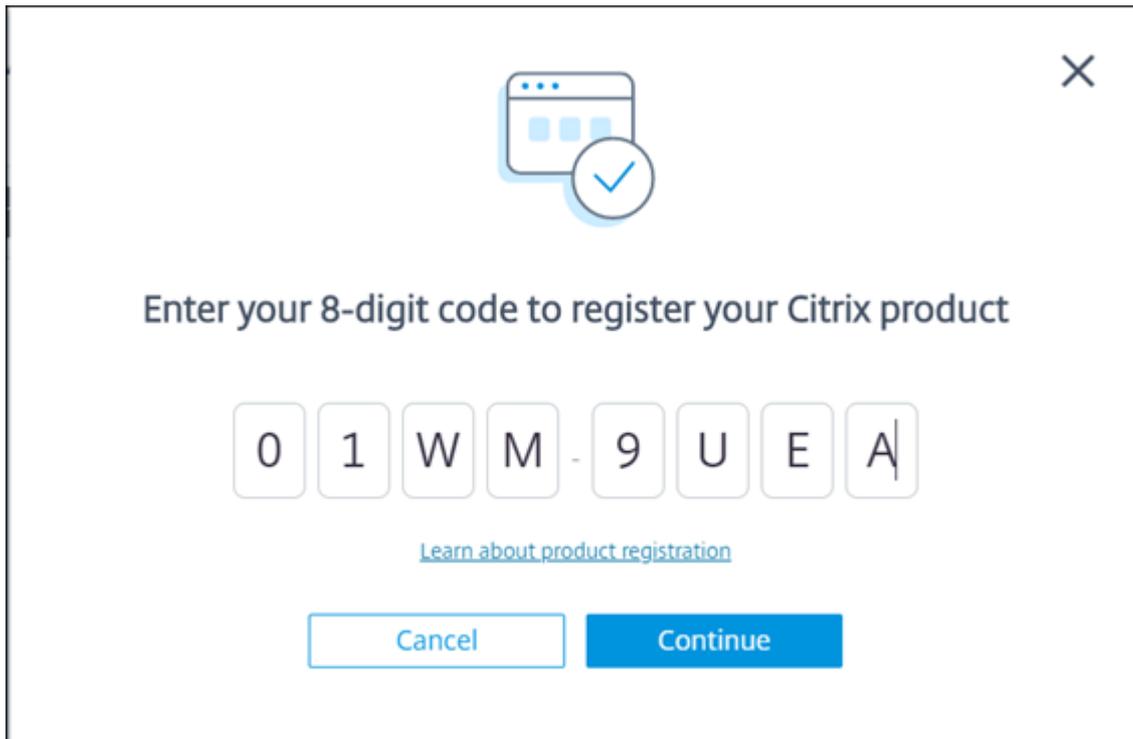
4. Revise los requisitos previos y asegúrese de que se cumplen. Revise los detalles del sitio.
5. Haga clic en **Conectar sitio** para iniciar el proceso de configuración.



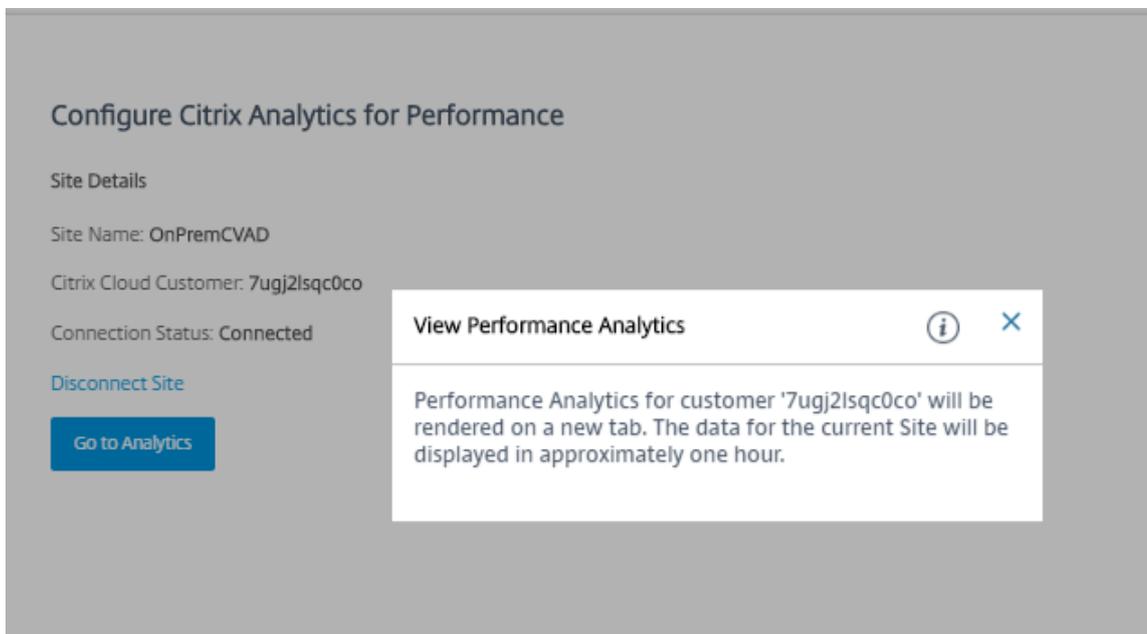
6. Se genera un código único de registro de 8 dígitos que se utilizará para registrar este sitio en Citrix Cloud.



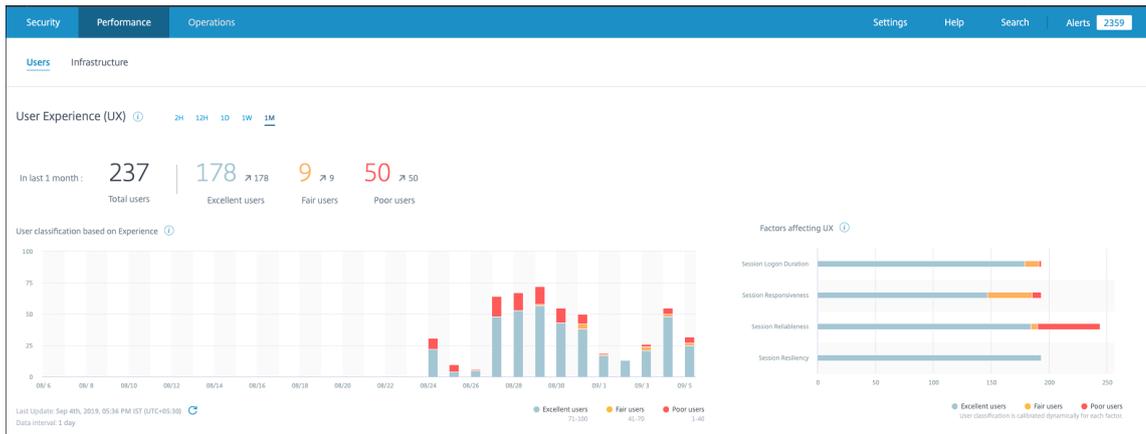
7. Haga clic en **Copiar código** para copiar el código y, a continuación, haga clic en **Registrar en Citrix Cloud**.
8. Se le redirigirá a la URL de registro de Citrix Cloud. Inicie sesión con sus credenciales de Citrix Cloud y seleccione el cliente.
9. Pegue el código de registro copiado en la página Registros de productos de Citrix Cloud. Haga clic en **Continuar** para registrarse. Revise los detalles de registro y haga clic en **Registrar**.



10. El sitio local se registra en Citrix Cloud. Ahora, desde **Director**, haga clic en **Ir a Analytics**, en la ficha **Analytics**.



11. El análisis de rendimiento se abre en una ficha nueva del explorador.



Si la sesión de Citrix Cloud ha caducado, es posible que se le redirija a la página de inicio de sesión en cuenta de Citrix.com o My Citrix.

12. Para registrar varios sitios en el análisis de rendimiento, repita para cada sitio de Director los pasos de configuración anteriores. Las métricas de todos los sitios configurados se muestran en el panel de mandos del análisis de rendimiento.
13. Para desconectar el sitio de Citrix Cloud, haga clic en **Desconectar sitio**. Esta opción elimina la configuración existente.

**Notas:**

La primera vez que configure un sitio, los eventos del sitio pueden tardar un poco (aproximadamente una hora) en procesarse, lo que retrasa la visualización de las métricas en el panel de mandos del análisis de rendimiento. A partir de entonces, los eventos se actualizan a intervalos regulares.

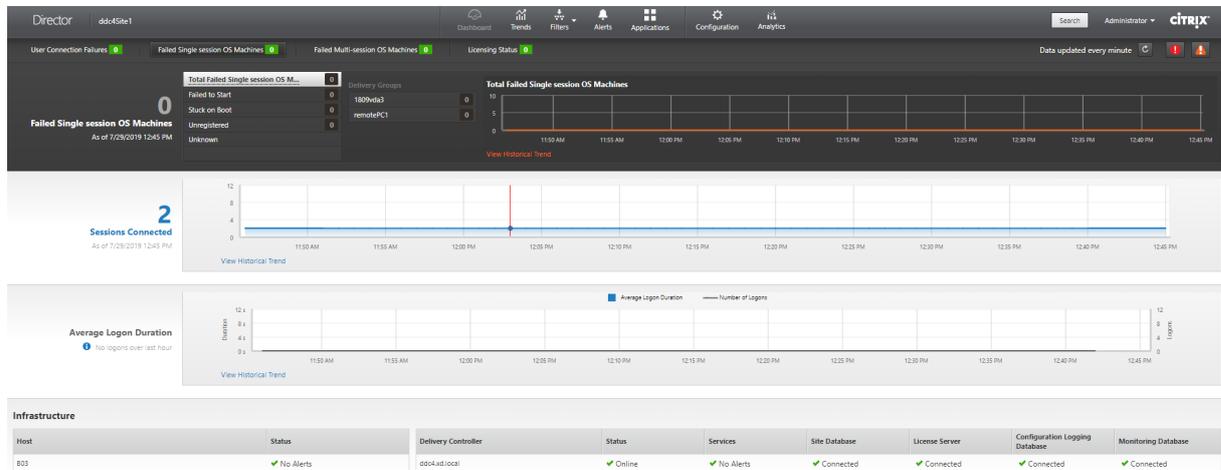
Al desconectarse, la transmisión de datos desde la cuenta antigua continúa durante un tiempo hasta que se transmiten los eventos de la nueva cuenta. Durante aproximadamente una hora después de que se haya detenido la transmisión de datos, los análisis relacionados con la cuenta antigua se siguen mostrando en el panel de mandos del análisis de rendimiento.

Al caducar el derecho a Citrix Analytics Service, se tarda hasta un día en dejar de enviar las métricas del sitio al análisis de rendimiento.

**Análisis de sitios**

September 22, 2021

Con permisos de administrador total, al abrir Director, el Panel de mandos ofrece una ubicación centralizada desde la que puede supervisar el estado y el uso de un sitio.



Si no hay fallos y no se han producido fallos en los últimos 60 minutos, los paneles permanecen contraídos. Cuando hay fallos, el panel de fallos específicos aparecerá automáticamente.

**Nota:**

Es posible que algunas opciones o funciones no estén disponibles, ya que dependen de la licencia que tenga su organización y de sus privilegios de administrador.

Panel	Descripción
Fallos de conexión de usuario	Fallos de conexión en los últimos 60 minutos. Haga clic en las categorías junto al número total para ver las mediciones para ese tipo de fallo. En la tabla adyacente, esa cantidad se desglosa por grupos de entrega. Los fallos de conexión incluyen fallos provocados por haberse alcanzado el límite de las aplicaciones. Para obtener más información acerca de los límites para aplicaciones, consulte <a href="#">Aplicaciones</a> .
Máquinas con SO de sesión única fallidas o Máquinas con SO multisesión fallidas	Total de fallos en los últimos 60 minutos clasificados por grupos de entrega. Fallos clasificados por tipos, incluidos los tipos “No se iniciaron”, “Atascadas en el arranque” y “Sin registrar”. Para máquinas con sistema operativo multisesión, los fallos también incluyen máquinas que alcanzan el máximo de carga.

---

Panel	Descripción
Estado de licencia	En las alertas del servidor de licencias se incluyen las alertas enviadas por el servidor de licencias y las acciones necesarias para resolverlas. Requiere Citrix License Server 11.12.1 o una versión posterior. En las alertas de Delivery Controller se incluyen detalles del estado de las licencias según las ve el Controller y son enviadas por éste. Requiere Controller para XenApp 7.6 o XenDesktop 7.6 o versiones posteriores. Puede establecer el umbral para alertas en Studio. El estado de las licencias que se muestra en <b>Delivery Controllers &gt; Detalles &gt; Ediciones de producto &gt; PLT</b> indica <b>Premium</b> y no <b>Platinum</b> .
Sesiones conectadas	Sesiones conectadas en todos los grupos de entrega durante los últimos 60 minutos.
Promedio de duración de inicio de sesión	Datos de inicio de sesión durante los últimos 60 minutos. El número grande a la izquierda es el promedio de la duración de los inicios de sesión durante la última hora. Los datos de inicio de sesión de VDA anteriores a XenDesktop 7.0 no están incluidos en esta media. Para obtener más información, consulte <a href="#">Diagnosticar problemas de inicio de sesión de los usuarios</a> .

---

Panel	Descripción
Infraestructura	Ofrece una lista de la infraestructura de su sitio: hosts y Controllers. Para conocer la infraestructura de Citrix Hypervisor o VMware, puede consultar las alertas de rendimiento. Por ejemplo, puede configurar XenCenter para generar alertas de rendimiento cuando el uso de la CPU, E/S de red o uso de E/S de disco supere un umbral especificado en un servidor administrado o una máquina virtual. De forma predeterminada, el intervalo de repetición de alertas es de 60 minutos, pero también lo puede configurar. Para obtener más información, consulte la sección Alertas de rendimiento de XenCenter de la <a href="#">documentación del producto Citrix Hypervisor</a> .

---

**Nota:**

Si no aparece el icono para una métrica concreta, significa que el tipo de métrica no es compatible con el tipo de host que está utilizando. Por ejemplo, no hay información de estado disponible de los hosts de System Center Virtual Machine Manager (SCVMM), de Amazon Web Services ni de CloudStack.

Continúe solucionando problemas con estas opciones (documentadas a continuación):

- [Controlar la energía de la máquina del usuario](#)
- [Impedir conexiones a máquinas](#)

**Supervisar sesiones**

Si una sesión se desconecta, la sesión permanece activa y sus aplicaciones siguen ejecutándose, pero el dispositivo de usuario ya no se comunica con el servidor.

---

Acción	Descripción
Ver la máquina o sesión a la que está conectado un usuario	En las vistas Administrador de actividades y Detalles del usuario, se puede ver la máquina o la sesión a la que está conectado un usuario en ese momento, así como una lista de todas las máquinas y sesiones a las que dicho usuario tiene acceso. Para tener acceso a esta lista, haga clic en el icono de cambio de sesión en la barra de título de usuario. Para obtener más información, consulte <a href="#">Restaurar sesiones</a> .
Ver la cantidad total de sesiones conectadas en todos los grupos de entrega	En el Panel de mandos, en el panel <b>Sesiones conectadas</b> , se puede ver la cantidad total de sesiones conectadas en todos los grupos de entrega durante los últimos 60 minutos. A continuación, puede hacer clic en el número correspondiente al total, y se abre la vista Filtros, donde se pueden ver los datos de sesiones en un gráfico, basados en grupos de entrega seleccionados e intervalos.
Finalizar sesiones inactivas	La vista Filtros de sesiones muestra los datos relacionados con todas las sesiones activas. Puede filtrar las sesiones en función del usuario asociado, grupo de entrega, estado de la sesión y de un tiempo de inactividad mayor a un umbral de período de tiempo. En la lista filtrada, seleccione las sesiones a cerrar o desconectar. Para obtener más información, consulte <a href="#">Solucionar problemas de aplicaciones</a> .
Ver datos para un período de tiempo más largo	En la vista “Tendencias”, seleccione la ficha <b>Sesiones</b> para desglosar más datos y ver usos más específicos de sesiones conectadas y desconectadas correspondientes a un período de tiempo más largo (es decir, totales de sesiones anteriores a los últimos 60 minutos). Para ver esta información, haga clic en <b>Ver tendencias históricas</b> .

---

**Nota:**

Si el dispositivo del usuario ejecuta un agente Virtual Delivery Agent (VDA) antiguo (por ejemplo, un agente VDA anterior a la versión 7 o Linux VDA), Director no puede mostrar información completa sobre la sesión. En vez de ello, aparece un mensaje donde se indica que la información no está disponible.

**Limitación de reglas de asignación de escritorios:**

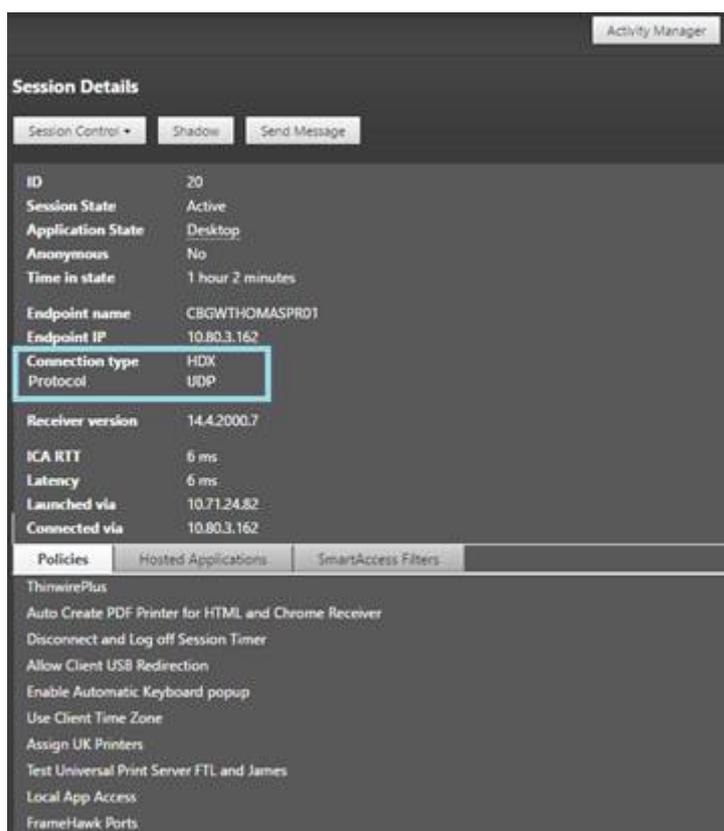
Citrix Studio permite la asignación de varias reglas de asignación de escritorios (DAR) para distintos usuarios o grupos de usuarios a un solo VDA en el grupo de entrega. StoreFront muestra el escritorio asignado con el **nombre simplificado** correspondiente a las reglas DAR para el usuario que ha iniciado sesión. Sin embargo, Director no admite las reglas de asignación de escritorios y, por tanto, muestra el escritorio asignado mediante el nombre del grupo de entrega, sin tener en cuenta qué usuario está conectado a la sesión. Como resultado de ello, no se puede asignar un escritorio específico a una máquina en Director.

Puede asignar el escritorio asignado que se muestra en StoreFront al nombre del grupo de entrega que se muestra en Director mediante el siguiente comando de PowerShell:

```
1 Get-BrokerDesktopGroup | Where-Object {
2   \$_ .Uid -eq \((Get-BrokerAssignmentPolicyRule | Where-Object {
3     \$_ .PublishedName -eq "\"<Name on StoreFront\>\" }
4   ).DesktopGroupUid }
5   | Select-Object -Property Name, Uid
```

**Protocolo de transporte en la sesión**

El protocolo de transporte que se utiliza para el tipo de conexión HDX en la sesión actual aparece en el panel **Detalles de la sesión**. Esta información está disponible para las sesiones iniciadas en los VDA 7.13 o una versión posterior.



- Para el tipo de conexión **HDX**:
  - El protocolo que se muestra es **UDP** si se utiliza EDT para la conexión HDX.
  - El protocolo que se muestra es **TCP** si se utiliza TCP para la conexión HDX.
- Para el tipo de conexión **RDP**, el protocolo se muestra como **n/d**.

Cuando se configura el transporte adaptable, el protocolo de transporte de la sesión cambia dinámicamente entre EDT (sobre UDP) y TCP, según las condiciones de red. Si no se puede establecer la sesión HDX por el protocolo EDT, se recurre al protocolo TCP.

Para obtener más información sobre cómo configurar el transporte adaptable, consulte [Transporte adaptable](#).

## Exportar informes

Puede exportar los datos de tendencias para generar informes de uso habitual y administración de capacidad. En la exportación, se admiten los formatos PDF, Excel y CSV. Los informes en formatos PDF o Excel contienen datos de tendencias representados en gráficos y tablas. Los informes en formato CSV contienen datos tabulares que se pueden procesar para generar vistas, o bien se pueden archivar.

Para exportar un informe:

1. Vaya a la ficha **Tendencias**.
2. Establezca los criterios de filtrado, el período de tiempo y haga clic en **Aplicar**. La tabla y el gráfico de tendencias se rellenan con los datos.
3. Haga clic en **Exportar**, y escriba el nombre y el formato del informe.

Director genera el informe en función de los criterios de filtrado que haya seleccionado. Si cambia los criterios de filtrado, haga clic en **Aplicar** antes de hacer clic en **Exportar**.

**Nota:**

La exportación de una gran cantidad de datos implica un aumento significativo en el consumo de memoria y de CPU en el servidor de Director, el Delivery Controller y los servidores SQL. Se establecen límites predeterminados a la cantidad admitida de operaciones de exportación simultáneas y a la cantidad de datos que pueden exportarse con el fin de lograr un rendimiento óptimo de exportación.

### Límites de exportación admitidos

Los informes en PDF y Excel exportados contienen gráficos completos de los criterios de filtrado seleccionados. Sin embargo, los datos tabulares de todos los formatos de informe se truncan si superan los límites predeterminados de cantidad de filas o registros que haya en la tabla. La cantidad predeterminada de registros admitidos se define en función del formato de informe.

Puede cambiar el límite predeterminado ajustando los parámetros de aplicaciones de Director en Internet Information Services (IIS).

Formato del informe	Cantidad predeterminada de registros admitidos	Campos de "Configuración de aplicaciones" en Director	Cantidad máxima admitida de registros
PDF	500	UI.ExportPdfDrilldownLimit	500
Excel	100 000	UI.ExportExcelDrilldownLimit	100 000
CSV	100 000 (10 000 000 en la ficha <b>Sesiones</b> )	UI.ExportCsvDrilldownLimit	100 000

Para cambiar el límite de la cantidad de registros que se pueden exportar:

1. Abra la consola del Administrador IIS.
2. Vaya al sitio web de Director en el sitio web predeterminado.
3. Haga doble clic en **Configuración de aplicaciones**.
4. Modifique o agregue un parámetro a los campos UI.ExportPdfDrilldownLimit, UI.ExportExcelDrilldownLimit o UI.ExportCsvDrilldownLimit si fuera necesario.

Al agregar valores en los campos de “Configuración de aplicaciones”, se sobrescriben los valores pre-determinados.

Advertencia:

Establecer en los campos unos valores más altos que la cantidad máxima admitida de registros puede afectar al rendimiento de la exportación, por eso esa acción no se admite.

## Gestión de errores

En esta sección, se ofrece información para solucionar los errores que puede encontrarse durante la operación de exportación.

- **Se agotó el tiempo de espera de Director**

Este error puede darse por problemas de red o por un consumo alto de recursos por parte de Monitor Service o en el servidor de Director.

La duración predeterminada del tiempo de espera es de 100 segundos. Para aumentar el tiempo de espera del servicio Director, establezca el valor del campo **Connector.DataServiceContext.Timeout** en la Configuración de aplicaciones de Director, en Internet Information Services (IIS):

1. Abra la consola del Administrador IIS.
2. Vaya al sitio web de Director en el sitio web predeterminado.
3. Haga doble clic en **Configuración de aplicaciones**.
4. Modifique el valor **Connector.DataServiceContext.Timeout**.

- **Se agotó el tiempo de espera del Monitor**

Este error puede darse por problemas de red o por un consumo alto de recursos por parte de Monitor Service o en SQL Server.

Para aumentar la duración del tiempo de espera de Monitor Service, ejecute los siguientes comandos de PowerShell en el Delivery Controller:

```
1 asnp Citrix.*
2 Get-MonitorConfiguration
3 Set-MonitorConfiguration -MonitorQueryTimeoutSeconds <timeout value>
```

- **Cantidad máxima de operaciones simultáneas de exportación o vista previa en curso**

Director admite una instancia de Exportar o Vista previa. Si recibe el error de **cantidad máxima de operaciones simultáneas de exportación o vista previa en curso**, vuelva a intentar más tarde esas operaciones.

Puede aumentar la cantidad de operaciones de exportación o vista previa simultáneas; sin embargo, eso puede afectar al rendimiento de Director y no se admite:

1. Abra la consola del Administrador IIS.
2. Vaya al sitio web de Director en el sitio web predeterminado.
3. Haga doble clic en **Configuración de aplicaciones**.
4. Modifique el valor **UI.ConcurrentExportLimit**.

- **Espacio en disco insuficiente en Director**

Cada operación de exportación requiere un máximo de 2 GB de espacio libre en la carpeta Temp de Windows. Vuelva a intentar la exportación después de liberar espacio en el disco duro, o bien agregue más espacio en el disco del servidor de Director.

## Supervisar parches rápidos

Para ver los parches rápidos instalados en la máquina (física o VM) de un VDA concreto, elija la vista **Detalles de la máquina**.

## Controlar los estados de energía de la máquina del usuario

Para controlar el estado de las máquinas que selecciona en Director, use las opciones de Control de energía. Estas opciones están disponibles para máquinas con SO de sesión única, pero podrían no estar disponibles para máquinas con SO multisesión.

**Nota:**

Esta función no está disponible para máquinas físicas ni para máquinas que usan el acceso con Remote PC.

---

Comando	Función
<b>Reiniciar</b>	Realiza un apagado ordenado (suave) de la VM, y todos los procesos que se estén ejecutando se detienen uno por uno antes de reiniciar la VM. Por ejemplo, seleccione las máquinas que aparecen en Director como “No se iniciaron”, y use este comando para reiniciarlas.

Comando	Función
<b>Forzar reinicio</b>	Reinicia la máquina virtual sin antes realizar un procedimiento de apagado. Este comando funciona igual que desenchufar un servidor físico y, a continuación, volverlo a enchufar y volverlo a iniciar.
<b>Apagar</b>	Realiza un apagado ordenado (suave) de la VM, y todos los procesos que se estén ejecutando se detienen uno por uno.
<b>Forzar apagado</b>	Apaga la máquina virtual sin realizar un procedimiento de apagado ordenado. Este comando funciona igual que desenchufar un servidor físico. No siempre se cierran todos los procesos en ejecución, por lo que corre el riesgo de perder datos si apaga una VM de este modo.
<b>Suspender</b>	Suspende una VM en ejecución en su estado actual y guarda ese estado en el repositorio de almacenamiento predeterminado. Esta opción permite apagar el servidor host de la VM y más tarde, después de un reinicio, reanudar la VM devolviéndola al estado de ejecución en que estaba.
<b>Reanudar</b>	Reanuda una VM que fue suspendida, devolviéndola al estado de ejecución en el que se encontraba.
<b>Iniciar</b>	Inicia una VM cuando está desactivada (también llamado un inicio “en frío”).

---

Si las acciones de control de energía fallan, pase el puntero sobre la alerta y aparecerá un mensaje emergente con información detallada sobre el fallo.

### **Impedir conexiones a máquinas**

Use el modo de mantenimiento para impedir nuevas conexiones temporalmente, mientras el administrador realiza tareas de mantenimiento en la imagen.

Cuando se habilita el modo de mantenimiento en las máquinas, no se permiten nuevas conexiones hasta que se inhabilita dicho modo. Si hay usuarios con sesiones ya iniciadas, el modo de mantenimiento entra en vigor tan pronto como todos los usuarios cierran sus sesiones. Si hay usuarios que

no cierran la sesión, envíeles un mensaje para notificarles que las máquinas se apagarán al cabo de un cierto tiempo, y use los controles de energía para forzar el apagado de las máquinas.

1. Seleccione la máquina en, por ejemplo, la vista Detalles del usuario o un grupo de máquinas en la vista Filtros.
2. Seleccione **Modo de mantenimiento** y active esta opción.

Si un usuario intenta conectarse a un escritorio asignado mientras éste se encuentra en el modo de mantenimiento, aparecerá un mensaje indicándole que el escritorio no se encuentra disponible por el momento. No se pueden establecer nuevas conexiones hasta que se inhabilite el modo de mantenimiento.

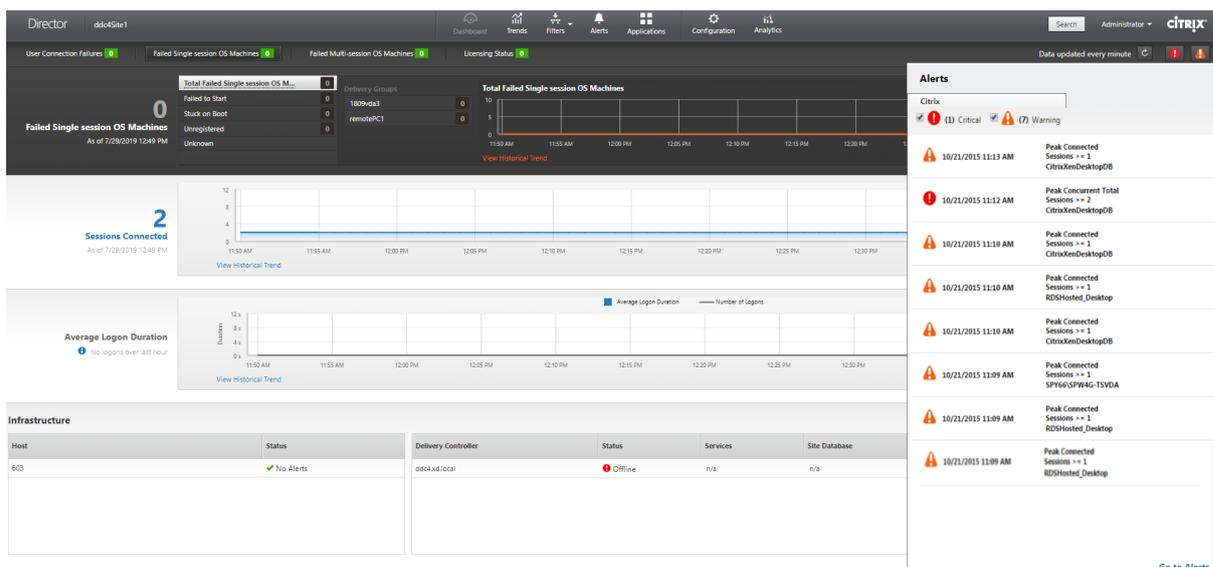
## Análisis de aplicaciones

La ficha **Aplicaciones** muestra datos de análisis de aplicaciones en una vista única y consolidada, con el fin de ayudar a analizar y gestionar de forma eficiente el rendimiento de las aplicaciones. Puede obtener información valiosa sobre el estado y el uso de todas las aplicaciones publicadas en el sitio. Muestra diferentes métricas, como los resultados del sondeo, la cantidad de instancias por aplicación y los fallos y errores asociados a las aplicaciones publicadas. Para obtener más información, consulte la sección [Análisis de aplicaciones](#) en **Solucionar problemas de aplicaciones**.

## Alertas y notificaciones

May 5, 2023

En Director, las alertas se muestran en el panel de mandos y en otras vistas de alto nivel mediante símbolos de alertas críticas y advertencias. Las alertas están disponibles para los sitios con licencia **Premium**. Las alertas se actualizan automáticamente cada minuto, aunque también se pueden actualizar a petición.

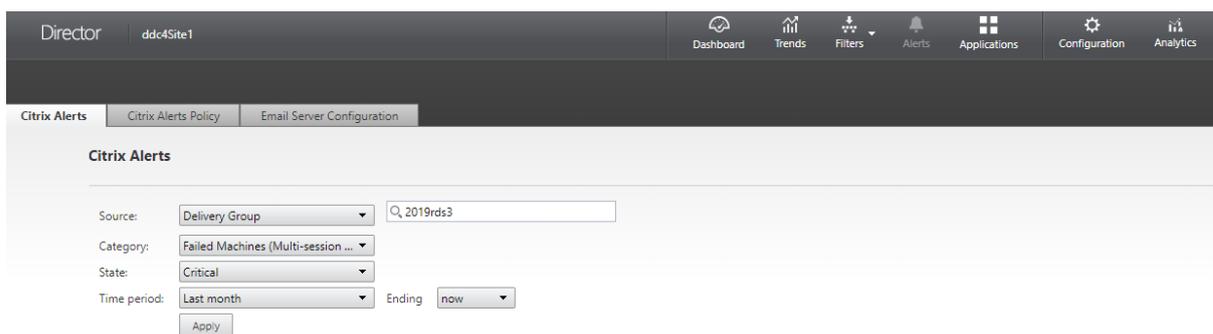


Una alerta de advertencia (un triángulo ámbar) indica que se ha alcanzado o superado el umbral de advertencia de una condición.

Una alerta crítica (un círculo rojo) indica que se ha alcanzado o superado el umbral crítico de una condición.

Puede acceder a información más detallada acerca de las alertas. Para ello, seleccione una alerta de la barra lateral, y haga clic en el enlace **Ir a Alertas** situado en la parte inferior de la barra lateral, o bien, seleccione **Alertas** en la parte superior de la página de Director.

En la vista Alertas, puede filtrar y exportar alertas. Por ejemplo, puede ver las máquinas con sistema operativo multisesión pertenecientes a un grupo de entrega específico que han fallado durante el último mes, o bien puede ver todas las alertas de un usuario concreto. Para obtener más información, consulte [Exportar informes](#).



## Alertas de Citrix

Estas alertas son avisos que se supervisan en Director y que se originan en componentes de Citrix. Puede configurar las alertas de Citrix desde Director, en **Alertas > Directiva de alertas de Citrix**.

Durante la configuración, puede definir las notificaciones que se enviarán por correo electrónico a usuarios y grupos cuando las alertas superen los umbrales que haya configurado. Para obtener más información sobre la configuración de alertas de Citrix, consulte [Crear directivas de alertas](#).

## Directivas de alertas inteligentes

Dispone de un conjunto de directivas de alertas integradas con valores de umbral predefinidos para el ámbito Grupos de entrega y el ámbito VDA con SO multisesión. Esta función requiere Delivery Controllers 7.18 o posterior. Puede modificar los parámetros de umbral de las directivas de alertas integradas en **Alertas > Directiva de alertas de Citrix**.

Las directivas de alertas integradas se crean cuando hay al menos un objetivo de alerta: un grupo de entrega o un VDA de SO multisesión definido en el sitio. Además, estas alertas integradas se agregan automáticamente a un nuevo grupo de entrega o a un VDA de SO multisesión.

En caso de que actualice Director y el sitio, se transfieren las directivas de alertas provenientes de la instancia anterior de Director. Las directivas de alertas integradas se crean solo si no existen reglas de alertas correspondientes en la base de datos de supervisión.

Para conocer los valores de umbral que tienen las directivas de alertas integradas, consulte la sección [Condiciones para directivas de alertas](#).

## Alertas de SCOM

Las alertas de SCOM muestran información de alertas de Microsoft System Center 2012 Operations Manager (SCOM). Con ellas, se ofrece información más detallada acerca del estado y el rendimiento

del centro de datos desde Director. Para obtener más información, consulte [Configurar la integración de SCOM](#).

La cantidad de alertas que aparecen junto a los iconos de alertas antes de expandir la barra lateral es la suma de las alertas de SCOM y Citrix.

## Crear directivas de alertas

The screenshot shows the 'Multi-session OS Policy' configuration page in Citrix Director. It includes a 'Back to Alert Policies' link, input fields for 'Name of Alert' and 'Description', and a 'Scope' field set to 'No Multi-session OS Machines assigned'. The 'Conditions' section is expanded to show 'Peak Connected Sessions' with 'Warning' and 'Critical' thresholds and a 'Re-alert interval' of 60 minutes. A 'Notifications preferences' section is also present with an 'Add' button.

Para crear una nueva directiva de alertas (por ejemplo, para que se genere una alerta cuando se cumple un conjunto concreto de criterios referentes al recuento de sesiones):

1. Vaya a **Alertas > Directiva de alertas de Citrix** y seleccione, por ejemplo, la directiva de SO multisesión.
2. Haga clic en **Crear**.
3. Denomine y describa la directiva. A continuación, establezca las condiciones que deben cumplirse para que se active la alerta. Por ejemplo, especifique recuentos críticos y de advertencia para el máximo de sesiones conectadas, el máximo de sesiones desconectadas y el máximo total de sesiones simultáneas. Los valores de advertencia no deben ser superiores a los valores críticos. Para obtener más información, consulte [Condiciones para directivas de alertas](#).
4. Establezca el intervalo de Repetición de alerta. Si se siguen cumpliendo las condiciones de la alerta, esta se activa de nuevo en este intervalo de tiempo y, si lo define en la directiva de alertas, se generará un correo electrónico de notificación. Una alerta descartada no genera ninguna notificación por correo electrónico en el intervalo de repetición de alerta.
5. Establezca el Ámbito. Por ejemplo, defínala para un grupo de entrega determinado.
6. En las preferencias de notificación, especifique a quién debe notificarse por correo electrónico cuando se active la alerta. Debe especificar un servidor de correo electrónico en la ficha **Config-**

**uración del servidor de correo electrónico** para poder establecer preferencias de notificación en las directivas de alertas.

7. Haga clic en **Guardar**.

Crear una directiva con 20 o más grupos de entrega definidos en el ámbito puede llevar aproximadamente 30 segundos en completar la configuración. Aparece un cursor giratorio durante este tiempo.

Crear más de 50 directivas para un máximo de 20 grupos de entrega distintos (1000 grupos de entrega de destino en total) puede hacer que aumente el tiempo de respuesta (más de 5 segundos).

Mover una máquina que contiene sesiones activas desde un grupo de entrega a otro puede provocar alertas de grupo de entrega erróneas, al estar definidas mediante parámetros de máquina.

## Condiciones para directivas de alertas

A continuación, dispone de las categorías de alertas, las acciones recomendadas para mitigar la alerta y las condiciones de directiva integrada, si están definidas. Las directivas de alertas integradas se definen para alertar cada 60 minutos.

### Pico de sesiones conectadas

- En Director, consulte la vista “Tendencias de sesiones” para ver la cantidad máxima de sesiones conectadas.
- Compruebe que haya capacidad suficiente para admitir la carga de las sesiones.
- Agregue más máquinas, si fuera necesario.

### Pico de sesiones desconectadas

- En Director, consulte la vista “Tendencias de sesiones” para ver la cantidad máxima de sesiones desconectadas.
- Compruebe que haya capacidad suficiente para admitir la carga de las sesiones.
- Agregue más máquinas, si fuera necesario.
- Cierre sesiones desconectadas, si fuera necesario.

### Pico de total de sesiones simultáneas

- En Director, consulte la vista “Tendencias de sesiones” para ver la cantidad máxima de sesiones simultáneas.
- Compruebe que haya capacidad suficiente para admitir la carga de las sesiones.

- Agregue más máquinas, si fuera necesario.
- Cierre sesiones desconectadas, si fuera necesario.

## CPU

El porcentaje de uso de CPU indica el consumo general de CPU en el VDA, incluido el de los procesos. Puede obtener más información sobre la utilización de CPU por parte de procesos individuales en la página **Detalles de la máquina** del VDA correspondiente.

- Vaya a **Detalles de la máquina > Ver utilización histórica > 10 procesos principales** para identificar los procesos que consumen CPU. Compruebe que la directiva de supervisión de procesos esté habilitada para iniciar la recopilación de estadísticas de uso de recursos a nivel de procesos.
- Finalice el proceso, si fuera necesario.
- Finalizar el proceso provocará la pérdida de los datos que no se hayan guardado.
- Si todo funciona según lo previsto, agregue más recursos de CPU en el futuro.

### Nota:

De forma predeterminada, la configuración de directiva **Habilitar supervisión de recursos** está habilitada para supervisar los contadores de rendimiento de memoria y CPU en máquinas con agentes VDA. Si esta configuración de directiva está inhabilitada, las alertas que tengan condiciones de memoria y CPU no se activarán. Para obtener más información, consulte [Configuraciones de directiva de Supervisión](#).

### Condiciones para directivas inteligentes:

- **Ámbito:** Grupo de entrega, SO multisesión
- **Valores de umbral:** Advertencia (80%), Crítico (90%)

## Memoria

El porcentaje de uso de memoria indica el consumo general de memoria en el VDA, incluido el de los procesos. Puede obtener más información sobre el uso de memoria por parte de procesos individuales en la página **Detalles de la máquina** del VDA correspondiente.

- Vaya a **Detalles de la máquina > Ver utilización histórica > 10 procesos principales** para identificar los procesos que consumen memoria. Compruebe que la directiva de supervisión de procesos esté habilitada para iniciar la recopilación de estadísticas de uso de recursos a nivel de procesos.

- Finalice el proceso, si fuera necesario.
- Finalizar el proceso provocará la pérdida de los datos que no se hayan guardado.
- Si todo funciona según lo previsto, agregue más capacidad de memoria en el futuro.

Nota:

De forma predeterminada, la configuración de directiva **Habilitar supervisión de recursos** está habilitada para supervisar los contadores de rendimiento de memoria y CPU en máquinas con agentes VDA. Si esta configuración de directiva está inhabilitada, las alertas que tengan condiciones de memoria y CPU no se activarán. Para obtener más información, consulte [Configuraciones de directiva de Supervisión](#).

### Condiciones para directivas inteligentes:

- **Ámbito:** Grupo de entrega, SO multisesión
- **Valores de umbral:** Advertencia (80%), Crítico (90%)

### Tasa de fallos de conexión

Porcentaje de fallos de conexión durante la última hora.

- Se calcula a partir del total de fallos según el total de intentos de conexión.
- En Director, consulte la vista “Tendencias de fallos de conexión” para ver eventos registrados en el registro de configuración.
- Determine si las aplicaciones o los escritorios son accesibles.

### Recuento de fallos de conexión

Cantidad de fallos de conexión durante la última hora.

- En Director, consulte la vista “Tendencias de fallos de conexión” para ver eventos registrados en el registro de configuración.
- Determine si las aplicaciones o los escritorios son accesibles.

### RTT de ICA (promedio)

Tiempo medio de ida y vuelta del protocolo Independent Computing Architecture.

- Consulte Citrix ADM para ver un desglose del RTT de ICA para determinar la causa raíz. Para obtener más información, consulte la documentación de [Citrix ADM](#).

- Si Citrix ADM no está disponible, consulte la vista “Detalles del usuario” de Director para ver los tiempos de ida y vuelta (RTT) de ICA y la latencia, y determinar si se trata de un problema de red o de aplicaciones o escritorios.

### **RTT de ICA (n.º de sesiones)**

Cantidad de sesiones que superan el umbral de tiempos de ida y vuelta (RTT) de ICA.

- Consulte Citrix ADM para ver la cantidad de sesiones que tienen tiempos RTT de ICA altos. Para obtener más información, consulte la documentación de [Citrix ADM](#).
- Si Citrix ADM no está disponible, contacte con el equipo de red para determinar con ellos la causa del problema.

#### **Condiciones para directivas inteligentes:**

- **Ámbito:** Grupo de entrega, SO multisesión
- **Valores de umbral:** Advertencia (300 ms para 5 sesiones o más), Crítico (400 ms para 10 sesiones o más)

### **RTT de ICA (% de sesiones)**

Porcentaje de sesiones que superan el tiempo medio de ida y vuelta de ICA.

- Consulte Citrix ADM para ver la cantidad de sesiones que tienen tiempos RTT de ICA altos. Para obtener más información, consulte la documentación de [Citrix ADM](#).
- Si Citrix ADM no está disponible, contacte con el equipo de red para determinar con ellos la causa del problema.

### **RTT de ICA (usuario)**

El tiempo de ida y vuelta de ICA que se aplica a las sesiones iniciadas por el usuario especificado. La alerta se activa si el tiempo RTT de ICA supera el umbral en al menos una sesión.

### **Máquinas fallidas (SO de sesión única)**

Cantidad de máquinas fallidas con SO de sesión única. Los errores pueden ocurrir por diversos motivos, como se muestra en las vistas Panel de mandos y Filtros de Director.

- Ejecute diagnósticos de Citrix Scout para determinar la causa principal. Para obtener más información, consulte [Solucionar problemas de usuarios](#).

#### **Condiciones para directivas inteligentes:**

- **Ámbito:** Grupo de entrega
- **Valores de umbral:** Advertencia (1), Crítico (2)

### **Máquinas fallidas (SO multisesión)**

Cantidad de máquinas fallidas de SO multisesión. Los errores pueden ocurrir por diversos motivos, como se muestra en las vistas Panel de mandos y Filtros de Director.

- Ejecute diagnósticos de Citrix Scout para determinar la causa principal.

#### **Condiciones para directivas inteligentes:**

- **Ámbito:** Grupo de entrega, SO multisesión
- **Valores de umbral:** Advertencia (1), Crítico (2)

### **Promedio de duración de inicio de sesión**

Duración media de los inicios de sesión que se han producido durante la última hora.

- Consulte el panel de mandos de Director para obtener métricas actualizadas sobre la duración de los inicios de sesión. Si una gran cantidad de usuarios intenta iniciar sesión en un corto período de tiempo, el tiempo que tardan los inicios de sesión puede alargarse.
- Consulte la referencia y el desglose de los inicios de sesión para determinar la causa. Para obtener más información, consulte [Diagnosticar problemas de inicio de sesión de los usuarios](#).

#### **Condiciones para directivas inteligentes:**

- **Ámbito:** Grupo de entrega, SO multisesión
- **Valores de umbral:** Advertencia (45 segundos), Crítico (60 segundos)

### **Duración de inicio de sesión (Usuario)**

La duración de los inicios de sesión de un usuario especificado que tuvieron lugar durante la pasada hora.

### **Índice de patrón de carga**

Valor del Índice de patrón de carga en los últimos 5 minutos.

- Consulte Director para ver las máquinas con sistema operativo multisesión que puedan tener un máximo de carga. Consulte el panel de mandos (para ver errores) y el informe de tendencias en el índice del patrón de carga.

**Condiciones para directivas inteligentes:**

- **Ámbito:** Grupo de entrega, SO multisesión
- **Valores de umbral:** Advertencia (80%), Crítico (90%)

**Supervisar alertas de hipervisor**

Director muestra alertas para supervisar el estado del hipervisor. Las alertas de Citrix Hypervisor y VMware vSphere ayudan a supervisar los parámetros y estados del hipervisor. El estado de conexión al hipervisor también se supervisa, y se genera una alerta si el clúster o el grupo de hosts se reinicia o no está disponible.

Para recibir las alertas de hipervisor, compruebe que se haya creado una conexión de alojamiento en Citrix Studio. Para obtener más información, consulte [Conexiones y recursos](#). Solo se supervisan estas conexiones para las alertas de hipervisor. En la tabla siguiente se describen los distintos parámetros y estados de las alertas de hipervisor.

Alerta	Hipervisores compatibles	Desencadenada por	Condición	Configuración
Uso de CPU	Citrix Hypervisor, VMware vSphere	Hipervisor	Se alcanza o supera el umbral de alerta que tiene el consumo de CPU.	Los umbrales de alerta deben configurarse en el hipervisor.
Uso de memoria	Citrix Hypervisor, VMware vSphere	Hipervisor	Se alcanza o supera el umbral de alerta que tiene el consumo de memoria.	Los umbrales de alerta deben configurarse en el hipervisor.
Uso de la red	Citrix Hypervisor, VMware vSphere	Hipervisor	Se alcanza o supera el umbral de alerta que tiene el uso de la red.	Los umbrales de alerta deben configurarse en el hipervisor.
Uso del disco	VMware vSphere	Hipervisor	Se alcanza o supera el umbral de alerta que tiene el uso del disco.	Los umbrales de alerta deben configurarse en el hipervisor.

Alerta	Hipervisores compatibles	Desencadenada por	Condición	Configuración
Conexión de host o estado de energía	VMware vSphere	Hipervisor	El host del hipervisor se ha reiniciado o no está disponible.	Las alertas están preintegradas en VMware vSphere. No se necesita ninguna configuración adicional.
Conexión de hipervisor no disponible.	Citrix Hypervisor, VMware vSphere	Delivery Controller	La conexión con el hipervisor (grupo o clúster) se pierde, se apaga o se reinicia. Esta alerta se genera cada hora mientras la conexión no esté disponible.	Las alertas están preintegradas en el Delivery Controller. No se necesita ninguna configuración adicional.

**Nota:**

Para obtener más información sobre la configuración de alertas, consulte [Alertas de Citrix Xen-Center](#) o la documentación sobre alertas de VMware vCenter.

La preferencia de notificación por correo electrónico se puede configurar en **Directiva de alertas de Citrix > Directiva de sitio > Estado del hipervisor**. Las condiciones de umbral para las directivas de alertas del hipervisor se pueden configurar, modificar, inhabilitar o eliminar únicamente desde el hipervisor, no desde Director. Sin embargo, en Director se pueden modificar las preferencias de correo electrónico y se puede descartar una alerta.

**Importante:**

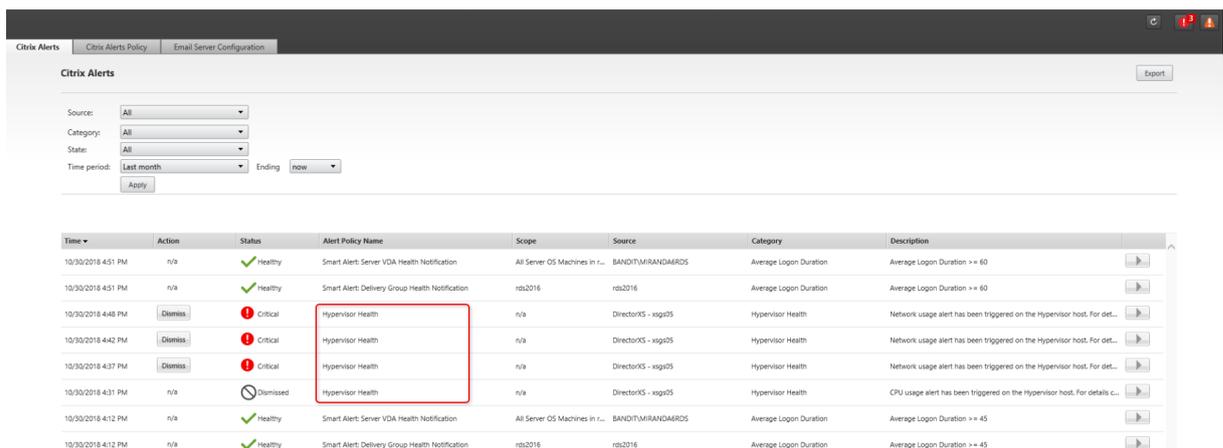
- Las alertas activadas por el hipervisor se obtienen y se muestran en Director. Sin embargo, los cambios en el ciclo de vida o el estado de las alertas del hipervisor no se reflejan en Director.
- Las alertas descartadas, inhabilitadas o las que indican un estado correcto en la consola del hipervisor seguirán apareciendo en Director y deberán descartarse explícitamente.
- Las alertas que se descartan en Director no se descartan automáticamente en la consola

del hipervisor.



Se ha agregado una nueva categoría de alerta denominada **Estado del hipervisor** para habilitar el filtrado únicamente de las alertas del hipervisor. Estas alertas se muestran una vez que se alcanzan o superan los umbrales. Las alertas del hipervisor pueden ser:

- **Crítico:** Se ha alcanzado o superado el umbral crítico de la directiva de alertas del hipervisor.
- **Advertencia:** Se ha alcanzado o superado el umbral de advertencia de la directiva de alertas del hipervisor.
- **Descartado:** La alerta ya no se muestra como activa.



Esta función requiere Delivery Controller 7 1811 o posterior. Si utiliza una versión anterior de Director con la versión 7 1811 o más reciente del sitio, solo se muestra el recuento de alertas del hipervisor. Para ver las alertas, debe actualizar Director.

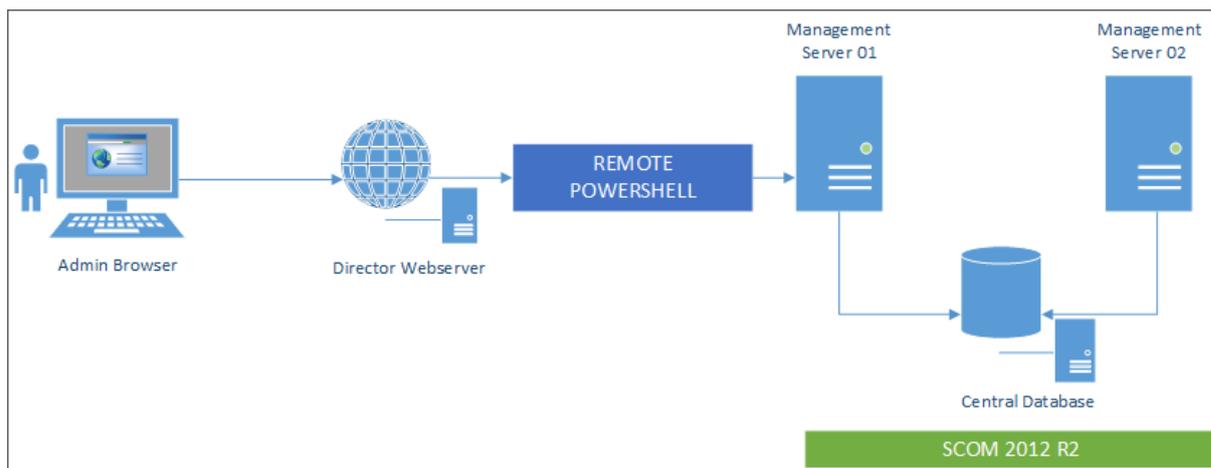
## Configurar la integración de alertas de SCOM

La integración de SCOM con Director permite ver la información de alertas provenientes de SCOM en el panel de mandos y en otras vistas de alto nivel de Director.

Las alertas de SCOM se muestran junto a las alertas de Citrix. Puede acceder y consultar los detalles de las alertas de SCOM. Para ello, vaya a la ficha SCOM, situada en la barra lateral.

Puede ver el historial de alertas que datan, como máximo, del mes anterior. Asimismo, puede ordenar, filtrar y exportar la información filtrada a informes en formatos CSV, Excel y PDF. Para obtener más información, consulte [Exportar informes](#).

La integración de SCOM usa PowerShell 3.0 (o una versión posterior) de forma remota para consultar datos del servidor de administración de SCOM y mantiene una conexión persistente en el espacio de ejecución de la sesión de usuario en Director. Director y el servidor SCOM deben tener la misma versión de PowerShell.



Los requisitos para la integración de SCOM son:

- Windows Server 2012 R2
- System Center 2012 R2 Operations Manager
- PowerShell 3.0 o una versión posterior (las versiones de PowerShell en Director y en el servidor SCOM deben coincidir)
- CPU de cuatro núcleos con 16 GB de RAM (recomendado)
- Debe configurarse un servidor de administración principal para SCOM en el archivo web.config de Director. Puede hacerlo mediante la herramienta DirectorConfig.

Citrix recomienda que la cuenta de administrador de Director se configure como rol de Operador de SCOM, para que los administradores puedan obtener información completa de alertas en Director. Si no es posible, se puede configurar una cuenta de administrador de SCOM en el archivo web.config mediante la herramienta DirectorConfig.

Para un rendimiento óptimo, Citrix recomienda no configurar más de 10 administradores de Director por servidor de administración de SCOM.

En el servidor de Director:

1. Escriba **Enable-PSRemoting** para habilitar la comunicación remota de PowerShell.
2. Agregue el servidor de administración de SCOM a la lista TrustedHosts. Abra un símbolo del sistema de PowerShell y ejecute los siguientes comandos:

- Obtenga la lista actual de TrustedHosts

```
Get-Item WSMAN:\localhost\Client\TrustedHosts
```

- Agregue el nombre de dominio completo (FQDN) del servidor de administración de SCOM a la lista TrustedHosts. <Old Values> representa el conjunto de entradas existentes devuelto por el cmdlet Get-Item.

```
Set-Item WSMAN:localhostClientTrustedHosts -Value "<FQDN del servidor de administración de SCOM>,<Old Values>"
```

3. Configure SCOM mediante la herramienta DirectorConfig.

```
C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configscom
```

En el servidor de administración de SCOM:

1. Asigne administradores de Director al rol de administrador de SCOM.
  - a) Abra la consola de administración de SCOM y vaya a **Administración > Seguridad > Funciones de usuario**.
  - b) En “Funciones de usuario”, puede crear un rol de usuario o modificar uno existente. Existen cuatro categorías de roles de operador de SCOM que definen la clase de acceso a los datos de SCOM. Por ejemplo, un rol de Solo lectura no verá el panel Administración y no podrá detectar ni administrar reglas, máquinas o cuentas. Un rol de Operador de SCOM es un rol de administrador total.

Nota:

Las operaciones siguientes no están disponibles si se asigna un rol que no sea Operador al administrador de Director:

- 1 > - If there are multiple management servers configured and the primary management server is not available, the Director administrator cannot connect to the secondary management server . The primary management server is the server configured in the Director web.config file, that is the same server as the one specified with the DirectorConfig tool in step 3 above. The secondary management servers are peer management servers of the primary server.
- 2 > - While filtering alerts, the Director administrator cannot search **for** the alert source. This requires an operator level permission.

- a) Para modificar un Rol de usuario, haga clic con el botón secundario en el rol y, a continuación, haga clic en las **Propiedades**.
- b) En el cuadro de diálogo “Propiedades de función de usuario”, puede agregar o quitar administradores de Director que tengan la función de usuario especificada.

2. Agregue administradores de Director al grupo Usuarios de administración remota en el servidor de administración de SCOM. Esto permite a los administradores de Director establecer una conexión remota con PowerShell.
3. Escriba **Enable-PSRemoting** para habilitar la comunicación remota de PowerShell.
4. Establezca los límites de las propiedades de WS-Management:

- a) Modifique MaxConcurrentUsers:

En la interfaz de línea de comandos:

```
“winrm set winrm/config/winrs @{MaxConcurrentUsers = “20”}
```

```
1 En PowerShell:
2
3 ``Set -Item WSMAN:\localhost\Shell\MaxConcurrentUsers 20<!--
   NeedCopy-->
```

- b) Modifique MaxShellsPerUser:

En la interfaz de línea de comandos:

```
winrm set winrm/config/winrs @{ MaxShellsPerUser="20"} <!--
NeedCopy-->
```

En PowerShell:

```
“Set-Item WSMAN:\localhost\Shell\MaxShellsPerUser 20
```

```
1 1. Modifique MaxMemoryPerShellMB:
2
3 En la interfaz de línea de comandos:
4
5 ``winrm set winrm/config/winrs @{
6 MaxMemoryPerShellMB="1024" }
7 <!--NeedCopy-->
```

```
1 En PowerShell:
```

```
Set-Item WSMAN:\localhost\Shell\MaxMemoryPerShellMB 1024<!--
NeedCopy-->
```

5. Para que la integración de SCOM funcione en entornos de dominios mixtos, configure la siguiente entrada del Registro.

Ruta: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Clave: LocalAccountTokenFilterPolicy

Tipo: DWORD

Valor: 1

**Precaución:** Una modificación incorrecta del Registro puede provocar problemas graves, que pueden obligar a la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Una vez configurada la integración de SCOM, es posible que aparezca el mensaje “No se pueden obtener las alertas recientes de SCOM. Revise los registros de eventos del servidor de Director para obtener más información”. Los registros de eventos del servidor ayudarán a identificar y corregir el problema. Las causas pueden ser:

- Pérdida de conectividad de red a la máquina de SCOM o Director.
- El servicio de System Center Operations Manager no está disponible o está demasiado ocupado para responder.
- Error de autorización debido a un cambio en los permisos del usuario configurado.
- Un error en Director al procesar datos de SCOM.
- Las versiones de PowerShell en Director y en el servidor SCOM no coinciden.

## Filtrar datos para solucionar fallos

March 31, 2021

Cuando haga clic en números en el panel de mandos o seleccione un filtro predefinido desde el menú Filtros, la vista Filtros se abre y muestra los datos en función de la máquina seleccionada o del tipo de fallo.

Los filtros predefinidos no se pueden modificar, pero puede guardar un filtro predefinido como un filtro personalizado y, a continuación, modificarlo. Además, puede crear vistas con filtros personalizados de máquinas, conexiones, sesiones e instancias de aplicación en todos los grupos de entrega.

### 1. Seleccione una vista:

- **Máquinas.** Seleccione Máquinas con SO de sesión única o Máquinas con SO multisesión. Estas vistas muestran la cantidad de máquinas configuradas. La ficha Máquinas con SO multisesión también incluye el índice del patrón de carga. Este índice indica la distribución de contadores de rendimiento, así como información sobre herramientas del recuento de sesiones si pasa el puntero sobre el vínculo.
- **Sesiones.** También puede ver el recuento de sesiones desde la vista Sesiones. Use las mediciones del tiempo de inactividad para identificar las sesiones que estén inactivas transcurrido un cierto período de tiempo.

- **Conexiones.** Filtre conexiones por distintos períodos de tiempo, incluidos los últimos 60 minutos, las últimas 24 horas o los últimos 7 días.
- **Instancias de aplicación.** Esta vista muestra las propiedades de todas las instancias de aplicación que haya en los VDA con SO de servidor y con SO de sesión única. Las métricas del tiempo de inactividad de la sesión están disponibles para las instancias de aplicación en los VDA de SO multisesión.

**Nota:**

Si ha iniciado sesiones de escritorio en los VDA instalados en un equipo con Windows 10 1809, el Administrador de actividades de Director puede, en ocasiones, mostrar Microsoft Edge y Office como aplicaciones activas cuando, en realidad, solo se ejecutan en segundo plano.

2. En **Filtrar por**, seleccione un criterio de filtro.
3. Utilice las fichas adicionales para cada vista, según sea necesario, para completar el filtro.
4. Seleccione columnas adicionales, según sea necesario, para solucionar problemas más complejos.
5. Guarde el filtro y cámbiele el nombre.
6. Para acceder a los filtros desde múltiples servidores de Director, almacene los filtros en una carpeta compartida accesible desde esos servidores:
  - Las cuentas del servidor de Director deben tener permiso para modificar la carpeta compartida.
  - Los servidores de Director deben configurarse con acceso a la carpeta compartida. Para ello, ejecute el **Administrador de IIS**. En Sitios > Sitio web predeterminado > Director > Parámetros de la aplicación, modifique el parámetro **Service.UserSettingsPath** para reflejar la ruta UNC de la carpeta compartida.
7. Para abrir el filtro más adelante, en el menú **Filtros**, seleccione el tipo de filtro (Máquinas, Sesiones, Conexiones o Instancias de aplicaciones) y, a continuación, seleccione el filtro guardado.
8. Haga clic en **Exportar** para exportar los datos a archivos en formato CSV. Se pueden exportar datos de hasta 100 000 registros. Esta función está disponible en Delivery Controller 1808 y versiones posteriores.
9. Si es necesario, para las vistas **Máquinas** o **Conexiones**, use los controles de energía para todas las máquinas que seleccione en la lista filtrada. Para la vista Sesiones, utilice los controles de sesión u opciones para enviar mensajes.
10. En las vistas **Máquinas** y **Conexiones**, haga clic en **Motivo del fallo** de la máquina o conexión donde se ha producido el error para obtener una descripción detallada del error y las acciones

recomendadas para solucionarlo. Los motivos de los errores y las acciones recomendadas para fallos de máquinas y conexiones están disponibles en [Citrix Director 7.12 Failure Reasons Troubleshooting Guide](#).

11. En la vista **Máquinas**, haga clic en un enlace del nombre de la máquina para ir a la página correspondiente de **Detalles de la máquina**. Esta página muestra los datos de la máquina, ofrece controles de alimentación, y muestra gráficos de CPU, memoria, supervisión de disco y supervisión de GPU. Además, puede hacer clic en **Ver utilización histórica** para ver las tendencias de utilización de los recursos en la máquina. Para obtener más información, consulte [Solucionar problemas de máquinas](#).
12. En la vista **Instancias de aplicación**, ordene o filtre en función del **Tiempo de inactividad** superior al período de tiempo del umbral. Seleccione las instancias de aplicación inactivas que quiere finalizar. Cerrar o desconectar una instancia de aplicación finaliza todas las instancias de aplicación activas que haya en la misma sesión. Para obtener más información, consulte [Solucionar problemas de aplicaciones](#). La página de filtro “Instancias de aplicaciones” y las mediciones del tiempo de inactividad en la página de filtro “Sesiones” están disponibles si Director, los Delivery Controllers y los agentes VDA son de la versión 7.13 o posterior.

**Nota:**

Citrix Studio permite la asignación de varias reglas de asignación de escritorios (DAR) para distintos usuarios o grupos de usuarios a un solo VDA en el grupo de entrega. StoreFront muestra el escritorio asignado con el nombre simplificado correspondiente a las reglas DAR para el usuario que ha iniciado sesión. Sin embargo, Director no admite las reglas de asignación de escritorios y, por tanto, muestra el escritorio asignado mediante el nombre del grupo de entrega, sin tener en cuenta qué usuario está conectado a la sesión. Como resultado de ello, no se puede asignar un escritorio específico a una máquina en Director. Para asignar el escritorio asignado que se muestra en StoreFront al nombre del grupo de entrega que se muestra en Director, use el siguiente comando de PowerShell:

```
1 Get-BrokerDesktopGroup | Where-Object {
2   $_.Uid -eq (Get-BrokerAssignmentPolicyRule | Where-Object {
3     $_.PublishedName -eq "<Name on StoreFront>" }
4   ).DesktopGroupUid }
5   | Select-Object -Property Name, Uid
6 <!--NeedCopy-->
```

## Supervisar tendencias históricas en un sitio

September 22, 2021

En la vista “Tendencias”, verá la información histórica sobre tendencias de sesiones, fallos de conexión, fallos de máquinas, rendimiento de los inicios de sesión, evaluación de la carga, administración de capacidad, uso de máquinas, utilización de recursos y análisis de red para cada sitio. Para buscar esta información, haga clic en el menú **Tendencias**.

La función de consulta detallada de datos permite navegar entre los gráficos de tendencias, acercarse al gráfico para ver en detalle un período de tiempo concreto (haciendo clic en un punto de datos en el gráfico) y consultar los detalles asociados a la tendencia. Esta función permite comprender mejor qué o quién se ve afectado por las tendencias que se muestran.

Para cambiar el ámbito predeterminado de cada gráfico, aplique un filtro distinto a los datos.

Elija el período de tiempo del que quiere obtener información histórica sobre tendencias. La disponibilidad de un período de tiempo depende de la implementación de Director, como se indica a continuación:

- En los sitios con licencia Premium, están disponibles los informes de tendencias del último año (365 días) como máximo.
- En los sitios con licencia Advanced, están disponibles los informes de tendencias del último mes (31 días) como máximo.
- Informes de tendencias de hasta los últimos 7 días en sitios sin licencia Premium ni Advanced.

**Nota:**

- En todas las implementaciones de Director, la información de tendencias referentes a sesiones, fallos y rendimiento de inicios de sesión está representada en gráficos y tablas cuando el período de tiempo es “Último mes” (**hasta el día de hoy**) o menos. Cuando el período de tiempo es “Último mes” (con una fecha de finalización personalizada) o “Último año”, la información de tendencias se representa en gráficos, pero no en tablas.
- Con los valores de la retención de limpieza de Monitor Service, se controla la disponibilidad de los datos de las tendencias. Los valores predeterminados están disponibles en [Granularidad y retención de datos](#). Los clientes de los sitios con licencia Premium pueden cambiar la retención de la limpieza de datos a la cantidad de días de retención que quieran.
- Los siguientes parámetros en el Administrador de IIS controlan el intervalo de las fechas de finalización personalizadas disponibles para la selección. Estos parámetros se pueden personalizar. Sin embargo, la disponibilidad de los datos para las fechas seleccionadas depende del parámetro de retención de la limpieza para la métrica específica que mide.

Parámetro	Valores predeterminados
UI.TrendsLast2HoursRange	3
UI.TrendsLast24HoursRange	32

---

Parámetro	Valores predeterminados
UI.TrendsLast7DaysRange	32
UI.TrendsLastMonthRange	365

---

## Tendencias disponibles

**Ver tendencias de sesiones:** En la ficha Sesiones, seleccione el grupo de entrega y el período de tiempo para ver información más detallada sobre el recuento de sesiones simultáneas.

La columna **Reconexión automática de sesión** muestra la cantidad de reconexiones automáticas en una sesión. La reconexión automática se habilita cuando las directivas de fiabilidad de la sesión o de reconexión automática del cliente están activas. Cuando hay una interrupción de la red en el dispositivo de punto final, entran en vigor las siguientes directivas:

- La fiabilidad de la sesión se activa (de forma predeterminada durante 3 minutos) cuando la aplicación Citrix Receiver o Citrix Workspace intenta conectarse al VDA.
- La reconexión automática del cliente surte efecto entre 3 y 5 minutos cuando el cliente intenta conectarse al VDA.

Ambas reconexiones se capturan y se muestran al usuario. Esta información puede tardar un tiempo máximo de 5 minutos en aparecer en la interfaz de usuario de Director después de que se haya producido la reconexión.

La información de reconexión automática le ayuda a ver y solucionar problemas de conexión de red que sufren interrupciones, así como a analizar las redes que tienen una experiencia fluida y sin problemas. Puede ver la cantidad de reconexiones de un grupo de entrega específico o un período de tiempo que haya seleccionado en los filtros. Un desglose proporciona información adicional, como la fiabilidad de la sesión o la reconexión automática del cliente, las marcas de tiempo, la dirección IP del dispositivo de punto final o el nombre de la máquina de punto final en la que está instalada la aplicación Workspace. De forma predeterminada, los registros se ordenan por las marcas de tiempo del evento en orden descendente. Esta función está disponible para la aplicación Citrix Workspace para Windows, la aplicación Citrix Workspace para Mac, Citrix Receiver para Windows y Citrix Receiver para Mac. Esta función requiere la versión 7 1906 de Delivery Controller o una posterior y la versión 1906 de VDA o una posterior. Para obtener más información acerca de la reconexión de sesiones, consulte [Sesiones](#). Para obtener más información, consulte [Configuraciones de directiva de Reconexión automática de clientes](#) y [Configuraciones de directiva de Fiabilidad de la sesión](#).

A veces, es posible que los datos de reconexión automática no aparezcan en Director por los siguientes motivos:

- La aplicación Workspace no envía los datos de reconexión automática al VDA.

- El VDA no envía datos al servicio de supervisión.
- Los Delivery Controllers descartan las cargas útiles de VDA ya que es posible que no tengan las sesiones correspondientes.

Nota:

A veces, es posible que la dirección IP del cliente no se obtenga correctamente si se establecen ciertas directivas NSG.

**Ver tendencias de fallos de conexión:** En la ficha “Fallos”, seleccione la conexión, el tipo de máquina, el tipo de fallo, el grupo de entrega y el período de tiempo, para ver un gráfico con información más detallada sobre los fallos de conexión de los usuarios en el sitio.

**Ver tendencias de fallos de máquinas:** En la ficha “Fallos de máquina de SO de sesión única” o en la ficha “Fallos de máquina de SO multisesión”, seleccione el tipo de fallo, el grupo de entrega y el período de tiempo, para ver un gráfico con información más detallada sobre los fallos de máquinas en el sitio.

**Ver tendencias del rendimiento de los inicios de sesión:** En la ficha “Rendimiento de inicio de sesión”, seleccione el grupo de entrega y el período de tiempo para ver un gráfico con información más detallada sobre cuánto tardan los inicios de sesión de los usuarios en el sitio, y si la cantidad de inicios de sesión afecta al rendimiento. En esta vista, también se puede ver el promedio de duración de las fases de inicio de sesión, tales como la duración de la intermediación y la hora de inicio de la VM.

Estos datos son específicos para inicios de sesión de usuario y no incluyen a los usuarios que intentan volver a conectarse a sesiones desconectadas.

La tabla que aparece debajo del gráfico muestra la Duración de inicio de sesión por sesión de usuario. Usted puede elegir las columnas que quiere mostrar y ordenar el informe por cualquiera de las columnas.

Para obtener más información, consulte [Diagnosticar problemas de inicio de sesión de los usuarios](#).

**Ver tendencias de evaluación de carga:** En la ficha “Índice de patrón de carga”, dispone de un gráfico con información detallada sobre la carga que se distribuye entre las máquinas con SO multisesión. Las opciones de filtro para este gráfico incluyen: grupo de entrega o máquina con SO multisesión en un grupo de entrega, máquina con SO multisesión (disponible solo si se selecciona Máquina con SO multisesión en un grupo de entrega) y un intervalo.

**Ver uso de aplicaciones alojadas:** La disponibilidad de esta función depende de la licencia que tenga en su organización.

En la ficha “Administración de capacidad”, seleccione la ficha “Uso de aplicaciones alojadas”, el grupo de entrega y el período de tiempo para ver un gráfico con el uso simultáneo en las horas punta y una tabla que muestra el uso de aplicaciones. Desde la tabla de Uso basado en aplicaciones, puede elegir una aplicación específica para ver más detalles y una lista de usuarios que están utilizando, o han usado, la aplicación.

**Ver el uso de SO de sesión única y multisesión:** La vista “Tendencias” muestra el uso del SO de sesión única por sitio y por grupo de entrega. Al seleccionar Sitio, se muestra el uso por grupo de entrega. Cuando se selecciona un grupo de entrega, se muestra el uso por usuario.

La vista Tendencias muestra también el uso del SO multisesión por sitio, por máquina y por grupo de entrega. Al seleccionar Sitio, se muestra el uso por grupo de entrega. Cuando se selecciona un grupo de entrega, se muestra el uso por máquina y por usuario. Cuando se selecciona una máquina, se muestra el uso por usuario.

**Ver uso de máquinas virtuales:** En la ficha Uso de máquinas, seleccione Máquinas con SO de sesión única o Máquinas con SO multisesión para obtener una vista en directo del uso de las máquinas virtuales, lo que le permite hacerse una idea rápidamente de las necesidades de capacidad del sitio.

Disponibilidad de SO de sesión única: Muestra el estado actual de las máquinas de SO de sesión única (VDI) por disponibilidad, para el sitio entero o para un grupo de entrega específico.

Disponibilidad de SO multisesión: Muestra el estado actual de las máquinas de SO multisesión por disponibilidad, para el sitio entero o para un grupo de entrega específico.

**Nota:**

La cantidad de máquinas mostradas en Contadores disponibles incluye máquinas en modo de mantenimiento.

**Ver utilización de recursos:** Para una planificación más precisa de la capacidad, vaya a la ficha Utilización de recursos y seleccione Máquinas con SO de sesión única o Máquinas con SO multisesión para obtener información detallada sobre tendencias históricas de uso de CPU, memoria, IOPS y latencia de disco en cada máquina VDI.

Esta función requiere agentes VDA y Delivery Controllers de la **versión 7.11** o una posterior.

Los gráficos muestran datos sobre el promedio de CPU, el promedio de memoria, el promedio de E/S por segundo, la latencia de disco y el máximo de sesiones simultáneas. Puede explorar en profundidad una máquina para ver datos y gráficos sobre los 10 procesos principales que consumen la CPU. Asimismo, puede filtrar por grupo de entrega y período de tiempo. Los gráficos de CPU, consumo de memoria y pico de sesiones simultáneas están disponibles para las últimas 2 horas, 24 horas, 7 días, mes y año. Los gráficos del promedio de E/S por segundo y la latencia de disco están disponibles para las últimas 24 horas, el último mes y el último año.

**Nota:**

- La configuración de la directiva de Supervisión, [Habilitar supervisión de procesos](#), debe estar establecida en “Permitida” para recopilar y mostrar datos en la tabla “10 procesos principales” de la página “Utilización histórica de máquinas”. De forma predeterminada, la directiva está establecida en “Prohibida”. De forma predeterminada, se recopilan los datos referentes al uso de recursos. Esto se puede inhabilitar mediante [Habilitar supervisión de recursos](#). La tabla situada bajo los gráficos muestra los datos de utilización de recursos por máquina.

- El Promedio de E/S por segundo muestra los promedios diarios. Para indicar el pico de E/S por segundo, se calcula la mayor de las E/S medias para el intervalo de tiempo seleccionado. (Un promedio de E/S por segundo son las operaciones medias de E/S por segundo recopiladas durante una hora en el VDA.)

**Ver datos de análisis de red:** La disponibilidad de esta función depende de la licencia de la organización y los permisos de administrador. Esta función requiere Delivery Controllers **7.11** o de una versión posterior.

Desde la ficha Red, se puede supervisar el análisis de red, que ofrece una vista en contexto de los usuarios, las aplicaciones y los escritorios de la red. Con esta función, Director ofrece un análisis avanzado del tráfico ICA en la implementación, mediante informes de HDX Insight desde Citrix ADM. Para obtener más información, consulte [Configurar el análisis de la red](#).

**Ver fallos de las aplicaciones:** La ficha “Fallos y errores de aplicación” muestra los fallos asociados a las aplicaciones publicadas en los VDA.

Esta función requiere agentes VDA y Delivery Controllers de la **versión 7.15** o posterior. Se admiten los VDA de SO de sesión única con Windows Vista o posterior y los VDA de SO multisesión con Windows Server 2008 o posterior.

Para obtener más información, consulte [Supervisar fallos históricos de aplicaciones](#).

De forma predeterminada, solo se muestran los fallos de aplicaciones en los VDA de SO multisesión. Puede configurar la supervisión de los fallos de aplicación mediante las directivas de Supervisión. Para obtener más información, consulte [Configuraciones de directiva de Supervisión](#).

**Ver resultados del sondeo de aplicaciones:** En la ficha “Resultados del sondeo de aplicaciones”, se muestran los resultados del sondeo de las aplicaciones que se han configurado para el sondeo en la página “Configuración”. En esa página, se registra la fase del inicio durante el que ocurrió el fallo de la aplicación.

Esta función requiere agentes VDA y Delivery Controllers de la **versión 7.18** o posterior. Para obtener más información, consulte [Sondeo de aplicaciones](#).

**Crear informes personalizados:** La ficha “Informes personalizados” ofrece una interfaz de usuario para generar informes personalizados que contienen datos históricos y en tiempo real obtenidos de la base de datos de supervisión en formato tabular.

Esta función requiere Delivery Controllers **7.12** o posterior.

Desde la lista de las consultas de “Informe personalizado” previamente guardadas, puede hacer clic en **Ejecutar y descargar** para exportar un informe en formato CSV, y hacer clic en **Copiar OData** para copiar y compartir la consulta de OData correspondiente, o hacer clic en **Modificar** para modificarla. Puede crear una consulta de informe personalizado en función de las máquinas, las conexiones, las sesiones o las instancias de aplicación. Especifique las condiciones de filtro, que pueden establecerse en función de campos como la máquina, el grupo de entrega o el período de tiempo. Especifique

columnas adicionales necesarias en el informe personalizado. La vista previa muestra un ejemplo de los datos del informe. Si guarda la consulta del informe personalizado, esta se agrega a la lista de consultas guardadas.

Puede crear una nueva consulta de informe personalizado a partir de una consulta de OData copiada. Para ello, seleccione la opción de consulta de OData y pegue la consulta de OData copiada. Puede guardar la consulta resultante para ejecutarla más adelante.

**Nota:**

Los nombres de las columnas en el informe de vista previa y exportación que se generan mediante consultas de OData no están localizados, aparecen en inglés.

Los iconos de marcas del gráfico indican acciones o sucesos significativos para un intervalo de tiempo concreto. Pase el puntero sobre el marcador y haga clic en la lista de sucesos o acciones.

**Nota:**

- Los datos de inicio de sesión de conexiones HDX no se recopilan para versiones del VDA anteriores a 7. Para los VDA anteriores, los datos gráficos se muestran como 0.
- Los grupos de entrega eliminados en Citrix Studio pueden seleccionarse en los filtros de tendencias de Director hasta que los datos relacionados con ellos se hayan limpiado y eliminado. Si se selecciona un grupo de entrega eliminado se muestran gráficos para los datos disponibles durante el período de retención. Sin embargo, las tablas no mostrarán datos.
- Al mover una máquina que contiene sesiones activas de un grupo de entrega a otro, las tablas de **Utilización de recursos e Índice de patrón de carga** del nuevo grupo de entrega muestran métricas consolidadas de ambos grupos de entrega, el antiguo y el nuevo.

## Solucionar problemas de implementaciones

February 6, 2020

Como administrador de asistencia técnica, puede buscar al usuario que informa un problema y ver datos de las sesiones o las aplicaciones asociadas a ese usuario. Del mismo modo, puede buscar máquinas o dispositivos de punto final donde se han producido problemas. Los problemas se pueden resolver rápidamente supervisando las métricas relevantes y realizando las acciones correspondientes. Las acciones disponibles pueden ser: finalizar una aplicación o un proceso que no responde, remedar operaciones en la máquina del usuario, cerrar una sesión que no responde, reiniciar la máquina, colocar una máquina en el modo de mantenimiento o restablecer el perfil del usuario.

## Solucionar problemas de aplicaciones

September 22, 2021

### Análisis de aplicaciones

La vista **Aplicaciones** muestra datos de análisis de aplicaciones en una vista única y consolidada a fin de ayudar a analizar y administrar de forma eficiente el rendimiento de las aplicaciones. Puede obtener información valiosa sobre el estado y el uso de todas las aplicaciones publicadas en el sitio. La vista predeterminada ayuda a identificar las aplicaciones que se ejecutan con mayor frecuencia. Esta función requiere Delivery Controllers 7.16 o posterior y agentes VDA 7.15 o posterior.

Application Name	Probe Result (Last 24 hours)	Instances ↓	Application Faults (Last hour)	Application Errors (Last hour)
APAC Visio 2019	1 Probes Passed	1	0	0
APAC Chrome	1 Probes Passed	1	0	0
APAC XenCenter7	1 out of 4 probe	1	0	0
APAC XenRtCenter	n/a	1	0	0
APAC Citrix Videos	n/a	0	0	0
APAC Firefox	n/a	0	0	0

Summary of Application Probe Failures (Last 24 hours)

Application Probes

- Probe Endpoints
- StoreFront Reachability: No Failure
- StoreFront Authentication: No Failure
- StoreFront Enumeration: No Failure
- ICA File Download: No Failure
- Application Launch: No Failure

En la columna **Resultado del sondeo**, se muestra el resultado del sondeo de aplicaciones ejecutado en las últimas 24 horas. Haga clic en el enlace de resultados del sondeo para ver más datos en la página **Tendencias > Resultados del sondeo de aplicaciones**. Para obtener más información sobre cómo configurar los sondeos de aplicaciones, consulte [Sondeo de aplicaciones](#).

La columna **Instancias** muestra el uso de las aplicaciones. Indica la cantidad de instancias de aplicación que se ejecutan en ese momento (instancias conectadas y desconectadas). Para solucionar problemas complejos, haga clic en el campo **Instancias** para ver la página de filtros de **Instancias de aplicación** correspondientes. En ella, puede seleccionar las instancias de aplicación que se van a cerrar o desconectar.

#### Nota:

Para los administradores con ámbito personalizado, Director no muestra las instancias de aplicación creadas en Grupos de aplicaciones. Para ver todas las instancias de aplicación, debe ser administrador total. Para obtener más información, consulte el artículo [CTX256001](#) de Knowl-

edge Center.

Puede supervisar el estado de las aplicaciones publicadas en el sitio con las columnas **Fallos de aplicación** y **Errores de aplicación**. Esas columnas muestran la cantidad total de fallos y errores que se han producido mientras se iniciaba la aplicación en cuestión durante la última hora. Haga clic en el campo **Fallos de aplicación** o **Errores de aplicación** para ver datos sobre los fallos y errores en la página **Tendencias > Fallos y errores de aplicación** que corresponde a la aplicación seleccionada.

La disponibilidad y la presentación de los fallos y los errores se define con las configuraciones de directiva de fallos de aplicación. Para obtener más información acerca de las directivas y cómo modificarlas, consulte [Directivas para supervisar fallos de aplicación](#) en “Configuraciones de directiva de Supervisión”.

## Supervisar aplicaciones en tiempo real

Puede solucionar las aplicaciones y las sesiones con la ayuda de métricas de inactividad para identificar las instancias que llevan inactivas más de un límite de tiempo concreto.

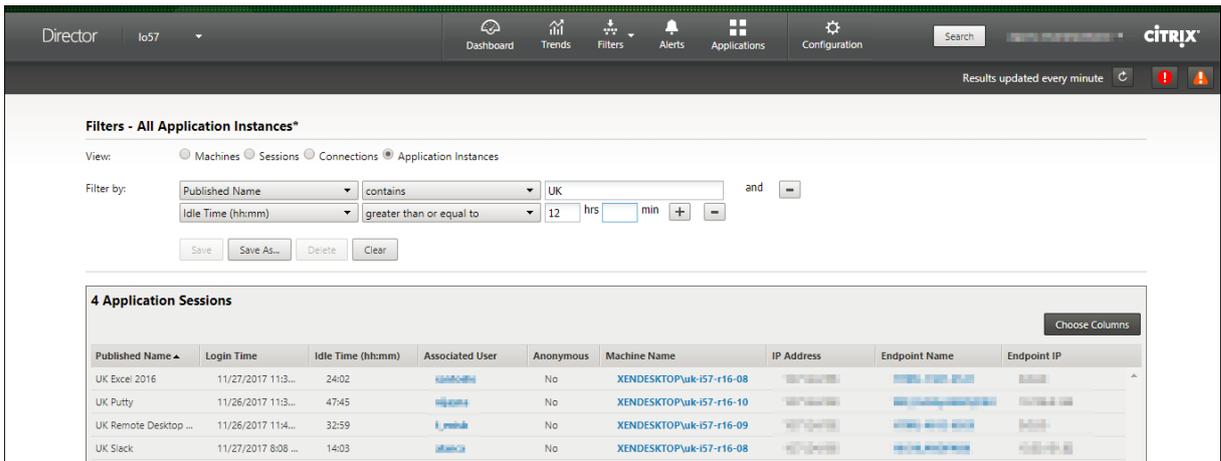
Los casos típicos donde solucionar problemas de aplicaciones pertenecen al sector de la asistencia médica, donde los empleados comparten licencias de aplicación. Allí, debe finalizar las sesiones inactivas y las instancias de aplicación inactivas para purgar el entorno de Citrix Virtual Apps and Desktops, para reconfigurar los servidores de bajo rendimiento o para mantener y actualizar aplicaciones.

La página de filtros **Instancias de aplicación** ofrece una lista de todas las instancias de aplicación que están presentes en los VDA con SO de servidor y SO de sesión única. Se muestran las métricas del tiempo de inactividad asociadas a las instancias de aplicación en los VDA de SO multisesión que hayan estado inactivas durante al menos 10 minutos.

### Nota:

Las métricas de instancias de aplicaciones están disponibles en los sitios de todas las ediciones de licencias.

Utilice esta información para identificar las instancias de aplicación que estén inactivas transcurrido un período de tiempo concreto con el objetivo de cerrarles o desconectarlas, según corresponda. Para ello, seleccione **Filtros > Instancias de aplicación**. A continuación, seleccione un filtro guardado previamente o elija **Todas las instancias de aplicación** y cree su propio filtro.

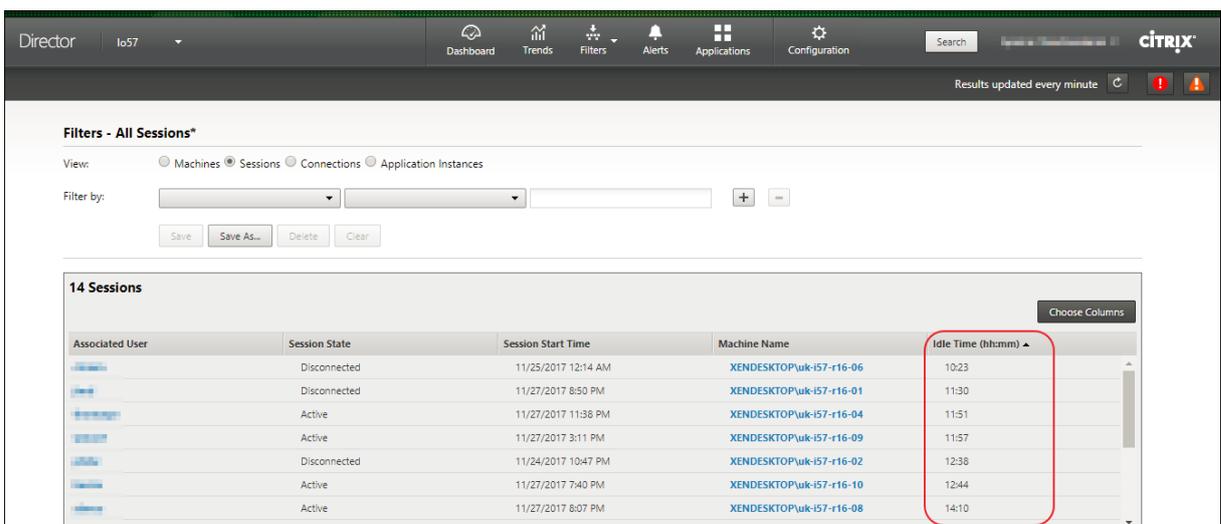


A continuación, se ofrece un filtro de ejemplo. Como criterio **Filtrar por**, elija **Nombre publicado** (de la aplicación) y **Tiempo de inactividad**. A continuación, establezca **Tiempo de inactividad en mayor o igual que** un límite de tiempo concreto y guarde el filtro si quiere volver a utilizarlo en el futuro. En la lista filtrada, seleccione las instancias de aplicación. Seleccione la opción para enviar mensajes o, desde la lista desplegable **Control de sesión**, elija **Cerrar sesión** o **Desconectar** para finalizar las instancias.

**Nota:**

Cerrar la sesión o desconectar una instancia de aplicación cierra o desconecta la sesión actual, lo que finaliza todas las instancias de aplicación que pertenezcan a la misma sesión.

Puede identificar las sesiones inactivas desde la página de filtro **Sesiones** si utiliza el estado de la sesión y la métrica del tiempo de inactividad de la sesión. Ordene por la columna **Tiempo de inactividad** o defina un filtro para identificar las sesiones que estén inactivas transcurrido un tiempo específico. Se muestra el tiempo de inactividad de las sesiones en los VDA de SO multisesión que hayan estado inactivas durante al menos 10 minutos.



El **Tiempo de inactividad** se muestra como **N/D** cuando la instancia de aplicación o sesión

- no ha estado inactiva durante más de 10 minutos,
- se ha iniciado en un VDA de SO de sesión única o
- se ha iniciado en un VDA que ejecuta la versión 7.12 o una versión anterior.

## Supervisar fallos históricos de aplicaciones

La ficha **Tendencias > Fallos y errores de aplicación** muestra los fallos y los errores asociados a las aplicaciones publicadas en los VDA.

Las tendencias de fallos de aplicaciones están disponibles para las últimas 2 horas, las últimas 24 horas, los últimos 7 días y el último mes para los sitios con licencia Premium y Advanced. Están disponibles para las últimas 2 horas, las últimas 24 horas y los últimos 7 días cuando se trata de otros tipos de licencias. Se supervisan aquellos fallos de aplicaciones que se registran en el Visor de eventos con el origen “Errores de aplicación”. Haga clic en **Exportar** para generar informes en formato CSV, Excel o PDF.

Los parámetros de limpieza para los datos retenidos de la supervisión de fallos de aplicaciones GroomApplicationErrorsRetentionDays y GroomApplicationFaultsRetentionDays están configurados a un día de forma predeterminada para sitios con y sin licencia Premium. Puede cambiar este parámetro con el comando de PowerShell:

```
PowerShell command Set-MonitorConfiguration -<setting name> <value>
<!--NeedCopy-->
```

The screenshot displays the 'Application Failures' section in the Citrix Director interface. It includes a search and filter area with fields for Application Name, Process Name, Delivery Group, and Time Period. Below this is a table of 'Application Fault Details' with columns for Time, Application Name, Process Name, Version, and Machine Name. A tooltip is visible over one of the rows, providing detailed error information such as the faulting application name, version, time stamp, and module name.

Time	Application Name	Process Name	Version	Machine Name
01/17/2019 11:53 AM	ThrowException	ThrowException.exe	1.0.0.0	BVT\NIXR052
01/17/2019 11:53 AM	PassArguments	PassArguments.exe	1.0.0.0	BVT\NIXR052
01/17/2019 11:52 AM	Unknown	CoeEngine.exe	7.21.101.0	BVT\NIXR052

Los fallos se muestran como **Fallos de aplicación** o **Errores de aplicación** en función de su gravedad. La ficha “Fallos de aplicación” muestra fallos asociados a la pérdida de datos o de funcionalidad. En

cambio, “Errores de aplicación” indica problemas que no son inmediatamente relevantes; representan condiciones que pueden provocar problemas en el futuro.

Puede filtrar los fallos en función del **Nombre de la aplicación publicada**, **Nombre del proceso** o **Grupo de entrega** y **Período de tiempo**. La tabla muestra el código del error o del fallo junto con una breve descripción de este. La descripción detallada de errores y fallos se muestra como un cuadro de información.

**Nota:**

El “Nombre de la aplicación publicada” aparece como “Desconocido” cuando no se puede derivar el nombre de la aplicación correspondiente. Esto ocurre normalmente cuando falla una aplicación iniciada en una sesión de escritorio, o bien cuando falla debido a una excepción no controlada ocasionada por un archivo ejecutable de dependencia.

De forma predeterminada, se supervisan solo los fallos de las aplicaciones alojadas en agentes VDA de SO multisesión. Puede modificar los parámetros de supervisión desde las directivas de grupo de supervisión (Habilitar supervisión de fallos y errores de aplicación, Habilitar supervisión de fallos de aplicación en VDA de SO de sesión única y Lista de aplicaciones excluidas de la supervisión de fallos). Para obtener más información, consulte [Directivas para supervisar fallos de aplicación](#) en “Configuraciones de directiva de Supervisión”.

En la página **Tendencias > Resultados del sondeo de aplicaciones**, se muestran los resultados de los sondeos de aplicaciones ejecutados en el sitio en las últimas 24 horas y los últimos 7 días. Para obtener más información sobre cómo configurar los sondeos de aplicaciones, consulte [Sondeo de aplicaciones](#).

## Sondeo de aplicaciones

September 22, 2021

El sondeo de aplicaciones automatiza las comprobaciones de estado de las aplicaciones de Citrix Virtual Apps publicadas en un sitio. Los resultados del sondeo de aplicaciones están disponibles en Director.

Requisitos:

- Delivery Controller ejecuta la versión 7.18 o una posterior.
- Las máquinas de punto final que ejecutan Probe Agents son máquinas de Windows con la versión 4.8 de Citrix Receiver para Windows o una posterior, o la versión 1808 de la aplicación Citrix Workspace para Windows (anteriormente Citrix Receiver para Windows) o una posterior. No se admite la aplicación Workspace para UWP.
- Director y StoreFront admiten la autenticación predeterminada basada en formularios.

Cuentas de usuario o permisos requeridos para ejecutar el sondeo de aplicaciones:

- Un usuario único de StoreFront para sondear aplicaciones en cada máquina de punto final. No es necesario que el usuario de StoreFront sea un administrador; los sondeos pueden ejecutarse en un contexto no administrativo.
- Cuentas de usuario con permisos de administrador de Windows para instalar y configurar Citrix Probe Agent en las máquinas de punto final
- Una cuenta de administrador total o un rol personalizado con los siguientes permisos. Si reutiliza cuentas de usuarios existentes para el sondeo de aplicaciones, podrían cerrarse las sesiones activas de esos usuarios.
  - Permisos de grupo de entrega:
    - \* Solo lectura
  - Permisos de Director:
    - \* Crear, modificar y eliminar la configuración del servidor de correo electrónico de alertas (si el servidor de correo electrónico aún no está configurado)
    - \* Crear, modificar y eliminar configuraciones de sondeo
    - \* Ver página Configuraciones
    - \* Ver página Tendencias

## Configurar el sondeo de aplicaciones

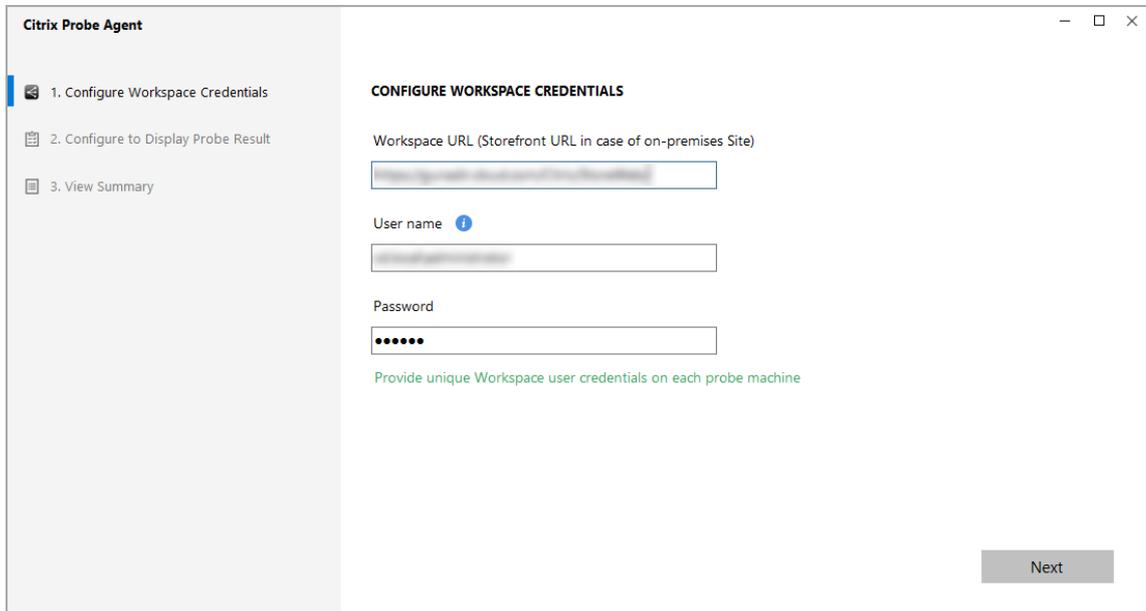
Puede programar los sondeos de aplicaciones para que se ejecuten durante las horas de menor actividad en varios puntos geográficos. Unos resultados exhaustivos pueden ayudar a solucionar problemas relacionados con las aplicaciones aprovisionadas, las máquinas de host o las conexiones antes de que los usuarios los experimenten.

### Paso 1: Instale y configure el Citrix Probe Agent

Citrix Probe Agent es un ejecutable de Windows que simula el inicio de la aplicación por parte del usuario a través de StoreFront. Prueba los inicios de las aplicaciones siguiendo las pautas configuradas en Director e informa de los resultados a Director.

1. Identifique las máquinas de punto final desde donde ejecutar el sondeo de aplicaciones.
2. Los usuarios con privilegios administrativos pueden instalar y configurar Citrix Probe Agent en la máquina de punto final. Descargue el ejecutable de Citrix Probe Agent disponible en <https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html>

3. Inicie el agente y configure sus credenciales de StoreFront y Receiver para Web. Configure un usuario único de StoreFront en cada máquina de punto final. Las credenciales se cifran y se almacenan de forma segura.



The screenshot shows the Citrix Probe Agent configuration window. On the left, a sidebar lists three steps: 1. Configure Workspace Credentials (selected), 2. Configure to Display Probe Result, and 3. View Summary. The main area is titled 'CONFIGURE WORKSPACE CREDENTIALS' and contains three input fields: 'Workspace URL (Storefront URL in case of on-premises Site)', 'User name', and 'Password'. Below the fields, a green note states: 'Provide unique Workspace user credentials on each probe machine'. A 'Next' button is located at the bottom right of the main area.

**Nota:**

Para acceder al sitio que va a sondear desde fuera de la red, escriba la URL de inicio de sesión de Citrix Gateway en el campo de URL de StoreFront. Citrix Gateway redirige automáticamente la solicitud a la URL de StoreFront del sitio correspondiente. Esta función está disponible para Citrix Gateway 12.1 y posterior (tema RfWebUI) y Delivery Controllers 1811 y posterior.

4. En la ficha **Configurar para mostrar el resultado del sondeo**, introduzca sus credenciales de Director y haga clic en **Validar**.

**Citrix Probe Agent**

1. Configure Workspace Credentials

2. Configure to Display Probe Result

3. View Summary

VIEW THE PROBE RESULT ON CITRIX CLOUD:  No

Citrix Director URL  
Ex : http(s)://x.x.x.x/Directory

User name

Domain

Password

Select Site  
Selected Site

Validate

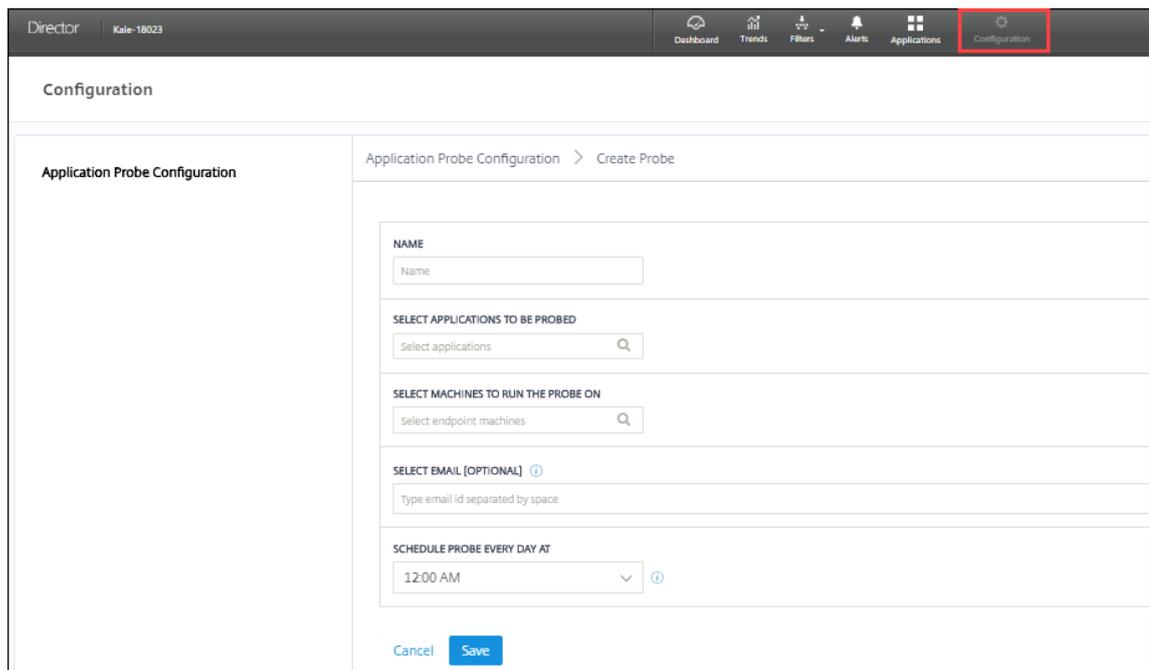
Next

5. Seleccione el sitio y haga clic en **Siguiente**.

## Paso 2: Configure el sondeo de aplicaciones en Director

1. Vaya a **Configuración > Configuración del sondeo de aplicaciones**.
2. Cree un sondeo y elija los siguientes elementos:
  - Las aplicaciones que sondear
  - Las máquinas de punto final en las que debe llevarse a cabo el sondeo
  - Las direcciones de correo electrónico a las que se enviarán los resultados de errores en el sondeo (configure su servidor de correo electrónico en **Alertas > Configuración del servidor de correo electrónico**)
  - La hora a la que debe llevarse a cabo el sondeo (según la zona horaria local de la máquina de punto final)

Una vez configurado en Director, el agente tarda 10 minutos en prepararse para comenzar el sondeo. Luego, ejecuta los sondeos configurados a partir de la hora siguiente.



The screenshot shows the Citrix Director interface. The top navigation bar includes 'Director', 'Kale-18023', and several icons: Dashboard, Trends, Filters, Alerts, Applications, and Configuration (highlighted with a red box). The main content area is titled 'Configuration' and contains a sidebar for 'Application Probe Configuration' and a main panel for 'Application Probe Configuration > Create Probe'. The 'Create Probe' form includes the following fields:

- NAME:** A text input field labeled 'Name'.
- SELECT APPLICATIONS TO BE PROBED:** A search input field labeled 'Select applications' with a magnifying glass icon.
- SELECT MACHINES TO RUN THE PROBE ON:** A search input field labeled 'Select endpoint machines' with a magnifying glass icon.
- SELECT EMAIL [OPTIONAL]:** A text input field with a help icon and the instruction 'Type email id separated by space'.
- SCHEDULE PROBE EVERY DAY AT:** A dropdown menu currently set to '12:00 AM' with a help icon.

At the bottom of the form are 'Cancel' and 'Save' buttons.

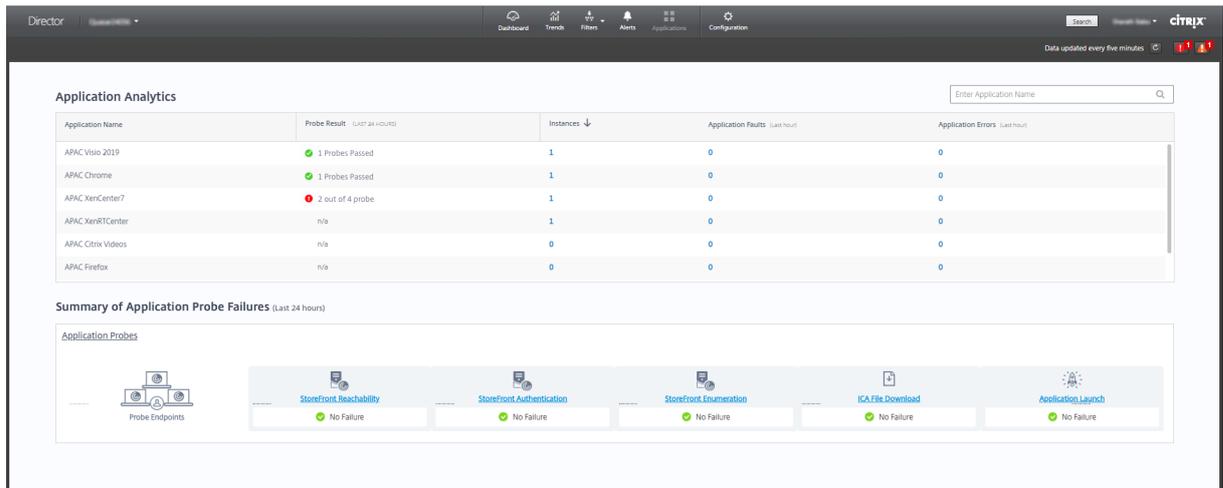
### Paso 3: Ejecute el sondeo

El agente ejecuta el sondeo de aplicaciones según esté configurado cada sondeo (la configuración se obtiene de Director periódicamente). Inicia las aplicaciones seleccionadas en serie mediante StoreFront. El agente informa de los resultados a Director a través de la base de datos de supervisión. Los fallos se informan en cinco etapas específicas:

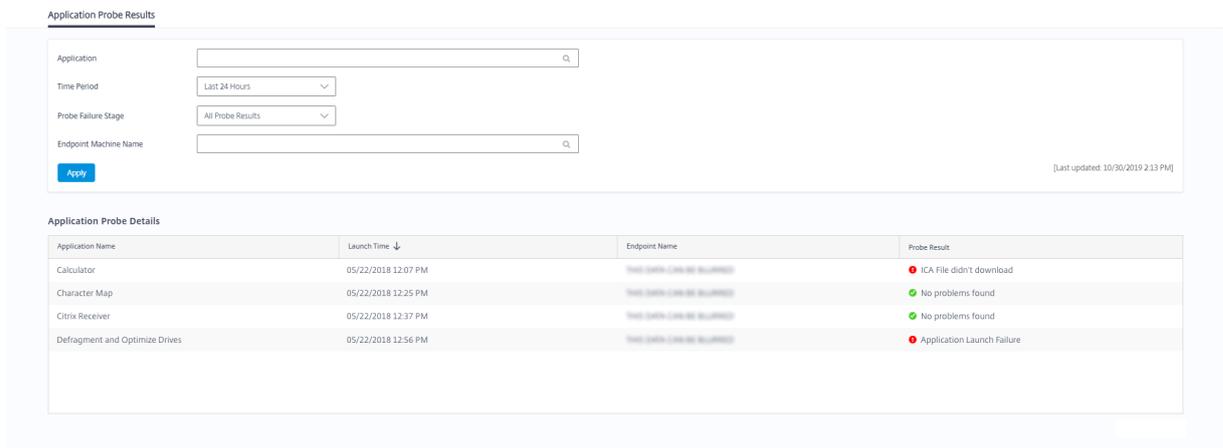
- **Accesibilidad de StoreFront:** No se puede acceder a la URL configurada en StoreFront.
- **Autenticación de StoreFront:** Las credenciales configuradas en StoreFront no son válidas.
- **Enumeración de StoreFront:** La lista de aplicaciones en StoreFront no contiene la aplicación a sondear.
- **Descarga de ICA:** El archivo ICA no está disponible.
- **Inicio de aplicación:** La aplicación no se ha podido iniciar.

### Paso 4: Consulte los resultados del sondeo

Los resultados del último sondeo se encuentran en la página **Aplicaciones**.



Haga clic en el enlace de resultados del sondeo para ver más datos en la página **Tendencias > Resultados del sondeo de aplicaciones**.



En esta página, están disponibles los resultados completos de los sondeos realizados durante las últimas 24 horas o los últimos 7 días. Puede ver la etapa en la que falló el sondeo. Asimismo, puede filtrar la tabla para ver la aplicación específica, la etapa exacta del fallo del sondeo o la máquina de punto final concreta.

## Sondeo de escritorios

September 22, 2021

El sondeo de escritorios automatiza las comprobaciones de estado de las aplicaciones de Citrix Virtual Desktops publicadas en un sitio. Los resultados del sondeo de escritorios están disponibles en Director.

En la página Configuración de Director, configure los escritorios que se sondearán, las máquinas de punto final en las que se ejecutará el sondeo y el tiempo dedicado al sondeo. El agente realiza pruebas con el inicio de los escritorios seleccionados mediante StoreFront e informa de los resultados a Director. Los resultados del sondeo se muestran en la interfaz de usuario de Director: los datos de las últimas 24 horas en la página Aplicaciones y los datos históricos del sondeo en la página Tendencias > Resultados del sondeo > Resultados del sondeo de escritorios. Aquí verá la etapa en la que falló el sondeo: Accesibilidad de StoreFront, Autenticación de StoreFront, Enumeración de StoreFront, Descarga de ICA o Inicio de escritorio. El informe de errores se envía a las direcciones de correo configuradas. Puede programar los sondeos de escritorios para que se ejecuten durante las horas de menor actividad en varios puntos geográficos. Unos resultados exhaustivos pueden ayudar a solucionar proactivamente los problemas relacionados con los escritorios aprovisionados, las máquinas de host o las conexiones, entre otros, antes de que los usuarios los experimenten. El sondeo de escritorios está disponible para los sitios con licencia Premium. Esta función requiere la versión 7 1906 o una versión posterior de los Delivery Controllers y Probe Agent 1903 o una versión posterior.

#### Requisitos:

- Delivery Controller ejecuta la versión 1906 o una posterior.
- Las máquinas de punto final con Probe Agents son máquinas Windows con la versión 4.8 de Citrix Receiver para Windows o una posterior, o versión 1906 de la aplicación Citrix Workspace para Windows (anteriormente Citrix Receiver para Windows) o una posterior. No se admite la aplicación Workspace para UWP.
- Director y StoreFront admiten la autenticación predeterminada basada en formularios.

#### Cuentas de usuario o permisos requeridos para ejecutar el sondeo de escritorios:

- Un usuario único de StoreFront para sondear aplicaciones en cada máquina de punto final. No es necesario que el usuario de StoreFront sea un administrador; los sondeos pueden ejecutarse en un contexto no administrativo.
- Cuentas de usuario con permisos de administrador de Windows para instalar y configurar Citrix Probe Agent en las máquinas de punto final
- Una cuenta de administrador total o un rol personalizado con los siguientes permisos. Si reutiliza cuentas de usuarios normales para el sondeo de escritorios, podrían cerrarse las sesiones activas de esos usuarios.
  - Permisos de grupo de entrega:
    - \* Solo lectura
  - Permisos de Director:
    - \* Crear, modificar y eliminar la configuración del servidor de correo electrónico de alertas (si el servidor de correo electrónico aún no está configurado)
    - \* Crear, modificar y eliminar configuraciones de sondeo
    - \* Ver página Configuraciones

★ Ver página Tendencias

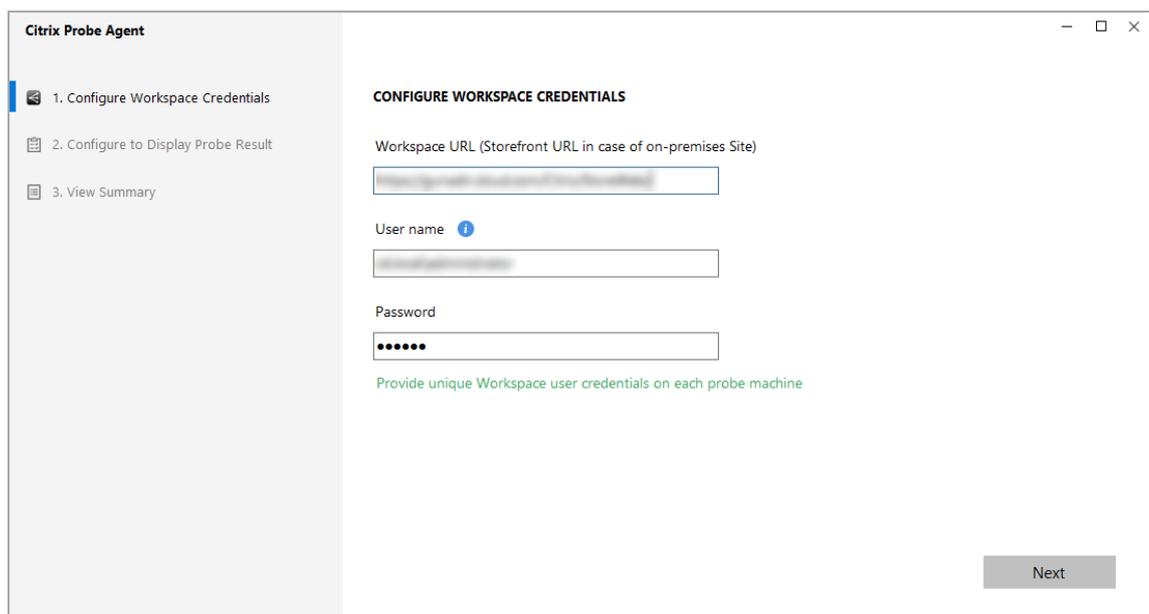
## Configurar sondeo de escritorios

Puede programar los sondeos de escritorios para que se ejecuten durante las horas de menor actividad en varios puntos geográficos. Unos resultados exhaustivos pueden ayudar a solucionar problemas relacionados con los escritorios aprovisionados, las máquinas de host o las conexiones antes de que los usuarios los experimenten.

### Paso 1: Instale y configure el Citrix Probe Agent

Citrix Probe Agent es un ejecutable de Windows que simula el inicio del escritorio por parte del usuario a través de StoreFront. Prueba los inicios de los escritorios en base a las pautas configuradas en Director e informa de los resultados a Director.

1. Identifique las máquinas de punto final desde donde ejecutar el sondeo de escritorios.
2. Los usuarios con privilegios administrativos pueden instalar y configurar Citrix Probe Agent en la máquina de punto final. Descargue el ejecutable de Citrix Probe Agent disponible en <https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html>
3. Inicie el agente y configure sus credenciales de StoreFront y Receiver para Web. Configure un usuario único de StoreFront en cada máquina de punto final. Las credenciales se cifran y se almacenan de forma segura.



The screenshot shows the Citrix Probe Agent configuration window. The title bar reads 'Citrix Probe Agent'. On the left, there is a navigation pane with three steps: '1. Configure Workspace Credentials' (selected), '2. Configure to Display Probe Result', and '3. View Summary'. The main area is titled 'CONFIGURE WORKSPACE CREDENTIALS' and contains the following fields:

- Workspace URL (Storefront URL in case of on-premises Site): [Redacted]
- User name: [Redacted]
- Password: [Redacted]

Below the fields, there is a green note: 'Provide unique Workspace user credentials on each probe machine'. A 'Next' button is located at the bottom right of the window.

Nota:

Para acceder al sitio que va a sondear desde fuera de la red, escriba la URL de la página de inicio de sesión de Citrix Gateway en el campo de URL de StoreFront. Citrix Gateway redirige automáticamente la solicitud a la URL de StoreFront del sitio correspondiente. Esta función está disponible para Citrix Gateway 12.1 o posterior, y Delivery Controllers 1811 o posterior.

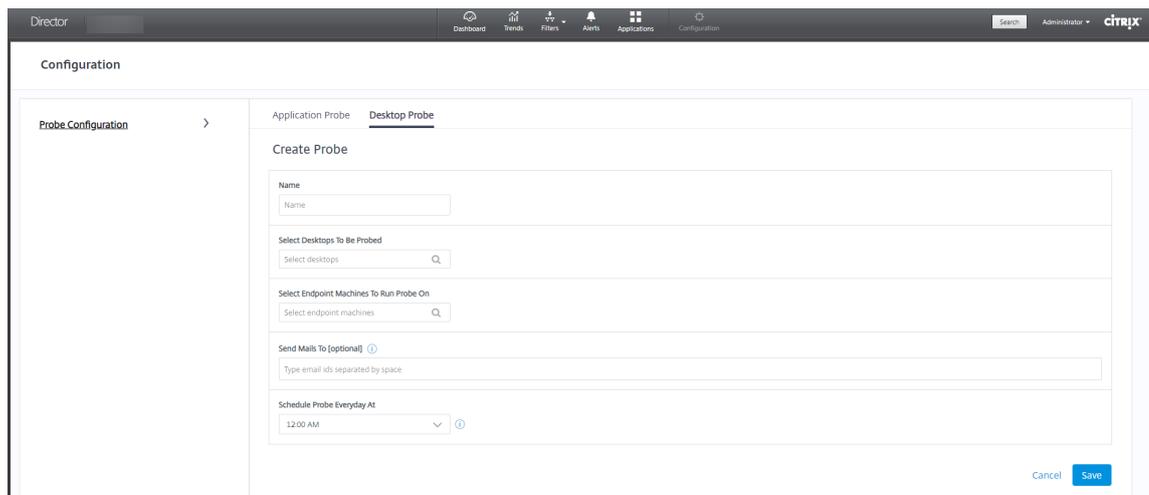
4. En la ficha **Configurar para mostrar el resultado del sondeo**, introduzca sus credenciales de Director y haga clic en **Validar**.

The screenshot shows the 'Citrix Probe Agent' configuration window. On the left, a sidebar lists three steps: '1. Configure Workspace Credentials', '2. Configure to Display Probe Result' (which is selected), and '3. View Summary'. The main area contains a toggle switch for 'VIEW THE PROBE RESULT ON CITRIX CLOUD:' set to 'No'. Below this are input fields for 'Citrix Director URL' (with an example 'Ex : http(s)://x.x.x.x/Directory'), 'User name', 'Domain', and 'Password'. At the bottom, there is a 'Select Site' dropdown menu currently showing 'Selected Site'. On the right side, there are two buttons: 'Validate' and 'Next'.

5. Seleccione el sitio y haga clic en **Siguiente**.

## Paso 2: Configure el sondeo de escritorios en Director

1. Vaya a **Configuración > Configuración del sondeo de escritorios**.
2. Para crear un sondeo, introduzca los detalles y haga clic en **Guardar**.



Nota:

Configure su servidor de correo electrónico en **Alertas > Configuración del servidor de correo electrónico**.

Una vez configurado el sondeo de escritorios, el agente tarda 10 minutos en prepararse para comenzar el sondeo. Luego, ejecuta los sondeos configurados a partir de la hora siguiente.

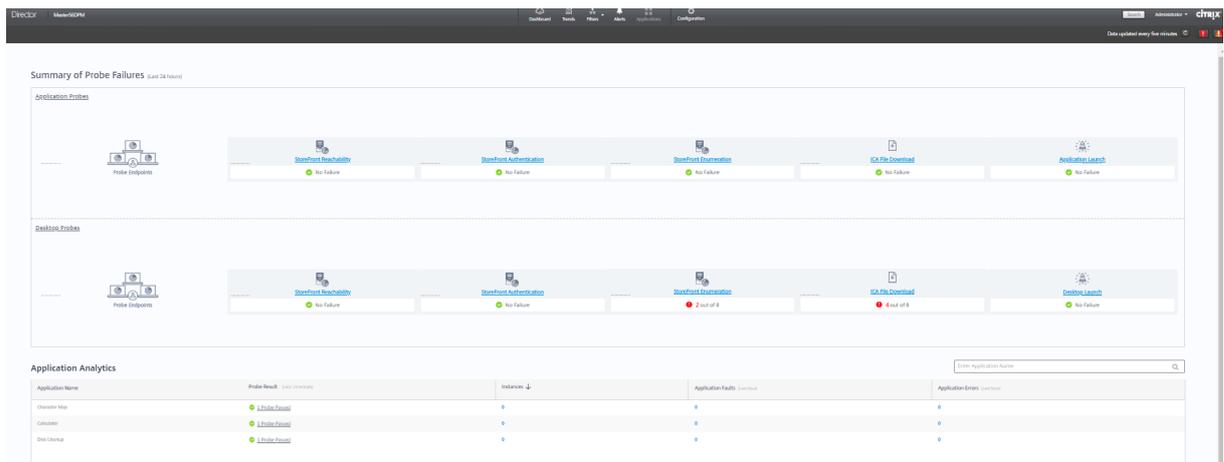
### Paso 3: Ejecute el sondeo

El agente ejecuta el sondeo de escritorios según la configuración de cada sondeo (esta se obtiene de Director periódicamente). Inicia los escritorios seleccionados en serie mediante StoreFront. El agente informa de los resultados a Director a través de la base de datos de supervisión. Los fallos se informan en cinco etapas específicas:

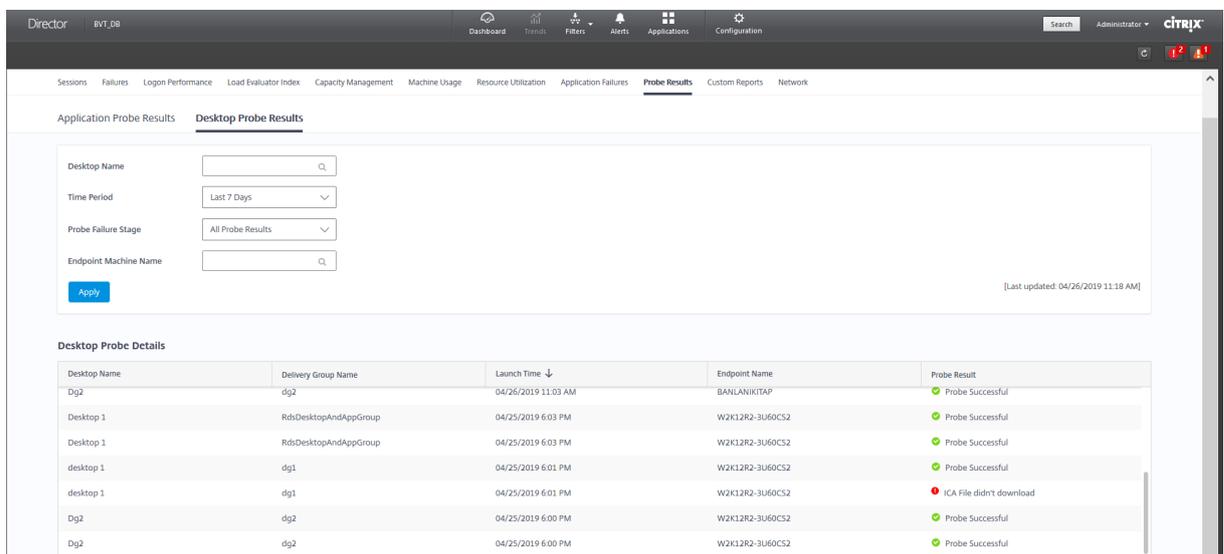
- **Accesibilidad de StoreFront:** No se puede acceder a la URL configurada en StoreFront.
- **Autenticación de StoreFront:** Las credenciales configuradas en StoreFront no son válidas.
- **Enumeración de StoreFront:** La lista de escritorios en StoreFront no contiene el escritorio a sondear.
- **Descarga de ICA:** El archivo ICA no está disponible.
- **Inicio del escritorio:** No se puede iniciar el escritorio.

### Paso 4: Consulte los resultados del sondeo

Los resultados del último sondeo se encuentran en la página **Escritorios**.



Haga clic en el enlace de resultados del sondeo para ver más datos en la página **Tendencias > Resultados del sondeo > Resultados del sondeo de escritorios**.



En esta página, están disponibles los resultados completos de los sondeos realizados durante las últimas 24 horas o los últimos 7 días. Puede ver la etapa en la que falló el sondeo. Asimismo, puede filtrar la tabla para ver el escritorio específico, la etapa exacta del fallo del sondeo o la máquina de punto final concreta.

## Solucionar problemas de máquinas

June 28, 2024

### Nota:

Con la herramienta **Citrix Health Assistant**, puede solucionar problemas de configuración en

agentes VDA no registrados. La herramienta automatiza una serie de comprobaciones de estado para identificar las posibles causas de problemas en el registro de los VDA, el inicio de sesión y la configuración de la redirección de zonas horarias. Dispone de las instrucciones de descarga y uso de la herramienta **Citrix Health Assistant** en el artículo [Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch](#) de Citrix Knowledge Center.

La vista **Filtros > Máquinas** en la consola de Director muestra las máquinas configuradas en el sitio. La ficha Máquinas con SO multisesión incluye el índice del patrón de carga. Este índice indica la distribución de contadores de rendimiento, así como texto de ayuda sobre el recuento de sesiones si pasa el puntero sobre el vínculo.

Haga clic en la columna **Motivo del fallo** de la máquina donde se ha producido el fallo para obtener una descripción detallada de este y las acciones recomendadas para solucionarlo. Los motivos de los errores y las acciones recomendadas para fallos de máquinas y conexiones están disponibles en [Citrix Director 7.12 Failure Reasons Troubleshooting Guide](#).

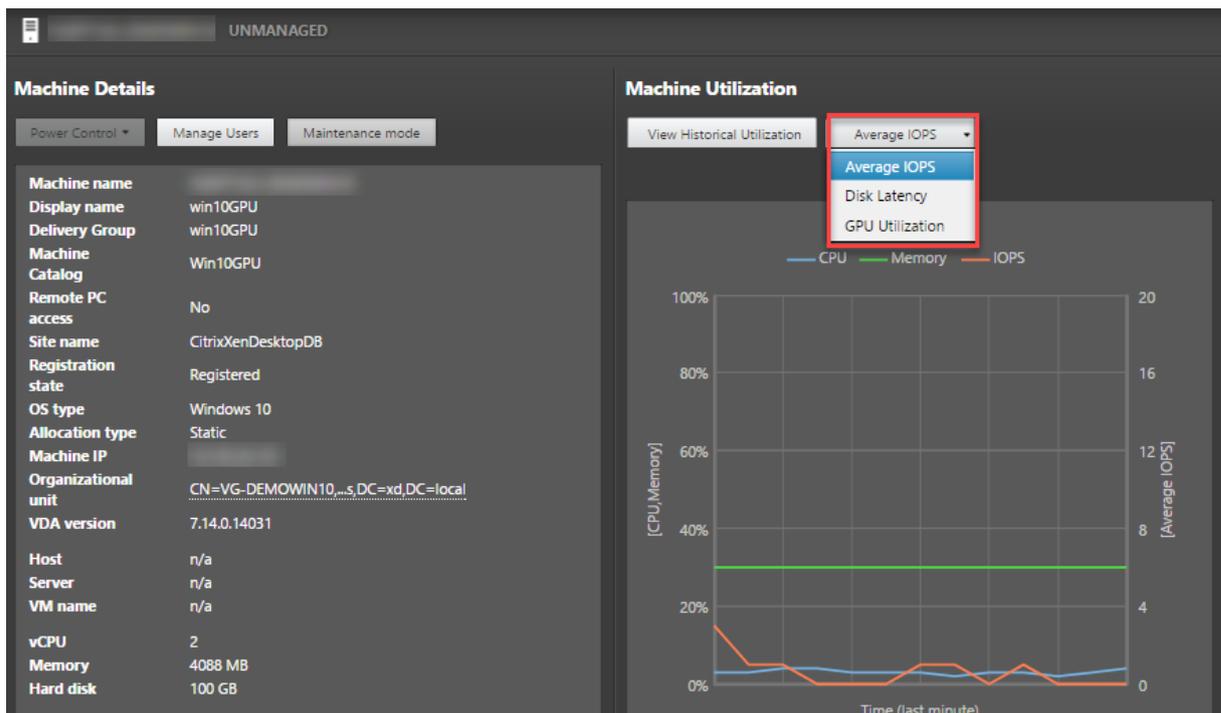
Haga clic en el enlace del nombre de máquina para ir a la página **Detalles de la máquina**.

La página “Detalles de la máquina” muestra datos de la máquina, de la infraestructura y de los parches rápidos que se hayan aplicado a la máquina.

## Usar recursos en tiempo real en cada máquina

El panel **Utilización de máquinas** muestra gráficos del uso en tiempo real de la CPU y la memoria. Además, dispone de gráficos de supervisión del disco y la GPU para aquellos sitios que tengan Delivery Controllers y VDA **7.14** o una versión posterior.

Los gráficos de supervisión de disco, la latencia de disco y el promedio IOPS son métricas de rendimiento importantes que le ayudan a supervisar y solucionar problemas relacionados con los discos VDA. El gráfico de IOPS medias muestra la cantidad media de lecturas y escrituras en un disco. Seleccione **Latencia de disco** para ver un gráfico de la demora entre una solicitud de datos y su retorno desde el disco, medida en milésimas de segundo.



Seleccione **Utilización de GPU** para ver, en porcentajes, el uso de la GPU, la memoria de la GPU y del codificador y el decodificador para solucionar problemas relacionados con la GPU en los agentes VDA con SO de servidor o SO de sesión única. Los gráficos de uso de la GPU están únicamente disponibles para los VDA que ejecutan Windows de 64 bits con GPU de NVIDIA Tesla M60 y que ejecutan la versión de controlador de pantalla 369.17 o posterior.

Los VDA deben tener HDX 3D Pro habilitado para proporcionar la aceleración de GPU. Para obtener más información, consulte [Aceleración de GPU para sistemas operativos de sesión única Windows](#) y [Aceleración de GPU para sistemas operativos multisesión Windows](#).

Cuando el VDA accede a más de una GPU, el gráfico de uso muestra el promedio de las métricas de GPU recopiladas a partir de las GPU individuales. Las métricas de la GPU se recopilan del VDA entero, no de procesos individuales.

## Usar recursos históricos en cada máquina

En el panel **Utilización de máquinas**, haga clic en **Ver utilización histórica** para ver el historial del uso de los recursos en la máquina seleccionada.

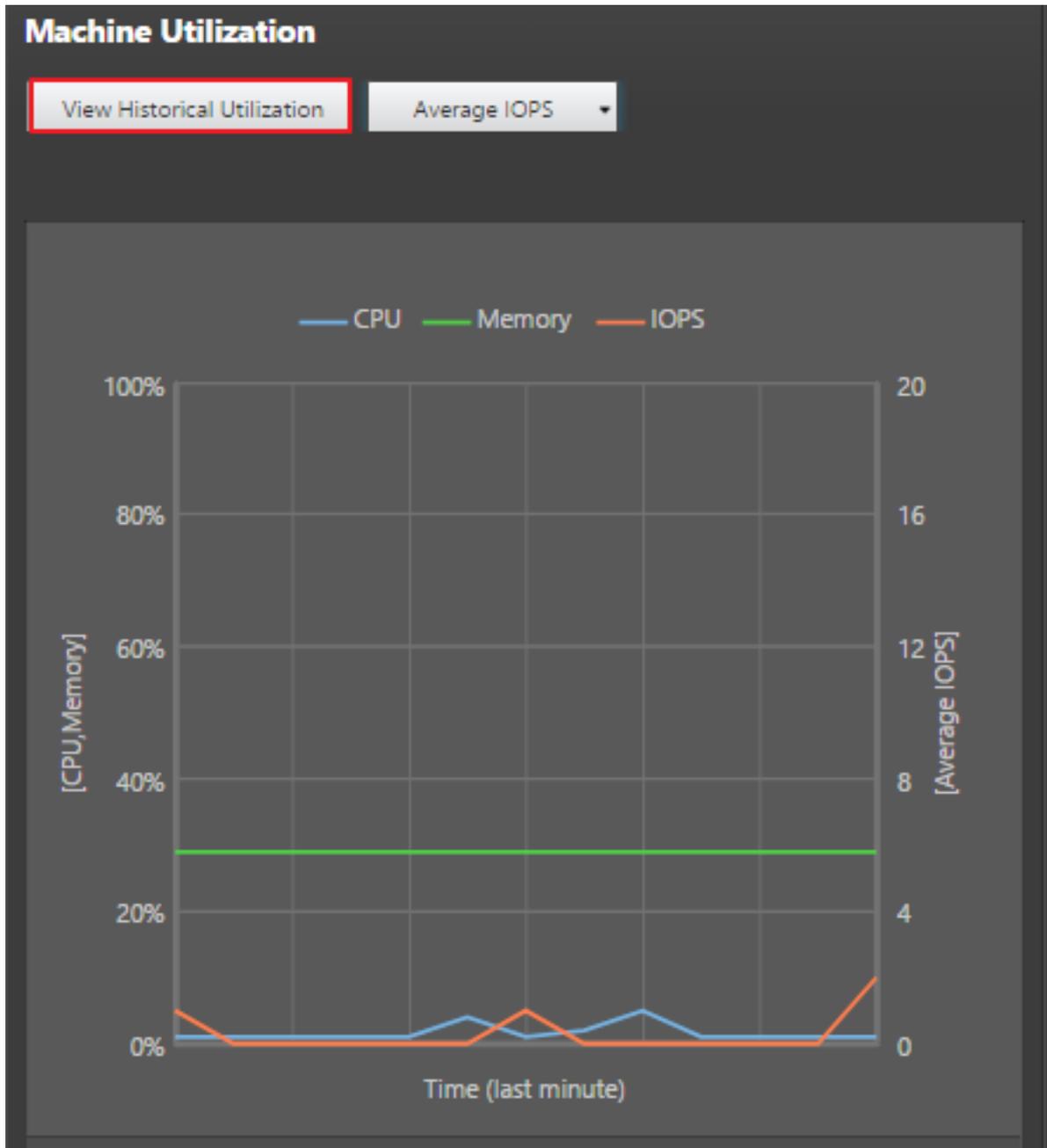
Los gráficos de utilización contienen contadores de rendimiento de la CPU, la memoria, el pico de sesiones simultáneas, el promedio de IOPS y la latencia de disco.

### Nota:

La configuración de directiva de Supervisión **Habilitar supervisión de procesos** debe estar establecida en "Permitida" para recopilar y mostrar datos en la tabla "10 procesos principales" de la

página “Utilización histórica de máquinas”. La recopilación de datos está inhabilitada de forma predeterminada.

De forma predeterminada, se recopilan los datos referentes al uso de la CPU, la memoria, el promedio de IOPS y la latencia de disco. Puede inhabilitar la recopilación mediante la configuración de directiva **Habilitar supervisión de recursos**.



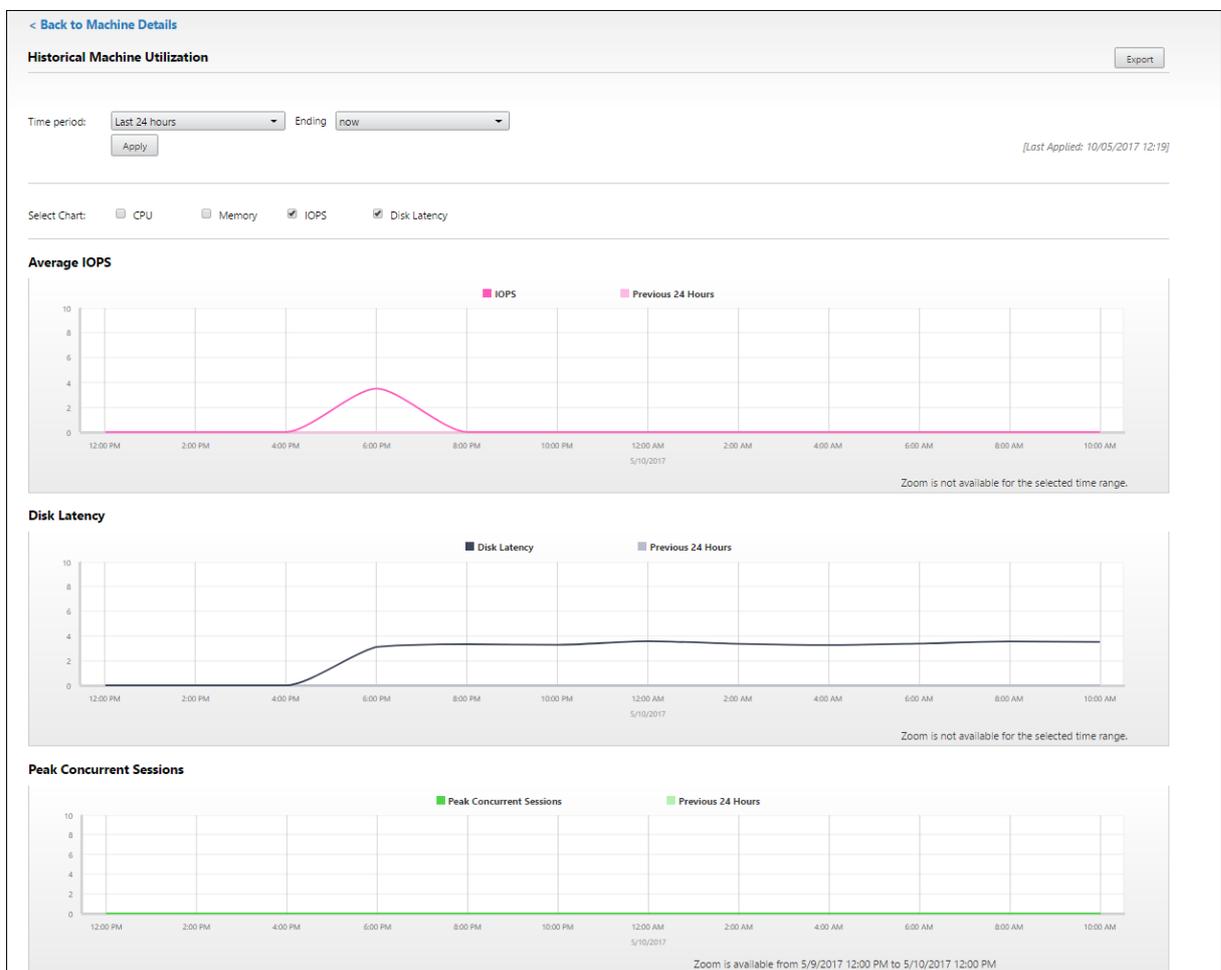
1. En el panel **Utilización de máquinas** de la vista **Detalles de la máquina**, seleccione **Ver utilización histórica**.

- En la página **Utilización histórica de máquinas**, establezca el **Período de tiempo** para ver las últimas 2 horas, 24 horas, 7 días, o bien el último mes o año.

**Nota:**

Los datos de uso del promedio de IOPS y la latencia de disco están disponibles solamente para las últimas 24 horas, el último mes y el último año contando hasta el momento actual. No se admite establecer un tiempo de finalización personalizado.

- Haga clic en **Aplicar** y seleccione los gráficos necesarios.
- Pase el cursor sobre las diferentes secciones del gráfico para ver más información sobre un período de tiempo seleccionado.



Por ejemplo: si selecciona **Últimas 2 horas**, el período de referencia será de 2 horas antes del intervalo de tiempo seleccionado. Verá las tendencias de uso de la CPU, la memoria y la sesión entre las últimas 2 horas y el punto de referencia. Si selecciona **Último mes**, el período de referencia será el mes anterior. Seleccione esta opción para ver la latencia de disco y el promedio de IOPS entre el último mes y el punto de referencia.

1. Haga clic en **Exportar** para exportar los datos de utilización de recursos durante el período seleccionado. Para obtener más información, consulte la sección [Exportar informes](#) en “Supervisar implementaciones”.
2. Debajo de los gráficos, en la tabla, aparecen los 10 procesos principales que consumen más CPU o memoria. Puede ordenarla por cualquiera de las columnas: Nombre de la aplicación, Nombre de usuario, ID de sesión, Promedio de CPU, Pico de CPU, Promedio de memoria y Pico de memoria durante el intervalo de tiempo seleccionado. Las columnas IOPS y Latencia de disco no se pueden ordenar.

**Nota:**

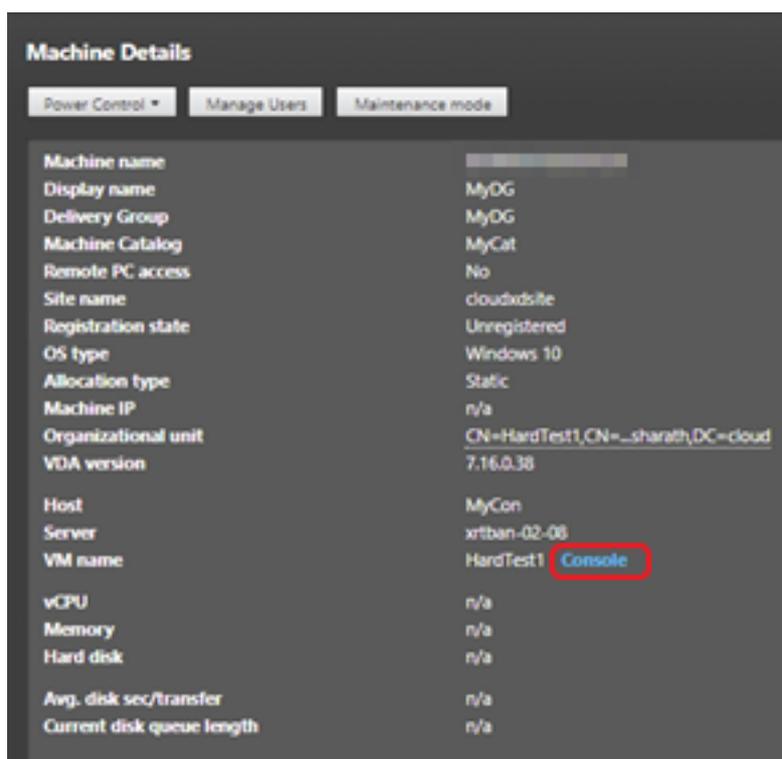
El ID de sesión aparece como “0000” para los procesos del sistema.

3. Para ver la tendencia histórica en el consumo de recursos de un proceso concreto, consulte los detalles de cualquiera de los diez procesos principales.

### **Acceso a la consola de la máquina**

Puede acceder a las consolas de las máquinas con SO de sesión única y SO multisesión alojadas en XenServer 7.3 y versiones posteriores directamente desde Director. De esta manera, no necesita XenCenter para solucionar problemas en los VDA alojados en XenServer. Para que esta función esté disponible:

- Se requiere Delivery Controller 7.16 o posterior.
- El XenServer que aloja la máquina debe ser de la versión 7.3 o posterior, y debe poder accederse a él desde la interfaz gráfica de Director.



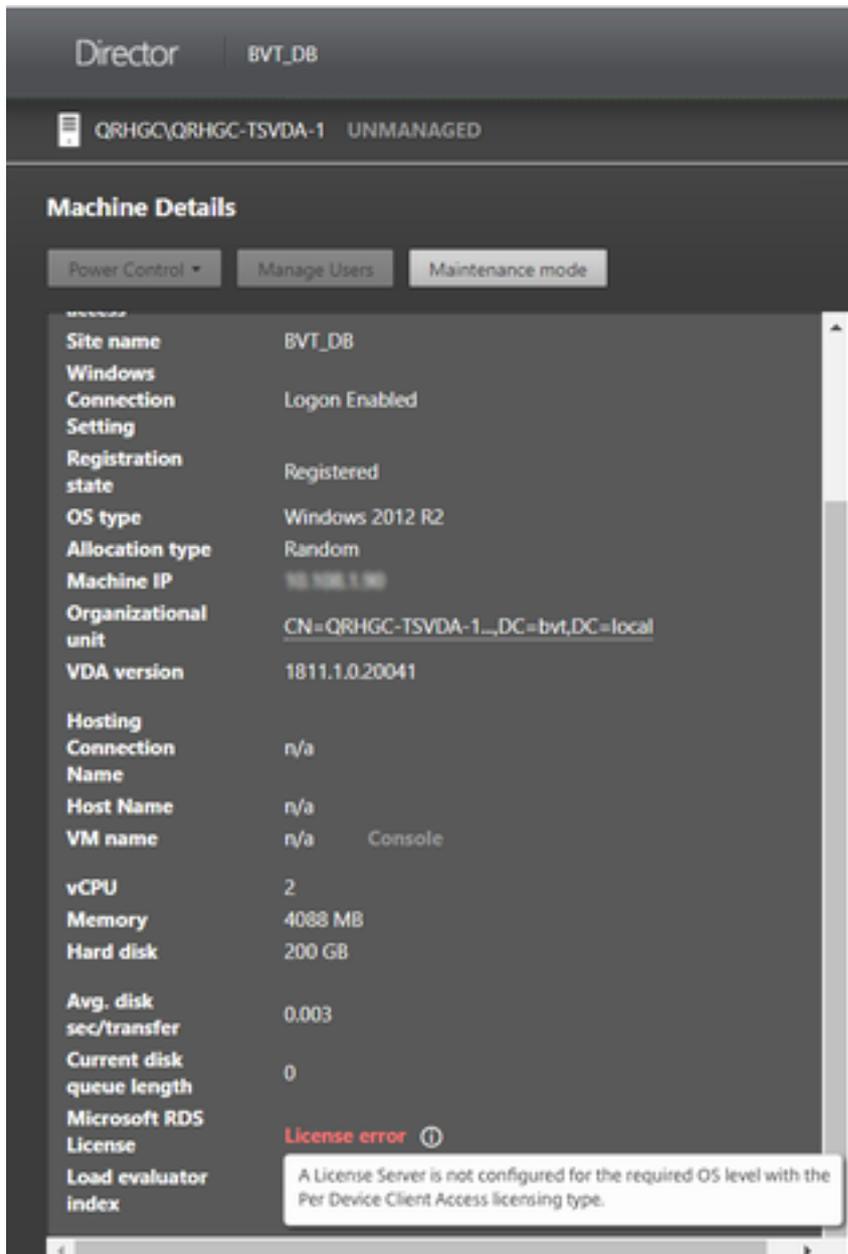
Para solucionar un problema en una máquina, haga clic en el enlace **Consola** en el panel “Detalles de la máquina” en la máquina correspondiente. Después de la autenticación de las credenciales de host que proporcione, la consola de la máquina se abrirá en otra ficha mediante noVNC, un cliente web VNC. Ahora tiene acceso por teclado y mouse a la consola.

#### Nota:

- Esta función no es compatible con Internet Explorer 11.
- Si la posición del puntero en la consola no coincide con la posición del puntero en la máquina, consulte [CTX230727](#) para conocer los pasos para solucionar el problema.
- Director inicia el acceso a la consola en una nueva ficha; por eso, su explorador web debe permitir las ventanas emergentes.
- Por razones de seguridad, Citrix recomienda instalar certificados SSL en su explorador web.

## Estado de licencias RDS de Microsoft

El estado de la licencia RDS (Servicios de Escritorio remoto) de Microsoft aparece en el panel “Detalles” de la página **Detalles de la máquina** y **Detalles del usuario** para las máquinas de SO multisesión.



Se muestra uno de los siguientes mensajes:

- Licencia disponible
- No se ha configurado correctamente (advertencia)
- Error de licencia (error)
- Versión incompatible de VDA (error)

**Nota:**

En el estado de licencias RDS de Microsoft para máquinas en período de gracia con licencias válidas, se muestra el mensaje **Licencia disponible** en color verde. Renueve la licencia antes de

que caduque.

Cuando se trata de mensajes de advertencia y de error, coloque el puntero sobre el icono de información para ver información adicional como se indica en la tabla siguiente.

Tipo de mensaje	Mensajes en Director
Error	Disponible para VDA 7.16 y posterior.
Error	No se permiten nuevas conexiones RDS.
Error	La licencia RDS de Microsoft ha superado su período de gracia.
Error	Hay un servidor de licencias que no está configurado para el nivel de SO requerido con el tipo de licencia de acceso de cliente por dispositivo.
Error	El servidor de licencias configurado no es compatible con el nivel de SO del host RDS con el tipo de licencia de acceso de cliente por dispositivo.
Advertencia	Una licencia de Terminal Server temporal no es un tipo de licencia RDS válido en una implementación de Citrix Virtual Apps and Desktops.
Advertencia	El escritorio remoto para administración no es un tipo de licencia válido en una implementación de Citrix Virtual Apps and Desktops.
Advertencia	No hay ningún tipo de licencia RDS configurado.
Advertencia	No se puede acceder al controlador de dominio o al servidor de licencias con el tipo de licencia RDS de acceso de cliente por dispositivo.
Advertencia	Con el tipo de licencia de acceso de cliente por dispositivo, la licencia del dispositivo de cliente no se pudo determinar, ya que no se puede acceder al servidor de licencias para el nivel de SO que se requiere.

**Nota:**

Esta función solo se aplica a Microsoft RDS CAL (Licencia de acceso de cliente).

## Solucionar problemas de usuarios

March 10, 2022

Use el **Servicio de asistencia** de Director (página **Administrador de actividades**) para ver información sobre el usuario:

- Compruebe la información acerca del inicio de sesión, la conexión y las aplicaciones del usuario.
- Remede la máquina del usuario.
- Grabe la sesión ICA.
- Solucione el problema con las acciones recomendadas en la tabla siguiente y, si es necesario, remita el problema al administrador que corresponda.

### Sugerencias para solucionar problemas

---

<b>Problema de los usuarios</b>	<b>Sugerencias</b>
El inicio de sesión tarda mucho tiempo o falla de forma intermitente o repetidamente	<a href="#">Diagnosticar problemas de inicio de sesión de los usuarios</a>
El inicio de sesión tarda mucho tiempo o falla de forma intermitente o repetidamente	<a href="#">Diagnosticar problemas de inicio de sesión</a>
La aplicación es lenta o no responde	<a href="#">Resolver fallos de aplicación</a>
La conexión falló	<a href="#">Restaurar conexiones de escritorio</a>
La sesión es lenta o no responde	<a href="#">Restaurar sesiones</a>
Grabar sesiones	<a href="#">Grabar sesiones</a>
El vídeo es lento o de poca calidad	<a href="#">Generar informes de sistema de canales HDX</a>

---

**Nota:**

Para comprobar que la máquina no está en modo de mantenimiento, en la vista “Detalles del usuario”, consulte el panel “Detalles de la máquina”.

## Sugerencias para la búsqueda

Cuando se introduce un nombre de usuario en el campo Buscar, Director busca usuarios en Active Directory en todos los sitios configurados para admitir Director.

Cuando se escribe un nombre de máquina multiusuario en el campo Buscar, Director muestra los Detalles de la máquina para la máquina especificada.

Cuando se escribe un nombre de punto final en el campo Buscar, Director utiliza las sesiones sin autenticar (anónimas) y las sesiones autenticadas que están conectadas a un punto final específico, lo que permite resolver problemas en las sesiones no autenticadas. Asegúrese de que los nombres de los dispositivos de punto final son exclusivos para poder resolver problemas de sesiones no autenticadas.

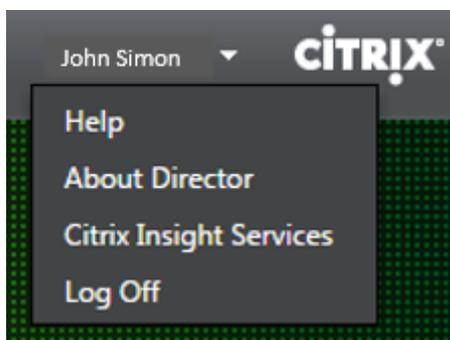
Los resultados de la búsqueda incluyen también usuarios que no están utilizando máquinas en ese momento o no tienen asignada ninguna.

- Las búsquedas no distinguen el uso de mayúsculas y minúsculas.
- Las entradas parciales generan una lista de posibles coincidencias.
- Después de escribir unas pocas letras de un nombre que tiene dos partes (nombre de usuario, nombre y apellidos o nombre simplificado) separadas por un espacio, los resultados incluyen coincidencias para ambas cadenas. Por ejemplo, si escribe ju rod, los resultados pueden incluir cadenas como “Juan Rodríguez” o Rodrigo, Juárez.

Para volver a la página inicial, haga clic en el logotipo de Director.

## Acceder a Citrix Insight Services

Puede acceder a [Citrix Insight Services](#) (CIS) desde la lista desplegable Usuario en Director para acceder a otras perspectivas de diagnóstico. Los datos disponibles en CIS proceden de orígenes como Call Home y Citrix Scout.



## Cargar información de solución de problemas para la asistencia técnica de Citrix

Ejecute Citrix Scout desde un solo Delivery Controller o VDA para capturar puntos de datos clave y rastreos de Citrix Diagnosis Facility (CDF) para solucionar problemas en los equipos seleccionados. Scout ofrece la opción de cargar datos de forma segura en la plataforma CIS para guiar al servicio de asistencia técnica de Citrix en la solución de problemas. El servicio de asistencia técnica de Citrix usa la plataforma CIS para reducir el tiempo de resolución de los problemas de que informan los clientes.

Scout se instala con los componentes de Citrix Virtual Apps and Desktops. Según la versión de Windows, Scout aparece en el menú Inicio de Windows o en la pantalla Inicio al instalar o actualizar a Citrix Virtual Apps and Desktops.

Para iniciar Scout, desde el menú Inicio o la pantalla Inicio, seleccione Citrix > Citrix Scout.

Para obtener información sobre el uso y la configuración de Citrix Scout, y para ver las preguntas frecuentes, consulte [CTX130147](#).

## Diagnosticar problemas de inicio de sesión

May 24, 2024

Además de las fases del proceso de inicio de sesión mencionadas en la sección [Diagnosticar problemas de inicio de sesión de los usuarios](#), Director muestra la duración del inicio de la sesión. Esto se divide en la duración de Inicio de sesión en la aplicación Workspace e Inicio de sesión en VDA, en la página **Detalles del usuario** y en las páginas **Detalles de la máquina**. Estas dos duraciones contienen más fases individuales cuyas duraciones de inicio también se muestran. Estos datos le ayudan a comprender y solucionar problemas con una duración elevada para iniciar las sesiones. Además, la duración de cada fase involucrada en el inicio de las sesiones ayuda a solucionar problemas asociados a fases individuales. Por ejemplo: si el tiempo de asignación de unidades es elevado, puede comprobar si todas las unidades válidas se asignan correctamente en el objeto de directiva de grupo o en el script. Esta función está disponible en Delivery Controller 7 1906 y versiones posteriores, y en VDA 1903 y versiones posteriores.

### Requisitos previos

Debe cumplir los siguientes requisitos previos para que se muestren los datos de duración de inicio de sesión:

- Delivery Controller 7 1906 o una versión posterior.
- VDA 1903 o una versión posterior.

- El servicio Citrix End User Experience Monitoring (EUEM) debe ejecutarse en el VDA.

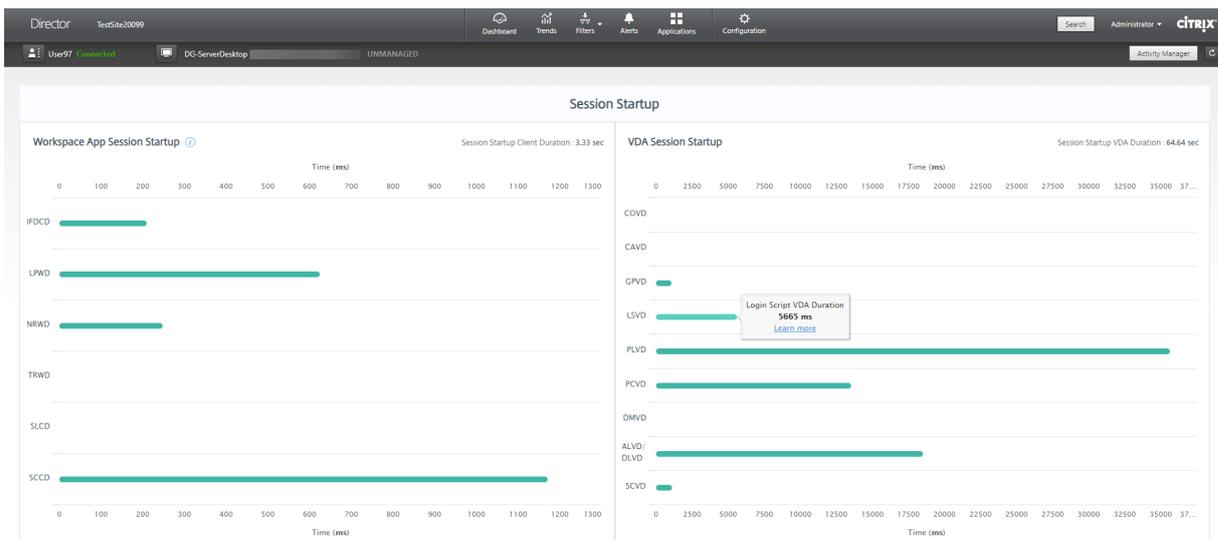
## Limitaciones

Las siguientes limitaciones se aplican cuando Director muestra los datos de duración de inicio de sesión.

- La duración de inicio de sesión solo está disponible para sesiones HDX.
- Para el inicio de sesiones desde los sistemas operativos iOS y Android, solo está disponible la duración de inicio en VDA.
- Duración de la descarga de archivos ICA (IFDCD) solo está disponible cuando se detecta la aplicación Workspace al llevar a cabo el inicio desde un explorador.
- Para el inicio de sesiones desde Mac OS, IFDCD solo está disponible para la aplicación Workspace 1902 o una versión posterior.
- Para el inicio de sesiones desde el sistema operativo Windows, IFDCD está disponible para la aplicación Workspace 1902 y versiones posteriores. Para las versiones anteriores, IFDCD solo se muestra para el inicio de aplicaciones desde el explorador con la aplicación Workspace detectada.

### Notas:

- Si tiene problemas en la pantalla de duración de inicio de sesiones una vez que se hayan cumplido los requisitos previos, consulte los registros del servidor de Director y de VDA tal y como se describe en [CTX130320](#). Para las sesiones compartidas (varias aplicaciones iniciadas en la misma sesión), se muestran las métricas de inicio de la aplicación Workspace para la conexión más reciente o el inicio más reciente de la aplicación.
- Algunas métricas del inicio de sesión en VDA no son aplicables en las reconexiones. En tales casos, se muestra un mensaje.



## Fases del inicio de sesión de la aplicación Workspace

### Duración del inicio de sesión en el cliente (SSCD)

Cuando esta métrica es elevada, indica un problema del lado del cliente que está alargando los tiempos de inicio. Revise las métricas siguientes para determinar la raíz probable del problema. Esto comienza lo más cerca posible del momento de la solicitud (clic del mouse) y finaliza cuando se ha establecido la conexión ICA entre el dispositivo cliente y el VDA. En una sesión compartida, esta duración es mucho menor, ya que no se incurre en gran parte de los costes de instalación asociados a la creación de una nueva conexión con el servidor. En el siguiente nivel, más abajo, hay varias métricas detalladas disponibles.

### Duración de la descarga de archivos ICA

Este es el tiempo que tarda el cliente en descargar el archivo ICA del servidor. El proceso general es el siguiente:

1. El usuario hace clic en un recurso (aplicación o escritorio) de la aplicación de Workspace.
2. Una solicitud del usuario se envía a StoreFront a través de Citrix Gateway (si está configurado), que envía la solicitud al Delivery Controller.
3. El Delivery Controller busca una máquina disponible para la solicitud y envía la información de la máquina y otros detalles a StoreFront. Además, StoreFront solicita y recibe un ticket único de Secure Ticket Authority.
4. StoreFront genera un archivo ICA y lo envía al usuario a través de Citrix Gateway (si está configurado).

IFDCD representa el tiempo que tarda todo el proceso (del paso 1 al 4). La duración de IFDCD deja de contar cuando el cliente recibe el archivo ICA.

LPWD es el componente de StoreFront del proceso.

Si el valor de IFDCD es elevado (pero el de LPWD es normal), el procesamiento del lado del servidor del inicio se ha realizado correctamente, pero se han producido problemas de comunicación entre el dispositivo cliente y StoreFront. Esto se debe a problemas de red entre las dos máquinas. Por lo tanto, primero podría solucionar problemas potenciales de red.

### **Duración de la carga de páginas en el servidor web (LPWD)**

Este es el tiempo que se tarda en procesar la carga de páginas (launch.aspx) en StoreFront. Si el valor de LPWD es elevado, puede haber un cuello de botella en StoreFront.

He aquí las posibles causas:

- Carga elevada en StoreFront. Intente identificar la causa de la desaceleración; para ello, compruebe los registros de Internet Information Services (IIS) y las herramientas de supervisión, el Administrador de tareas, el Monitor de rendimiento, etc.
- StoreFront tiene problemas para comunicarse con otros componentes, como Delivery Controller. Compruebe si la conexión de red entre StoreFront y Delivery Controller es lenta o hay Delivery Controllers desconectados o sobrecargados.

### **Duración de la resolución de nombres en el servidor web (NRWD)**

Este es el tiempo que tarda el Delivery Controller en resolver el nombre de una aplicación o escritorio publicados en la dirección IP de una máquina VDA.

Cuando esta métrica es elevada, indica que el Delivery Controller tarda mucho tiempo en resolver el nombre de una aplicación publicada en una dirección IP. Las posibles causas pueden deberse a un problema en el cliente, problemas con el Delivery Controller, como, por ejemplo, que el Delivery Controller esté sobrecargado, o un problema con el enlace de red que los une.

### **Duración de respuestas a tíquets en el servidor web (TRWD)**

Esta duración indica el tiempo que se tarda en obtener un tíquet (si es necesario) del servidor Secure Ticket Authority (STA) o de Delivery Controller. Cuando esta duración es elevada, indica que el servidor STA o el Delivery Controller están sobrecargados.

### **Duración de la búsqueda de sesiones en el cliente (SLCD)**

Esta duración representa el tiempo que se tarda en enviar una consulta a cada sesión para alojar la aplicación publicada solicitada. La comprobación se realiza en el cliente para determinar si una sesión existente puede gestionar la solicitud de inicio de la aplicación. El método utilizado depende de si la sesión es nueva o compartida.

### **Duración de la creación de sesiones en el cliente (SCCD)**

Esta duración representa el tiempo que se tarda en crear una sesión, desde el momento en que se inicia wfica32.exe (o un archivo equivalente similar) hasta el momento en que se establece la conexión.

### **Fases de inicio de sesión en VDA**

#### **Duración del inicio de sesión en el VDA (SSVD)**

Esta duración es la métrica de alto nivel relacionada con el inicio de conexiones del lado del servidor que abarca el tiempo que tarda VDA en realizar toda la operación de inicio. Cuando esta métrica es elevada, indica que hay un problema en VDA que alarga los tiempos de inicio de sesión. Esto incluye el tiempo dedicado en el VDA a realizar toda la operación de inicio.

#### **Duración de la obtención de credenciales en el VDA (COVD)**

Tiempo que tarda el VDA en obtener las credenciales de usuario.

Esta duración se puede inflar artificialmente si un usuario no proporciona las credenciales a tiempo y, por lo tanto, no se incluye en la duración de inicio en VDA. Es probable que este tiempo sea importante solo si se está utilizando el inicio de sesión manual y se muestra el cuadro de diálogo de credenciales del lado del servidor (o si se muestra un aviso legal antes de iniciar el inicio de sesión).

#### **Duración de la autenticación de credenciales en el VDA (CAVD)**

Este es el tiempo que tarda el VDA en autenticar las credenciales del usuario en el proveedor de autenticación, que puede ser Kerberos, Active Directory o una interfaz del proveedor de compatibilidad para seguridad (SSPI).

### **Duración de directivas de grupo en el VDA (GPVD)**

Esta duración es el tiempo que se tarda en aplicar objetos de directiva de grupo durante el inicio de sesión.

### **Duración de scripts de inicio de sesión en el VDA (LSVD)**

Este es el tiempo que tarda el VDA en ejecutar los scripts de inicio de sesión del usuario.

Considere la posibilidad de hacer asíncronos los scripts de inicio de sesión del usuario o grupo. Piense igualmente en optimizar cualquier script de compatibilidad con aplicaciones o, en su lugar, utilizar variables de entorno.

### **Duración de carga de perfil en el VDA (PLVD)**

Este es el tiempo que tarda el VDA en cargar el perfil del usuario.

Si esta duración es elevada, piense en la configuración de su perfil de usuario. El tamaño y la ubicación del perfil de itinerancia contribuyen a ralentizar el inicio de sesión. Cuando un usuario inicia una sesión en la que los perfiles de itinerancia y las carpetas principales de Terminal Services están habilitados, el contenido del perfil de itinerancia y el acceso a esa carpeta se asignan durante el inicio de sesión, lo que consume recursos adicionales. A veces, esto equivale a una parte importante de la CPU. Para mitigar este problema, considere la posibilidad de utilizar las carpetas principales de Terminal Services con carpetas personales redirigidas. De manera general, considere la posibilidad de utilizar Citrix Profile Management para administrar perfiles de usuario en entornos Citrix. Si utiliza Citrix Profile Management y tiene tiempos de inicio de sesión lentos, compruebe si el software antivirus está bloqueando la herramienta Citrix Profile Management.

### **Duración de la creación de impresoras en el VDA (PCVD)**

Este es el tiempo que tarda el VDA en asignar de forma sincrónica las impresoras cliente del usuario. Si se establece la configuración para que la creación de impresoras se realice de forma asíncrona, no se registra ningún valor para PCVD, ya que no afecta a la finalización del inicio de la sesión.

El tiempo excesivo dedicado a la asignación de impresoras suele ser el resultado de la configuración de la directiva de creación automática de impresoras. La cantidad de impresoras agregadas localmente en los dispositivos cliente de los usuarios y la configuración de impresión pueden afectar directamente a los tiempos de inicio de sesión. Cuando se inicia una sesión, Citrix Virtual Apps and Desktops tiene que crear todas las impresoras asignadas localmente en el dispositivo cliente. Considere la posibilidad de volver a configurar las directivas de impresión para reducir la cantidad de impresoras

que se crean, concretamente cuando los usuarios tienen muchas impresoras locales. Para ello, modifique la directiva de creación automática de impresoras en Delivery Controller y Citrix Virtual Apps and Desktops.

### **Duración de la asignación de unidades en el VDA (DMVD)**

Este es el tiempo que tarda el VDA en asignar las unidades, los dispositivos y los puertos cliente del usuario.

Compruebe que las directivas base incluyen configuraciones para inhabilitar los canales virtuales no utilizados, como la asignación de puertos COM o audio, para optimizar el protocolo ICA y mejorar el rendimiento general de la sesión.

### **Duración de inicio de aplicaciones/escritorios en el VDA (ALVD/DLVD)**

Esta fase es una combinación de la duración de UserInit y de Shell. Cuando un usuario inicia sesión en una máquina con Windows, Winlogon ejecuta userinit.exe. Userinit.exe ejecuta scripts de inicio de sesión, restablece las conexiones de red y luego inicia Explorer.exe, la interfaz de usuario de Windows. Userinit representa la duración entre el inicio de Userinit.exe y el inicio de la interfaz de usuario para el escritorio o la aplicación virtual. La duración de Shell es el tiempo que transcurre entre la inicialización de la interfaz de usuario y la hora en que el usuario recibe el control del teclado y del mouse.

### **Duración de la creación de sesiones en el VDA (SCVD)**

Este tiempo incluye varios retrasos en el tiempo de creación de sesiones en VDA.

## **Diagnosticar problemas de inicio de sesión de los usuarios**

March 10, 2022

Use los datos de Duración de inicio de sesión para solucionar problemas de inicio de sesión.

La duración del inicio de sesión se mide solo para las conexiones iniciales a un escritorio o aplicación que usa HDX. Esta información no incluye a los usuarios que intentan conectarse con el protocolo de escritorio remoto (RDP) o que se vuelven a conectar desde sesiones desconectadas. Específicamente, la duración del inicio de sesión no se mide cuando un usuario se conecta inicialmente mediante un protocolo que no es HDX y vuelve a conectarse por HDX.

En la vista “Detalles del usuario”, la duración se muestra como un valor numérico; debajo se muestra la hora en que se produjo el inicio de sesión y un gráfico de las fases de ese inicio.

A medida que los usuarios inician sesión en Citrix Virtual Apps and Desktops, Monitor Service supervisa las fases del proceso de inicio de sesión desde el momento en que el usuario se conecta desde la aplicación Citrix Workspace al momento en que el escritorio está listo para usarse.

El número elevado de la parte izquierda es el tiempo total de inicio de sesión. Se calcula sumando el tiempo que se tarda en establecer la conexión y en obtener un escritorio desde Delivery Controller más el tiempo que se tarda en autenticarse e iniciar sesión en un escritorio virtual. La información de duración se presenta en segundos (o fracciones de segundo).

## Requisitos previos

Deben cumplirse los siguientes requisitos previos para que aparezcan los datos de duración del inicio de sesión y los resultados detallados:

1. Instale **Citrix User Profile Manager** y **Citrix User Profile Manager WMI Plugin** en el VDA.
2. Compruebe que el servicio de Citrix Profile Management se esté ejecutando.
3. Para los sitios de XenApp y XenDesktop 7.15 y versiones anteriores, inhabilite la configuración de GPO llamada **No procesar la lista de ejecución antigua**.
4. La auditoría del seguimiento de procesos debe estar habilitada para obtener el desglose de la sesión interactiva.
5. Para obtener el desglose del GPO, aumente el tamaño de los registros de operaciones de las directivas de grupo.

### Nota:

La duración del inicio de sesión solo se admite en el shell predeterminado de Windows (explorer.exe), no en los shells personalizados.

## Pasos para solucionar problemas en el inicio de sesión de los usuarios

1. En la vista **Detalles del usuario**, puede resolver problemas del estado de inicio de sesión desde el panel “Duración de inicio de sesión”.
  - Si el usuario está iniciando una sesión, esta vista refleja dicho proceso.
  - Si el usuario tiene una sesión ya iniciada actualmente, el panel “Duración de inicio de sesión” muestra el tiempo que tardó el inicio de sesión del usuario.
2. Examine las fases del proceso de inicio de sesión.

## **Fases del proceso de inicio de sesión**

### **Intermediación con broker**

Cuánto tiempo se tardó en decidir qué escritorio asignar al usuario.

### **Inicio de la VM**

Si la sesión requería el inicio de una máquina virtual, este es el tiempo que tardó en iniciarse la máquina.

### **Conexión HDX**

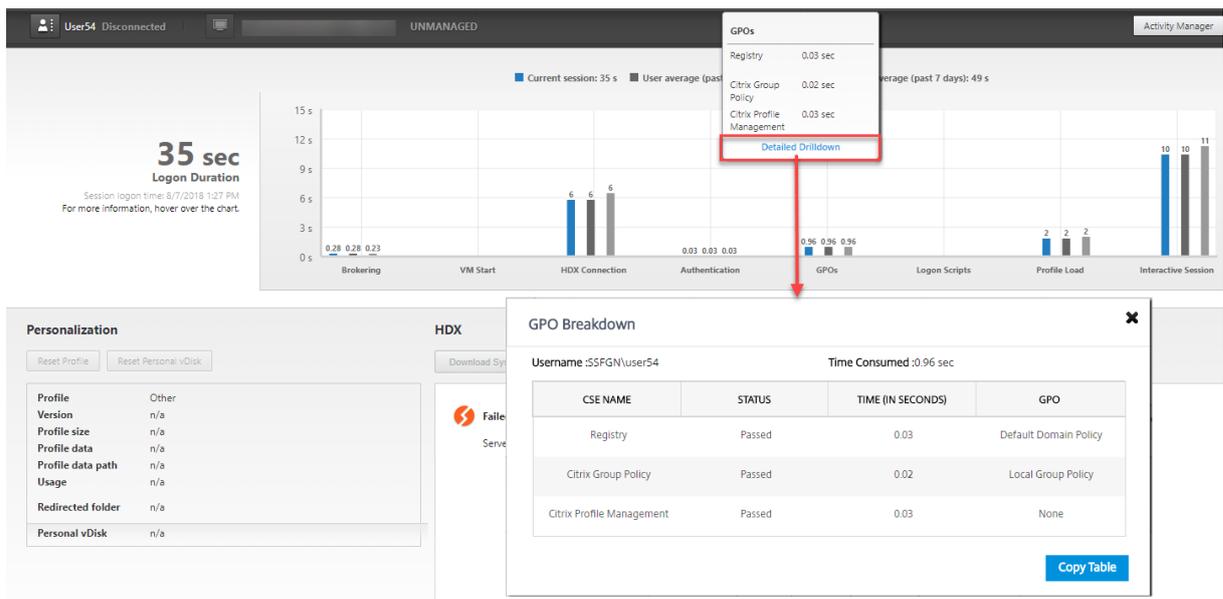
Tiempo que se tardó en completar los pasos requeridos para configurar la conexión HDX desde el cliente a la máquina virtual.

### **Autenticación**

Tiempo que se tardó en completar la autenticación en la sesión remota.

### **Objetos de directiva de grupo (GPO)**

Si había configuraciones de directiva de grupo habilitadas en las máquinas virtuales, este es el tiempo que se tardó en aplicar los objetos de directiva de grupo durante el inicio de sesión. El desglose del tiempo necesario para aplicar cada directiva por cada CSE (extensión del lado del cliente) está disponible como texto de ayuda cuando pasa el cursor sobre la barra de GPO.



Haga clic en **Desglose detallado** para ver una tabla con el estado de la directiva y el nombre del GPO correspondiente. Las duraciones del desglose representan solo el tiempo de procesamiento de CSE, no se suman al tiempo total de GPO. Puede copiar la tabla de detalles para resolver problemas o utilizarla en los informes. El tiempo de GPO para las directivas se obtiene de los registros del Visor de eventos. Los registros se pueden sobrescribir dependiendo de la memoria asignada para los registros de operaciones (el tamaño predeterminado es 4 MB). Para obtener más información sobre cómo aumentar el tamaño del registro para los registros de operaciones, consulte el artículo [Configuring the Event Logs](#) de Microsoft.

### Scripts de inicio de sesión

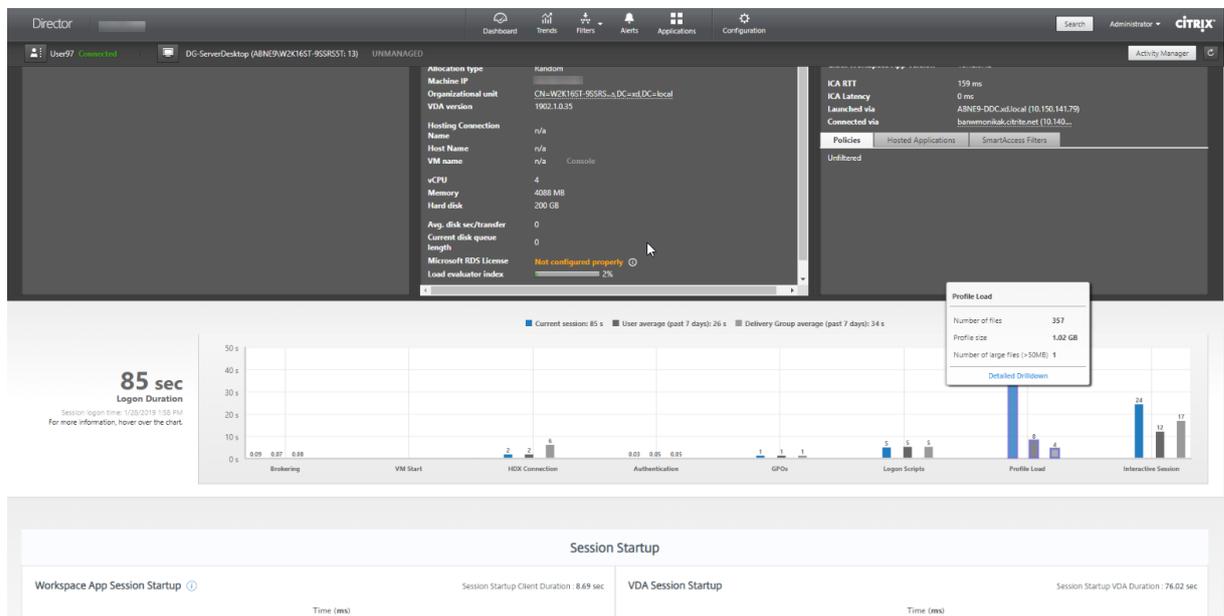
Si había scripts de inicio de sesión configurados para la sesión, este es el tiempo que se tardó en ejecutarlos.

### Carga de perfil

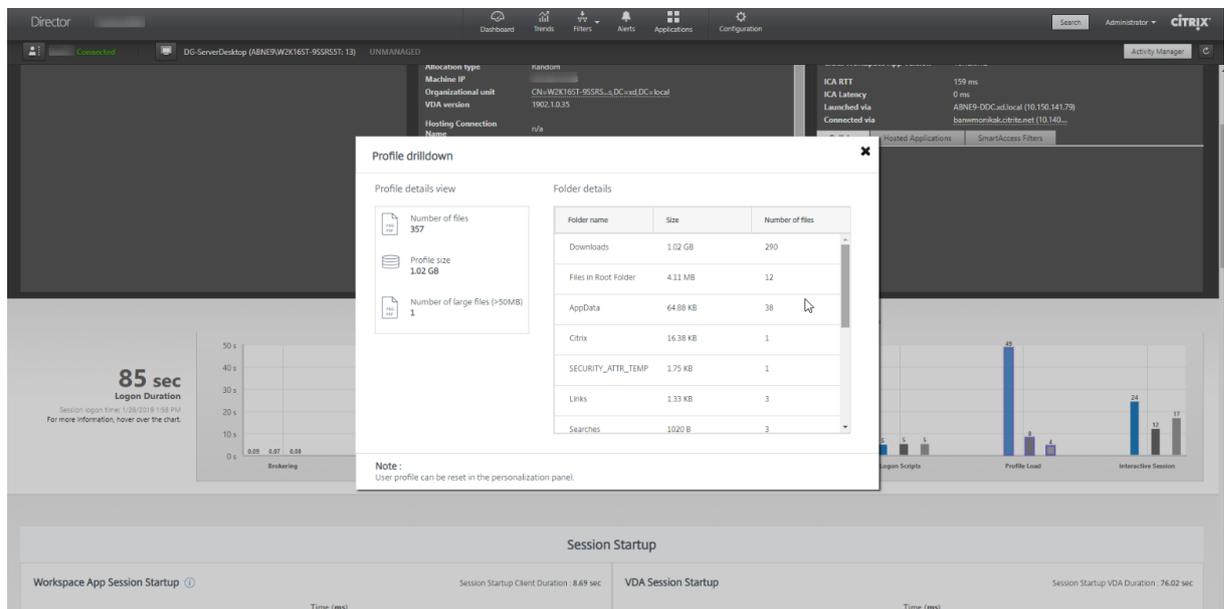
Si había parámetros de perfil configurados para el usuario o para la máquina virtual, este es el tiempo que tardó el perfil en cargarse.

Si Citrix Profile Management está configurado, la barra Carga de perfil indica el tiempo que Citrix Profile Management tarda en procesar perfiles de usuario. Esta información ayuda a los administradores a solucionar problemas con la duración elevada de cargas de perfil. Cuando se configura Profile Management, la barra Carga de perfil muestra una duración mayor. Este aumento se debe a esta mejora y no refleja ninguna degradación del rendimiento. Esta mejora está disponible en VDA 1903 o en versiones posteriores.

Al pasar el cursor sobre la barra Carga de perfil, aparece un texto de ayuda que muestra datos del perfil del usuario de la sesión actual.



Hacer clic en **Desglose detallado** para ver cada carpeta individual que hubiera en la carpeta raíz del perfil (por ejemplo, C:/Usuarios/nombre de usuario), su tamaño y la cantidad de archivos (incluidos los archivos dentro de las carpetas anidadas).



El desglose de perfiles está disponible en Delivery Controller 7 1811 o posterior y VDA 1811 o posterior. Con la información desglosada del perfil, puede resolver problemas de tiempos de carga largos para los perfiles. Puede hacer lo siguiente:

- Restablecer el perfil de usuario

- Optimizar el perfil eliminando archivos de gran tamaño no deseados
- Reducir la cantidad de archivos para reducir la carga de la red
- Usar streaming de perfiles

De forma predeterminada, todas las carpetas de la raíz del perfil se muestran en el desglose. Para ocultar la visibilidad de las carpetas, modifique el siguiente valor de Registro en la máquina VDA:

**Advertencia:**

Si se modifica el Registro o se le agregan valores de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

1. En el VDA, agregue el nuevo valor de Registro **ProfileFoldersNameHidden** a HKEY\_LOCAL\_MACHINE\Software
2. Establezca el valor en 1. Este debe ser un valor DWORD (32 bits). La visibilidad de los nombres de las carpetas está ahora inhabilitada.
3. Para volver a ver los nombres de las carpetas, establezca el valor en 0.

**Nota:**

Puede usar GPO o comandos de PowerShell para aplicar el cambio del valor de Registro a varias máquinas. Para obtener más información sobre el uso de GPO para implementar cambios en el Registro, consulte el [blog](#).

### Información adicional

- En el desglose de perfil no se tienen en cuenta las carpetas redirigidas.
- Puede que los usuarios finales no vean los archivos NTUser.dat de la carpeta raíz. Sin embargo, están incluidos en el desglose de perfil y se muestran en la lista de archivos de la **Carpeta raíz**.
- Algunos archivos ocultos en la carpeta AppData no se incluyen en el desglose de perfil.
- Es posible que el número de archivos y los datos de tamaño de perfil no coincidan con los datos del panel de Personalización, debido a ciertas limitaciones de Windows.

### Sesión interactiva

Este es el tiempo que se tardó en entregar el control del teclado y del mouse al usuario después de cargar el perfil de usuario. Suele ser la fase más larga de todas las fases de inicio de sesión y se calcula de este modo: **Duración de la sesión interactiva = Marca de hora del evento en el escritorio preparado (EventId 1000 en el VDA) - Marca de hora en el evento de perfil de usuario cargado (EventId 2 en el VDA)**. La fase Sesión interactiva está compuesta de tres subfases: Pre-userinit,

Userinit y Shell. Al pasar el mouse sobre la sesión interactiva, se muestran las subfases, el tiempo empleado para cada una de ellas, el tiempo total de demora acumulada entre esas subfases y un enlace a la documentación.

Nota:

Esta función solamente está disponible en agentes VDA 1811 y versiones posteriores. Si ha iniciado sesiones en sitios cuya versión es anterior a la 7.18 y, a continuación, la ha actualizado a la 7.18 o una versión posterior, aparecerá el mensaje “El desglose no está disponible debido a un error del servidor”. Sin embargo, si ha iniciado ninguna sesión después de actualizar la versión, no se muestra ningún mensaje de error.

Para ver la duración de cada subfase, habilite la opción “Auditar el seguimiento de procesos” en la VM (VDA). Cuando la opción “Auditar el seguimiento de procesos” está inhabilitada (predeterminado), se muestra la duración de Pre-userinit y la duración combinada de Userinit y Shell. Puede habilitar la opción “Auditar el seguimiento de procesos” a través de un objeto de directiva de grupo (GPO) de la siguiente manera:

1. Cree un GPO y modifíquelo mediante el editor de GPO.
2. Vaya a Configuración del equipo > Configuración de Windows > Configuración de seguridad > Directivas locales > Directiva de auditoría.
3. En el panel de la derecha, haga doble clic en **Auditar el seguimiento de procesos**.
4. Seleccione **Correcto** y haga clic en “Aceptar”.
5. Aplique este GPO a los VDA o grupos requeridos.

Para obtener más información sobre la auditoría del seguimiento de procesos y cómo habilitarla o inhabilitarla, consulte [Audit process tracking](#) en la documentación de Microsoft.



Panel “Duración de inicio de sesión” en la vista “Detalles del usuario”.

- **Sesión interactiva: Pre-userinit:** Este es el segmento de Sesión Interactiva que se superpone con los scripts y los objetos de directivas de grupo. Esta subfase se puede reducir optimizando los GPO y los scripts.
- **Sesión interactiva: Userinit:** Cuando un usuario inicia sesión en una máquina con Windows, Winlogon ejecuta userinit.exe. Userinit.exe ejecuta scripts de inicio de sesión, restablece las conexiones de red y luego inicia Explorer.exe, la interfaz de usuario de Windows. Esta subfase de Sesión interactiva representa la duración entre el inicio de Userinit.exe y el inicio de la interfaz de usuario para el escritorio o la aplicación virtual.

- **Sesión interactiva: Shell:** En la fase previa, Userinit comienza a inicializar la interfaz de usuario de Windows. La subfase Shell captura la duración entre la inicialización de la interfaz de usuario y la hora en que el usuario recibe el control del teclado y del mouse.
- **Demora:** Este es el tiempo de demora que se haya acumulado entre las subfases **Pre-userinit y Userinit** y las subfases **Userinit y Shell**.

El tiempo total de inicio de sesión no es exactamente la suma de esas fases. Por ejemplo, algunas fases se dan simultáneamente y, en otras fases, se llevan a cabo procesos adicionales que pueden llevar a una duración de inicio de sesión más larga que la suma de las fases.

El tiempo total del inicio de sesión no incluye el tiempo de inactividad de ICA; es decir, el tiempo transcurrido entre la descarga del archivo ICA y el inicio del archivo ICA para una aplicación.

Para habilitar la apertura automática del archivo ICA en el inicio de la aplicación, configure el explorador para que abra automáticamente el archivo ICA tras descargarlo. Para obtener más información, consulte [CTX804493](#).

**Nota:**

El gráfico “Duración de inicio de sesión” muestra las fases de inicio de sesión en segundos. Los valores por debajo de un segundo se muestran en valores inferiores al segundo. Los valores por encima de 1 segundo se redondean al medio (0,5) segundo más cercano. El gráfico se ha diseñado para mostrar el valor más alto del eje Y como 200 segundos. Cualquier valor por encima de los 200 segundos se muestra con el valor real mostrado encima de la barra.

## Sugerencias para solucionar problemas

Para identificar valores poco habituales o inesperados en el gráfico, compare el tiempo tomado en cada fase de la sesión actual con los valores promedio para este usuario correspondientes a los últimos siete días, y los valores promedio para todos los usuarios del grupo de entrega, también correspondientes a los últimos siete días.

Si observa algún problema, remita la cuestión a otros administradores según sea necesario. Por ejemplo, si el inicio de la VM es lento, el problema puede estar en el hipervisor. En ese caso, contacte con el administrador del hipervisor. O bien, si la intermediación del broker es lenta, se puede remitir el problema al administrador del sitio para que compruebe el equilibrio de carga en el Delivery Controller.

Examine diferencias inusuales, como:

- Cuando falten barras de inicios de sesión (actuales)
- Discrepancias importantes entre los valores de duración actual y de duración promedio para un usuario. Las causas pueden ser:
  - Se ha instalado una nueva aplicación.
  - Se ha actualizado el sistema operativo.
  - Se realizaron cambios en la configuración.

- El tamaño del perfil del usuario es muy grande. En este caso el valor de Carga del perfil puede ser alto.
- Discrepancias importantes entre los valores de inicios de sesión del usuario (duración actual y duración promedio) y el valor de duración promedio del grupo de entrega.

Si fuera necesario, haga clic en **Reiniciar** para observar el proceso de inicio de sesión del usuario y, así, solucionar problemas de intermediación con broker o inicio de VM.

## Remedar usuarios

September 22, 2021

En Director, utilice la función Remedar usuario para ver o trabajar directamente en la máquina virtual o la sesión de un usuario. Puede remedar agentes VDA para Windows y Linux. El usuario debe estar conectado a la máquina que se va a remedar. Para comprobarlo, consulte el nombre de máquina que aparece en la barra de título del usuario.

Director inicia el remedo en una ficha nueva, por lo que debe actualizar los parámetros del explorador web para permitir elementos emergentes provenientes de la URL de Director.

Acceda a la función de remedo desde la vista **Detalles de usuario**. Seleccione la sesión del usuario y haga clic en **Remedar** en la vista “Administrador de actividades” o el panel “Detalles de la sesión”.

### Remedar agentes Linux VDA

El remedo está disponible para agentes Linux VDA 7.16 y versiones posteriores que ejecutan las distribuciones Linux RHEL 7.3 o Ubuntu 16.04.

#### Nota:

- Se debe poder acceder al VDA desde la interfaz de usuario de Director para que el remedo funcione. Por tanto, el remedo solo es posible para agentes Linux VDA que se encuentren en la misma intranet que el cliente de Director.
- Director utiliza el FQDN para conectarse al Linux VDA de destino. El cliente de Director debe poder resolver el FQDN del Linux VDA.
- El VDA debe tener instalados los paquetes python-websocketify y x11vnc.
- En la conexión noVNC al VDA, se utiliza el protocolo WebSocket. De forma predeterminada, se usa el protocolo WebSocket **ws://**. Por motivos de seguridad, Citrix recomienda usar el protocolo seguro **wss://**. Instale certificados SSL en cada cliente de Director y Linux VDA.

Siga las instrucciones indicadas en [Remedar sesiones](#) para configurar el VDA para el remedo.

1. Después de hacer clic en **Remedar**, se inicia la conexión de remedo y aparece un mensaje de confirmación en el dispositivo del usuario.
2. Indique al usuario que haga clic en **Sí** para empezar a compartir la máquina o la sesión.
3. El administrador solo puede ver la sesión a la que se aplica el remedo.

## Remedar agentes Windows VDA

Las sesiones de Windows VDA se remedan mediante la Asistencia remota de Windows. Habilite la función Asistencia remota de Windows en la máquina del usuario durante la instalación del VDA. Para obtener más información, consulte la sección [Habilitar o inhabilitar funciones](#) en “Instalar agentes VDA”.

1. Después de hacer clic en **Remedar**, se inicia la conexión de remedo y un cuadro de diálogo le pide que abra o guarde el archivo del incidente MSRC.
2. Abra el archivo del incidente con el Visor de Asistencia remota de Microsoft, si no está ya seleccionado de forma predeterminada. Aparecerá un mensaje de confirmación en el dispositivo del usuario.
3. Indique al usuario que haga clic en **Sí** para empezar a compartir la máquina o la sesión.
4. Para mayor control, pida al usuario que comparta su puntero y su teclado.

## Optimizar exploradores Microsoft Internet Explorer para el remedo

Configure Microsoft Internet Explorer para que abra automáticamente el archivo descargado de Asistencia remota de Microsoft (.msra) con el cliente de Asistencia remota.

Para ello, debe habilitar la configuración Pedir intervención del usuario automática para descargas de archivo en el Editor de directivas de grupo:

Configuración del equipo > Plantillas administrativas > Componentes de Windows > Internet Explorer > Panel de control de Internet > Página Seguridad > Zona Internet > Pedir intervención del usuario automática para descargas de archivo.

De forma predeterminada, esta opción está habilitada para los sitios en la zona de Intranet local. Si el sitio de Director no se encuentra en la zona de Intranet local, puede agregar el sitio a esta zona manualmente.

## Enviar mensajes a usuarios

September 22, 2021

Desde Director, puede enviar un mensaje a un usuario que está conectado a una o varias máquinas. Por ejemplo, puede usar esta función para enviar notificaciones inmediatas acerca de acciones administrativas, tales como unas operaciones de mantenimiento de escritorios que están a punto de tener lugar, cierres de sesión y reinicios de máquinas y restablecimientos de perfiles.

Para enviar un mensaje a un usuario, siga estos pasos:

1. Vaya a **Supervisor > Filtros > Máquinas > Todas las máquinas**.
2. Seleccione una máquina a la que desee enviar un mensaje y haga clic en **Enviar mensaje**.
3. Escriba el mensaje y haga clic en **Enviar**.

Si el mensaje se envió correctamente, aparece un mensaje de confirmación en Director. Si la máquina del usuario está conectada, aparece el mensaje allí.

Si el mensaje no se envió correctamente, aparece un mensaje de error en Director. Solucione el problema de acuerdo con el mensaje de error. Cuando haya terminado, escriba de nuevo el asunto y el texto del mensaje, y haga clic en la opción Reintentar.

## Resolver fallos de aplicación

September 22, 2021

En la vista Administrador de actividades, haga clic en la ficha Aplicaciones. Puede ver todas las aplicaciones de todas las máquinas a las que el usuario tiene acceso, incluidas las aplicaciones locales y las alojadas para la máquina conectada actualmente, y el estado actual de cada una de ellas.

**Nota:**

Si la ficha Aplicaciones aparece atenuada, póngase en contacto con un administrador con permisos para habilitarla.

La lista incluye solo las aplicaciones que se han iniciado en la sesión.

Para máquinas con sistema operativo de sesión única o multisesión, se muestran las aplicaciones para cada sesión desconectada. Si el usuario no está conectado, no se muestra ninguna aplicación.

---

Acción	Descripción
Finalizar una aplicación que dejó de responder	Elija la aplicación que no responde, y haga clic en Finalizar aplicación. Una vez que la aplicación haya finalizado, solicite al usuario que la abra de nuevo.

---

Acción	Descripción
Finalizar procesos que dejaron de responder	Si dispone de los permisos necesarios, haga clic en la ficha Procesos. Seleccione un proceso que está relacionado con la aplicación o el que está utilizando una gran cantidad de recursos de la CPU o la memoria y haga clic en Finalizar proceso. No obstante, si no dispone de los permisos necesarios para finalizar el proceso, los intentos de finalizarlo fallarán.
Reiniciar la máquina del usuario	Si se trata solo de máquinas con sistema operativo de sesión única, para la sesión seleccionada, haga clic en “Reiniciar”. Como alternativa, en la vista “Detalles de la máquina”, use los controles de energía para reiniciar o apagar la máquina. Pida al usuario que vuelva a iniciar la sesión para poder comprobar de nuevo la aplicación. Si se trata de máquinas con sistema operativo multisesión, la opción de reinicio no está disponible. En vez de reiniciar, cierre la sesión del usuario y permita que el usuario inicie sesión de nuevo.
Colocar la máquina en modo de mantenimiento	Si la imagen de la máquina necesita mantenimiento (por ejemplo, instalar una revisión o actualización de software), colóquela en modo de mantenimiento. Desde la vista “Detalles de la máquina”, haga clic en Detalles y active el modo de mantenimiento. Remita la cuestión al administrador que corresponda.

---

## Restaurar conexiones de escritorio

September 22, 2021

Desde Director, compruebe el estado de conexión del usuario a la máquina actual en la barra de título del usuario.

Si ha fallado la conexión de escritorio, se mostrará el error que hizo que fallara la conexión, lo que

puede ayudarle a solucionar el problema.

---

Acción	Descripción
Comprobar que la máquina no está en modo de mantenimiento	En la página Detalles del usuario, asegúrese de que el modo de mantenimiento está desactivado.
Reiniciar la máquina del usuario	Seleccione la máquina y haga clic en Reiniciar. Utilice esta opción si la máquina del usuario no responde o no puede conectarse a ella porque, por ejemplo, está utilizando una cantidad inusualmente alta de recursos de la CPU, lo que puede inutilizar la CPU.

---

## Restaurar sesiones

September 22, 2021

Si una sesión se desconecta, la sesión permanece activa y sus aplicaciones siguen ejecutándose, pero el dispositivo de usuario ya no se comunica con el servidor.

En la vista Detalles del usuario, se pueden solucionar fallos de sesión en el panel Detalles de la sesión. Puede ver los detalles de la sesión actual, indicada por el ID de sesión.

---

Acción	Descripción
Finalizar aplicaciones o procesos que dejaron de responder	Haga clic en la ficha Aplicaciones. Elija la aplicación que no responde y haga clic en Finalizar aplicación. Del mismo modo, seleccione los procesos correspondientes que no respondan y haga clic en Finalizar proceso. Además de eso, finalice los procesos que estén consumiendo una cantidad inusualmente alta de memoria o de recursos de la CPU, lo que puede inutilizar la CPU.

Acción	Descripción
Desconectar la sesión de Windows	Haga clic en Control de sesión y seleccione Desconectar. Esta opción solo está disponible para las máquinas con sistema operativo multisesión intermediario. En caso de sesiones sin intermediarios, la opción está inhabilitada.
Cerrar la sesión de un usuario	Haga clic en Control de sesión y seleccione Cerrar sesión.

Para probar la sesión, el usuario puede intentar volver a iniciar la sesión. También puede remedar al usuario para supervisar más de cerca esta sesión.

## Generar informes de sistema de canales HDX

January 4, 2021

En la vista

Detalles del usuario, se puede comprobar el estado de los canales HDX en la máquina del usuario en el panel HDX. Este panel solo está disponible si la máquina del usuario está conectada mediante HDX.

Si aparece un mensaje que indica que la información no está disponible actualmente, espere un minuto para que se actualice la página o haga clic en el botón Actualizar. Los datos de HDX tardan un poco más que otros datos en actualizarse.

Haga clic en el icono de advertencia o error para obtener más información.

Sugerencia:

Puede ver información acerca de otros canales en el mismo cuadro de diálogo. Para ello, haga clic en las flechas izquierda y derecha situadas en la esquina izquierda de la barra de título.

Citrix Support es quien suele utilizar los informes del sistema de canales HDX para solucionar problemas más complejos.

1. En el panel HDX, haga clic en Descargar informe del sistema.
2. Puede ver o guardar el archivo XML del informe.
  - Para ver el archivo .xml, haga clic en Abrir. El archivo .xml aparece en la misma ventana que la aplicación Director.

- Para guardar el archivo .xml, haga clic en Guardar. Aparecerá la ventana Guardar como, que pedirá una ubicación en la máquina de Director a la que descargar el archivo.

## Restablecer un perfil de usuario

January 4, 2021

### Precaución:

Cuando se restablece un perfil, aunque las carpetas y los archivos del usuario se guarden y se copian al nuevo perfil, la mayor parte de los datos del perfil se eliminan (por ejemplo, el Registro se restablece y los parámetros de aplicaciones podrían eliminarse).

1. Desde Director, busque al usuario cuyo perfil quiere restablecer y seleccione la sesión de ese usuario.
2. Haga clic en **Restablecer perfil**.
3. Indique al usuario que cierre todas las sesiones.
4. Indique al usuario que vuelva a iniciar sesión. Las carpetas y archivos del perfil de usuario que se guardaron se copian en el nuevo perfil.

### Importante:

Si el usuario tiene perfiles en varias plataformas (por ejemplo, en Windows 8 y en Windows 7), indíquele que inicie sesión primero en el mismo escritorio o aplicación que notificó como un problema. Esto garantiza el restablecimiento del perfil adecuado. Si el perfil es un perfil de usuario de Citrix, el perfil se habrá restablecido para cuando aparezca el escritorio del usuario. Si el perfil es un perfil itinerante de Microsoft, es posible que la restauración de carpetas aún esté en curso durante unos momentos. El usuario puede permanecer conectado hasta que se complete la restauración.

En los pasos anteriores, se presupone que está utilizando Citrix Virtual Desktops (VDA de escritorio). Si está utilizando Citrix Virtual Desktops (VDA de servidor) necesitará tener una sesión iniciada para realizar el restablecimiento del perfil. El usuario tiene que cerrar la sesión y volver a iniciarla para completar el restablecimiento del perfil.

Si el perfil no se restablece correctamente (por ejemplo, el usuario no puede volver a iniciar la sesión en la máquina o faltan algunos archivos), debe restaurar manualmente el perfil original.

Las carpetas (y sus archivos) del perfil del usuario se guardan y se copian en el nuevo perfil. Se copian por este orden:

- Escritorio

- Cookies
- Favoritos
- Documentos
- Imágenes
- Música
- Vídeos

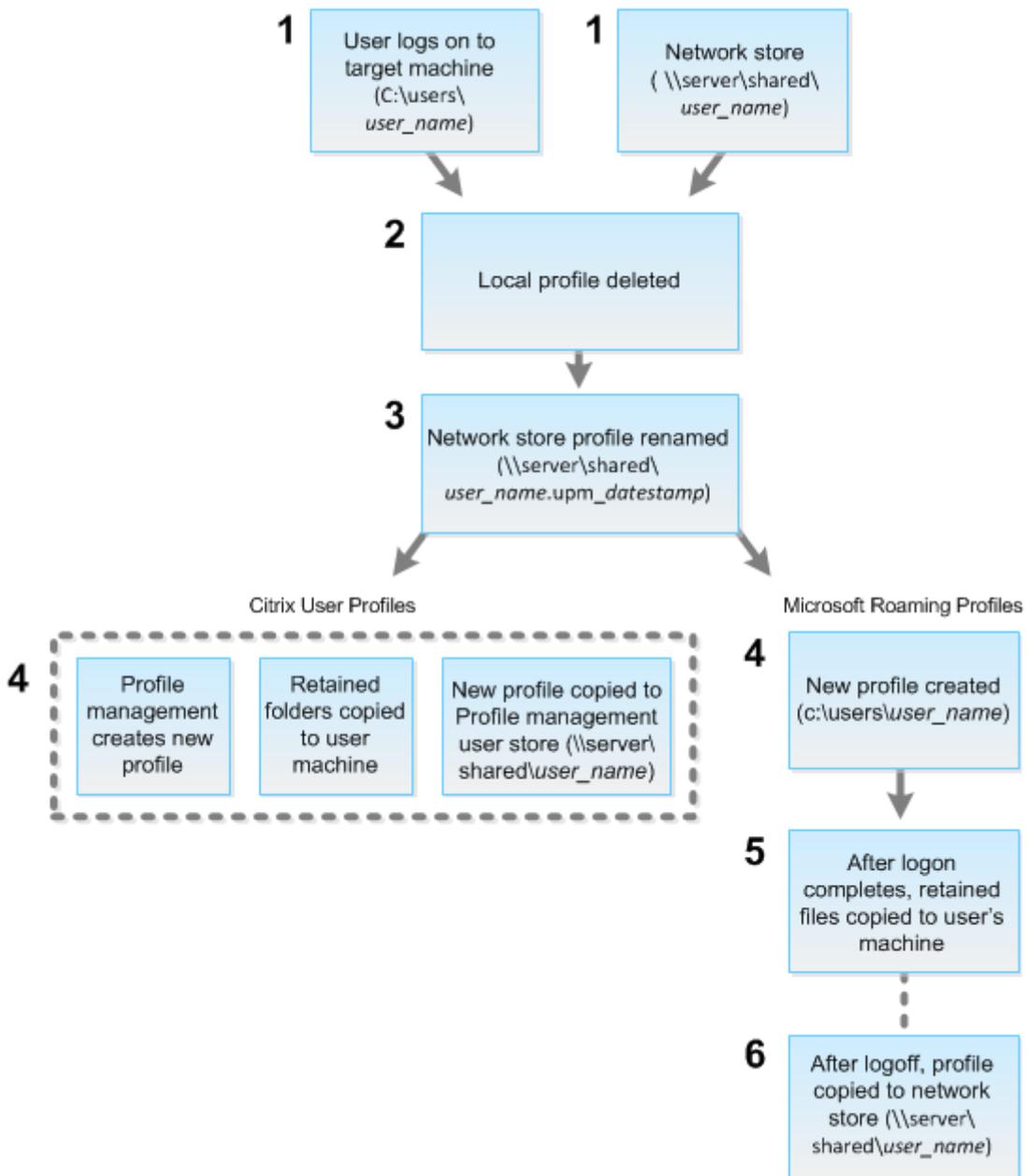
**Nota:**

En Windows 8 y versiones posteriores, las cookies no se copian cuando los perfiles se restablecen.

### **Cómo se procesan los perfiles restablecidos**

Es posible restablecer cualquier perfil de usuario de Citrix o perfil itinerante de Microsoft. Después de que el usuario cierra la sesión y se selecciona el comando para restablecer (ya sea en Director o en el SDK de PowerShell), Director primero identifica el perfil de usuario en uso y emite un comando de restablecimiento apropiado. Director recibe la información a través de Profile Management, incluida la información sobre el tamaño del perfil, el tipo de perfil y los tiempos de inicio de sesión.

Este diagrama ilustra el proceso que tiene lugar después de que el usuario inicie sesión tras restablecerse el perfil.



El comando de restablecimiento emitido por Director especifica el tipo de perfil. Después, el servicio de Profile Management intenta restablecer un perfil de ese tipo y busca el recurso compartido de red (el almacén de usuarios). Si el usuario está procesado por Profile Management, pero recibe un comando de perfil itinerante, se rechaza (o viceversa).

1. Si hay un perfil local está presente, se elimina.
2. El perfil de red se cambia de nombre.
3. La siguiente acción depende de si el perfil que se restablece es un perfil de usuario de Citrix o un perfil itinerante de Microsoft.

Para los perfiles de usuario de Citrix, el nuevo perfil se crea mediante las reglas de importación de Profile Management, y las carpetas se copian de vuelta en el perfil de red, y el usuario puede iniciar una sesión como lo hace normalmente. Si se usa un perfil itinerante para el restablecimiento, los parámetros de Registro en el perfil itinerante se conservan en el perfil restablecido. Si es necesario, puede configurar Profile Management para que un perfil de plantilla sobrescriba el perfil itinerante.

Para los perfiles móviles de Microsoft, Windows crea un perfil y, cuando el usuario inicia sesión, las carpetas se copian de nuevo en el dispositivo del usuario. Cuando el usuario cierra la sesión de nuevo, el nuevo perfil se copia en el almacén de la red.

### **Para restablecer un perfil manualmente después de un error de restablecimiento**

1. Indique al usuario que cierre todas las sesiones.
2. Elimine el perfil local si existe.
3. Busque la carpeta archivada en el recurso compartido de red que contiene la fecha y hora junto con el nombre de la carpeta, la carpeta con la extensión .upm\_fecha y hora.
4. Elimine el nombre del perfil actual; es decir, el que no tiene la extensión .upm\_fecha y hora.
5. Cambie el nombre de la carpeta archivada mediante el nombre de perfil original; es decir, elimine la extensión de fecha y hora. Con ello, habrá devuelto el perfil a su estado original, pre-restablecido.

### **Para restablecer un perfil mediante PowerShell SDK**

Puede restablecer un perfil mediante el kit Broker PowerShell SDK.

#### **New-BrokerMachineCommand**

Crea un comando en cola para su entrega a un usuario, sesión o equipo específicos. Para obtener más información sobre este cmdlet, consulte <https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerMachineCommand/>.

#### **Ejemplos**

Consulte los ejemplos siguientes para obtener detalles acerca de cómo utilizar los cmdlets de PowerShell para restablecer un perfil:

Restablecer un perfil de Profile Management

- Supongamos que quiere restablecer el perfil del usuario1. Utilice el comando de PowerShell New-BrokerMachineCommand. Por ejemplo:

```
- New-BrokerMachineCommand -Category UserProfileManager -CommandName  
  "ResetUpmProfile"-DesktopGroups 1 -CommandData $byteArray -  
  SendTrigger logon -user domain1\user1
```

**Importante:**

CommandData \$byteArray debe tener el siguiente formato: <SID>[,<backup path>]  
. Si no proporciona la ruta de acceso a la copia de seguridad, Profile Management genera una carpeta de copia de seguridad con el nombre de la fecha y hora actuales.

### Restablecer un perfil móvil de Windows

- Supongamos que quiere restablecer el perfil móvil del usuario1. Utilice el comando de PowerShell New-BrokerMachineCommand. Por ejemplo:

```
- New-BrokerMachineCommand -Category UserProfileManager -CommandName  
  "ResetRoamingProfile"-DesktopGroups 1 -CommandData $byteArray  
  -SendTrigger logon -user domain1\user1
```

## Grabar sesiones

January 4, 2021

En Director, puede grabar sesiones ICA mediante los controles de la función Grabación de sesiones, desde las pantallas **Detalles del usuario** y **Detalles de la máquina**. Esta función está disponible para los clientes de los sitios con licencia **Premium**.

Para configurar la Grabación de sesiones en Director mediante la herramienta DirectorConfig, consulte la sección **Configurar Director para usar el Servidor de grabación de sesiones** en [Crear y activar directivas de grabación](#).

Los controles de la Grabación de sesiones solo están disponibles en Director si el usuario que ha iniciado sesión tiene el permiso para modificar las directivas de la Grabación de sesiones. Este permiso puede establecerse en la consola de autorización de la Grabación de sesiones, como se describe en [Crear y activar directivas de grabación](#).

**Nota:**

Los cambios realizados en los parámetros de la Grabación de sesiones a través de Director o la Consola de directivas de grabación de sesiones surten efecto a partir de la siguiente sesión ICA.

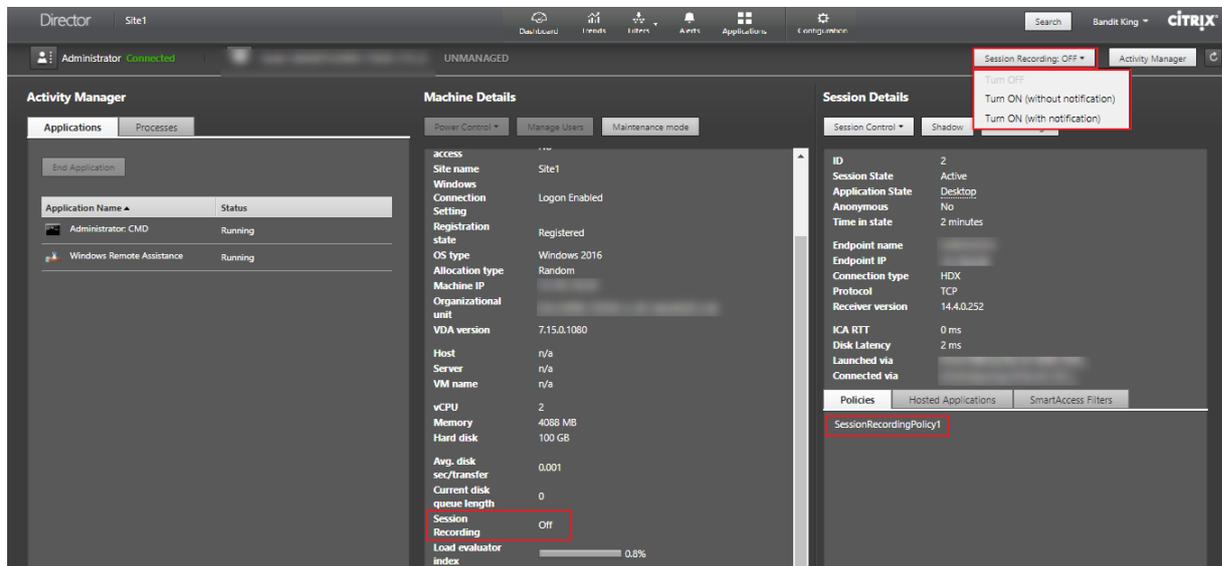
## Controles de Grabación de sesiones en Director

Puede habilitar la Grabación de sesiones para un usuario específico desde la pantalla **Administrador de actividades** o **Detalles del usuario**. Las sesiones subsiguientes de ese usuario específico se grabarán en todos los servidores compatibles.

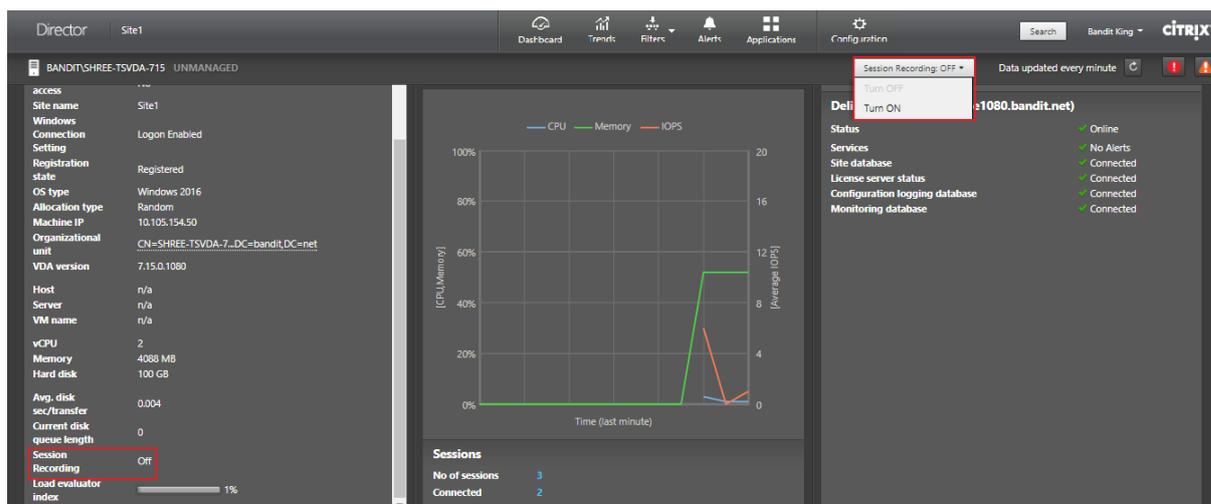
Puede hacer lo siguiente:

- Activar (con notificación): Se notifica al usuario de que la sesión se está grabando cuando este inicia una sesión ICA.
- Activar (sin notificación): La sesión se graba de forma silenciosa, sin notificar al usuario.
- Desactivar: Inhabilitar la grabación de las sesiones del usuario.

El nombre de la directiva activa de Grabación de sesiones aparece en el panel Directivas.



Puede habilitar la Grabación de sesiones para una máquina específica desde la página Detalles de la máquina. Se grabarán las sesiones subsiguientes de la máquina. El panel Detalles de la máquina muestra el estado de la directiva Grabación de sesiones de la máquina.



## Tabla de compatibilidad de funciones

August 23, 2022

Citrix Director 7 1912 es compatible con:

- Citrix Virtual Apps and Desktops 7 1909 y versiones posteriores
- Versión 7.15 LTSR de XenApp y XenDesktop

En cada sitio, aunque se puede usar Director con versiones anteriores de Delivery Controller, es posible que no estén disponibles todas las funciones de la versión más reciente de Director. Citrix recomienda tener la misma versión de Director, el Delivery Controller y los VDA.

### Nota:

Después de actualizar un Delivery Controller, se le solicitará que actualice el sitio cuando abra Studio. Para obtener más información, consulte **Secuencia de actualización** en [Actualizar la versión de una implementación](#).

La primera vez que inicie sesión después de una actualización de Director, se realiza una comprobación de versión en los sitios configurados. Si un sitio ejecuta una versión de Controller anterior a la de Director, aparece un mensaje en la consola de Director, donde se recomienda actualizar el sitio. Además, mientras la versión del sitio sea anterior a la de Director, aparecerá una nota en el panel de mandos de Director donde se indicará la diferencia de versiones.

### Nota:

Las versiones anteriores de Citrix Director no muestran directivas aplicadas a sesiones de usuario que se ejecutan en versiones recientes de VDA. Citrix Director 1912 y versiones anteriores no

muestran directivas aplicadas a las sesiones de usuario que se ejecutan en las versiones 2003 y posteriores de VDA. Utilice Citrix Director 2003 y versiones posteriores para ver esas directivas.

A continuación, se presentan las funciones específicas de Director con la versión mínima de Delivery Controller (DC), VDA y otros componentes dependientes requeridos, junto con la edición de las licencias.

<b>Versión de Director</b>	<b>Función</b>	<b>Dependencias: Versión mínima requerida</b>	<b>Edición</b>
1909	<a href="#">Configurar sitios locales con Citrix Analytics for Performance</a>	DC 7 1906 y VDA 1906	Todas
1906	<a href="#">Reconexión automática de sesión</a>	DC 7 1906 y VDA 1906	Todas
1906	<a href="#">Duración de inicio de sesión</a>	DC 7 1906 y VDA 1903	Todas
1906	<a href="#">Sondeo de escritorios</a>	DC 7 1906 y Citrix Probe Agent 1903	Premium
7.9 y versiones posteriores	<a href="#">Duración de Citrix Profile Management en la carga de perfil</a>	VDA 1903	Todas
1811	<a href="#">Desglose de perfil</a>	DC 7 1811 y VDA 1811	Todas
1811	<a href="#">Supervisar alertas de hipervisor</a>	DC 7 1811	Premium
1811	<a href="#">Sondeo de aplicaciones</a>	DC 7 1811 y Citrix Application Probe Agent 1811	Premium
1811	<a href="#">Estado de licencias RDS de Microsoft</a>	DC 7 1811 y VDA 7.16	Todas
1808	<a href="#">Exportación de datos de filtros</a>	DC 7 1808	Todas
1808	<a href="#">Desglose de la sesión interactiva</a>	DC 7 1808 y VDA 1808	Todas
1808	<a href="#">Desglose de GPO</a>	DC 7 1808 y VDA 1808	Todas

<b>Versión de Director</b>	<b>Función</b>	<b>Dependencias: Versión mínima requerida</b>	<b>Edición</b>
1808	Datos históricos disponibles de la máquina mediante la API de OData	DC 7 1808	Todas
7.18	Sondeo de aplicaciones	DC 7.18	Premium (anteriormente Platinum)
7.18	Directivas de alertas inteligentes	DC 7.18	Premium (anteriormente Platinum)
7.18	Enlace de Health Assistant	Nada	Todas
7.18	Desglose de la sesión interactiva	Nada	Todas
7.17	Autenticación con tarjetas inteligentes PIV	Nada	Todas
7.16	Análisis de aplicaciones	DC 7.16 y VDA 7.15	Todas
7.16	API de OData 4	DC 7.16	Todas
7.16	Remedo de usuarios en Linux VDA	VDA 7.16	Todas
7.16	Admitir el grupo local de dominio	Nada	Todas
7.16	Acceso a la consola de la máquina	DC 7.16	Todas
7.15	Supervisión de fallos de aplicación	DC 7.15 y VDA 7.15	Todas
7.14	Solución de problemas de aplicación	DC 7.13 y VDA 7.13	Todas
7.14	Supervisar discos	DC 7.14 y VDA 7.14	Todas
7.14	Supervisar GPU	DC 7.14 y VDA 7.14	Todas

<b>Versión de Director</b>	<b>Función</b>	<b>Dependencias: Versión mínima requerida</b>	<b>Edición</b>
7.13	Protocolo de transporte en el panel “Detalles de la sesión”	DC 7.x y VDA 7.13	Todas
7.12	Descripciones claras de los errores de conexión y de máquina	DC 7.12 y VDA 7.x	Todas
7.12	Mayor disponibilidad de datos históricos en la edición Enterprise	DC 7.12 y VDA 7.x	Empresarial
7.12	Informes personalizados	DC 7.12 y VDA 7.x	Premium (anteriormente Platinum)
7.11	Informes de utilización de recursos	DC 7.11 y VDA 7.11	Todas
7.11	Alertas extendidas para condiciones de CPU, memoria y RTT de ICA	DC 7.11 y VDA 7.11	Premium (anteriormente Platinum)
7.11	Mejoras en la exportación de informes	DC 7.11 y VDA 7.x	Todas
7.11	Integración en Citrix ADM	DC 7.11, VDA 7.x y MAS versión 11.1, compilación 49.16	Premium (anteriormente Platinum)
7.9	Desglose de la duración del inicio de sesión	DC 7.9 y VDA 7.x	Todas
7.7	Supervisión y alertas mejoradas	DC 7.7 y VDA 7.x	Premium (anteriormente Platinum)
7.7	Integrar en SCOM	DC 7.7, VDA 7.x, SCOM 2012 R2 y PowerShell 3.0	Premium (anteriormente Platinum)

<b>Versión de Director</b>	<b>Función</b>	<b>Dependencias: Versión mínima requerida</b>	<b>Edición</b>
7.7	<a href="#">Integrar en Autenticación de Windows</a>	DC 7.x y VDA 7.x	Todas
7.7	<a href="#">Uso de SO de sesión única y SO multisesión</a>	DC 7.7 y VDA 7.x	Premium (anteriormente Platinum)
7.6.300	<a href="#">Compatibilidad con canal virtual Framehawk</a>	DC 7.6 y VDA 7.6	Todas
7.6.200	<a href="#">Integrar en la Grabación de sesiones</a>	DC 7.6 y VDA 7.x	Premium (anteriormente Platinum)
7	<a href="#">Integrar en HDX Insight</a>	DC 7.6, VDA 7.x y Citrix ADM	Premium (anteriormente Platinum)

## Granularidad y retención de datos

December 1, 2022

### Agregar valores de datos

Monitor Service recopila una serie de datos, incluidos el uso de las sesiones de usuario, la información del rendimiento de los inicios de sesión de usuario, la información del equilibrio de carga de las sesiones y la información de fallos de conexión y de las máquinas. Los datos se agregan de forma diferente en función de la categoría. Para interpretar los datos, es fundamental comprender la agregación de los valores de los datos presentados mediante las API de Método de OData. Por ejemplo:

- Los errores de máquinas y sesiones conectadas se producen durante un período de tiempo. Por lo tanto, se exponen como máximos a lo largo de un período de tiempo.
- La duración del inicio de sesión es una medida de tiempo, por lo que se expone como el promedio en las métricas tomadas a lo largo de un período de tiempo.

- Los recuentos de inicio de sesión y los fallos de conexión son el número de casos a lo largo de un período de tiempo, por lo que se exponen como sumas para un período de tiempo.

## **Evaluar datos simultáneos**

Las sesiones deben superponerse para considerarse simultáneas. No obstante, cuando el intervalo de tiempo es de 1 minuto, todas las sesiones en ese minuto (se superpongan o no) se consideran simultáneas; es decir, el tamaño del intervalo es tan pequeño que se considera que el esfuerzo de rendimiento que conlleva un cálculo más preciso no agrega mucho valor. Si las sesiones se producen en la misma hora, pero no en el mismo minuto, no se consideran superpuestas.

## **Correlacionar tablas de resumen con datos sin procesar**

El modelo de datos representa las métricas de dos maneras diferentes:

- Las tablas de resumen representan vistas agregadas de las métricas por minuto, por hora y por día.
- Los datos sin procesar representan eventos individuales o de estado actual de seguimiento de una sesión, conexión, aplicación y otros objetos.

Al intentar establecer una correlación entre las llamadas de la API o en el modelo de datos mismo, es importante comprender los conceptos y las limitaciones siguientes:

- **No hay datos de resumen para intervalos parciales.** Los resúmenes de métricas están diseñados para satisfacer las necesidades de tendencias históricas en períodos de tiempo prolongados. Estas métricas se agregan en la tabla de resumen para intervalos completos. No habrá datos de resumen para un intervalo parcial al comienzo (en los datos más antiguos) de la recopilación de datos ni al final de esta. Cuando se consultan los datos agregados de un día (Intervalo=1440), esto significa que los días incompletos al principio y los más recientes no tendrán datos. Aunque es posible que existan datos sin formato para esos intervalos parciales, estos datos no se resumirán. Para determinar el intervalo combinado más antiguo y reciente para una granularidad de datos en particular, se puede usar la fecha de resumen (SummaryDate) máxima y mínima de una tabla de resumen. La columna SummaryDate representa el inicio del intervalo. El valor de la columna Granularity representa la duración del intervalo para los datos agregados.
- **Correlación por tiempo.** Las métricas se agregan en la tabla de resumen para intervalos completos, como se ha descrito antes. Se pueden usar para descubrir tendencias históricas, pero los eventos sin procesar pueden ser más actualizados en los datos de estado que lo que se resumió para el análisis de tendencias. En cualquier comparación basada en el tiempo entre datos de resumen y datos sin procesar, hay que tener en cuenta que no habrá datos de resumen para

intervalos parciales que puedan ocurrir ni para el comienzo o el final del periodo de tiempo en cuestión.

- **Eventos latentes y perdidos.** Las métricas agregadas en tablas de resumen pueden ser ligeramente inexactas si hay eventos perdidos o latentes en el periodo de agregación. Aunque Monitor Service intenta mantener un alto nivel de precisión del estado actual, no vuelve atrás en el tiempo para recalcular la agregación en las tablas de resumen para eventos perdidos o latentes.
- **Alta disponibilidad de conexiones.** Durante la alta disponibilidad de conexiones, habrá huecos en los datos de resumen sobre los recuentos de las conexiones actuales, pero las instancias de sesión seguirán ejecutándose en los datos sin procesar.
- **Períodos de retención de datos.** Los datos de las tablas de resumen se conservan siguiendo una programación de limpieza distinta de la programación para datos de eventos sin procesar. Puede que falten datos porque se hayan limpiado las tablas de resumen y de datos sin procesar. Los períodos de retención también pueden diferir según las distintas granularidades de los datos de resumen. Una granularidad de datos menor (minutos) se limpia más rápidamente que una granularidad de datos mayor (días). Si faltan datos de una granularidad debido a una limpieza, puede que los encuentre en una granularidad mayor. Puesto que las llamadas de API solo devuelven la granularidad solicitada, si no se reciben datos para una granularidad, eso no significa que los datos no existan en una granularidad mayor para el mismo período de tiempo.
- **Zonas horarias.** Las métricas se guardan con marcas de hora UTC. Las tablas de resumen se agregan en límites de una hora de la zona horaria. Para las zonas horarias que no caen en límites de una hora, puede haber una discrepancia en cuanto a dónde se agregan los datos.

## Granularidad y retención

La granularidad de los datos agregados obtenida por Director es una función del intervalo de tiempo (T) solicitado. Las reglas son las siguientes:

- $0 < T \leq 1$  hora, se utiliza granularidad de minutos
- $0 < T \leq 30$  días, se utiliza granularidad de horas
- $T > 31$  días, se utiliza granularidad de días

Los datos solicitados que no provienen de datos agregados provienen de la información sin procesar sobre sesiones y conexiones. Estos datos tienden a aumentar rápidamente y, por lo tanto, tienen su propia configuración de limpieza. La limpieza de la base de datos garantiza que solo se conserven los datos que sean relevantes a largo plazo. Esto garantiza un mejor rendimiento, al tiempo que se mantiene la granularidad necesaria para crear informes. Los clientes de Premium pueden cambiar la retención de limpieza por la cantidad de días de retención que quieran; si no la cambian, se usa la predeterminada. En caso de pérdida de conectividad con la base de datos del sitio, Monitor Service

utilizará los días de retención predeterminados para el derecho de uso de Premium, tal y como se especifica en esta tabla.

Para acceder a los parámetros, ejecute los siguientes comandos de PowerShell en el Delivery Controller:

```

1 asnp Citrix.*
2 Get-MonitorConfiguration
3 Set-MonitorConfiguration -<setting name> <value>
4 <!--NeedCopy-->
    
```

	Nombre del parámetro	Limpieza afectada	Valor predeterminado (días) con Premium	Valor predeterminado (días) sin Premium
1	GroomSessionsRetentionDays	registros de conexión y de sesión después de cerrar la sesión	90	7
2	GroomFailuresRetentionDays	Registro de MachineFailureLog y Connection-FailureLog	90	7
3	GroomLoadIndexRetentionDays	Registro de LoadIndex	90	7

	Nombre del parámetro	Limpieza afectada	Valor prede-terminado (días) con Premium	Valor prede-terminado (días) sin Premium
4	GroomDeletedResources	Entidad de máquina, catálogo de máquinas, grupo de escritorios e hipervisor cuyo estado de ciclo de vida (LifecycleState) es “Eliminado” (Deleted). Esta acción también elimina los registros de Session, SessionDetail, Summary, Failure o LoadIndex relacionados.	90	7
5	GroomSummaryReports	Desktop-GroupSummary, FailureLog-Summary y LoadIndex-Summary. Datos agregados: granularidad diaria	90	7

	Nombre del parámetro	Limpieza afectada	Valor prede-terminado (días) con Premium	Valor prede-terminado (días) sin Premium
6	GroomMachineFiles	Archivos rápidos aplicados a las máquinas de VDA y Controllers	90	90
7	GroomMinuteRetention	agregados: granularidad de minuto	3	3
8	GroomHourlyRetention	agregados: granularidad horaria	32	7
9	GroomApplicationInstance	instancias de aplicación	0	0
10	GroomNotificationRegister	registro de notificaciones	0	0
11	GroomResourceUsageData	utilización de recursos: datos sin procesar	1	1
12	GroomResourceUsageData	resumidos de utilización de recursos: granularidad de minuto	7	7

	Nombre del parámetro	Limpieza afectada	Valor predefinido (días) con Premium	Valor predefinido (días) sin Premium
13	GroomResourceUsageHourDataRetentionDays	resumidos de utilización de recursos: granularidad de hora	30	7
14	GroomResourceUsageDayDataRetentionDays	resumidos de utilización de recursos: granularidad de día	30	7
15	GroomProcessUsageDataRetentionDays	utilización de procesos: datos sin procesar	1	1
16	GroomProcessUsageMinuteDataRetentionDays	utilización de procesos: granularidad de minuto	3	3
17	GroomProcessUsageHourDataRetentionDays	utilización de procesos: granularidad horaria	7	7
18	GroomProcessUsageDayDataRetentionDays	utilización de procesos: granularidad diaria	30	7
19	GroomSessionMetricsDataRetentionDays	métricas de sesiones	1	1

	Nombre del parámetro	Limpieza afectada	Valor predefinido (días) con Premium	Valor predefinido (días) sin Premium
20	GroomMachineMetricsDataRetentionDays	Datos de métricas de máquinas	3	3
21	GroomMachineMetricsDaySummaryDataRetentionDays	resumidos de métricas de máquinas	3	3
22	GroomApplicationErrorsDataRetentionDays	errores de aplicaciones	1	1
23	GroomApplicationCrashesDataRetentionDays	fallos de aplicaciones	1	1

**Precaución:**

Modificar valores de la base de datos de Monitor Service requiere reiniciar el servicio para que los nuevos valores surtan efecto. Se recomienda realizar cambios en la base de datos de Monitor Service solo cuando se lo indique el personal de asistencia técnica de Citrix.

Los parámetros GroomProcessUsageRawDataRetentionDays, GroomResourceUsageRawDataRetentionDays y GroomSessionMetricsDataRetentionDays se limitan a sus valores predeterminados de 1, mientras que GroomProcessUsageMinuteDataRetentionDays se limita a su valor predeterminado de 3. Los comandos de PowerShell para establecer estos valores se han inhabilitado, ya que los datos de uso del proceso tienden a crecer con rapidez.

Además, los parámetros de la retención basada en licencia son los siguientes:

- **Sitios con licencias Premium:** Se puede actualizar la configuración de retención de limpieza de datos con cualquier cantidad de días.
- **Sitios con licencias Advanced:** La retención de limpieza de datos para todos los parámetros se limita a 31 días.
- **Todos los demás sitios:** La retención de limpieza de datos para todos los parámetros se limita a 7 días.

**Excepciones:**

- GroomApplicationInstanceRetentionDays solo se puede establecer en sitios con licencia Premium.
- GroomApplicationErrorsRetentionDays y GroomApplicationFaultsRetentionDays están limitados a 31 días en sitios con licencia Premium.

La retención de datos durante largos períodos de tiempo tiene las implicaciones siguientes en los tamaños de las tablas:

- **Datos por hora.** Si se conservan datos por hora en la base de datos durante dos años, un sitio con 1000 grupos de entrega puede hacer que la base de datos crezca así:

1000 grupos de entrega x 24 horas/día x 365 días/año x 2 años = 17 520 000 filas de datos. El impacto que esta gran cantidad de datos tiene en el rendimiento de las tablas agregadas es importante. Puesto que los datos de panel de mandos se sacan de esta tabla, los requisitos del servidor de la base de datos pueden ser altos. Si la cantidad de datos es excesiva, el impacto en el rendimiento puede resultar significativo.

- **Datos de sesiones y eventos.** Estos datos se recopilan cada vez que comienza una sesión y se realiza una conexión o reconexión. En sitios grandes (100 000 usuarios), estos datos pueden crecer muy rápidamente. Por ejemplo, las tablas correspondientes a dos años recopilarían más de un TB de datos, para lo cual se necesitaría una base de datos de nivel empresarial de gama alta.

## Motivos de fallo y solución de problemas en Citrix Director

May 24, 2024

En las tablas siguientes, se describen las distintas categorías de errores, los motivos de estos y la acción necesaria para resolver los problemas. Para obtener más información, consulte [Enumeraciones, códigos de error y descripciones](#).

### Errores de conexión

Categoría	Motivo	Problema	Acción
N/D	[0] Unknown. Este código de error no está asignado.	El servicio de supervisión no puede determinar el motivo del fallo de inicio o conexión notificado a partir de la información compartida desde el servicio de intermediación.	Recopile registros de CDF en el Controller y contacte con Citrix Support.
[0] None	[1] None	Ninguno	N/D
[2] MachineFailure	[2] SessionPreparation	Ha fallado la solicitud de preparación de sesión enviada desde el Delivery Controller al VDA. Causas posibles: Problemas de comunicación entre el Controller y el VDA, problemas que tiene el Broker Service al crear una solicitud de preparación o problemas de red que provocan que el VDA no acepte la solicitud.	Consulte los pasos de solución de problemas indicados en el artículo <a href="#">Solución de problemas al registrar Virtual Delivery Agent en Delivery Controllers en Citrix Virtual Apps and Desktops</a> de Knowledge Center para ver los motivos frecuentes de problemas de comunicación entre el Controller y el VDA.
[2] MachineFailure	[3] RegistrationTimeout	El VDA estaba encendido, pero se agotó el tiempo de espera al intentar registrarse en el Delivery Controller.	Compruebe que Citrix Broker Service se está ejecutando en el Delivery Controller y que Desktop Service se está ejecutando en el VDA. Si estos servicios están detenidos, inícielos.

Categoría	Motivo	Problema	Acción
[1] ClientConnection-Failure	[4] ConnectionTimeout	El cliente no se conectó al VDA, aunque el VDA estuviera preparado para iniciar la sesión. La sesión se negoció correctamente, pero se agotó el tiempo de espera mientras se esperaba a que el cliente se conectara al VDA. Causas posibles: Configuración del firewall, interrupciones de red o configuraciones que impiden las conexiones remotas.	Consulte la consola de Director para ver si el cliente tiene alguna conexión activa, lo que significa que ningún usuario se ve afectado. Si no hay ninguna sesión, revise los registros de eventos en el cliente y en el VDA en busca de errores. Resuelva los problemas que haya relacionados con la conectividad de red entre el cliente y el VDA.
[4] NoLicensesAvailable	[5] Licensing	Ha fallado la solicitud de licencias. Causas posibles: Cantidad insuficiente de licencias, o bien, el servidor de licencias ha estado inactivo durante más de 30 días.	Compruebe que el servidor de licencias esté en línea y sea accesible. Resuelva los problemas de conectividad de red que hubiera con el servidor de licencias o reinicie el servidor de licencias si parece que no funciona correctamente. Verifique que hay licencias suficientes en el entorno y asigne más si es necesario.

Categoría	Motivo	Problema	Acción
[1] ClientConnection-Failure	[6] Ticketing	Ocurrió un error de tíquets, que indica que la conexión del cliente al VDA no coincide con la solicitud del broker. El broker prepara un tíquet de solicitud de inicio y lo entrega en el archivo ICA. Cuando el usuario intenta iniciar una sesión, el VDA valida con el broker el tíquet de inicio presente en el archivo ICA. Causas posibles: El archivo ICA está dañado o el usuario intenta realizar una conexión no autorizada.	Verifique que el usuario tiene acceso a la aplicación o al escritorio en función de los grupos de usuarios definidos en los grupos de entrega. Indique al usuario que vuelva a iniciar la aplicación o el escritorio para determinar si se trata de un problema puntual. Si el problema se vuelve a producir, revise los registros de eventos del dispositivo cliente en busca de errores. Compruebe que el VDA al que el usuario está intentando conectarse está registrado. Si no está registrado, revise los registros de eventos en el VDA y resuelva los problemas de registro.
[1] ClientConnection-Failure	[7] Otros	El VDA notificó que la sesión fue terminada después de que el cliente contactara inicialmente con el VDA pero antes de completarse la secuencia de conexión.	Verifique que la sesión no fue terminada por el usuario antes del inicio. Intente volver a iniciar la sesión. Si el problema continúa, recopile registros de CDF y contacte con Citrix Support.

Categoría	Motivo	Problema	Acción
[1] ClientConnection-Failure	[8] GeneralFail	La sesión no se inició. Causas posibles: Se solicitó un inicio con broker mientras este todavía estaba iniciándose o inicializándose, o bien, se produjo un error interno durante la fase del broker de un inicio.	Verifique que Citrix Broker Service se está ejecutando y vuelva a intentar iniciar la sesión.
[5] Configuration	[9] MaintenanceMode	El VDA, o el grupo de entrega al que pertenece el VDA, está en modo de mantenimiento.	Determine si se requiere el modo de mantenimiento. Inhabilite el modo de mantenimiento en el grupo de entrega o la máquina en cuestión si no es necesario e indique al usuario que intente volver a conectarse.
[5] Configuration	[10] ApplicationDisabled	La aplicación fue inhabilitada por el administrador y los usuarios finales no pueden acceder a ella.	Si la aplicación tiene que estar disponible para su uso en producción, habilítela y pida al usuario que se reconecte.
[4] NoLicensesAvailable	[11] LicenseFeatureRefused	La función utilizada no está cubierta por las licencias existentes.	Contacte con un representante de ventas de Citrix para verificar las funciones que están cubiertas por el tipo de licencias y la edición de Citrix Virtual Apps and Desktops que tiene.

Categoría	Motivo	Problema	Acción
[3] NoCapacityAvailable	[13] SessionLimitReached	Todos los VDA están en uso y no hay capacidad para alojar sesiones adicionales. Causas posibles: Todos los VDA están ocupados (para VDA con SO de sesión única), o bien, todos los VDA han alcanzado el máximo configurado de sesiones simultáneas permitidas (para VDA con SO multisesión).	Compruebe si hay algún VDA en modo de mantenimiento. Desactive el modo de mantenimiento si no es necesario para obtener más capacidad. Puede aumentar el valor de <b>Número máximo de sesiones</b> en la configuración de directiva de Citrix para permitir más sesiones por VDA de servidor. También puede agregar más VDA con SO multisesión. Asimismo, tenga en cuenta la opción de agregar más VDA con SO de sesión única.
[5] Configuration	[14] DisallowedProtocol	Los protocolos ICA y RDP no están permitidos.	Ejecute el comando <b>Get-BrokerAccessPolicyRule</b> de PowerShell en un Delivery Controller y compruebe si el valor de <b>AllowedProtocols</b> incluye todos los protocolos necesarios. Este problema se produce solo si hay una configuración incorrecta.

Categoría	Motivo	Problema	Acción
[5] Configuration	[15] ResourceUnavailable	La aplicación o el escritorio al que el usuario intenta conectarse no está disponible. Es posible que esta aplicación o escritorio no existan, o bien, no haya agentes VDA disponibles para ejecutarlos. Causas posibles: Se ha anulado la publicación de la aplicación o el escritorio, o bien, los agentes VDA que alojan la aplicación o el escritorio han alcanzado la carga máxima, o bien, la aplicación o el escritorio están en modo de mantenimiento.	Verifique que la aplicación o el escritorio aún siguen publicados y que los VDA no están en modo de mantenimiento. Determine si los VDA con SO multisesión están a plena carga. Si es así, aprovisiona más VDA con SO multisesión. Compruebe que haya VDA con SO de sesión única disponibles para las conexiones. Aprovisiona más VDA con SO de sesión única si es necesario.
[5] Configuration	[16] ActiveSessionReconnectDisabled	La sesión ICA está activa y conectada a otro dispositivo de punto final. Sin embargo, dado que la <b>reconexión para sesiones activas</b> está inhabilitada, el cliente no puede conectarse a la sesión activa.	En el Controller, compruebe que la <b>reconexión para sesiones activas</b> está habilitada. Compruebe que el valor de <b>DisableActiveSessionReconnect</b> en el Registro, en <b>HKEY_LOCAL_MACHINE\Software</b> está establecido en 0.

Categoría	Motivo	Problema	Acción
[2] MachineFailure	[17] NoSessionToReconnect	El cliente intentó reconectarse a una sesión específica, pero la sesión fue terminada.	Vuelva a intentar la reconexión de control del espacio de trabajo.
[2] MachineFailure	[18] SpinUpFailed	El VDA no se puede encender para iniciar la sesión. Se trata de un problema del que informa el hipervisor.	Si la máquina sigue apagada, intente iniciarla desde Citrix Studio. Si eso falla, revise la conectividad y los permisos del hipervisor. Si el VDA es una máquina provisionada con PVS, compruebe en la consola de PVS que la máquina se está ejecutando. Si no es el caso, compruebe que la máquina tiene asignado un disco Personal vDisk, e inicie sesión en el hipervisor para restablecer la máquina virtual.
[2] MachineFailure	[19] Refused	El Delivery Controller envía una solicitud al VDA para prepararse para una conexión desde un usuario final, pero el VDA rechaza activamente esta solicitud.	Verifique por ping que el Controller y el VDA puedan comunicarse correctamente. De lo contrario, resuelva cualquier problema de enrutamiento de red o firewall.

Categoría	Motivo	Problema	Acción
[2] MachineFailure	[20] ConfigurationSet Failure	El Delivery Controller no envió al VDA los datos de configuración requeridos, tales como información de la sesión y configuración de directivas, durante el inicio de la sesión. Causas posibles: Problemas de comunicación entre el Controller y el VDA, problemas que tiene el Broker Service al crear una solicitud de configuración o problemas de red que provocan que el VDA no acepte la solicitud.	-
[3] NoCapacityAvailable	[21] MaxTotalInstancesExceeded	Se alcanzó la cantidad máxima de instancias de una aplicación. No se pueden abrir instancias adicionales de la aplicación en el VDA. Este problema está relacionado con la función de límites de aplicaciones.	Considere la opción de incrementar el valor del parámetro de la aplicación <b>Limitar la cantidad de instancias ejecutadas a la vez a</b> , si el sistema de licencias lo permite.

Categoría	Motivo	Problema	Acción
[3] NoCapacityAvailable	[22] MaxPerUserInstancesExceeded	El usuario está intentando abrir más de una instancia de una aplicación, pero dicha aplicación está configurada para permitir ejecutar solo una instancia por usuario. Este problema está relacionado con la función de límites de aplicaciones.	De forma predeterminada, solo se permite una instancia de la aplicación por usuario. Si se requieren varias instancias por usuario, puede desmarcar <b>Limitar a una sola instancia por usuario</b> en la configuración de la aplicación.
[1] ClientConnection-Failure	[23] Communication error	El Delivery Controller intentó enviar información al VDA (por ejemplo, una solicitud para prepararse para una conexión), pero ocurrió un error durante el intento de comunicación. Este error puede deberse a interrupciones de la red.	Si ya se ha iniciado, reinicie Desktop Service en el VDA para reiniciar el proceso de registro y compruebe que el VDA se registra correctamente. Confirme que los Controllers configurados para el VDA son los correctos. Para ello, consulte los datos del registro de eventos de la aplicación.

---

Categoría	Motivo	Problema	Acción
[3] NoCapacityAvailable	[100] NoMachineAvailable El servicio de supervisión convierte [12] NoDesktopAvailable a este código de error.	El estado del VDA asignado para iniciar la sesión no es válido, o el VDA no está disponible. Causas posibles: El estado de energía del VDA es desconocido o no está disponible, el VDA no se reinició desde la última sesión del usuario, el uso compartido de sesiones está inhabilitado pero la sesión actual requiere que esté habilitado, o bien, el VDA se quitó del grupo de entrega o del sitio.	Compruebe que el VDA se encuentra en el grupo de entrega. De lo contrario, agréguelo al grupo de entrega apropiado. Verifique que haya suficientes VDA registrados y preparados para el inicio de la aplicación o el escritorio compartidos y publicados que ha solicitado el usuario. Verifique que el hipervisor que aloja el VDA no está en modo de mantenimiento.

Categoría	Motivo	Problema	Acción
[2] MachineFailure	[101] MachineNotFunctional. El servicio de supervisión convierte [12] NoDesktopAvailable a este código de error.	El VDA no está operativo. Causas posibles: El VDA se quitó del grupo de entrega, el VDA no está registrado, el estado de energía del VDA no está disponible o el VDA tiene problemas internos.	Compruebe que el VDA se encuentra en el grupo de entrega. De lo contrario, agréguelo al grupo de entrega apropiado. Compruebe que el VDA se muestra como encendido en Citrix Studio. Si se desconoce el estado de energía de varias máquinas, resuelva cualquier problema que haya relacionado con la conectividad al hipervisor o con errores del host. Verifique que el hipervisor que aloja el VDA no está en modo de mantenimiento. Reinicie el VDA una vez que se hayan solucionado estos problemas.

### Tipo de fallo de la máquina

Código de error	ID del código de error	Problema	Acción
Desconocido	-	-	-
Sin registrar	3	-	-

---

Código de error	ID del código de error	Problema	Acción
MaxCapacity	4	El índice de carga en el hipervisor está a máxima capacidad.	Compruebe que todos los hipervisores están iniciados. Aumente la capacidad del hipervisor. Agregue más hipervisores.
StuckOnBoot	2	La VM no completó su secuencia de arranque y no se está comunicando con el hipervisor.	Compruebe que la máquina virtual ha arrancado correctamente en el hipervisor. Compruebe si hay otros mensajes en la VM, tales como problemas de SO. Compruebe que la VM tiene instaladas las herramientas de hipervisor. Compruebe que el VDA está instalado en la VM.
FailedToStart	1	La VM tuvo problemas al intentar iniciarse en el hipervisor.	Consulte los registros del hipervisor.
Ninguno	0	-	-

---

**Motivo de anulación del registro de la máquina (se aplica cuando el tipo de fallo es Sin registrar o Desconocido)**

---

Código de error	ID del código de error	Problema	Acción
AgentShutdown	0	El VDA se apagó correctamente.	Encienda el VDA si no debería estar apagado según las directivas de administración de energía existentes. Revise los errores que haya en los registros de eventos.
AgentSuspended	1	El VDA está en modo de suspensión o hibernación.	Saque al VDA del modo de hibernación. Considere la opción de inhabilitar la hibernación de los VDA de Citrix Virtual Apps and Desktops en los parámetros de energía.
IncompatibleVersion	100	El VDA no se puede comunicar con el Delivery Controller debido a que las versiones del protocolo de Citrix no coinciden.	Equipare las versiones del VDA y del Delivery Controller.

Código de error	ID del código de error	Problema	Acción
AgentAddressResolutionFailed		El Delivery Controller no pudo resolver la dirección IP del VDA.	Compruebe que la cuenta de la máquina del VDA existe en AD. Si no es así, créela. Compruebe que sean correctos el nombre y la dirección IP del VDA en DNS. Si no es así, corríjalos. Si se trata de un problema generalizado, compruebe los parámetros de DNS en los Controllers. Verifique la resolución de DNS desde el Controller. Para ello, ejecute el comando <code>nslookup</code> .
	101	El Delivery Controller no pudo resolver la dirección IP del VDA.	Compruebe que la cuenta de la máquina del VDA existe en AD. Si no es así, créela. Compruebe que sean correctos el nombre y la dirección IP del VDA en DNS. Si no es así, corríjalos.

---

Código de error	ID del código de error	Problema	Acción
AgentNotContactable	102	Hubo un problema de comunicación entre el Delivery Controller y el VDA.	Utilice ping para comprobar que el Delivery Controller y el VDA pueden comunicarse. Si no es el caso, resuelva los problemas de firewall o red que haya. Consulte los pasos de solución de problemas indicados en el artículo <a href="#">Solución de problemas al registrar Virtual Delivery Agent en Delivery Controllers en Citrix Virtual Apps and Desktops (CTX136668)</a> de Knowledge Center para ver los motivos frecuentes de problemas de comunicación entre el Controller y el VDA.

Código de error	ID del código de error	Problema	Acción
	102	Hubo un problema de comunicación entre el Delivery Controller y el VDA.	Consulte los pasos de solución de problemas indicados en el artículo <a href="#">Solución de problemas al registrar Virtual Delivery Agent en Delivery Controllers en Citrix Virtual Apps and Desktops (CTX136668)</a> de Knowledge Center para ver los motivos frecuentes de problemas de comunicación entre el Controller y el VDA. Contacte con Citrix Support.
AgentWrongActiveDirectory	103U	Configuración incorrecta de la detección de Active Directory. La unidad organizativa específica del sitio (donde se guarda la información de Controllers del sitio en AD) configurada en el Registro del VDA corresponde a otro sitio.	Compruebe que la configuración de Active Directory es correcta o consulte los parámetros del Registro.

Código de error	ID del código de error	Problema	Acción
EmptyRegistrationRequest	104	La solicitud de registro enviada desde el VDA al Delivery Controller estaba vacía. Puede deberse a una instalación dañada del software del VDA.	Reinicie Desktop Service en el VDA para reiniciar el proceso de registro y compruebe si el VDA se registra correctamente. Para ello, consulte los registros de eventos de aplicación.
MissingRegistrationCapabilities	105	La versión del VDA no es compatible con el Delivery Controller.	Actualice el VDA, o quítelo y vuelva a instalarlo.
MissingAgentVersion	106	La versión del VDA no es compatible con el Delivery Controller.	Reinstale el software del VDA si el problema afecta a todas las máquinas.
InconsistentRegistrationCapabilities	107	El VDA no puede comunicar sus capacidades al broker. Puede deberse a una incompatibilidad entre las versiones del VDA y del Delivery Controller. Las capacidades de registro, que cambian con cada versión, están expresadas de una forma que no coincide con la solicitud de registro.	Equipare las versiones del VDA y del Delivery Controller.
NotLicensedForFeature	108	La función que intenta usar no tiene licencia.	Consulte su edición de Citrix Licensing o quite el VDA y vuelva a instalarlo.
	108	La función que intenta usar no tiene licencia.	Contacte con Citrix Support.

Código de error	ID del código de error	Problema	Acción
UnsupportedCredentialSecurity version	109	El VDA y el Delivery Controller no están usando el mismo mecanismo de cifrado.	Equipare las versiones del VDA y del Delivery Controller.
InvalidRegistrationRequest	110	El VDA hizo una solicitud de registro al broker, pero el contenido de la solicitud de registro está dañado o no es válido.	Consulte los pasos de solución de problemas indicados en el artículo <a href="#">Solución de problemas al registrar Virtual Delivery Agent en Delivery Controllers en Citrix Virtual Apps and Desktops (CTX136668)</a> de Knowledge Center para ver los motivos frecuentes de problemas de comunicación entre el Controller y el VDA.
SingleMultiSessionMismatch	111	El tipo de sistema operativo del VDA no es compatible con el catálogo de máquinas o el grupo de entrega.	Agregue la máquina VDA al tipo de catálogo de máquinas o grupo de entrega correcto que contenga máquinas con el mismo sistema operativo.
FunctionalLevelTooLowForCatalog	112	El catálogo de máquinas está definido con un nivel funcional de VDA superior al de la versión de VDA instalada.	Compruebe que el nivel funcional del catálogo de máquinas del VDA coincide con el del VDA. Actualice o revierta la versión del catálogo de máquinas para que coincida con la del VDA.

Código de error	ID del código de error	Problema	Acción
FunctionalLevelTooLowForDesktopGroup	100	El grupo de entrega está definido con un nivel funcional de VDA superior al de la versión de VDA instalada.	Compruebe que el nivel funcional del grupo de entrega del VDA coincide con el del VDA. Actualice o revierta la versión del catálogo de máquinas para que coincida con la del VDA.
PowerOff	200	El VDA no se apagó correctamente.	Si el VDA debiera estar encendido, intente iniciarlo desde Citrix Studio y compruebe que arranca y se registra correctamente. Solucione cualquier problema de arranque o registro. Consulte los registros de eventos en el VDA una vez que se haya iniciado para determinar la causa del apagado.
AgentRejectedSettingsUpdate	100	Se cambiaron o actualizaron algunos parámetros, tales como directivas de Citrix, pero hubo un error al enviar las actualizaciones al VDA. Puede ocurrir si las actualizaciones son incompatibles con la versión de VDA que está instalada.	Actualice el VDA si fuera necesario. Compruebe si esa versión del VDA admite las actualizaciones en cuestión.

---

Código de error	ID del código de error	Problema	Acción
SessionPrepareFailure	206	El broker no completó una auditoría de las sesiones activas en el VDA.	Si el problema es generalizado, reinicie Citrix Broker Service en el Delivery Controller.
	206	El broker no completó una auditoría de las sesiones activas en el VDA.	Contacte con Citrix Support.

Código de error	ID del código de error	Problema	Acción
ContactLost	207	El Delivery Controller perdió la conexión con el VDA. Esto puede deberse a interrupciones de la red.	Compruebe que Citrix Broker Service se está ejecutando en el Delivery Controller y que Desktop Service se está ejecutando en el VDA. Si estos servicios están detenidos, inícielos. Si ya se ha iniciado, reinicie Desktop Service en el VDA para reiniciar el proceso de registro y compruebe que el VDA se registra correctamente. Confirme que los Controllers configurados para el VDA son los correctos. Para ello, consulte los datos del registro de eventos de la aplicación. Utilice ping para comprobar que el Delivery Controller y el VDA pueden comunicarse. Si no es el caso, resuelva los problemas de firewall o red que haya.
	207	El Delivery Controller perdió la conexión con el VDA. Esto puede deberse a interrupciones de la red.	Compruebe que Desktop Service se está ejecutando en el VDA. Si este servicio está detenido, inícielo.

Código de error	ID del código de error	Problema	Acción
BrokerRegistrationLimitReached	301	El Delivery Controller ha alcanzado la cantidad máxima configurada de VDA que se pueden registrar simultáneamente en él. De forma predeterminada, el Delivery Controller permite 10 000 registros de VDA simultáneos.	<p>Considere la opción de agregar Delivery Controllers al sitio o crear un sitio nuevo. También puede aumentar la cantidad de VDA que se pueden registrar simultáneamente en el Delivery Controller. Para ello, modifique la clave de Registro <b>HKEY_LOCAL_MACHINE\Software</b></p> <p>Consulte el artículo <a href="#">Entradas de clave de Registro utilizadas por Citrix Virtual Apps and Desktops (CTX117446)</a> de Knowledge Center para obtener más información. Al aumentar esta cantidad, puede que el Controller requiera más recursos de CPU y memoria.</p>

Código de error	ID del código de error	Problema	Acción
SettingsCreationFailure	208	El broker no construyó ningún conjunto de parámetros y configuraciones que enviar al VDA. Si el broker no puede recopilar los datos, el registro falla y se anula el registro del VDA.	Consulte los registros de eventos del Controller en busca de errores. Si no ve un problema claro en los registros de eventos, reinicie Broker Service. Una vez reiniciado Broker Service, reinicie Desktop Service en los VDA afectados y compruebe que se registran correctamente.
	208	El broker no construyó ningún conjunto de parámetros y configuraciones que enviar al VDA. Si el broker no puede recopilar los datos, el registro falla y se anula el registro del VDA.	Reinicie Desktop Service en los VDA afectados y compruebe que se registran correctamente. Contacte con Citrix Support.

Código de error	ID del código de error	Problema	Acción
SendSettingsFailure	204	El broker no envió datos de parámetros y configuraciones al VDA. Si el broker puede reunir los datos pero no puede enviarlos, el registro falla.	Si el problema se limita a un solo VDA, reinicie Desktop Service en el VDA para forzar un nuevo registro y compruebe que el VDA se registra correctamente. Para esto último, consulte los eventos de aplicación. Solucione los errores que vea. Consulte los pasos de solución de problemas indicados en el artículo <a href="#">Solución de problemas al registrar Virtual Delivery Agent en Delivery Controllers en Citrix Virtual Apps and Desktops (CTX136668)</a> de Knowledge Center para ver los motivos frecuentes de problemas de comunicación entre el Controller y el VDA.
AgentRequested	2	Ocurrió un error desconocido.	Contacte con Citrix Support.
DesktopRestart	201	Ocurrió un error desconocido.	Contacte con Citrix Support.
DesktopRemoved	202	Ocurrió un error desconocido.	Contacte con Citrix Support.
SessionAuditFailure	205	Ocurrió un error desconocido.	Contacte con Citrix Support.

Código de error	ID del código de error	Problema	Acción
UnknownError	300	Ocurrió un error desconocido.	Contacte con Citrix Support.
RegistrationStateMismatch	302	Ocurrió un error desconocido.	Contacte con Citrix Support.
Desconocido	-	Ocurrió un error desconocido.	Contacte con Citrix Support.

## SDK y API

November 4, 2021

Se ofrecen varios SDK y API en esta versión. Para acceder a los SDK y las API, vaya a [Build anything with Citrix](#). Allí, seleccione **Citrix Workspace** para acceder a la información sobre la programación de Citrix Virtual Apps and Desktops y sus componentes.

### Nota:

El SDK de Citrix Virtual Apps and Desktops y Citrix Group Policy SDK se pueden instalar como módulos o complementos. Varios SDK de componentes (como Citrix Licensing, Citrix Provisioning y StoreFront) se instalan mediante un complemento solamente.

## SDK de Citrix Virtual Apps and Desktops

Este SDK se instala automáticamente como módulo de PowerShell al instalar un Delivery Controller o Studio. Esto le permite utilizar los cmdlets de este SDK sin tener que agregar complementos (las instrucciones se proporcionan a continuación si decide instalar este SDK como complemento).

### Permisos

Debe ejecutar el shell o el script mediante una identidad que posea derechos de administración de Citrix. Si bien los miembros del grupo de administradores locales del Controller disponen automáticamente de privilegios administrativos totales para permitir la instalación de Citrix Virtual Apps o Citrix Virtual Desktops, Citrix recomienda crear administradores Citrix con los derechos adecuados para un funcionamiento normal, en lugar de usar la cuenta de administradores locales.

## Acceder a los cmdlets y ejecutarlos

1. Inicie un shell en PowerShell: Abra Studio, seleccione la ficha **PowerShell** y, a continuación, haga clic en **Iniciar PowerShell**.
2. Para utilizar los cmdlets del SDK en scripts, configure la directiva de ejecución en PowerShell. Para obtener información acerca de la directiva de ejecución de PowerShell, consulte la documentación de Microsoft.
3. Si quiere utilizar el complemento (en lugar del módulo), agréguelo mediante el cmdlet `Add-PSSnapin` (o `asnp`).

V1 y V2 indican la versión del complemento. Los complementos de XenDesktop 5 son de la versión 1. Citrix Virtual Apps and Desktops y los complementos de versiones anteriores a XenDesktop 7 son de la versión 2. Por ejemplo, para instalar los complementos de Citrix Virtual Apps and Desktops, escriba `Add-PSSnapin Citrix.ADIdentity.Admin.V2`. Para importar todos los cmdlets, escriba: `Add-PSSnapin Citrix.*.Admin.V*`

Ya puede utilizar los cmdlets y los archivos de ayuda.

- Para acceder a los archivos de ayuda de este SDK, seleccione el producto o el componente de la lista [Categorías](#) y, a continuación, seleccione **SDK de Citrix Virtual Apps and Desktops**.
- Para obtener instrucciones sobre PowerShell, consulte [Entorno de scripting integrado \(ISE\) de Windows PowerShell](#).

## Group Policy SDK

Citrix Group Policy SDK le permite visualizar y definir filtros y configuraciones de directivas de grupo. Este SDK utiliza un proveedor de PowerShell para crear una unidad virtual que corresponda a la máquina, configuraciones de usuario y filtros. El proveedor aparece como una extensión de `New-PSDrive`.

Para utilizar Group Policy SDK, es necesario tener instalado Studio o el SDK de Citrix Virtual Apps and Desktops.

El proveedor de PowerShell de directivas de grupo de Citrix está disponible como módulo o complemento.

- Para utilizar el módulo, no hace falta hacer nada más.
- Para agregar el complemento, escriba `Add-PSSnapin citrix.common.grouppolicy`.

Para acceder a la ayuda, escriba: `help New-PSDrive -path localgpo:/.`

Para crear una unidad virtual y cargarla con la configuración, escriba `New-PSDrive <Standard Parameters> [-PSProvider] CitrixGroupPolicy -Controller <string>`, donde

la cadena de Controller es el nombre de dominio completo de un Controller en el sitio al que quiere conectarse y del que quiere cargar la configuración.

## **OData de Monitor Service**

La API de Monitor permite el acceso a los datos de Monitor Service mediante la versión 3 o 4 de la API de OData. Puede crear paneles personalizados de supervisión e informes basados en los datos consultados en Monitor Service. OData 4 se basa en la [API web de ASP.NET](#) y admite consultas de agregación.

Para obtener más información, consulte [API de OData de Monitor Service](#).

## **Plantillas voluntarias de accesibilidad de productos WCAG 2.0**

May 13, 2021

### **Conformidad con la sección 508 y compromiso con WCAG 2.0**

Citrix se compromete a hacer que la tecnología sea accesible para todos. En la actualidad, participamos en iniciativas de alta prioridad para el diseño y fabricación de productos centrados en mejorar la usabilidad y accesibilidad para todos los clientes, con o sin discapacidad. Citrix se compromete a ofrecer soporte a estándares de accesibilidad conocidos, como la conformidad con la Sección 508 y WCAG 2.0.

### **Armonización de la conformidad con la Sección 508 y WCAG 2.0**

World Wide Web Consortium (W3C) desarrolló las *Directrices de Accesibilidad al Contenido Web* o WCAG. Se trata de un estándar reconocido internacionalmente, ISO/IEC 40500, que incluye una serie de estipulaciones para hacer que el contenido web sea más accesible. En los Estados Unidos, también existe un requisito similar. La Sección 508 forma parte del Reglamento Federal de Adquisición (FAR) que procede de la Ley de Rehabilitación de 1973. Al igual que WCAG, su principal objetivo es proporcionar a las personas con discapacidad acceso a las tecnologías electrónicas y de la información (TIC) de los organismos federales. En enero de 2017, el Consejo de Acceso de los Estados Unidos publicó una norma para armonizar la Sección 508 y WCAG 2.0. Como consecuencia, Citrix se está centrando principalmente en las actualizaciones más recientes de WCAG para ofrecer productos más accesibles a nuestros clientes.

## **Plantillas voluntarias de accesibilidad de productos (VPAT)**

Los documentos VPAT para los distintos productos y componentes de Citrix están disponibles para descarga desde <https://www.citrix.com/about/legal/security-compliance/section-508.html>.



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).