Citrix Virtual Apps and Desktops 7 2407

Contents

Citrix Virtual Apps and Desktops 7 2407 14

Citrix Virtual Apps and Desktops 7 2407 15

Problemas resueltos 45

Problemas conocidos 47

Elementos retirados 53

Requisitos del sistema 69

Información técnica general 81

Bases de datos 92

Métodos de entrega 101

Puertos de red 105

HDX 106

Canales virtuales ICA de Citrix 118

Doble salto en Citrix Virtual Apps and Desktops 128

Instalación y configuración 131

Identidades de las máquinas 133

Unidos a Azure Active Directory 135

Unidos a Azure Active Directory híbrido 139

Antes de la instalación 141

Entornos en la nube de AWS 153

Entornos de virtualización de XenServer 159

Entornos de Google Cloud 160

Entornos de virtualización de HPE Moonshot 172

Entornos en la nube de Microsoft Azure Resource Manager 174

Entornos de Microsoft System Center Configuration Manager 175

Entornos de virtualización de Microsoft System Center Virtual Machine Manager 177

Entornos de virtualización de Nutanix 181

Soluciones de Nutanix Cloud y de partners 183

Entornos de virtualización de VMware 184

Soluciones de VMware Cloud y de partners 185

Instalar componentes principales 212

Instalación desde la línea de comandos 225

Instalar Web Studio 243

Instalar VDA 250

Configurar el control de acceso de Windows Defender relacionado con la instalación del VDA 269

Instalar agentes VDA mediante scripts 271

Métodos de implementación de VDA de terceros 274

Instalar agentes VDA mediante SCCM 274

Instalar agentes VDA mediante Microsoft Intune 292

Crear un sitio 307

Crear y administrar conexiones y recursos 311

Conexión con AWS 327

Conexión a XenServer 341

Conexión con entornos de Google Cloud 344

Conexión a HPE Moonshot 358

Conexión con Microsoft Azure 361

Conexión con Microsoft System Center Virtual Machine Manager 384

Conexión con Nutanix 385

Conexión con soluciones de Nutanix Cloud y de partners **387**

Conexión con VMware **389**

Conexión con soluciones de VMware Cloud y de partners **397**

Administración de imágenes (Technical Preview) **398**

Crear catálogos de máquinas **417**

Crear un catálogo de AWS **453**

Crear un catálogo de XenServer **466**

Crear un catálogo de Google Cloud Platform **469**

Crear un catálogo de máquinas de HPE Moonshot **497**

Crear un catálogo de Microsoft Azure **499**

Crear un catálogo de Microsoft System Center Virtual Machine Manager **618**

Crear un catálogo de Nutanix **622**

Crear un catálogo de VMware **624**

Crear catálogos de diferentes tipos de unión **630**

Crear catálogos unidos a Azure Active Directory híbrido **630**

Administrar catálogos de máquinas **633**

Administrar un catálogo de AWS **668**

Administrar un catálogo de XenServer **673**

Administrar un catálogo de Google Cloud Platform **674**

Administrar un catálogo de HPE Moonshot **679**

Administrar un catálogo de Microsoft Azure **680**

Administrar un catálogo de Microsoft System Center Virtual Machine Manager **701**

Administrar un catálogo de VMware **702**

Administración de energía **706**

Administrar la energía de las VM de AWS **707**

Administrar la energía de las VM de Azure **710**

Directivas de seguridad **727**

Grupos de seguridad **727**

Arranque seguro **729**

Prestaciones de cifrado **730**

Crear grupos de entrega **732**

Administrar grupos de entrega **741**

Crear grupos de aplicaciones **779**

Administrar grupos de aplicaciones **788**

Acceso con Remote PC **796**

Publicar contenido **814**

VDI de servidor **818**

Capa de personalización de usuarios **820**

Eliminar componentes **838**

Actualización y migración **840**

Actualizar la versión de una implementación **844**

Compatibilidad de proxy con el agente de actualización de VDA **870**

Hacer copia de seguridad o migrar la configuración **872**

Protección **874**

Autenticación FIDO2 y WebAuthn **876**

Integrar Citrix Virtual Apps and Desktops con Citrix Gateway **880**

Recomendaciones y consideraciones de seguridad **881**

Tarjetas inteligentes **891**

Implementaciones de tarjeta inteligente **899**

Autenticación PassThrough y Single Sign-On con tarjetas inteligentes **906**

Transport Layer Security (TLS) **908**

Protocolo TLS en Universal Print Server **927**

Lista de canales virtuales permitidos **938**

Comunicación WebSocket entre el VDA y el Delivery Controller **942**

Conectividad HDX **944**

Transporte adaptable **945**

Enlightened Data Transport **949**

Solución de problemas **950**

HDX Direct (Technical Preview) **954**

Compatibilidad con NAT **960**

Solución de problemas **962**

Secure HDX (Tech Preview) **966**

Lista de canales virtuales permitidos **969**

Solución de problemas **973**

Canales virtuales de terceros conocidos **976**

Dispositivos **977**

Escaneo **978**

Redirección TWAIN **979**

Dispositivos WIA **981**

Dispositivos USB genéricos **982**

Configuración **983**

Dispositivos compuestos y división de dispositivos **988**

Solución de problemas **992**

Herramienta de diagnóstico USB **997**

Configuración de la redirección USB antigua **1002**

Asignación de unidades del cliente (CDM) **1007**

Compatibilidad con dispositivos cliente móviles y con pantalla táctil **1009**

Puertos serie **1014**

Teclados especiales **1019**

Cámaras web **1021**

Gráficos **1022**

Alto rango dinámico (HDR) de 10 bits **1024**

HDX 3D Pro **1027**

Aceleración de GPU para SO Windows multisesión **1030**

Aceleración de GPU para SO Windows de sesión única **1033**

Thinwire **1039**

Marca de agua de texto en sesión **1048**

Uso compartido de pantalla **1050**

Distribución de pantallas virtuales **1054**

Frecuencia de actualización adaptativa **1057**

Modo tolerante a pérdidas para gráficos **1059**

Contenido multimedia **1059**

Funciones de audio **1063**

Redirección de contenido del explorador web **1075**

Conferencias de vídeo de HDX y compresión de vídeo para cámaras web de HDX **1086**

Redirección multimedia HTML5 **1091**

Optimización para Microsoft Teams **1094**

Supervisión, solución de problemas y asistencia para Microsoft Teams **1138**

Redirección de Windows Media **1146**

Redirección de contenido general **1147**

Redirección de carpetas de cliente **1147**

Redirección de la ubicación del cliente **1149**

Redirección bidireccional de contenido **1150**

Redirección del host al cliente **1153**

Acceso a aplicaciones locales y redirección de URL **1157**

Consideraciones sobre unidades del cliente y redirección de USB genérico **1166**

Imprimir **1178**

Ejemplo de configuración de la impresión **1186**

Prácticas recomendadas, consideraciones de seguridad y operaciones predeterminadas **1190**

Directivas y preferencias de impresión **1192**

Aprovisionar impresoras **1195**

Mantener el entorno de impresión **1205**

Directivas **1211**

Trabajar con directivas **1213**

Plantillas de directiva **1217**

Crear directivas **1221**

Conjuntos de directivas **1229**

Comparar, priorizar y solucionar problemas de directivas **1234**

Configuraciones predeterminadas de directivas **1239**

Referencia para configuraciones de directivas **1273**

Configuraciones de la directiva ICA **1278**

Configuraciones de directiva de Reconexión automática de clientes **1289**

Configuraciones de directiva de audio **1291**

Configuraciones de directiva de Ancho de banda **1293**

Configuraciones de directiva de Redirección bidireccional de contenido **1299**

Configuración de directiva Redirección de contenido de explorador web **1307**

Configuraciones de directiva de Sensores del cliente **1315**

Configuraciones de directiva de Interfaz de usuario de escritorio **1316**

Configuraciones de directiva de Supervisión de usuario final **1318**

Configuración de directiva de Enhanced Desktop Experience **1319**

Configuraciones de directiva de Redirección de archivos **1320**

Configuraciones de directiva de Gráficos **1325**

Configuraciones de directiva de Almacenamiento en caché **1333**

Configuraciones de directiva de Framehawk **1334**

Configuraciones de directiva de Keep Alive **1334**

Configuraciones de directiva de Acceso a aplicaciones locales **1335**

Configuraciones de directiva de Experiencia móvil **1336**

Configuraciones de directiva de Multimedia **1337**

Configuraciones de directiva de conexiones de multisecuencia **1345**

Configuraciones de directiva de Redirección de puertos **1349**

Configuraciones de directiva de Impresión **1350**

Configuraciones de directiva de Impresoras del cliente **1354**

Configuraciones de directiva de Controladores **1358**

Configuraciones de directiva de Universal Print Server **1360**

Configuraciones de directiva de Impresión universal **1367**

Configuraciones de directiva de Seguridad **1371**

Configuraciones de directiva de Límites de servidor **1372**

Configuraciones de directiva de Límites de sesión **1373**

Configuraciones de directiva de Fiabilidad de sesiones **1376**

Configuraciones de directiva de Marca de agua de la sesión **1377**

Parámetros de directiva de control de zona horaria **1381**

Configuraciones de directiva de Dispositivos TWAIN **1383**

Configuraciones de directiva de Dispositivos USB **1384**

Configuraciones de la directiva Lista de canales virtuales permitidos **1394**

Configuraciones de directiva de Presentación visual **1396**

Configuraciones de directiva de Imágenes en movimiento **1397**

Configuraciones de directiva de Imágenes fijas **1399**

Configuraciones de directiva de WebSockets **1401**

Configuraciones de directiva de Dispositivos WIA **1402**

Funciones HDX administradas a través del Registro **1403**

Configuraciones de la directiva Administración de carga **1419**

Configuraciones de directiva de Profile Management **1421**

Configuraciones avanzadas de directiva **1422**

Configuraciones básicas de directiva **1431**

Configuraciones de directiva de Multiplataforma **1436**

Configuraciones de directiva de Sistema de archivos **1438**

Configuraciones de directiva de Exclusiones **1438**

Configuraciones de directiva de Sincronización **1440**

Configuraciones de directiva de Redirección de carpetas **1442**

Configuraciones de directiva de AppData(Roaming) **1443**

Configuraciones de directiva de Contactos **1444**

Configuraciones de directiva de Escritorio **1444**

Configuraciones de directiva de Documentos **1445**

Configuraciones de directiva de Descargas **1446**

Configuraciones de directiva de Favoritos **1446**

Configuraciones de directiva de Vínculos **1447**

Configuraciones de directiva de Música **1447**

Configuraciones de directiva de Imágenes **1448**

Configuraciones de directiva de Juegos guardados **1449**

Configuraciones de directiva de Menú Inicio **1450**

Configuraciones de directiva de Búsquedas **1450**

Configuraciones de directiva de Vídeos **1451**

Configuraciones de directiva de Registro **1452**

Configuraciones de directiva de Gestión de perfiles **1457**

Configuraciones de directiva de Registro del sistema **1462**

Configuraciones de directiva para Perfiles de usuario de streaming **1463**

Configuraciones de la directiva Capa de personalización de usuarios **1465**

Configuraciones de directiva de Virtual Delivery Agent **1466**

Configuraciones de directiva de HDX 3D Pro **1468**

Configuraciones de directiva de Supervisión **1469**

Configuraciones de directiva de IP virtual **1474**

Configurar la redirección de puertos COM y puertos LPT mediante el Registro **1475**

Configuración de directivas de Connector for Configuration Manager 2012 **1476**

Cambios en directivas **1480**

Administrar **1481**

Aplicaciones **1483**

Paquetes de aplicaciones **1507**

Aplicaciones de la Plataforma universal de Windows **1519**

Autoscale **1522**

Introducción a Autoscale **1524**

Parámetros basados en la programación y en la carga **1530**

Tiempos de espera de sesión dinámicos **1554**

Autoscale de máquinas etiquetadas (ampliación en la nube) **1556**

Notificaciones de cierre de sesión del usuario (antes denominado "forzar el cierre de sesión del usuario") **1565**

Comandos del SDK de Broker PowerShell **1568**

Citrix Insight Services **1571**

Citrix Scout **1582**

Recopilar rastreos de Citrix Diagnostic Facility (CDF) durante el inicio del sistema **1608**

Administración delegada **1610**

Delivery Controllers **1621**

Compatibilidad con IPv4/IPv6 **1626**

Licencias de Citrix Virtual Apps and Desktops con Web Studio **1628**

Licencias de varios tipos **1632**

Preguntas frecuentes sobre licencias **1641**

Equilibrar la carga de las máquinas **1655**

Caché de host local **1656**

Supervisar y administrar máquinas y sesiones con Buscar **1672**

Acciones y columnas de máquina **1680**

Acciones y columnas de sesión **1692**

Administrar las claves de seguridad **1696**

Parámetros de resistencia de las sesiones **1711**

Parámetros **1719**

Etiquetas **1724**

Perfiles de usuario **1735**

Registro de VDA **1742**

IP virtual y bucle invertido virtual **1754**

Zonas **1758**

Supervisar **1771**

Registro de configuraciones **1773**

Registros de eventos **1781**

Director **1781**

Instalación y configuración **1788**

Configuración avanzada **1790**

Configurar la autenticación con tarjetas inteligentes PIV **1794**

Configurar el análisis de red **1801**

Administración delegada y Director **1802**

Implementación segura de Director **1806**

Configurar sitios locales con Citrix Analytics for Performance **1809**

Análisis de sitios **1816**

Alertas y notificaciones **1826**

Filtrar datos para solucionar fallos **1854**

Supervisar tendencias históricas en un sitio **1856**

Supervisar máquinas administradas con Autoscale **1862**

Solucionar problemas de implementaciones **1865**

Solucionar problemas de aplicaciones **1865**

Solucionar problemas de máquinas **1870**

Solucionar problemas de usuarios **1880**

Diagnosticar problemas de inicio de sesión **1885**

Diagnosticar problemas de inicio de sesión de los usuarios **1891**

Diagnosticar problemas de rendimiento de sesión **1900**

Remedar usuarios **1908**

Enviar mensajes a usuarios **1910**

Resolver fallos de aplicaciones **1910**

Restaurar conexiones de escritorio **1912**

Restaurar sesiones **1912**

Generar informes del sistema de canales HDX **1913**

Restablecer un perfil de usuario **1914**

Grabar sesiones **1918**

Tabla de compatibilidad de funciones **1921**

Granularidad y retención de datos **1927**

Motivos de fallo y solución de problemas en Citrix Director **1935**

Avisos legales de terceros **1961**

SDK y API **1961**

Citrix Virtual Apps and Desktops 7 2407

August 17, 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 proporciona una solución de virtualización para la entrega de aplicaciones y escritorios a cualquier dispositivo, a través de cualquier red, a la vez que mejora la seguridad de los datos, reduce los costes y aumenta la productividad.

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 5 (CU5) es la actualización más reciente de la versión 2203 LTSR. Las versiones LTSR también están disponibles para Citrix Virtual Apps and Desktops 1912.

- 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 obtener más información, consulte Citrix DaaS.

Enlaces útiles

- Citrix Supportability Pack
- Preguntas frecuentes sobre la versión LTSR

- Opciones de servicio de Citrix Virtual Apps and Desktops
- Fechas de la vida útil del producto
- Programa LTSR para la aplicación Citrix Workspace

Citrix Virtual Apps and Desktops 7 2407

August 17, 2024

Acerca de la versión

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 la versión de los VDA y los componentes principales. Instalar o actualizar la versión a la más reciente permite utilizar 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. Puede interesarle actualizar la versión solamente de 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 acerca de la instalación y la actualización:

- 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 2407

Parámetros predeterminados seguros

El instalador del VDA tiene una nueva opción que cambia el parámetro predeterminado de varias funciones de habilitado a inhabilitado para obtener una configuración lista para usar más segura. Para

obtener más información, consulte Instalar agentes VDA.

Mejora de los informes de telemetría de uso

La función de informes de telemetría de uso ahora se ha mejorado para recopilar y procesar datos sobre cómo se usan las licencias de los productos, componentes y funciones de Citrix que se implementan en entornos administrados por los clientes. Esta mejora garantiza la conformidad en el uso de las licencias de los productos Citrix en entornos locales.

Para aprovechar esta mejora, actualice a la versión más reciente del servidor de licencias. Para obtener más información, consulte:

- Telemetría de Citrix Licensing
- Actualizaciones necesarias del servidor de licencias
- Preguntas frecuentes sobre telemetría de licencias de Citrix

Para ver la lista de elementos de datos de telemetría de las licencias, consulte Elementos de datos de la telemetría de Citrix Licensing.

Exclusiones de puertos de bucle invertido virtual

Ahora tiene la opción de excluir puertos específicos del bucle invertido virtual para que las llamadas realizadas por las aplicaciones a la dirección de bucle invertido de cualquier puerto especificado no cambien a la dirección de bucle invertido específica de la sesión. Para obtener más información, consulte Bucle invertido virtual.

Escalado mejorado de la ventana de LogonUI para aplicaciones integradas

La escala de las ventanas de **LogonUI** se ha mejorado para los casos en los que no tiene lugar la autenticación PassThrough. La ventana de LogonUI se escala en función de la resolución del monitor y la configuración de PPP usada, lo que garantiza que toda la ventana de LogonUI sea visible sin ningún recorte.
Para obtener más información, consulte Cómo modificar LogonUI para ver el mensaje de renuncia de responsabilidades de Windows a tamaño completo al abrir aplicaciones publicadas.

Mejoras en el comprobador de cierre de sesión para las aplicaciones publicadas

Con esta nueva función, ahora tiene la opción de detectar automáticamente las aplicaciones de inicio configuradas en el sistema y agregarlas automáticamente a la lista de procesos del sistema, de manera que no obstruyan el cierre de sesión cuando se cierre la última ventana de la aplicación publicada.

Para obtener más información, consulte Solución de problemas de cierre de sesión con aplicaciones publicadas.

Agentes Virtual Delivery Agent (VDA) 2407

Reestructuración de documentos para métodos de implementación de VDA de terceros

La página de implementaciones de VDA de terceros se ha reestructurado para incluir instrucciones detalladas adicionales. Para obtener más información, consulte Implementaciones de VDA de terceros.

Inscripción de VDA basada en tokens para VDA no aprovisionados por MCS (Technical Preview)

Con esta función, ahora puede generar y administrar los tokens de inscripción para los VDA no aprovisionados por MCS. Esta implementación permite el registro de VDA a través de WebSocket sin aprovisionar los VDA con MCS. Esta función también es compatible con Linux Virtual Delivery Agent, Citrix Virtual Delivery Agent para macOS y agentes VDA no unidos a un dominio con Citrix Virtual Apps and Desktops. Para obtener más información, consulte Inscribir agentes VDA no aprovisionados por MCS mediante tokens.

Web Studio

Contextual App Protection

Con esta función, los administradores pueden aplicar los controles de **protección contra la captura de pantalla** y **contra el registro de tecleo** de App Protection en los dispositivos y los usuarios de forma contextual, en lugar de tener los controles siempre habilitados o inhabilitados. Esta implementación le permite aplicar la protección contra la captura de pantalla y contra el registro de tecleo de App Protection solo cuando es necesario. Para obtener más información, consulte Administrar App Protection.

Compatibilidad con la autenticación con tarjeta inteligente

Web Studio ahora admite la autenticación con tarjeta inteligente, lo que permite a los administradores acceder a Web Studio mediante tarjetas PIV y CAC. Para obtener más información, consulte Configurar la autenticación con tarjeta inteligente para Web Studio y Habilitar la autenticación con tarjeta inteligente.

Administración de arrendatarios

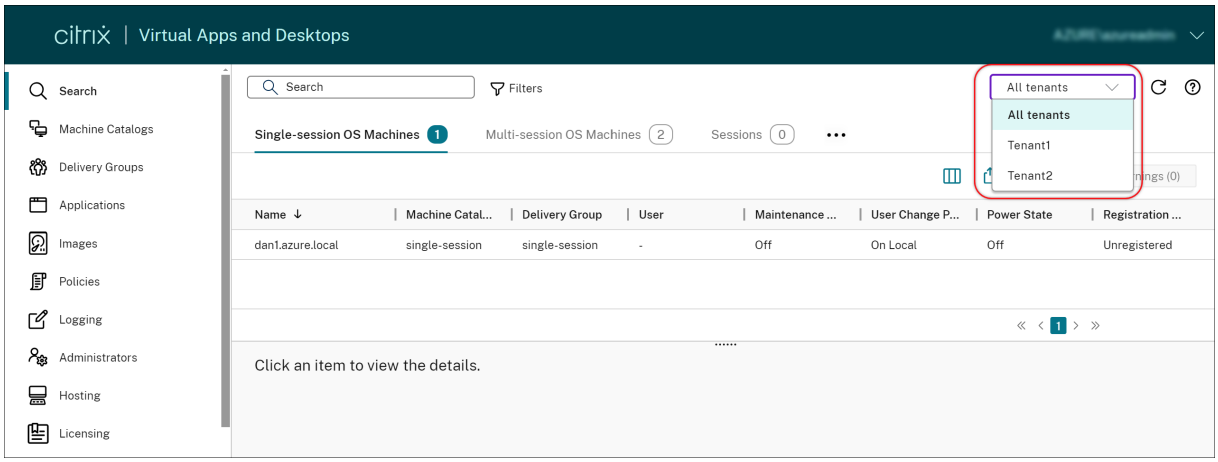
Con la administración de arrendatarios, ahora puede configurar particiones de administración en un único sitio de Citrix Virtual Apps and Desktops. Esta función es ideal para las organizaciones que:

- Operan con diferentes silos empresariales, como divisiones independientes o equipos de administración de TI independientes.
- Atienden a varios clientes, como Citrix Service Providers.

Para configurar la administración de arrendatarios, siga estos pasos:

1. Cree arrendatarios. Vaya a **Administradores > Ámbitos**, cree ámbitos de arrendatarios y asocie esos ámbitos a los recursos y configuraciones relacionados, como los catálogos de máquinas y los grupos de entrega.
2. Agregue administradores para los arrendatarios. Vaya a **Administradores > Administradores** y asigne cuentas de usuario con roles y arrendatarios según sea necesario.

Como administrador con el acceso adecuado a un arrendatario, puede ver y seleccionar su nombre en la lista desplegable **Todos los arrendatarios** en la esquina superior derecha de Web Studio. A continuación, administre los recursos y las configuraciones asociados únicamente a ese arrendatario. Para obtener más información, consulte Configurar la administración de arrendatarios.



Habilitar la caché de host local (LHC) para los VDA agrupados de sesión única con administración de energía

De forma predeterminada, los VDA agrupados de sesión única aprovisionados mediante MCS o Citrix Provisioning no están disponibles en modo LHC. Mediante Web Studio, ahora puede anular este comportamiento predeterminado para cada grupo de entrega, de modo que esos VDA estén disponibles para nuevas conexiones durante el modo LHC. Para obtener más información, consulte Crear grupos de entrega y Administrar grupos de entrega.

Generar y administrar tokens de inscripción de VDA

La inscripción de VDA basada en tokens reduce la carga en los Cloud Connectors y también los posibles puntos de fallo. Mediante Web Studio, ahora puede generar y administrar los tokens de inscripción para los VDA que no están aprovisionados por Citrix, lo que agiliza las implementaciones basadas en tokens de inscripción. Para obtener más información, consulte Generar y administrar los tokens de inscripción.

Crear VM multisesión persistentes

Al crear un catálogo de máquinas multisesión, ahora puede especificar si quiere que sean persistentes. En el caso de las máquinas multisesión persistentes, tenga en cuenta que los cambios que hagan los usuarios en los escritorios se guardan y pueden acceder a ellos todos los usuarios autorizados. Para obtener más información, consulte Crear catálogos de máquinas.

Encendido asignado a Autoscale en horas punta

Cuando los escritorios persistentes están encendidos, pero no se utilizan, o si ningún usuario inicia sesión, los administradores pueden definir el tiempo de espera para determinadas acciones como no realizar ninguna acción, suspender o apagar.

- En el caso de las máquinas asignadas, cuando están encendidas, pero no se ha conectado una sesión a las mismas dentro del tiempo establecido tras el comienzo de la hora punta, puede agregar una directiva al nivel del grupo de entrega para apagar las máquinas.
- En el caso de las máquinas asignadas que están en estado de reanudación, pero no se ha conectado una sesión a las mismas dentro del tiempo establecido desde el comienzo de la hora punta, puede agregar una directiva al nivel del grupo de entrega para suspender las máquinas.

Esta función resulta útil si hay un usuario final que está en días libres o que no ha iniciado sesión, o si una empresa tiene un fin de semana largo, para establecer el tiempo de espera y las acciones de desconexión de las máquinas a fin de reducir el coste por consumo de Azure. Para obtener más información, consulte Grupos de entrega aleatorios de SO de sesión única y Grupos de entrega estáticos de SO de sesión única.

Entregar aplicaciones empaquetadas a equipos de oficina y a escritorios estáticos de sesión única

Con esta mejora, ahora puede entregar aplicaciones empaquetadas a todos los tipos de escritorios. Para entregar aplicaciones empaquetadas a los escritorios, agregue esas aplicaciones a los grupos de entrega de estas maneras:

- Agregue aplicaciones durante la creación del grupo de entrega.
- Agregue aplicaciones a un grupo de entrega existente mediante una de estas entradas: **Grupos de entrega > Agregar aplicaciones > Aplicaciones**, **Aplicaciones > Propiedades > Grupos** o **Paquetes de aplicaciones > Paquetes > Agregar grupos de entrega**.

Para obtener más información, consulte Crear grupos de entrega, Administrar grupos de entrega y Agregar aplicaciones a grupos de entrega.

Modificar los nombres simplificados de escritorio

Hemos mejorado la página **Asignación de máquinas** para los grupos de entrega *estáticos con SO de sesión única* mediante la introducción de una nueva columna, **Nombre simplificado**. Con esta adición, ahora puede modificar el nombre simplificado de escritorio de las máquinas asignadas a los usuarios. Para obtener más información, consulte Administrar asignaciones de usuarios.

Reiniciar y apagar máquinas de sesión única desde la ficha Sesiones del nodo de búsqueda

En la ficha **Sesiones** del nodo **Buscar**, ahora puede buscar sesiones de usuario en mal estado y reiniciar o apagar sin problemas las máquinas de sesión única asociadas dentro de la misma ficha. Esta función mejora la eficiencia y permite actuar rápidamente dentro de una sola interfaz en caso de identificar problemas de sesión.

Asignar letras de unidad a los discos de memoria caché de reescritura

Antes, solo podía asignar una letra de unidad específica al disco de memoria caché de reescritura mediante un cmdlet de PowerShell. Ahora puede realizar la misma tarea con Web Studio. Para obtener más información, consulte Crear catálogos de Microsoft.

Posibilidad para intentar de nuevo crear un catálogo en caso de error

Ahora, si se produce un error en la creación de catálogos, puede intentar crearlos de nuevo. Para garantizar una creación correcta, compruebe la información sobre la solución de problemas y resuelva los problemas. La información describe los problemas encontrados y proporciona recomendaciones para resolverlos. Los catálogos con errores se marcan con un icono de error. Para ver los detalles, vaya a la ficha **Solucionar problemas** de cada catálogo. Para obtener más información, consulte Administrar catálogos de máquinas.

Mostrar las direcciones IP de los clientes en los registros de configuración

En **Registros > Eventos**, ahora puede ver los detalles de las direcciones IP en los registros, lo que facilita el seguimiento del origen de las acciones. Para mostrar la columna de direcciones IP en la vista principal, haga clic en el icono **Columnas que mostrar** en la parte superior derecha de los registros y, a continuación, seleccione **IP de cliente**.

Mejoras en la ayuda contextual

Hemos rediseñado el panel de ayuda para ofrecer una experiencia más informativa y ofrecer información específica para cada nodo dentro de Web Studio. Al hacer clic en el icono de ayuda de cualquier nodo, ahora puede acceder a un conjunto completo de recursos destinados a proporcionar una experiencia de aprendizaje integral que le ayude a comprender mejor las funciones relacionadas:

- Acceda a los documentos clave relacionados específicamente con el nodo seleccionado.
- Manténgase informado sobre las actualizaciones del servicio, como la hoja de ruta de Citrix, los problemas conocidos, los límites, los requisitos del sistema y las funciones nuevas.
- Acceda a recursos ampliados, como: blogs de Citrix, comunidad de Citrix, funciones de Citrix explicadas, documentación de productos de Citrix, Citrix Support y documentación para desarrolladores.

Búsqueda mejorada

Hemos mejorado el nodo de búsqueda con la introducción de las siguientes funciones:

- Dos nuevos filtros, **Zona** y **Tipo de aprovisionamiento**, a fin de mejorar la precisión y la usabilidad.
- Dos columnas nuevas:
  - Columna **Nombre simplificado de usuario** en la ficha **Sesiones**. Con esta columna, puede identificar rápidamente las sesiones asociadas a un usuario específico.
  - Columna **Nombre simplificado de escritorio** en las fichas **Máquinas con SO de sesión única** y Sesiones. Con esta columna, puede identificar rápidamente la máquina asociada a un escritorio específico.
- Nuevos filtros para una búsqueda eficiente. Para obtener más información sobre estas dos columnas, consulte Acciones y columnas de máquina y Acciones y columnas de sesión.
- Anclaje de filtros en el panel de búsqueda de los nodos **Buscar** y **Catálogos de máquinas**, lo que le permite mantener accesibles en las páginas los filtros de búsqueda más usados.

Mejoras en el nodo Aplicaciones

Hemos implementado las siguientes mejoras en el nodo Aplicaciones:

- Se extendió la funcionalidad Columnas que mostrar y Exportar a las fichas Aplicaciones y Grupos de aplicaciones. Con los iconos recién introducidos en la esquina superior derecha, ahora puede personalizar las vistas principales de las aplicaciones y los grupos de aplicaciones, y exportar los registros de esas vistas a archivos CSV.
- Se agregó el campo Zonas en el panel Detalles de las aplicaciones, que permite ver las zonas en las que reside una aplicación. Esta información es útil para distinguir entre aplicaciones que comparten nombres idénticos pero que se originan en zonas diferentes. Para obtener más información, consulte Zonas.

Almacenamiento en caché de datos para los nodos Catálogos de máquinas y Alojamiento

Hemos introducido el almacenamiento en caché de datos para el nodo **Catálogo de máquinas** de Citrix DaaS. Esta mejora reduce significativamente los tiempos de carga de las páginas al ir al nodo **Catálogo de máquinas**, lo que mejora la experiencia general del usuario.

Se rediseñó la interfaz de usuario de Directiva de acceso para ofrecer mayor flexibilidad en el control de acceso a los recursos

Hemos rediseñado la interfaz de usuario de **Modificar grupo de entrega > Directiva de acceso** para darle mayor flexibilidad a la hora de administrar el acceso a los recursos de los grupos de entrega. Estas son las principales funciones disponibles con el nuevo diseño:

- **Posibilidad de agregar directivas.** Ahora puede agregar directivas de acceso para restringir el acceso a los recursos en función de los atributos de las conexiones de los usuarios. Una directiva puede constar de dos tipos de criterios:
  - **Criterios de inclusión.** Permite especificar las conexiones de usuario a las que se les permite acceder al grupo de entrega.
  - **Criterios de exclusión.** Permite especificar las conexiones de usuario a las que se les prohíbe acceder al grupo de entrega.
- **Compatibilidad con filtros ampliada.** Ahora puede definir criterios de inclusión y exclusión mediante un rango de filtros de SmartAccess. Estos filtros incluyen filtros de Workspace, como `Citrix.Workspace.UsingDomain` y `Citrix-Via-Workspace`, así como filtros para el acceso adaptable basado en la ubicación de red.
- **Compatibilidad con la lógica Hacer coincidir todo para los criterios incluidos.** La nueva lógica le permite lograr un alto nivel de precisión y control a la hora de especificar las conexiones de usuario permitidas para los grupos de entrega.

Para obtener más información, consulte Restringir el acceso a los recursos de un grupo de entrega.

Filtrado de imágenes avanzado para la creación de catálogos de AWS

Al seleccionar plantillas de máquinas durante la creación de catálogos de AWS, ahora puede filtrar el inventario de la AMI de AWS para una plantilla de destino mediante los siguientes criterios de búsqueda:

- Nombre de la imagen
- ID de imagen
- Etiquetas de imagen

La lista de plantillas de máquinas se carga dinámicamente a medida que se desplaza por la lista. Inicialmente, se cargan 25 elementos, y se van cargando más a medida que se desplaza.

Posibilidad de crear máquinas virtuales de AWS que admitan la hibernación

Ahora puede crear catálogos de máquinas que admitan la hibernación de máquinas virtuales en sus entornos de AWS, lo que mejora la rentabilidad general de su implementación. Observe que también puede modificar un catálogo para incluir máquinas virtuales con capacidad de hibernación si el perfil de máquina asociado admite esta capacidad. Para obtener más información, consulte Hibernación.

Nuevas validaciones de directivas

Se agregan validaciones de directivas adicionales. Como resultado, habilitar directivas o realizar una actualización en contexto podría provocar la pérdida de datos de directivas si hay configuraciones de directivas no válidas. Si crea o modifica las directivas mediante un método que no sea Web Studio, Citrix recomienda usar la versión más reciente del SDK y el complemento. Para obtener más información, consulte CTX676686.

Conjuntos de directivas

En **Web Studio > Directivas**, ahora puede agrupar directivas para un acceso simplificado basado en roles mediante conjuntos de directivas. Puede asignar los ámbitos y los grupos de entrega a sus conjuntos de directivas para que solo los administradores autorizados puedan administrar las directivas que se aplican a sus usuarios y máquinas pertinentes. Para obtener más información, consulte Conjuntos de directivas.

Multiselección de directivas

Ahora puede seleccionar varias directivas y comprobar las siguientes mejoras:

1. Hacer clic en una fila de directivas: Si hace clic en una fila de directivas, la barra de acciones de la parte superior muestra las acciones de una sola directiva. El panel de detalles de la parte inferior proporciona información sobre la directiva.
2. Seleccionar las casillas de verificación de varias directivas: Si selecciona las casillas de verificación de varias directivas cuyos estados están habilitados o inhabilitados, la barra de acciones de la parte superior muestra las acciones de varias directivas. El panel de detalles de la parte inferior la cantidad de directivas seleccionadas.

> **Nota:**
>
> Después de seleccionar varias directivas, puede ver los detalles de otra directiva individual haciendo clic en la fila de esa directiva. Esta acción no borra las directivas seleccionadas anteriormente. Sin embargo, al hacer clic con el botón secundario no se muestran las acciones de esa fila de directivas.

Claridad sobre las directivas dependientes

Algunas configuraciones dependen de otras. Anteriormente, las configuraciones de directivas dependían unas de otras, pero la relación entre las configuraciones carecía de claridad. Por ejemplo, se puede configurar una configuración secundaria, pero si la configuración principal no está habilitada, la configuración secundaria configurada no surtirá efecto. Las dependencias no estaban claras antes. A partir de esta versión, se aclara cuáles son las directivas principales que se deben configurar primero antes de poder configurar las directivas secundarias. Para obtener más información, consulte Configuraciones de directiva.

Actualizaciones de subred simplificadas para catálogos de máquinas

Anteriormente, para cambiar los parámetros de subred de un catálogo de máquinas, había que eliminarlo y volver a crearlo. Con esta función, ahora puede lograr la misma funcionalidad modificando el catálogo. Tenga en cuenta que solo las nuevas máquinas virtuales creadas en el catálogo estarán en las subredes recién asociadas. Esta mejora reduce la necesidad de eliminar el catálogo y las tareas asociadas. Para obtener más información, consulte Modificar un catálogo.

Nueva configuración de directivas: Recopilación de métricas de sesión

Este parámetro permite a Citrix recopilar métricas de sesiones de usuario y máquina entre el VDA y Workspace para mejorar la experiencia del usuario.

Citrix recopila datos como el sistema operativo, el tiempo de actividad, información sobre el sistema informático, detalles del controlador de vídeo, la versión del VDA, el tipo de implementación y el estado de unión al dominio. Además, puede recopilar algunas configuraciones de sesión, junto con datos sobre rendimiento y fiabilidad, para contribuir a la mejora del producto. De manera predeterminada, esta configuración está habilitada. Para obtener más información, consulte Recopilación de métricas de sesión.

Integración de Secure Private Access con Web Studio

A partir de la versión 2407, la integración de Secure Private Access con Web Studio se ha mejorado para que los administradores puedan acceder a la consola de SPA desde la consola de Web Studio. Para obtener más información, consulte Integración de Secure Private Access con Web Studio.

Citrix Director

Gráficos de supervisión del uso de las aplicaciones en el panel de mandos

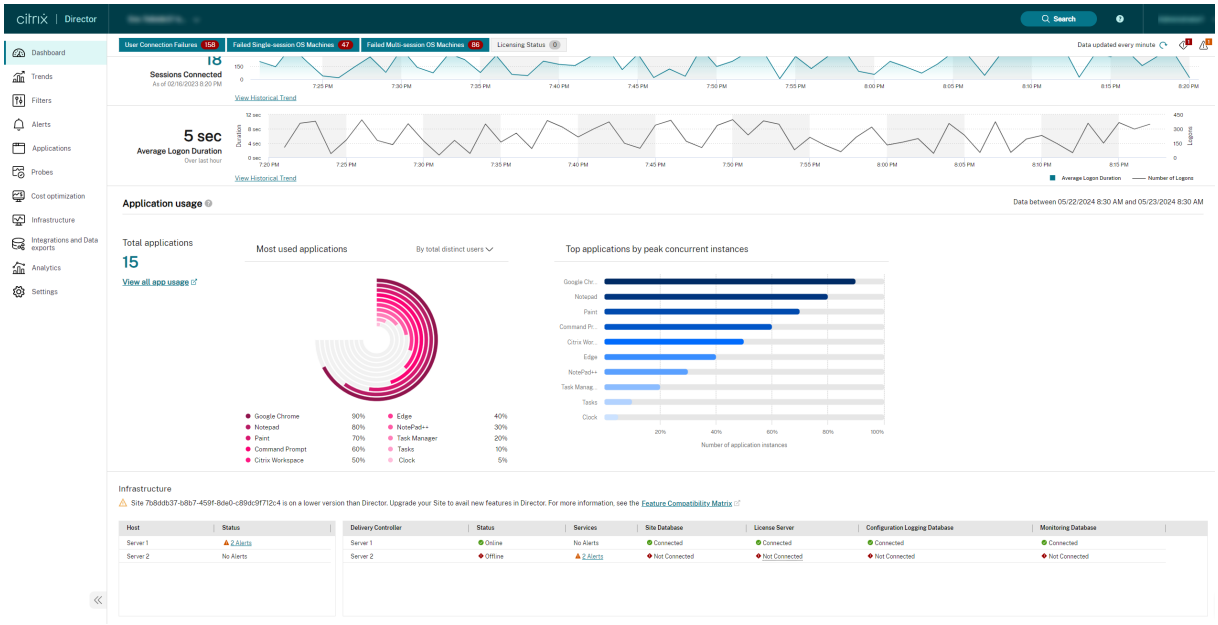
Ahora, Citrix Director le ayuda a supervisar el uso de las aplicaciones publicadas. Esta función está presente en el panel de control y contiene gráficos seleccionados para ayudar a los administradores de TI o a los administradores de aplicaciones a obtener información sobre qué aplicaciones se usan mucho y el alcance de su uso.

Estos gráficos incluyen los siguientes puntos de datos de las últimas 24 horas:

- Cantidad total de las aplicaciones en uso
- Aplicaciones más usadas (límite de 10) por total de usuarios distintos
- Aplicaciones más usadas (límite de 10) por total de inicios
- Pico de instancias de aplicación simultáneas

A través de esta imagen, los clientes pueden ver las aplicaciones publicadas más populares para realizar un análisis del consumo con respecto a los derechos a fin de optimizar el coste incurrido en la compra de licencias de software.

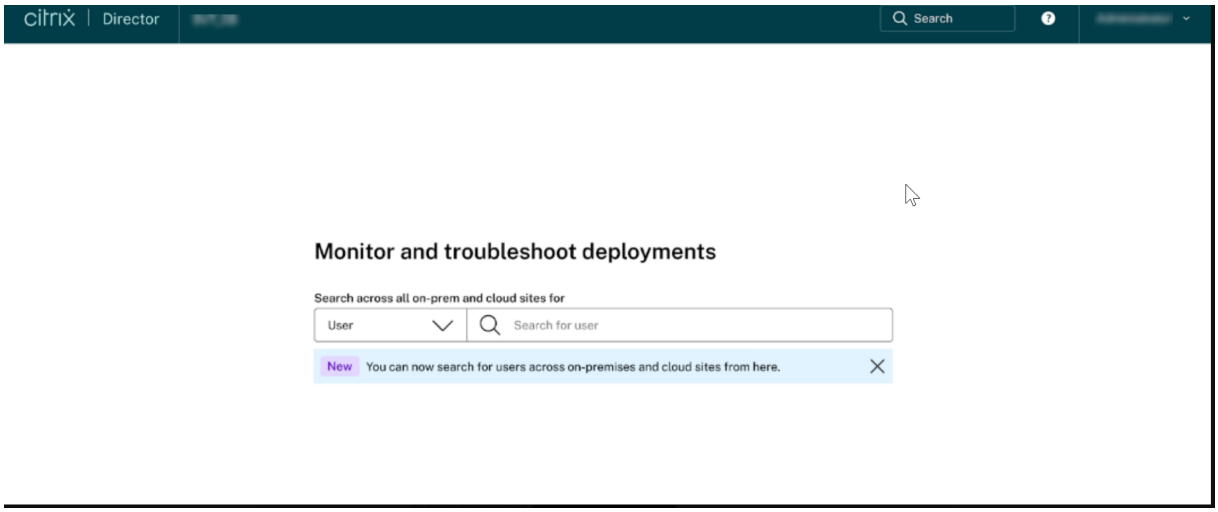
> **Nota:**
>
> Esta función solo está disponible para los sitios con licencia Platinum.

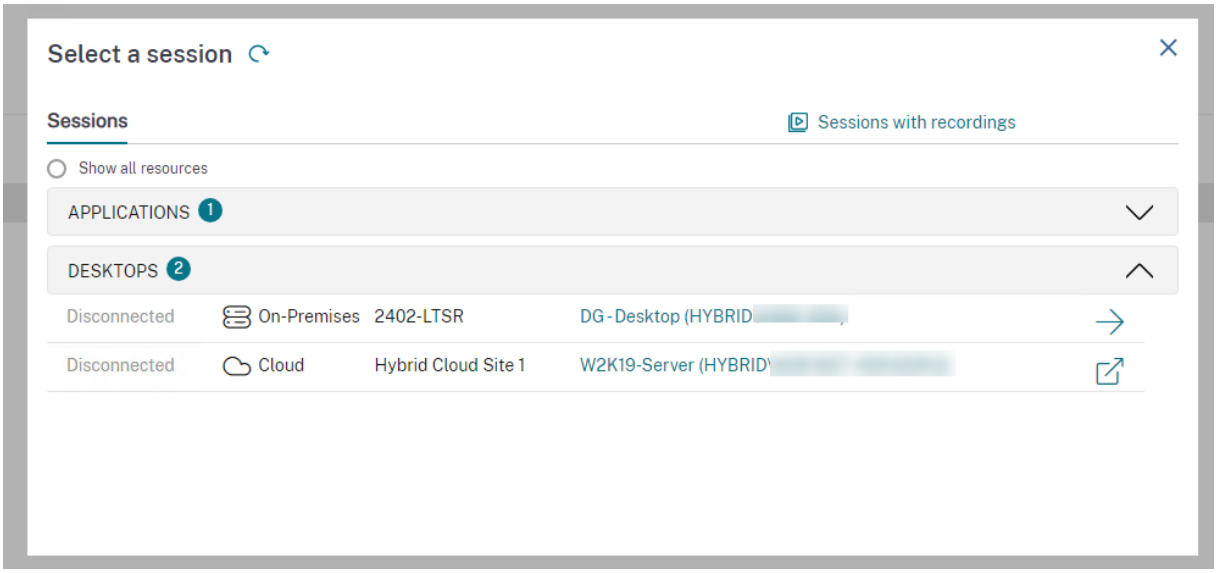


Para obtener más información, consulte Gráficos de supervisión del uso de las aplicaciones en el panel de mandos.

Búsqueda unificada de usuarios locales y en la nube

Anteriormente, durante la clasificación cuando se buscaba un usuario en Director, solo se obtenían los detalles del usuario si este procedía de un sitio local. Si el usuario provenía de un sitio en la nube, tenía que ir a Supervisar y buscar de nuevo. Con esta funcionalidad de búsqueda mejorada, puede buscar usuarios en sitios de la nube o sitios locales mediante la opción de **búsqueda** de Director. Esta función reduce el tiempo medio de resolución de problemas y proporciona una experiencia fluida, con una única consola y sin un rápido crecimiento del tamaño de la base de datos.





Para obtener más información, consulte Búsqueda unificada de usuarios locales y en la nube.

Vista de inicio de sesión mejorada

La nueva opción **Arranque de la máquina**, con las siguientes subsecciones en la ficha **Inicio de sesión** de la página **Filtros** -> **Detalles del usuario**, proporciona el desglose del tiempo empleado para iniciar una máquina virtual en las diferentes fases:

- **Encender**: Muestra el tiempo necesario para encender una máquina virtual
- **Arranque y registro**: Muestra el tiempo necesario para arrancar y registrar una máquina virtual

El botón desplegable recientemente introducido en la página **Inicio de sesión** ayuda a reducir o ampliar las opciones de **Arranque de la máquina** y **Sesión interactiva**.

Además de las opciones predeterminadas de la tabla **Fases de duración del inicio de sesión**, que son **Fase de inicio de la sesión** y **Duración**, también puede elegir las siguientes columnas en la página **Inicio de sesión**:

- Hora de inicio
- Hora de fin
- Promedio de 7 días de grupo de entrega (s)
- Promedio de 7 días del usuario (s)

También puede exportar los datos anteriores a un archivo.CSV.

Las columnas recién agregadas **Encender** y **Arranque y registro** se pueden agregar a la tabla **Duración de inicio de sesión por sesión de usuario** en **Tendencias** -> **Rendimiento de inicio de sesión** > **Elegir columnas**. También puede exportar los informes de la pantalla **Rendimiento de inicio de sesión**.

Esta mejora ayuda a comprender y solucionar fácilmente los problemas relacionados con la duración del inicio de sesión. Para obtener más información, consulte Diagnosticar problemas de inicio de sesión de los usuarios.

Opciones para solucionar problemas cuando no se rellenan los datos de RTT de ICA o Duración del inicio de sesión

Antes, cuando los servicios EUEM o Profile Management Service no se ejecutaban, no se mostraba el motivo por el que no se obtenían los datos relacionados con RTT de ICA o Duración del inicio de sesión. Con esta nueva función, puede obtener el motivo del fallo y la solución correspondiente.

Para obtener más información, consulte Opciones para solucionar problemas cuando no se rellenan los datos de RTT de ICA o Duración del inicio de sesión.

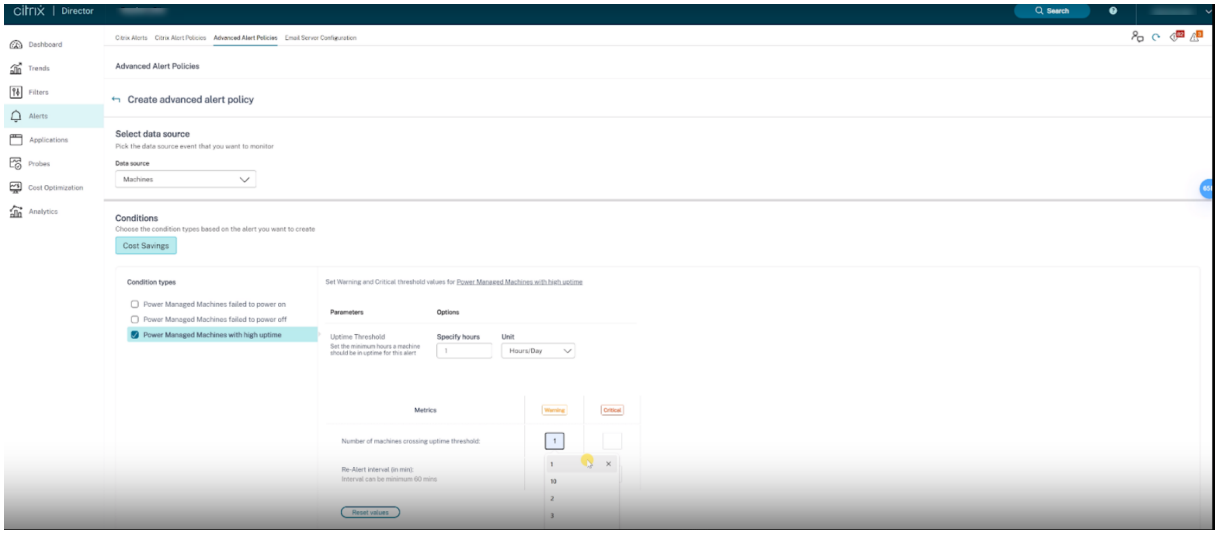
Nombre del escritorio publicado

Citrix Director ahora muestra el nombre del escritorio publicado en la interfaz de usuario. Este nuevo campo le permite diferenciar entre grupos de usuarios dentro de un mismo grupo de entrega. También puede generar informes personalizados para estos grupos de usuarios. Este nuevo campo se agrega a las secciones **Filtros**, **Informes personalizados** o **Detalles de la máquina** de la interfaz de usuario de Citrix Director.

Directivas de alerta avanzadas

La función de notificación y alertas proactivas de Director se ha mejorado para incluir un nuevo marco de alertas denominado **Directivas de alerta avanzadas**. Con esta función, puede crear alertas al incluir detalles granulares para cada elemento o condición, lo que mejora el control sobre el ámbito de las alertas. Actualmente, estas directivas incluyen alertas de ahorro de costes e infraestructura.

Esta función le ayuda a reducir el exceso de alertas, que podría reducir la capacidad de respuesta o la eficacia a la hora de abordar problemas importantes. Esta directiva ayuda a medir la eficacia de las directivas de alerta y la interacción por parte de los administradores.



Para obtener más información, consulte Directivas de alerta avanzadas.

Mejoras en el contenido de las alertas

La función de alerta de Director se ha mejorado para incluir un archivo adjunto CSV y una carga útil JSON. Con esta mejora, puede obtener los detalles de las alertas en un archivo adjunto CSV por correo electrónico o como carga útil JSON si se trata de un webhook. Con este archivo adjunto CSV y la carga útil JSON, puede recibir contenido enriquecido de forma detallada, lo que ayuda a identificar y resolver rápidamente los problemas.

Actualmente, esta mejora solo está disponible en las siguientes alertas:

- Tiempo de actividad de máquina
- Acciones de encendido fallidas
- Acciones de apagado fallidas
- Máquinas no registradas (en %)

Para obtener más información, consulte Mejoras en el contenido de las alertas.

Opción para ver y filtrar el tipo de sesión y la última hora de arranque

Citrix Director ahora ofrece la opción de agregar **Tipo de sesión** como una nueva columna. Los diferentes tipos de sesión disponibles son de escritorio y de aplicación. También puede agregar **Tipo de sesión** como una columna nueva agregándolo en **Filtros** > **Sesiones** > **Elegir columnas.** Esto también se agrega en **Tendencias > Sesiones.**

Del mismo modo, se agrega una nueva opción para averiguar la **Última hora de arranque** en la sección **Filtros** > **Máquinas**. También puede agregar la **Última hora de arranque** como una nueva columna en **Filtros** > **Máquinas** > **Elegir columnas**.

Opción para filtrar los datos por período de tiempo en las Instancias de aplicación y Sesiones

Citrix Director ahora incluye el filtro de período de tiempo en **Sesiones** e **Instancias de aplicación**, en la ficha **Filtros**. Ahora puede filtrar las sesiones y las instancias de aplicación para:

- Últimos 60 minutos
- Últimas 24 horas
- Últimos 7 días

Además, la opción de período de tiempo personalizado se agrega en **Sesiones**, **Conexiones** e **Instancias de aplicación** de la ficha **Filtros**.

Para obtener más información, consulte Filtrar datos para solucionar fallos.

Panel Métricas de rendimiento mejorado

El panel **Métricas de rendimiento** presenta una imagen mejorada de las métricas de datos históricos. Al hacer clic en la ficha **Rendimiento de la sesión**, junto con los datos de los últimos 15 minutos, puede ver los datos de las últimas 24 horas de ICARTT y latencia de ICA. Esta mejora ayuda a reducir el tiempo medio de resolución al permitir a los administradores clasificar los problemas aunque la sesión haya terminado en las últimas 24 horas.

Para obtener más información, consulte Métricas de rendimiento.

Mejora de la ficha Rendimiento de la sesión

La sección **Topología de la sesión** de la ficha **Rendimiento de la sesión** se ha mejorado para incluir lo siguiente:

- Detalles adicionales sobre Connector y Citrix Gateway en la vista de Topología de la sesión, como la dirección IP y el sistema operativo del dispositivo de punto final y la versión de la aplicación Citrix Workspace en el salto del dispositivo de punto final
- ID de PoP, ubicación y país del servicio de puerta de enlace, IP del conector, nombre del conector y ubicación de recursos
- Detalles sobre los elementos de datos que faltan en Connector y Citrix Gateway y enlaces para descargar la versión más reciente
- Detalles del hipervisor, como el tipo de hipervisor, el nombre de la conexión al host y el nombre del host
- Nombre del protocolo HDX en la sección de detalles de la sesión y en la vista de topología de la sesión
- Las siguientes métricas del dispositivo de punto final en la aplicación Citrix Workspace para Windows:

- Intensidad de la señal Wi-Fi
- Procesamiento entrante y saliente
- Tipo de interfaz de red
- Velocidad de enlace

Esta mejora ayuda a solucionar rápidamente problemas relacionados con las sesiones.

Mejora en la clasificación de los problemas de carga de perfiles de usuario

Citrix Director ahora admite la recopilación de métricas de contenedores y duración de carga de perfiles desde los contenedores de Citrix Profile Management y FSLogix. Con esta mejora, se facilitan a los administradores datos completos sobre el uso y el rendimiento de los perfiles en los informes de las sesiones de usuario. Con estos datos, puede identificar y resolver los problemas con mayor eficiencia.

Para obtener más información, consulte Carga de perfil.

Optimización de costes

Citrix Director ahora presenta una nueva función llamada Optimización de costes, que le ayuda a analizar de manera eficaz el uso de las máquinas virtuales y las sesiones. Esta función proporciona representaciones visuales interesantes sobre cómo optimizar el coste. También le ayuda a eliminar máquinas innecesarias y, por lo tanto, a reducir los costes.

La página **Optimización de costes** incluye las siguientes funciones:

- Ahorro de costes
- Redimensionamiento de la infraestructura

Ahorro de costes [Technical Preview]

La página **Ahorro de costes** proporciona una representación visual del ahorro en infraestructura acumulado durante un período seleccionado y calcula el ahorro previsto para los días restantes. Al analizar el uso de las máquinas y las sesiones, esta página le ayuda a identificar el ahorro logrado y las oportunidades de reducción de costes. Esta página ofrece:

- Una perspectiva sobre la optimización de costes de infraestructura
- El importe ahorrado
- Información sobre una serie de supuestos que podrían dar lugar a costes superiores a los previstos
- Posibles oportunidades de identificación y planificación estratégica para ahorrar costes de infraestructura

La página **Optimización de costes** > **Ahorro de costes** incluye el **Ahorro estimado** y un **Informe de ahorro de Autoscale.**

El **Ahorro estimado** sirve de ayuda a la hora de evaluar un uso eficiente de los recursos de infraestructura. El Ahorro estimado sirve de ayuda a la hora de evaluar un uso eficiente de los recursos de infraestructura. El ahorro de costes se muestra en la moneda del hipervisor o como un porcentaje del coste incurrido. Puede ver los resultados de los últimos:

- Siete días
- Treinta días
- Tres meses
- Seis meses
- Doce meses

El gráfico de **Ahorro estimado** muestra lo siguiente:

- Ahorro estimado: Muestra el ahorro logrado en infraestructura durante el período seleccionado
- Máquinas con administración de energía: Muestra la cantidad total de máquinas con administración de energía.
- Ahorro previsto: Muestra cuánto se puede ahorrar en infraestructura durante el tiempo restante

El **Informe de ahorro de Autoscale** muestra información sobre el grupo de entrega para el que Autoscale está configurado y habilitado. Este informe solo incluye las máquinas con administración de energía.

Para obtener más información, consulte Ahorro de costes.

Redimensionamiento de la infraestructura La página **Redimensionamiento de la infraestructura** le ayuda a analizar los aspectos de aprovisionamiento y dimensionamiento de su grupo de entrega en función de la utilización de recursos. Según este análisis, puede optimizar el aprovisionamiento y el tamaño de las máquinas para que se adapten al patrón de utilización. Puede optimizar el coste de su infraestructura al reducir el gasto en recursos no usados. También puede optar por máquinas con especificaciones de CPU y memoria más bajas si la utilización de recursos es sistemáticamente inferior a la aprovisionada. Puede optimizar el rendimiento si opta por máquinas con especificaciones de CPU y memoria más altas si la utilización de recursos es sistemáticamente superior y observa que esto afecta a la experiencia de la sesión, como las métricas de *inicio de sesión e ICARTT*.

Puede filtrar el redimensionamiento de la infraestructura de la siguiente manera:

- Grupo de entrega: Puede filtrar por grupos de entrega de SO de sesión única o de SO multisesión
- Etiquetas: Las etiquetas son los nombres de las etiquetas que se aplican a la máquina. Por lo tanto, puede filtrar máquinas con las mismas etiquetas. Puede seleccionar varias etiquetas,

hasta un máximo de cinco. Al seleccionar varias etiquetas, puede filtrar todas las máquinas que tengan aplicada al menos una de esas etiquetas de máquina seleccionadas.
- Período de tiempo: Puede filtrar los datos de las últimas 24 horas, 7 días y 30 días.

La página Redimensionamiento de la infraestructura ofrece:

- Información sobre los detalles de utilización
- Resumen de la utilización de los recursos
- Tendencias en la utilización de los recursos

Haga clic en la ficha **Optimización de costes** en el menú de la izquierda de la página de inicio. A continuación, haga clic en la ficha **Redimensionamiento de la infraestructura** para acceder a la página **Redimensionamiento de la infraestructura**.

También puede hacer clic en el **enlace Redimensionar este grupo de entrega** en la sección **Detalles de infraestructura** de la ficha **Optimización de costes** > **Ahorro de costes** para acceder a la página **Redimensionamiento de la infraestructura**.

Para obtener más información, consulte Redimensionamiento de la infraestructura.

Inspeccionar las máquinas con acciones de energía recientes

Ahora puede inspeccionar las máquinas con estado correcto o fallido para las acciones de energía. Esta función le ayuda a analizar lo siguiente:

- Fallos de encendido que causan problemas al usuario
- Fallos de apagado que aumentan los costes

> **Nota:**
>
> Los datos solo están disponibles para las máquinas con administración de energía. No hay datos disponibles sobre las acciones de energía ocurridas antes de que se admitiera el uso de esta función.

Para ver el estado de energía de las máquinas, puede usar uno de los métodos siguientes:

- En la ficha **Filtros** -> **Máquinas**. En este caso, las columnas **Hora de acción de energía** y **Resultado de la acción de energía** están visibles de forma predeterminada. También puede seleccionar qué columnas quiere hacer visibles.
- En la ficha **Optimización de costes**. En este caso, el filtro predeterminado **Acción de energía desencadenada por** está configurado en **Autoscale** y el valor de **Resultado de la acción de energía** está establecido en **Fallido.**

Con esta función, puede ver los detalles de los controles de las acciones de energía. Por ejemplo, puede ver quién desencadenó la acción, qué acción cambió el estado de energía, el motivo del fallo y la hora en que se completó la acción. También puede exportar estos detalles.

Para obtener más información, consulte Inspeccionar las máquinas con acciones de energía recientes.

Alerta de acción de encendido fallida y acción de apagado fallida

La función de notificación y alertas proactivas de Director se ha mejorado para incluir dos nuevas alertas, alertas por **Fallo de la acción de encendido** y **Fallo de la acción de apagado**, basadas en la cantidad de máquinas con administración de energía que no se encendieron o apagaron en un grupo de entrega. La nueva condición de alerta le permite configurar los umbrales de alerta según la cantidad de máquinas con administración de energía que no se encendieron o apagaron en un grupo de entrega.

Para obtener más información, consulte Acción de encendido fallida y acción de apagado fallida.

Alerta de tiempo de actividad de máquina

La función de alerta y notificación proactiva de Director se ha mejorado para incluir una nueva alerta, Alerta de tiempo de actividad de máquina, basada en el tiempo de actividad de una máquina con administración de energía en un grupo de entrega. Por cada grupo de entrega en el que las máquinas hayan superado el umbral, recibe un archivo adjunto o una alerta de webhook solo para ese grupo de entrega.

La nueva condición de alerta le permite configurar los umbrales de alerta según la cantidad de horas por día, horas por semana u horas por mes que una máquina está encendida en un grupo de entrega.

Para obtener más información, consulte Alerta de tiempo de actividad de máquina.

Alerta de máquinas sin registrar

La funcionalidad de notificaciones y alertas proactivas de Director se ha mejorado para incluir una nueva alerta, **Máquinas no registradas (en %)**, basada en el porcentaje de máquinas sin registrar de un grupo de entrega. La nueva condición de alerta le permite configurar los valores de umbral críticos y de advertencia como un porcentaje de máquinas no registradas de un grupo de entrega.

Para obtener más información, consulte Máquinas no registradas.

Integraciones y exportaciones de datos

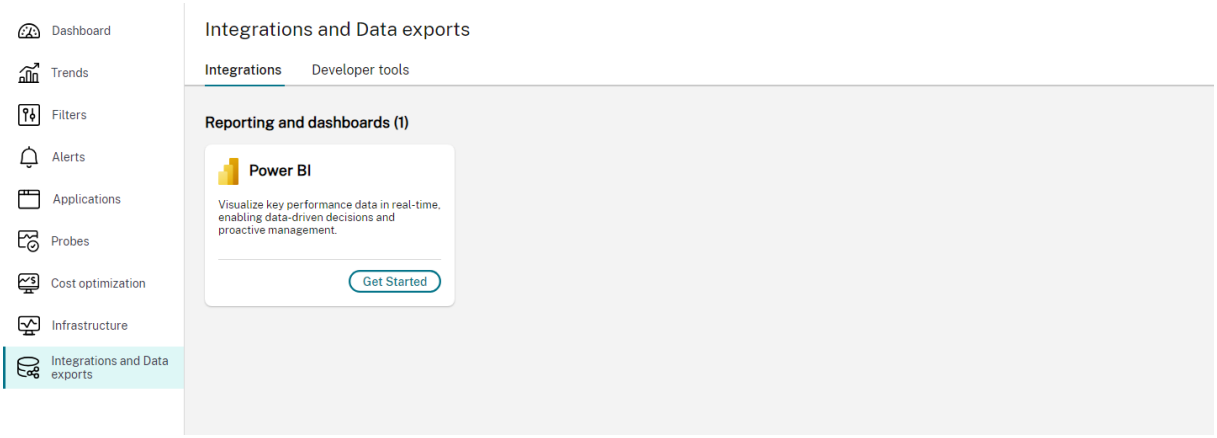
Citrix Director proporciona ahora una nueva interfaz de usuario para integraciones y exportaciones de datos. Esta función ayuda a comprender mejor las diversas interfaces e integraciones de terceros disponibles en Citrix Director. La página Integraciones y exportaciones de datos recientemente presentada incluye lo siguiente:

- Integraciones disponibles
- Herramientas de desarrollador compatibles

En esta página también se describe la API de REST configurada para la exportación de datos y se proporcionan enlaces de referencia a las guías y los documentos para ponerse en marcha con las integraciones y las herramientas para desarrolladores.

Actualmente, Citrix Director se integra con la observabilidad de Power BI. Puede usar esta función para exportar eventos y datos de rendimiento de Citrix Director a Power BI mediante las API REST.

Haz clic en **Integraciones y exportaciones de datos** en el menú de navegación de la izquierda. Aparece la página **Integraciones y exportaciones de datos**.



Para obtener más información, consulte Integraciones y exportaciones de datos.

Diagnosticar historial de sesiones de usuario [Technical Preview]

Citrix Director ahora muestra los detalles de las sesiones en estado activo, desconectado o finalizado. Anteriormente, solo podía ver los detalles de las sesiones activas. Con esta función, los administradores del servicio de asistencia técnica pueden solucionar problemas relacionados con una sesión que ha finalizado o está en estado cerrado. Los detalles de la sesión están disponibles para las últimas 24 horas y los últimos 2 días. Puede ver los siguientes detalles de una sesión finalizada o cerrada:

- Panel Detalles de la máquina: Muestra los detalles disponibles de la máquina en la que se inició la sesión seleccionada.

- Panel Detalles de la sesión: Muestra los detalles disponibles de la sesión seleccionada.
- Duración del inicio de sesión: Muestra la información sobre la duración del inicio de la sesión seleccionada. Puede ver el gráfico sobre el tiempo necesario para la intermediación con broker, el arranque de la máquina, la conexión HDX, la autenticación, los GPO, los scripts de inicio de sesión, la carga del perfil en disco y la sesión interactiva.

Para obtener más información, consulte Diagnosticar historial de sesiones de usuario.

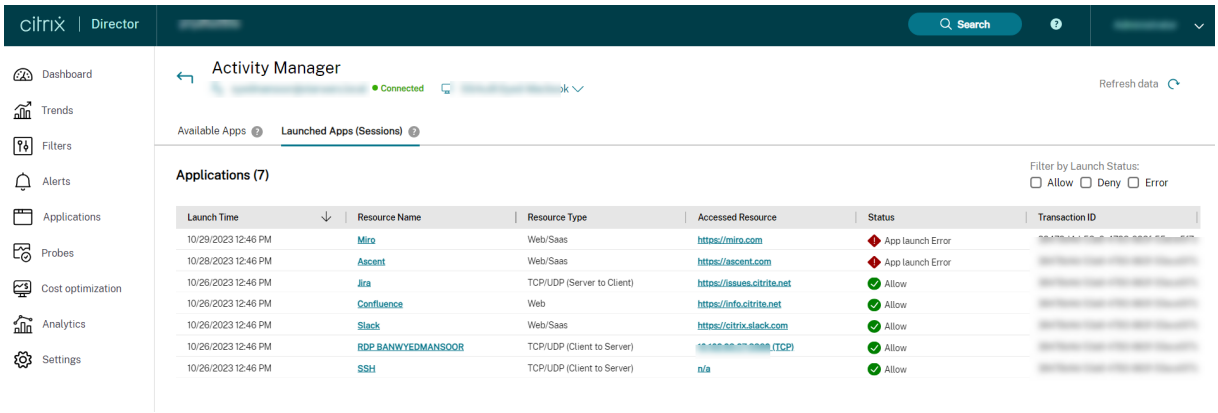
Sesión de Administrador de actividades para Secure Private Access [Technical Preview]

Citrix Director ofrece la vista Administrador de actividades para las sesiones de Secure Private Access, que le ofrece una visión general de las actividades de la sesión.El Administrador de actividades proporciona una vista completa de todas las aplicaciones y escritorios que se han abierto correctamente o que no se han podido abrir y del resultado de las directivas establecidas en la aplicación Secure Private Access.

El Administrador de actividades se muestra con los detalles de las **aplicaciones disponibles** y las **aplicaciones iniciadas**. Puede encontrar los siguientes detalles de la sesión:

- Hora de inicio
- Resource name
- Tipo de recurso
- Recurso accedido
- Estado
- ID de la transacción

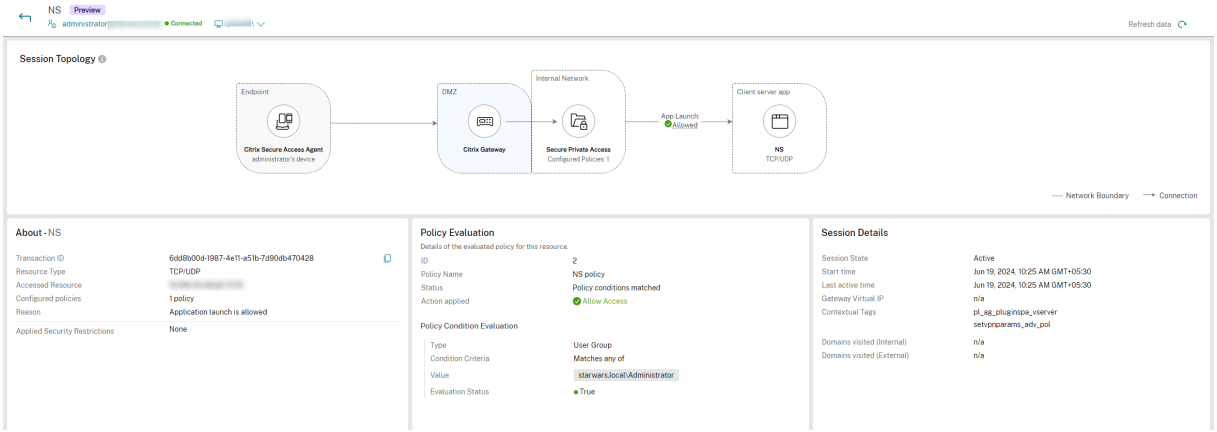
También puede filtrar los detalles anteriores con el estado de la aplicación, como Permitir, Denegar y Error. También puede ordenar los detalles con las flechas hacia arriba y hacia abajo.



Para obtener más información, consulte Ver la sesión de Administrador de actividades para Secure Private Access.

Vista de topología de sesión para aplicaciones de Secure Private Access [Technical Preview]

Puede ver la topología de sesión de las aplicaciones abiertas mediante Secure Private Access. Haga clic en la aplicación requerida en el Administrador de actividades para ver la topología de sesión de la aplicación seleccionada.



En la vista **Topología de la sesión**, puede ver la aplicación que se abre mediante Secure Private Access, el estado de evaluación de la directiva y el estado del inicio de la aplicación. También puede encontrar los detalles de la aplicación, la evaluación de directivas y los detalles de la sesión.

Para obtener más información, consulte Vista de topología de sesión para aplicaciones de Secure Private Access.

Supervisión de la infraestructura [Technical Preview]

Citrix Director ahora ofrece visibilidad del estado operativo de los componentes de Citrix Virtual Apps and Desktops. Esta función le ayuda a identificar, solucionar y resolver fácilmente los problemas relacionados con su infraestructura. Actualmente, se supervisa el estado de los componentes de Citrix Provisioning (PVS) y StoreFront.

Para admitir esta función, se ha introducido un nuevo ejecutable de Windows denominado Citrix Infra Monitor. Esto ayuda a recopilar las métricas de estado relevantes y transmitirlas desde los servidores de PVS o StoreFront a Director.

Esta función le ayuda a obtener conjuntos de datos de supervisión críticos y alertas proactivas con respecto a las métricas del sistema de servidor PVS y StoreFront en una única consola de Director. Los datos se recopilan cada cinco minutos de los componentes de supervisión para garantizar que se cuenta con la información más reciente.

Esta función tiene como objetivo mejorar la eficiencia operativa al ofrecer supervisión proactiva, métricas detalladas y alertas automatizadas, lo que garantiza que la infraestructura de Citrix funcione sin problemas y de manera eficiente.

Funciones principales Supervisión en tiempo real:

- Supervisión continua de los componentes de la infraestructura de Citrix, como los servidores de Citrix Provisioning (PVS) y StoreFront.
- Vistas de panel que presentan el estado del sistema, la utilización de los recursos y las métricas de rendimiento relevantes.

Análisis detallado:

- Proporciona un análisis detallado de las métricas de estado del sistema, como el estado de conectividad y el estado de servicio o proceso de cada componente.
- Detalles sobre las métricas de utilización de recursos, como la utilización de CPU, memoria y disco.

Alertas y notificaciones automatizadas:

- Umbrales de alerta personalizables para diversas métricas y estados con ámbitos granulares.
- Notificaciones en tiempo real a través de correo electrónico y webhooks.

Casos de uso Eficiencia operativa:

Garantiza que los equipos de administración de Citrix puedan mantener una alta disponibilidad y rendimiento de los servidores y servicios Citrix. Esta función también ayuda a minimizar el tiempo de inactividad al identificar y alertar de forma proactiva a los administradores sobre los problemas antes de que afecten a grupos de usuarios importantes.

Resolución de tíquets más rápida:

Supervisa las métricas clave sobre el estado y el rendimiento de los servidores para evaluar la entrega óptima de aplicaciones y escritorios virtuales a los usuarios. Use estas métricas para diagnosticar y resolver las quejas de los usuarios relacionadas con el rendimiento mediante el análisis de los componentes asociados.

Para obtener más información, consulte la sección Supervisión de la infraestructura [Technical Preview].

Directiva de infraestructura [Technical Preview]

Esta directiva se introduce para crear alertas relacionadas con el estado de los componentes compatibles de Citrix Virtual Apps and Desktops.

Una vez completada la configuración de Supervisión de la infraestructura, puede usar los datos de estado disponibles en Director para configurar las alertas para cualquier componente requerido. Los administradores pueden establecer condiciones, ámbitos y medios de notificación para recibir alertas

importantes por correo electrónico o una carga JSON a través de webhooks. Las alertas generadas también están disponibles en la sección **Alertas de Citrix** para su análisis y administración.

Como parte de esta directiva, se introducen las siguientes cuatro nuevas categorías:

- Accesibilidad
- Servicios dependientes
- Impacto
- Utilización de recursos

Puede establecer diferentes condiciones y modificar la gravedad de las categorías anteriores según sea necesario en la sección **Crítico** y **Advertencia**. También puede programar intervalos de repetición para estas alertas.

Las condiciones de cada categoría se pueden establecer con una gravedad crítica y de advertencia en función de las prioridades de la organización. También puede programar intervalos de repetición para estas alertas.

Para obtener más información, consulte la sección Directivas de infraestructura (Technical Preview).

Citrix Scout

Mejora del procedimiento de rastreo y reproducción

Anteriormente, podía usar la interfaz de usuario para importar las trazas de CDF guardadas en el procedimiento de rastreo y reproducción.

A partir de la versión 2407, se elimina esta opción de la interfaz de usuario. Cuando habilita la recopilación de registros adicionales, Scout detecta automáticamente las herramientas relacionadas con CDC instaladas en su máquina y recopila automáticamente los registros de seguimiento relacionados con las herramientas de CDC en el paquete ZIP. Puede personalizar este archivo ZIP y adjuntarlo a Scout. Con esta automatización, puede usar Citrix Scout de manera más eficaz y diagnosticar los problemas rápidamente.

Para obtener más información, consulte Habilitar la recopilación de registros adicionales.

Machine Creation Services (MCS)

Aumento del límite de réplicas por versión de imagen en Azure

Azure ha aumentado la cantidad máxima de réplicas de una versión única de imágenes de la galería a 100. Con el aumento del límite, ahora puede establecer la propiedad `SharedImageGalleryReplicaMaximur`

en un valor máximo de 100 al crear un catálogo de máquinas de MCS con la imagen de Azure Compute Gallery. Para obtener más información, consulte Configurar Azure Compute Gallery.

Compatibilidad con la virtualización anidada de Azure

Con esta función, si configura la VM maestra con virtualización anidada habilitada, todas las VM del catálogo de máquinas de MCS creadas con esa VM maestra tienen habilitada la virtualización anidada. Esta función se aplica a máquinas virtuales persistentes y no persistentes. Puede actualizar un catálogo de máquinas de MCS existente y las máquinas virtuales existentes para que tengan una virtualización anidada mediante la actualización de imágenes.

Actualmente, solo los tamaños de VM Dv3 y Ev3 admiten la virtualización anidada.

Para obtener información sobre la virtualización anidada, consulte el blog de Microsoft Nested Virtualization in Azure.

Recibir mensajes de advertencia en caso de error de hibernación

Ahora puede recibir mensajes de advertencia mediante un comando de PowerShell Get-ProvOperationEvent en caso de que se produzca un error de hibernación en las máquinas virtuales aprovisionadas por MCS y existentes con capacidad de hibernación. Para obtener más información, consulte Recibir mensajes de advertencia en caso de error de hibernación.

Validar permisos en la conexión de host en Azure

Anteriormente, en los entornos de Azure, solo podía validar las credenciales de conexión de host (ID de cliente o ID de aplicación) usadas para crear una conexión a Azure.

Con esta función, puede:

- Obtener la lista de permisos asignados a su credencial de conexión de host
- Obtener la lista de operaciones que se pueden realizar con los permisos asignados
- Información sobre los permisos requeridos
- Información sobre cómo agregar los permisos deseados

Esto le ayuda a solucionar problemas y a obtener los permisos necesarios con antelación para poder realizar las tareas sin quedar bloqueado. Para obtener más información, consulte Validar permisos en la conexión de host.

Cambiar el cifrado del disco en Azure

Con esta función, ahora puede cambiar el cifrado del disco en los entornos de virtualización de Azure. Puede realizar lo siguiente:

- Crear un catálogo de máquinas MCS con un conjunto de cifrado de disco (DES) distinto del DES de la imagen maestra.
- Cambiar el tipo de cifrado del disco de una clave DES a otra clave DES de un catálogo de máquinas de MCS existente y de las máquinas virtuales existentes.
- Actualizar una máquina virtual y un catálogo de máquinas de MCS que antes no estuvieran habilitados para CMEK para que tengan cifrado (DES) con clave de cifrado administrada por el cliente (CMEK), cifrado de disco en el host o cifrado doble.
- Actualizar una máquina virtual y un catálogo de máquinas de MCS cifrados para que dejen de estarlo.
- Habilitar el cifrado de discos con un dispositivo de punto final privado (un catálogo de máquinas de MCS que use una conexión de host habilitada con ProxyHypervisorTrafficThroughConnector).

Para obtener más información, consulte Cambiar el cifrado del disco.

Posibilidad de modificar los parámetros del archivo de paginación

Con esta función, puede modificar los parámetros del archivo de paginación de las máquinas virtuales recién agregadas a un catálogo existente sin actualizar la imagen maestra. Esta función se aplica actualmente a los entornos de Azure solamente.

Para modificar los parámetros del archivo de paginación, necesita la versión 2311 o posterior del VDA. Puede modificar los parámetros del archivo de paginación mediante los comandos de PowerShell. Para obtener más información sobre la modificación de los parámetros del archivo de paginación, consulte Modificar los parámetros del archivo de paginación.

MCS crea discos de ID con el tipo de volumen GP3 en un entorno de AWS

Anteriormente, en los entornos de AWS, los discos de identidad (ID) de las máquinas virtuales tenían el tipo de volumen GP2. Con esta función, MCS ahora puede aprovisionar máquinas virtuales con discos de identidad con el tipo de volumen GP3. Como el tipo de volumen GP3 es la opción más económica que ofrece AWS, esta función minimiza los costes.

La función solo se aplica a las máquinas virtuales agregadas a un nuevo catálogo y a las máquinas virtuales nuevas agregadas a un catálogo existente. Las máquinas virtuales existentes creadas antes

de esta función siguen teniendo discos de ID con el tipo de volumen GP2, a menos que se restablezca el disco de ID.

Función para capturar propiedades adicionales mediante el origen del perfil de máquina en AWS

En los entornos de AWS, con esta mejora, ahora puede crear o actualizar un catálogo basado en perfiles de máquinas para incluir lo siguiente:

- Opciones de captura de CPU, tipo de arrendamiento y capacidad de hibernación del origen del perfil de máquina mientras crea un catálogo de máquinas de MCS.
- Cambiar el tipo de arrendamiento del origen del perfil de máquina mientras modifica un catálogo de máquinas de MCS. Esta funcionalidad se aplica a las nuevas máquinas virtuales agregadas al catálogo.
- Cambiar la capacidad de hibernación del origen del perfil de máquina mientras modifica un catálogo de máquinas de MCS. Esta funcionalidad se aplica a las nuevas máquinas virtuales agregadas al catálogo.

El origen del perfil de máquina puede ser una máquina virtual o una versión de plantilla de inicio. Esta función se aplica tanto a los catálogos persistentes como a los no persistentes.

Para obtener más información, consulte Crear un catálogo mediante un perfil de máquina.

Función para cifrar el disco de ID de máquinas virtuales de un catálogo de máquinas de MCS en AWS

Anteriormente, en los entornos de AWS, MCS permitía solo el cifrado del disco del sistema operativo de las máquinas virtuales aprovisionadas. Con esta función, ahora puede cifrar el disco de ID además del disco del sistema operativo. Esta funcionalidad le permite usar las claves de AWS KMS (clave administrada por el cliente y clave administrada por AWS) para realizar operaciones criptográficas en los discos conectados a una máquina virtual.

Para el cifrado del sistema operativo y los discos de ID, configure una de las siguientes opciones:

- Use una imagen maestra cifrada (por ejemplo, una AMI creada a partir de una instancia o instantánea que contenga un volumen raíz cifrado con una clave de KMS)
- Use un origen de perfil de máquina (máquina virtual o plantilla de inicio) que contenga un volumen raíz cifrado.

Para obtener más información, consulte Cifrar los discos de ID y sistema operativo.

Validar permisos en la conexión de host en AWS

En los entornos de AWS, ahora puede validar los permisos en una conexión de host para realizar tareas relacionadas con la creación y la administración de catálogos de máquinas de MCS. Esta implementación le ayuda a conocer con antelación los permisos ausentes necesarios para diferentes situaciones, como la creación, la eliminación y la actualización de máquinas virtuales, la administración de energía de las máquinas virtuales y el cifrado de EBS, para evitar el bloqueo en momentos críticos. Para obtener más información, consulte Validar permisos en la conexión de host.

Función para heredar etiquetas de un origen de perfiles de máquina en las máquinas virtuales y los discos de GCP

Con esta función, las máquinas virtuales y los discos del catálogo de máquinas de MCS (disco de identidad, disco con caché de escritura y disco del sistema operativo) ahora pueden heredar las etiquetas de un origen de perfil de máquina (plantilla de instancia o instancia de máquina virtual de GCP). Puede usar las etiquetas para distinguir las instancias pertenecientes a diferentes equipos (por ejemplo, team:research y team:analytics) y usarlas para la contabilidad de costes o la elaboración de presupuestos. Para obtener más información sobre las etiquetas, consulte el documento de GCP Organize resources using labels.

Esta función se aplica a catálogos de máquinas de MCS persistentes y no persistentes.

Puede crear un nuevo catálogo de máquinas de MCS, actualizar un catálogo y actualizar las máquinas virtuales existentes para que hereden las etiquetas de un origen de perfil de máquina.

Para obtener más información, consulte Máquinas virtuales y discos con etiquetas heredadas.

Crear catálogos de Citrix Provisioning mediante comandos de MCS PowerShell en XenServer

Ahora puede crear catálogos de Citrix Provisioning mediante comandos de MCS PowerShell en entornos de XenServer. Puede crear catálogos de Citrix Provisioning basados en perfiles de máquina y no basados en perfiles de máquina. Para obtener más información, consulte Crear catálogos de Citrix Provisioning en Citrix Studio.

Función para heredar etiquetas personalizadas de un perfil de máquina en las máquinas virtuales aprovisionadas

Ahora puede agregar las etiquetas personalizadas de una máquina virtual SCVMM a las máquinas virtuales aprovisionadas por MCS junto con la etiqueta CitrixProvisioningSchemeId predeterminada. Para agregar las etiquetas personalizadas a las máquinas virtuales aprovisionadas, debe usar la máquina virtual SCVMM como perfil de máquina al crear o actualizar un catálogo de máquinas de MCS.

Si quita una máquina virtual de un catálogo, solo se quita de la etiqueta CitrixProvisioningSchemeID. Las etiquetas personalizadas no se eliminan de la máquina virtual. Esta función se aplica a un nuevo catálogo de máquinas de MCS y a las nuevas máquinas virtuales agregadas a un catálogo existente. Para obtener más información, consulte Crear un catálogo con un perfil de máquina.

Validar la configuración antes de crear un catálogo de máquinas MCS

Con esta función, ahora puede validar los parámetros de configuración antes de crear un catálogo de máquinas MCS mediante el parámetro -validate del comando New-ProvScheme. Después de ejecutar este comando de PowerShell con ese parámetro, se muestra el mensaje de error correspondiente si se usa un parámetro incorrecto o si un parámetro está en conflicto con otro parámetro. A continuación puede usar el mensaje de error para resolver el problema y crear sin problemas un catálogo de máquinas MCS con PowerShell.

Actualmente, esta función se aplica a los entornos de virtualización de Azure, GCP y VMware. Para obtener más información, consulte Validar la configuración antes de crear un catálogo de máquinas MCS.

Reparar la información de identidad de las cuentas de equipo activas en AWS, GCP y XenServer

En entornos de AWS, GCP y XenServer, ahora puede restablecer la información de identidad de las cuentas de equipo activas que tengan problemas relacionados con la identidad. Puede elegir restablecer solo la contraseña de la máquina y las claves de confianza, o bien restablecer toda la configuración del disco de identidad. Esta implementación se aplica tanto a catálogos de máquinas de MCS persistentes como no persistentes. En la actualidad, la función solo es compatible con los entornos de virtualización de AWS, Azure, GCP, VMware y XenServer. Para obtener más información, consulte Reparar la información de identidad de las cuentas de equipo activas.

Función para asignar una letra de unidad específica al disco de la memoria caché de reescritura de E/S de MCS

Antes, el sistema operativo Windows asignaba automáticamente una letra de unidad al disco de la memoria caché de reescritura de E/S de MCS. Con esta función, ahora puede asignar una letra de unidad específica a un disco de la memoria caché de reescritura de E/S de MCS. Esta implementación le ayuda a evitar conflictos entre la letra de la unidad de cualquier aplicación que utilice y la letra de la unidad del disco de la memoria caché de reescritura de E/S de MCS. Esta función solo se aplica al sistema operativo Windows. Para obtener más información, consulte Asignar una letra de unidad específica al disco de la memoria caché de reescritura de E/S de MCS.

Profile Management

Para obtener información sobre nuevas funciones, consulte el artículo Novedades en su propio documento.

Linux VDA

Para obtener información sobre nuevas funciones, consulte el artículo Novedades en su propio documento.

Grabación de sesiones

Para obtener información sobre nuevas funciones, consulte el artículo Novedades en su propio documento.

Workspace Environment Management

Para obtener información sobre nuevas funciones, consulte el artículo Novedades en su propio documento.

Citrix Provisioning

Para obtener información sobre nuevas funciones, consulte el artículo Novedades en su propio documento.

Servicio de autenticación federada

Para obtener información sobre nuevas funciones, consulte el artículo Novedades en su propio documento.

Problemas resueltos

August 17, 2024

Citrix Virtual Apps and Desktops 7 2407 incluye los siguientes problemas resueltos:

Gráficos

- Es posible que, mientras trabaja, se produzcan apagones intermitentes en la pantalla con una duración de aproximadamente 10 segundos, durante los cuales se restablece el proceso de gráficos del software Citrix (`Ctxgfx.exe`). El subproceso `twencode` sufre una excepción por infracción de acceso, lo que hace que `ctxExceptionHandler` registre minivolcados y cause este problema. `ctxExceptionHandler` está configurado para generar volcados completos para su examen. [CVADHELP-24877]

Machine Creation Services

- Al actualizar un sitio de Multi-Delivery Controller de algunas versiones LTSR anteriores a la 2402 (incluidas las versiones 2302, 2305, 2308 y 2311) a la 2402 LTSR, las acciones de energía de una máquina virtual podrían fallar si el sitio solo actualiza su versión parcialmente. Para obtener más información, consulte CTX666299.

VDA para SO de sesión única

Portapapeles

- Cuando usa el VDA 2203 LTSR CU4 y cuando copia y pega el contenido en formato WebP, `WfShell` deja de funcionar. [CVADHELP-25356]
- La opción de copiar al portapapeles de la aplicación remota publicada no funciona en las versiones CU3 y CU4. [CVADHELP-24687]
- Es posible que se produzca un problema de pérdida de memoria con el servicio Citrix Smart Card Service en las instancias de VDA de servidor en las que el consumo de memoria alcanza el 100%. [CVADHELP-25389]

Sesión/Conexión

- La aplicación OpenTEXT ETX no se abre debido a una infracción de acceso con el siguiente módulo:

  `C:\Program Files\Citrix\HDX\bin\CtxMFPlugin64.dll` [CVADHELP-24985]

Tarjetas inteligentes

- Es posible que se produzca un problema de pérdida de memoria con el servicio Citrix Smart Card Service en las instancias de VDA de servidor en las que el consumo de memoria alcanza el

100%. [CVADHELP-25389]

VDA para SO multisesión

Portapapeles

- Cuando usa el VDA 2203 LTSR CU4 y cuando copia y pega el contenido en formato WebP, `WfShell` deja de funcionar. [CVADHELP-25356]
- La opción de copiar al portapapeles de la aplicación remota publicada no funciona en las versiones CU3 y CU4. [CVADHELP-24687]
- Es posible que se produzca un problema de pérdida de memoria con el servicio Citrix Smart Card Service en las instancias de VDA de servidor en las que el consumo de memoria alcanza el 100%. [CVADHELP-25389]

Sesión/Conexión

- La aplicación OpenTEXT ETX no se abre debido a una infracción de acceso con el siguiente módulo:

  `C:\Program Files\Citrix\HDX\bin\CtxMFPlugin64.dll` [CVADHELP-24985]

Tarjetas inteligentes

- Es posible que se produzca un problema de pérdida de memoria con el servicio Citrix Smart Card Service en las instancias de VDA de servidor en las que el consumo de memoria alcanza el 100%. [CVADHELP-25389]

Problemas conocidos

August 17, 2024

Citrix Virtual Apps and Desktops 7 2407 incluye los siguientes problemas conocidos:

Notas

- 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. Use el Editor del Registro bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

General

- Si inicia la barra de aplicaciones y, a continuación, abre el menú Central de conexiones en la aplicación Citrix Workspace para Windows, la barra de aplicaciones no aparece en el servidor que la aloja. [HDX-27504]
- Si utiliza la aplicación Citrix Workspace para Windows e inicia la barra de aplicaciones en posición vertical, la barra cubre el menú Inicio o la bandeja del reloj del sistema. [HDX-27505]
- 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]
- Es posible que Citrix Desktop Service no se inicie después de realizar una actualización en contexto del sistema operativo de Windows 10 a Windows 11. Para resolver el problema, reinicie la máquina. [HDX-58399]
- Los parámetros de **Límites de sesión** para los VDA multisesión se rechazan en los hosts de sesión que ejecutan Windows Server 2022, Windows 10 Enterprise multisesión y Windows 11 Enterprise multisesión.
  Como solución temporal, puede configurar los **Límites de tiempo de sesión de RDS** mediante GPO. [HDX-47001]
- El cuadro de diálogo de seguridad de Windows asociado a FIDO2 no se mostrará delante de la ventana de la sesión ICA si está ejecutando la aplicación con privilegios de administrador. El diseño del sistema operativo hace que el cuadro de diálogo de seguridad de Windows se oculte detrás de la ventana de la sesión ICA si se ejecuta como un proceso elevado. [HDX-26794]
- Es posible que no se pueda copiar y pegar en el portapapeles con datos de más de 100 MB entre el cliente y la sesión ICA. No se admiten copias de búfer de gran tamaño. [HDX-59028]
- Aunque se crea un punto de restauración, no se puede restaurar un VDA si una instalación de VDA falló en la plataforma multisesión Windows 10 o Windows 11. La instalación del VDA se

inició a través de la interfaz de usuario o la línea de comandos. [HDX-58915]

- El sistema operativo multisesión Windows 10 o Windows 11 no es compatible con Restaurar sistema de Windows. Por lo tanto, la opción de crear un punto de restauración no está disponible en la interfaz de usuario. Las opciones de línea de comandos /`EnableRestore` o /`EnableRestoreCleanup` se ignoran y se registra un mensaje que indica la **inhabilitación de Restaurar sistema** por no ser compatible actualmente en el sistema operativo multisesión Windows 10/11. [HDX-58915]
- Citrix firma archivos binarios generados por Citrix y de terceros. Esto significa que Citrix autentica los archivos binarios. Las versiones de los archivos binarios de terceros no cambian, ya que se obtienen de terceros. Si ya hay un archivo binario instalado, la actualización de un VDA no instala el archivo binario correspondiente si las versiones coinciden. Para evitar esta limitación:

  1. Incluya los archivos binarios en una **lista de permitidos**. Esto elimina la necesidad de firmar los archivos binarios.
  2. Desinstale el VDA anterior e instale el nuevo. Es como una instalación nueva de un VDA y se aplicarán las versiones firmadas.

  [HDX-62302]
- En algunos casos, cuando se usa el filtro de directiva IP de cliente, la dirección IP usada para evaluar la directiva es incorrecta. [HDX-62375]
- Al usar PassThrough de dominio mejorado para Single Sign-On, es posible que el inicio de sesión falle si el dispositivo cliente o el host de la sesión ejecutan Windows 11. [HDX-62973]
- Los datos de las directivas pueden perderse cuando el sitio se actualiza con unas configuraciones de directiva no válidas. Si encuentra este problema, inicie un caso de asistencia técnica desde el portal de asistencia de Citrix. [GP-1671]
- Al instalar Citrix Rendezvous V2 con los paquetes VDAWorkstationSetup_2402, VDAServerSetup_2402 o VDAWorkstationCoreSetup_2402, la instalación puede fallar porque falta el archivo Citrix.Diagnostics.Tracing.dll en estos paquetes. Como solución temporal:

  - Instale Citrix Rendezvous V2 desde el paquete CVAD completo de Citrix Virtual Apps and Desktops 7 2402 LTSR o desde Citrix_Virtual_Apps_and_Desktops_7_2402_LTSR.iso.
  - Como alternativa, sustituya el archivo Citrix.Diagnostics.Tracing.dll que falta. Para sustituir el archivo:

    1. Copie el archivo Citrix.Diagnostics.Tracing.dll del paquete CVAD Citrix Virtual Apps and Desktops 7 2402 LTSR o de la ISO de la carpeta “x64\ XenDesktop Setup”.
    2. Cree una carpeta temporal. Por ejemplo: “C:\Workaround”.
    3. Extraiga el paquete de instalación mínimo a la carpeta temporal con el comando: VDAWorkstationSetup_2402.exe /extract “C:\Workaround”.

4. Copie el archivo Citrix.Diagnostics.Tracing.dll en la carpeta "C:\Workaround\Extract\Image-Full\x64\XenDesktop Setup".
5. Inicie la instalación del VDA. Para ello, ejecute el comando: "C:\Workaround\Extract\Image -Full\ x64\ XenDesktop Setup\ XenDesktopVdaSetup.exe» [HDX-65363]

Web Studio

Secure Private Access con Web Studio

- La barra de navegación está parcialmente visible cuando se redirige a un usuario desde la ficha Información general > enlace "Agregar URL del servidor de licencias"a la página Parámetros > Integraciones. Actualice la página para ver la barra de navegación. [SPAOP-4782]
- Aparece una ventana emergente de advertencia en blanco cuando se introduce una URL de puerta de enlace incorrecta. Pase el cursor sobre el icono de advertencia para ver el mensaje de advertencia. [SPAOP-4947]
- Cuando realiza una integración de día 0 e intenta configurar una base de datos, el texto de la ventana emergente de advertencia no se muestra después de cambiar del modo manual al automático. Pase el cursor sobre el icono de advertencia para ver el mensaje. [SPAOP-4948]
- La barra de desplazamiento vertical está parcialmente visible en todas las fichas de la consola. No se necesita ninguna solución temporal para este problema y no afecta a ninguna función o experiencia de usuario. [SPAOP-4851]
- En la ficha **Parámetros > Integraciones**, la barra de desplazamiento horizontal no está visible en la parte inferior de la página si la ventana del explorador es pequeña. La barra de desplazamiento horizontal no es necesaria si la ventana del explorador está maximizada. [SPAOP-4844]
- En los registros de **solución de problemas**, la barra de desplazamiento vertical no está visible en la parte inferior de la página cuando se abre el cuadro de diálogo de detalles del registro. No se necesita ninguna solución temporal para este problema y no afecta a ninguna función o experiencia de usuario. [SPAOP-4843]
- La ficha **Información general** no aparece resaltada al iniciar sesión en la consola de Secure Private Access o al volver a WS y volver a la consola de Secure Private Access. No se necesita ninguna solución temporal para este problema y no afecta a ninguna función o experiencia de usuario. [SPAOP-4691]
- En la ficha **Parámetros > Integraciones**, los mensajes de error aparecen detrás del cuadro de diálogo en lugar de delante de él. No hay ninguna solución temporal para este problema y no afecta a ninguna función o experiencia de usuario. [SPAOP-4856]

Nota:

Todos los problemas anteriores se producen solo cuando se accede a Secure Private Access desde Web Studio. No son aplicables si se accede a Secure Private Access independientemente.

Web Studio

Al modificar un catálogo en Web Studio para Google Cloud con CMEK para discos, saltarse los pasos del asistente puede provocar errores en futuros casos de agregar máquinas. Para evitar este problema, complete todo el asistente sin saltarse ningún paso o use el SDK de PowerShell para realizar la operación. [STUD-31280]

Gráficos

- 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]
- Es posible que note cámaras web adicionales conectadas al escritorio remoto en la aplicación Skype para escritorio. La vista previa de estas cámaras web adicionales está bloqueada y es posible que muestren una pantalla negra por motivos de seguridad. Puede ignorar las cámaras web adicionales y seguir usando la cámara web como dispositivo de punto final. [HDX-58807]
- La H265 444 en Intel y en algunas GPU de NVIDIA podría provocar la aparición de artefactos en la sesión. Para los problemas relacionados con las GPU Intel, existe una solución temporal para cambiar el tamaño de la sesión o cambiar el modo de pantalla completa. [PMCS-41084]

Machine Creation Services

- En un entorno de VMware alojado en AWS, no se pueden crear catálogos de máquinas de MCS si la imagen maestra está habilitada para vTPM. Este problema afecta a todas las versiones de Citrix Virtual Apps and Desktops. Para obtener asistencia de VMware, consulte Get Support. [PMCS-37603]

Impresión

- Las impresoras de Universal Print Server seleccionadas en el escritorio virtual no aparecen en la ventana **Dispositivos e impresoras** del panel de control. No obstante, cuando los usuarios trabajan en las aplicaciones, pueden usar esas impresoras. Este problema solo se produce en Windows 10. 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]
- Algunos trabajos de impresión de impresoras de red con equilibrio de carga pueden fallar cuando las conexiones SSL a Universal Print Servers están habilitadas. Esto ocurre cuando los trabajos de impresión se ejecutan rápidamente uno tras otro. [HDX-58316]

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]
- Es posible que vea una pantalla negra al iniciar una sesión si tiene FSLogix 2201 HF1 instalado en el host de la sesión. Para solucionar este problema, debe actualizar FSLogix a una versión más reciente. [HDX-46159]

Profile Management

- La documentación de Profile Management 2407 ofrece información específica acerca de las actualizaciones de esta versión.

Linux VDA

- La documentación de Linux VDA 2407 ofrece información específica acerca de las actualizaciones de esta versión.

Grabación de sesiones

- La documentación de Grabación de sesiones 2407 ofrece información específica acerca de las actualizaciones de esta versión.

Workspace Environment Management

- La documentación de Workspace Environment Management 2407 proporciona información específica sobre las novedades de esta versión.

Citrix Provisioning

- La documentación de Citrix Provisioning 2407 ofrece información específica acerca de las actualizaciones de esta versión.

Servicio de autenticación federada

- La documentación de la versión 2407 del Servicio de autenticación federada ofrece información específica sobre las novedades de esta versión.

Elementos retirados

August 17, 2024

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 acerca de la asistencia durante el ciclo de vida útil del producto, 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. Las fechas en **negrita** indican cambios en esta versión.

Elementos retirados

Elemento retirado indica que tenemos la intención de quitar la función o capacidad de una versión futura. La función o capacidad seguirá funcionando y es totalmente compatible hasta que se elimine oficialmente. Esta notificación de obsolescencia puede durar algunos meses o años. Al retirar la función o la capacidad, dejarán de funcionar. Este aviso sirve para que tenga tiempo suficiente para planificar y actualizar el código antes de que se retire la función o capacidad. Siempre que sea posible, se sugerirán soluciones alternativas a los elementos retirados.

Elemento	Retirada anunciada en la versión	Alternativa
Multiple monitor hooks (MMHook)	2407	-

Elemento	Retirada anunciada en la versión	Alternativa
Rendezvous V1	2402	Use Rendezvous V2.
Secure ICA	2402	-
Compatibilidad con VDA en Windows Server 2016	2402	Actualice a la versión más reciente de Windows Server.
Compatibilidad con Delivery Controller, Web Studio, Citrix Director, Servidor de licencias Citrix, Citrix StoreFront, VDI de servidor para sistemas operativos de sesión única, VDA para sistemas operativos multisesión, bosque y dominio de Active Directory y Universal Print Server en Windows Server 2016	2402	Actualice a la versión más reciente de Windows Server.
Versiones compatibles de Microsoft SQL Server 2016 y 2017 para la configuración del sitio, el registro de configuración y las bases de datos de supervisión	2402	Actualice a la versión más reciente de Microsoft SQL Server.
Función para configurar la caché de reescritura para que incluya solo una caché de disco y ninguna caché de memoria	2402	Use la opción de configuración del tamaño de la memoria caché y asigne un tamaño distinto de cero.
Compatibilidad con los catálogos de Azure creados antes de existir la función de aprovisionamiento bajo demanda (catálogos "antiguos")	2402	Cree de nuevo las máquinas virtuales del catálogo antiguo de Azure. Los catálogos se aprovisionan bajo demanda y ayudan a ahorrar costes de almacenamiento.
La directiva de **Velocidad de fotogramas mínima objetivo**	2311	Utilice **Indicador de estado de gráficos** para modificar la velocidad de fotogramas mínima objetivo.

Elemento	Retirada anunciada en la versión	Alternativa
Compatibilidad con Citrix Connector 3.1 para System Center Configuration Manager	2311	Actualice la imagen o la aplicación manualmente.
Compatibilidad para usar una imagen maestra en una región diferente de la región en la que se creó el catálogo	2311	Use Azure Compute Gallery para replicar la imagen maestra en la región deseada.
Parámetro del límite de memoria de la presentación de HDX Graphics	2311	Se asigna la cantidad mínima de memoria requerida para garantizar que el diseño de pantalla del cliente se adapte por completo.
Compatibilidad con el modo progresivo en HDX Graphics	2311	Use Thinwire. Consulte Modo progresivo.
Función disponible para la redirección de contenido del explorador en Internet Explorer 11	2311	Use la redirección de contenido del explorador basada en Google Chrome.
Ya no es compatible con AWS Volume Worker	2311	Use carga y descarga directa en disco. Consulte Carga y descarga directa en disco.
Compatibilidad con SQL Server 2016 en el intermediario	2308	Usar las versiones más recientes. Para obtener más información, consulte Requisitos del sistema.
Compatibilidad con XenApp 5.x en Director	2308	—
Compatibilidad con XenApp 6.x en Director	2308	—
Paquete SCOM para alertas en Director	2308	—
Compatibilidad con el plug-in en Director	2308	—
Compatibilidad con el formato SDP de WebRTC (Plan B)	2308	Actualice la aplicación Citrix Workspace a una versión compatible.

Elemento	Retirada anunciada en la versión	Alternativa
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 Tabla de funciones y compatibilidad de versiones.
Compatibilidad con `AwsCaptureInstanceProperties` de uso en entornos de AWS	2308	Usar un perfil de máquina. Consulte Crear un catálogo mediante un perfil de máquina.
Comando de PowerShell `Schedule-ProvVMUpdate`	2305	Utilice `Set-ProvVMUpdateTimeWindow`.
Comando de PowerShell `Request-ProvVMUpdate`	2305	Use `Set-ProvVMUpdateTimeWindow` con los parámetros `-StartsNow` y `-DurationInMinutes -1`.
Comando de PowerShell `Cancel-ProvVMUpdate`	2305	Utilice `Clear-ProvVMUpdateTimeWindow`.
Parámetro `DedicatedTenancy` utilizado en el comando `New-ProvScheme`	2303	Utilice el parámetro `TenancyType`.
License Server VPX	2206	—
Discos no administrados para aprovisionar máquinas virtuales en entornos de Azure	2206	Usar discos administrados.
Redirección de host a cliente (URL)	2203	Redirección bidireccional de contenido.

Elemento	Retirada anunciada en la versión	Alternativa
Compatibilidad con cuatro comandos específicos de AWS: `Revoke-HypSecurityGroupIngress`, `Revoke-HypSecurityGroupEgress`, `Grant-HypSecuritygroupegress` y `Grant-HypSecurityGroupIngress`, utilizados en entornos locales y de la nube.	2203	—
Citrix Files para Windows y Citrix Files para Outlook desde el metainstalador de VDA.	2203	Use los instaladores independientes.
Componente del agente de WEM del metainstalador de VDA.	2203	—
Opción Wake on LAN (WoL) integrada en SCCM para acceso con Remote PC.	2012	Use la función Wake on LAN independiente.
Citrix SCOM Management Packs para XenApp y XenDesktop, Provisioning Services y StoreFront. Para ver las versiones de productos que se pueden supervisar, consulte la documentación de Citrix SCOM Management Pack.	1912	Utilice Director para supervisar y administrar la implementación. Para obtener más información sobre el fin de vida de SCOM y sus alternativas, consulte https://support.citrix.com/article/CTX266943.

Elemento	Retirada anunciada en la versión	Alternativa
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.

Elementos eliminados

Los elementos eliminados se quitan (o ya no se ofrecen o se desarrollan) en Citrix Virtual Apps and Desktops.

Elemento	Retirada anunciada en la versión	Eliminado en la versión	Alternativa
Aplicación Citrix Workspace para Windows 1912	—	2402	Usar las versiones más recientes.
HDX Graphics FullScreen + Optimización de texto	2311	2311	
Compatibilidad con NVIDIA Frame Buffer Capture (NVFBC) con HDX 3D Pro	2308	2311	Utilice la API de duplicación de escritorios (DDAPI).
Compatibilidad de VDA con la configuración de directiva "Instalación automática de controladores de impresora".	7.16	2311	Ninguno. Configuración de directiva que se admitía solo para agentes VDA en sistemas operativos anteriores (Windows 7, Windows Server 2012 R2 y versiones anteriores).

Elemento	Retirada anunciada en la versión	Eliminado en la versión	Alternativa
Codificación por hardware de GPU de NVIDIA (NVENC) con: vGPU 11 y versiones anteriores, y versión 466.77 del controlador y versiones anteriores.	2305	2305	Uso de controladores NVIDIA actualmente compatibles: vGPU 13 o una versión posterior, versión 471.41 o una posterior.
Herramientas de compatibilidad de Citrix (Supportability-Tool_x64 .msi) del metainstalador de VDA.	—	2212	—
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).	2003	2006	Use Citrix Licensing Manager.
Compatibilidad con el adaptador de gráficos del Citrix Indirect Display Driver (IDD) en la versión 1709 de Windows 10 y en versiones anteriores.	2003	2003	Utilice los VDA de Citrix Virtual Apps and Desktops 7 1912 LTSR.

Elemento	Retirada anunciada en la versión	Eliminado en la versión	Alternativa
Codificación por hardware con las GPU de NVIDIA (NVENC) mediante GRID 9 o controladores de pantalla anteriores.	2003	2003	Utilice controladores de pantalla GRID 10 con los VDA de Citrix Virtual Apps and Desktops 7 2003 o versiones posteriores, o bien use los VDA de Citrix Virtual Apps and Desktops 7 1912 LTSR.
Función Autoservicio de restablecimiento de contraseñas (SSPR).	2003	2006	—
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.	1912	2003	Actualice a .NET Framework 4.8.
VDA en Windows Server 2012 R2.	1912	2003	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	2003	—
Instalación de Studio en máquinas de 32 bits (x86).	1909	2003	Realice la instalación en un sistema operativo x64 compatible.

Elemento	Retirada anunciada en la versión	Eliminado en la versión	Alternativa
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	2003	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	2003	Instale bases de datos en una versión compatible de Microsoft SQL Server.
Compatibilidad con VDA en Windows 10 en plataformas x86.	1906	1909*	Instale los VDA en un sistema operativo x64 compatible. *Esta función sigue ofreciéndose en Citrix Virtual Apps and Desktops 7 1912 LTSR.

Elemento	Retirada anunciada en la versión	Eliminado en la versión	Alternativa
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.
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	2203	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 https://docs.citrix.com/es-es/citrix-workspace-app.

Elemento	Retirada anunciada en la versión	Eliminado en la versión	Alternativa
Compatibilidad de VDA con la configuración de directiva "Instalación automática de controladores de impresora".	7.16	2311	Ninguno. Configuración de directiva que se admitía solo para agentes VDA en sistemas operativos anteriores (Windows 7, Windows Server 2012 R2 y versiones anteriores).
Acceso a escritorios en sitios de Desktop Appliance para usuarios de StoreFront	1811	1912	Use Desktop Lock para casos de uso que no pertenezcan a ningún dominio.
Compatibilidad con la tecnología de pantalla remota Framehawk	1811	1903	Utilice Thinwire con el transporte adaptable habilitado.
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 Virtual Apps and Desktops Service 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.)

Elemento	Retirada anunciada en la versión	Eliminado en la versión	Alternativa
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 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.
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 https://www.citrix.com/blogs/2018/01/08/the-citrix-strategy-for-windows-7-virtual-desktop-users/).	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 CTX224843.
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.

Elemento	Retirada anunciada en la versión	Eliminado en la versión	Alternativa
Redirección de composición del escritorio (anteriormente conocida como DirectX Command Remoting o DCR)	7.15 LTSR	7.16	Use Thinwire.
Experiencia clásica en Citrix Receiver para Web (interfaz de usuario "burbujas verdes").	7.15 LTSR (y StoreFront 3.12)	1903	Experiencia unificada de Citrix Receiver para Web.
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.

Elemento	Retirada anunciada en la versión	Eliminado en la versión	Alternativa
Redirección de Flash	7.15 LTSR	1912	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 Fin de vida para la redirección de Flash.
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.

Elemento	Retirada anunciada en la versión	Eliminado en la versión	Alternativa
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".
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.

Elemento	Retirada anunciada en la versión	Eliminado en la versión	Alternativa
Modo antiguo de Thinwire	7.12	7.16	Use Thinwire. 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.
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	7.12	7.16	Use Caché de host local.

Elemento	Retirada anunciada en la versión	Eliminado en la versión	Alternativa
XenDesktop 5.6 en Windows XP. No se admiten instalaciones de VDA en Windows XP.	7.12	7.16	Instale los VDA en un sistema operativo compatible.
Compatibilidad con conexiones de CloudPlatform	7.12	2003	Use un hipervisor o servicio de nube compatibles.
Compatibilidad con conexiones de Azure clásico (también conocido como Administración de servicios de Azure)	7.12	2003	Considere la posibilidad de utilizar Virtual Apps and Desktops Service en Citrix Cloud.
Funcionalidad de AppDisks (y la integración de AppDNA en Studio, que la admite)	7.13	2003	Consulte “Citrix App Layering”.
Funcionalidad Personal vDisk	7.15	2006†	Utilice la tecnología de capa de personalización de usuarios o capa de usuarios de Citrix App Layering.

† En Citrix Virtual Apps and Desktops 7 2003, el controlador de Personal vDisk se eliminó del instalador de VDA. En Citrix Virtual Apps and Desktops 7 2006, el flujo de trabajo del controlador de Personal vDisk se ha quitado de Studio.

Requisitos del sistema

August 17, 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. Los requisitos del sistema para aquellos componentes que no se incluyen aquí (por ejemplo, sistemas host, la aplicación Citrix Workspace y Citrix Provisioning) se describen en su documentación respectiva.

Consulte Antes de la instalación para prepararse.

A menos que se indique, 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 y StoreFront en un servidor, solo para un entorno de evaluación, no una implementación de producción.	5 GB de RAM
Todos los componentes principales y StoreFront en un servidor, para una implementación de prueba o un entorno de producción pequeño.	12 GB de RAM

Componente	Mínimo
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 Guía de tamaño.
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 documentación de StoreFront para conocer las recomendaciones de disco.
Servidor de licencias	8 GB de RAM; consulte la documentación sobre licencias 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 La excepción es la memoria RAM. Se necesita más RAM para aplicaciones que consuman más.

Para obtener más información:

- Citrix Tech Zone contiene directrices sobre el tamaño.
- La escalabilidad de un solo servidor para Citrix Virtual Apps and Desktops analiza cuántos usuarios o máquinas virtuales puede contener un único host físico.

Microsoft Visual C++

Al instalar un Delivery Controller, Virtual Delivery Agent (VDA) o Universal Print Server, el instalador de Citrix instala automáticamente Microsoft Visual C++ 2015–2022 Redistributable.

- Si la máquina contiene una versión anterior de runtime (por ejemplo, 2015-2019), el instalador de Citrix la actualiza.
- Si la máquina contiene una versión anterior a 2015, Citrix instala la versión más reciente en paralelo.

Delivery Controller

Sistemas operativos compatibles:

- Windows Server Core 2022
- Windows Server 2022
- Windows Server 2019, ediciones Standard y Datacenter, y con la opción Server Core

Requisitos:

- Microsoft .NET Framework 4.8 (o una versión posterior) se instala automáticamente si no está instalado.
- Windows PowerShell 3.0, 4.0 o 5.0.
- Microsoft Visual C++ 2015–2022 Redistributable.

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 2022, ediciones Express, Standard y Enterprise.
- 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 SP2, ediciones Express, Standard y Enterprise.

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.

Consideraciones sobre Caché de host local: 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.

- Al instalar un Controller, Microsoft SQL Server Express LocalDB 2019 con Cumulative Update 15 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 automáticamente. Para obtener información sobre los requisitos y los procedimientos de sustitución, consulte Reemplazar SQL Server Express LocalDB.

Más información sobre las bases de datos:

- Bases de datos
- En CTX114501 se indican las bases de datos compatibles más recientes
- Guía sobre tamaños de bases de datos
- Caché de host local

Web Studio

> **Nota:**
>
> - Puede administrar la implementación de Citrix Virtual Apps and Desktops mediante dos consolas de administración: Web Studio (basada en la web) y Citrix Studio (basada en Windows). Este artículo se refiere únicamente a Web Studio. Para obtener información sobre Citrix Studio, consulte el artículo equivalente en Citrix Virtual Apps and Desktops 7 2212 o versiones anteriores.
> - Web Studio es una consola web de administración que le permite configurar y administrar su implementación local de Citrix Virtual Apps and Desktops. Está diseñada para mejorar la experiencia de usuario y, por lo general, responde más rápido que Citrix Studio, la consola de administración basada en Windows. Consulte Instalar Web Studio.

Sistemas operativos compatibles:

- Windows Server Core 2022
- Windows Server 2022
- Windows Server 2019, ediciones Standard y Datacenter, y con la opción Server Core

Citrix Director

Sistemas operativos compatibles:

- Windows Server Core 2022
- Windows Server 2022
- Windows Server 2019, ediciones Standard y Datacenter, y con la opción Server Core

Requisitos:

- Microsoft .NET Framework 4.8 (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. A continuación, ese software se instalará.
- Para ver los registros de eventos en máquinas en las que está instalado Citrix Director, debe instalar Microsoft .NET Framework 2.0.

Citrix Profile Management:

- Asegúrese de que Citrix Profile Management y Plug-in WMI de Citrix Profile Management estén instalados en el VDA (página **Componentes adicionales** del asistente de instalación) y de que Citrix Profile Management Service se esté ejecutando para ver los detalles del perfil de usuario en Director.

Requisitos de integración de System Center Operations Manager (SCOM):

- System Center 2012 R2 Operations Manager

Exploradores compatibles para ver Director:

- Internet Explorer 11 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 resolución de pantalla recomendada para ver Director es de 1440 x 1024.

Virtual Delivery Agent (VDA) para SO de sesión única

Sistemas operativos compatibles:

- Windows 11
- Windows 10 (solo x64), cualquier versión actualmente con soporte estándar.

  - Para obtener información sobre las ediciones admitidas, consulte el artículo CTX224843 de Knowledge Center.

Requisitos:

- Microsoft .NET Framework 4.8 (o una versión posterior) se instala automáticamente si no está instalado.
- Microsoft Visual C++ 2015–2022 Redistributable.

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 11 y 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, las funciones de aceleración multimedia no se instalan y no funcionan. 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 Windows en una máquina Windows Server compatible. 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 11 (compatible solo con Citrix DaaS)
- Windows 10 (únicamente x64; solo compatible con Citrix DaaS), cualquier versión que siga en desarrollo estándar.
- Windows Server 2022
- Windows Server 2019, ediciones Standard y Datacenter

El instalador implementa automáticamente estos requisitos, que también están disponibles en las carpetas **Support** de los medios de instalación de Citrix:

- Microsoft .NET Framework 4.8 (o una versión posterior) se instala automáticamente si no está instalado.
- Microsoft Visual C++ 2015–2022 Redistributable.

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 instalan 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 una máquina con Windows Server 2008 R2, 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.

Puede que algunas funciones no se admitan en todas las plataformas de host ni todas las versiones de plataforma. 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.

Hipervisores compatibles:

- **XenServer (anteriormente Citrix Hypervisor)**

CTX131239 contiene información sobre la versión actual, además de enlaces a los problemas conocidos.

Para obtener más información, consulte Entornos de virtualización de XenServer.

- **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.

Hosts de nube pública compatibles:

- **Amazon Web Services (AWS)**

  Para obtener información sobre el uso de AWS para aprovisionar máquinas virtuales, consulte Entornos de virtualización de Amazon Web Services.

- **Google Cloud Platform**
  Para obtener más información, consulte Entornos de virtualización de Google Cloud Platform y Getting Started with Citrix DaaS on Google Cloud.

- **Microsoft Azure Resource Manager**

  Para obtener información sobre cómo usar Microsoft Azure Resource Manager para aprovisionar máquinas virtuales, consulte Entornos de virtualización de Microsoft Azure Resource Manager.

- **Soluciones de Nutanix Cloud y de partners**

  Para obtener información sobre el uso de las soluciones de Nutanix Cloud y de partners, consulte Soluciones de Nutanix Cloud y de partners.

- **Soluciones de VMware Cloud y de partners**

  Para obtener información sobre el uso de las soluciones de VMware Cloud y de partners, consulte Soluciones de VMware Cloud y de partners.

Al agregar conexiones de host de nube pública a una implementación, tenga en cuenta lo siguiente:

- Necesita una licencia de derechos híbridos. Para obtener información sobre la licencia de derechos híbridos, consulte Transición e intercambios (TTU) con derechos híbridos. Para obtener información sobre cómo agregar una licencia, consulte Crear un sitio.
- Las fuentes de información le dirigen a la documentación de Citrix DaaS. Si está familiarizado con los hosts de nube pública en el producto Citrix DaaS, la versión local tiene algunas diferencias.
  - En Citrix DaaS, la interfaz de administración se conoce como Configuración completa. En Citrix Virtual Apps and Desktops local, la interfaz de administración se conoce como Web Studio.
  - En Citrix DaaS, las actualizaciones se implementan cada cuatro semanas aproximadamente. Por lo tanto, es posible que ciertas funciones disponibles con Citrix DaaS no estén disponibles en la versión local.

Niveles funcionales de Active Directory

Se admiten los siguientes niveles funcionales de bosque y dominio de Active Directory:

- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008

HDX

Audio

Se admite el audio UDP para ICA de multisecuencia 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:
  - XenServer
  - Nutanix AHV
  - VMware vSphere y VMware ESX, donde se le denomina aceleración de gráficos directa virtual (virtual Direct Graphics Acceleration, vDGA)
- vGPU está disponible con:
  - XenServer
  - Nutanix AHV
  - VMware vSphere

Consulte https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/graphics/hdx-3d-pro.

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 aceleración de gráficos virtualizados con la API NVIDIA GRID, puede usar HDX 3D Pro con todas las GPU NVIDIA GRID compatibles con la versión 13 y posteriores del software NVIDIA Virtual GPU (vGPU), consulte https://docs.nvidia.com/grid/index.html.

Para obtener una lista detallada de los hipervisores y el hardware compatibles, consulte la documentación del software de vGPU de NVIDIA.

- La aceleración de gráficos virtualizados se admite en la familia de procesadores Intel Xeon E3 de las plataformas de gráficos para el centro de datos y la serie GPU Flex para centro de datos de Intel. Para obtener más información, consulte la serie GPU Flex.
- Las GPU AMD son compatibles con la virtualización mxGPU de AMD. Para obtener más información sobre el hardware compatible, consulte la documentación de AMD.

Dispositivo del usuario:

- Citrix ofrece compatibilidad para hasta 8 monitores de 4K, según los recursos de hardware. En función de la GPU usada, este máximo puede estar sujeto a otras restricciones de hardware.
- Citrix también recomienda que la especificación de los dispositivos de usuario tenga, como mínimo, 4 GB de RAM y una CPU con una velocidad de reloj de 1,6 GHz o más. Para alcanzar un rendimiento óptimo, recomendamos que los dispositivos de usuario tengan 8 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.
- La aplicación Citrix Workspace debe estar instalada.

Para obtener más información, consulte los artículos de HDX 3D Pro y 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 2022
- Windows Server 2019

Requisitos:

- Microsoft Visual C++ 2015–2022 Redistributable
- Microsoft .NET Framework 4.8 (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 admiten Citrix License Server 11.17.2 y versiones posteriores. Para obtener más información, consulte Licencias.

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 Acceso a aplicaciones locales para obtener información acerca del explorador admitido para esa funcionalidad.

Esta versión de Citrix Virtual Apps and Desktops requiere, como mínimo, HDX RealTime Connector 2.9 LTSR. Para obtener más información, consulte la documentación de HDX RealTime Optimization Pack.

Este producto es compatible con las versiones 3 a 5 de PowerShell.

Información técnica general

August 17, 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.

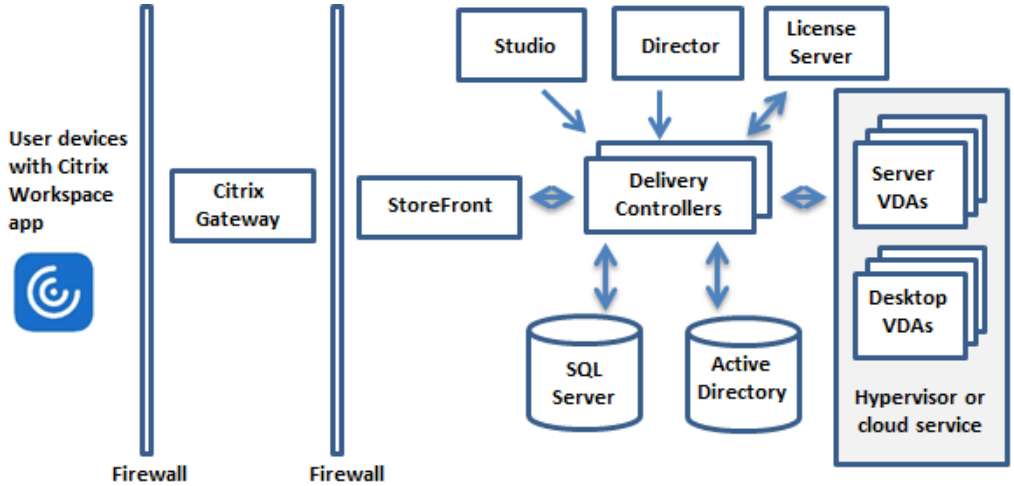
Citrix Virtual Apps and Desktops comparten una arquitectura unificada llamada FlexCast Management Architecture (FMA). Las funciones principales de la arquitectura FMA son el aprovisionamiento integrado y la capacidad de ejecutar distintas versiones de Citrix Virtual Apps o Citrix Virtual Desktops desde 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.

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 disponibilidad del sitio, conviene instalar Controllers en más de un servidor. Si la implementación incluye un hipervisor u otro servicio, los servicios del Controller se comunican con este para:

- Distribuir aplicaciones y escritorios
- Autenticar y administrar el acceso de los usuarios
- Intervenir como intermediario en conexiones entre los usuarios y sus aplicaciones o escritorios
- Optimizar conexiones de usuario
- Equilibrar la carga de las conexiones

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.

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 intermediario aloja varios plug-ins 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.

Studio

Puede administrar la implementación de Citrix Virtual Apps and Desktops mediante dos consolas de administración: Web Studio (basada en la web) y Citrix Studio (basada en Windows). La documentación de este producto solo cubre Web Studio. Para obtener información sobre Citrix Studio, consulte Citrix Virtual Apps and Desktops 7 2212 o versiones anteriores.

Web Studio Web Studio es una consola web de administración que le permite configurar y administrar su implementación local de Citrix Virtual Apps and Desktops. Está diseñada para mejorar la

experiencia de usuario y, por lo general, responde más rápido que Citrix Studio, la consola de administración basada en Windows. Consulte Instalar Web Studio.

Citrix Studio Citrix Studio es la consola de administración desde la que configurar y administrar la implementación de Citrix Virtual Apps and Desktops. Citrix Studio elimina la necesidad de consolas de administración independientes para administrar la entrega de aplicaciones y escritorios. Citrix 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 Citrix Studio se obtiene del Broker Service que hay en el Controller; se comunica a través del puerto TCP 80.

Secure Private Access

La solución local Citrix Secure Private Access mejora la postura general de seguridad y cumplimiento de una organización al ofrecer fácilmente acceso de red Zero Trust a las aplicaciones basadas en explorador (aplicaciones web y SaaS internas) mediante StoreFront como portal de acceso unificado a las aplicaciones web y SaaS, junto con aplicaciones y escritorios virtuales como parte integrada de Citrix Workspace. La solución es compatible con las versiones existentes de NetScaler y StoreFront sin necesidad de hacer ningún cambio en las versiones. Para obtener más información, consulte Secure Private Access para instalaciones locales.

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 u otro servicio

El hipervisor u otro servicio 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 otros servicios.

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.

Componentes adicionales

Los siguientes componentes 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. PVS 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

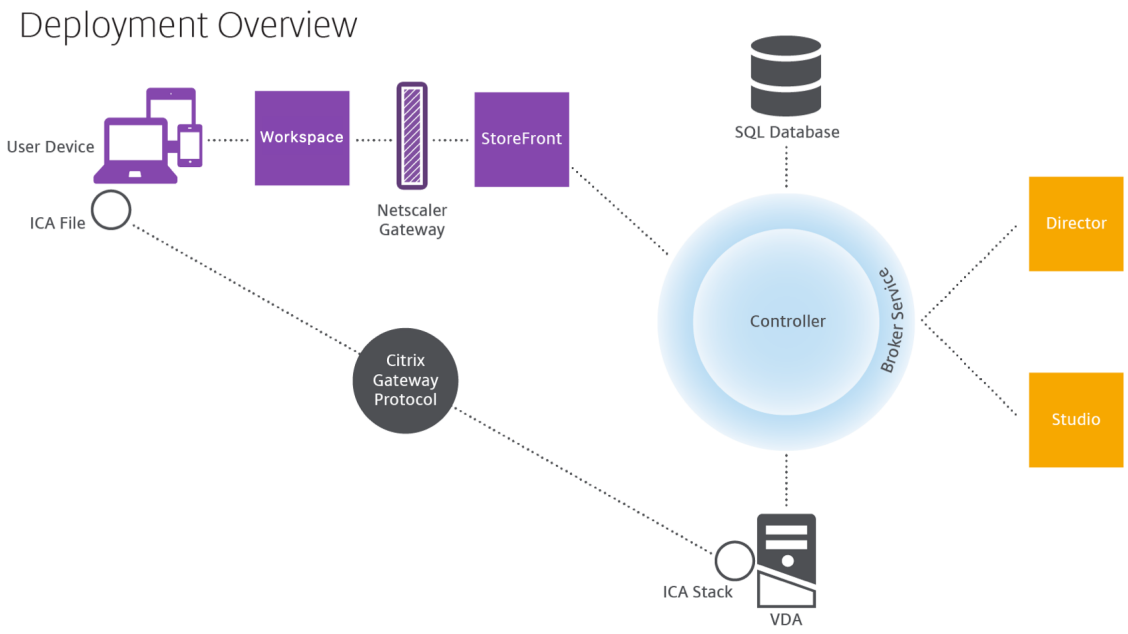
Cuando los usuarios se conectan desde fuera del firewall de la empresa, Citrix Virtual Apps and Desktops pueden usar la tecnología de Citrix Gateway (antes llamado Access Gateway y NetScaler Gateway) para proteger esas conexiones con TLS. El dispositivo virtual Citrix Gateway o VPX es un dispositivo 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 las redes WAN. 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 desduplicación 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 virtuales, 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, coloque todos los Controllers en la misma red LAN si fuera posible.

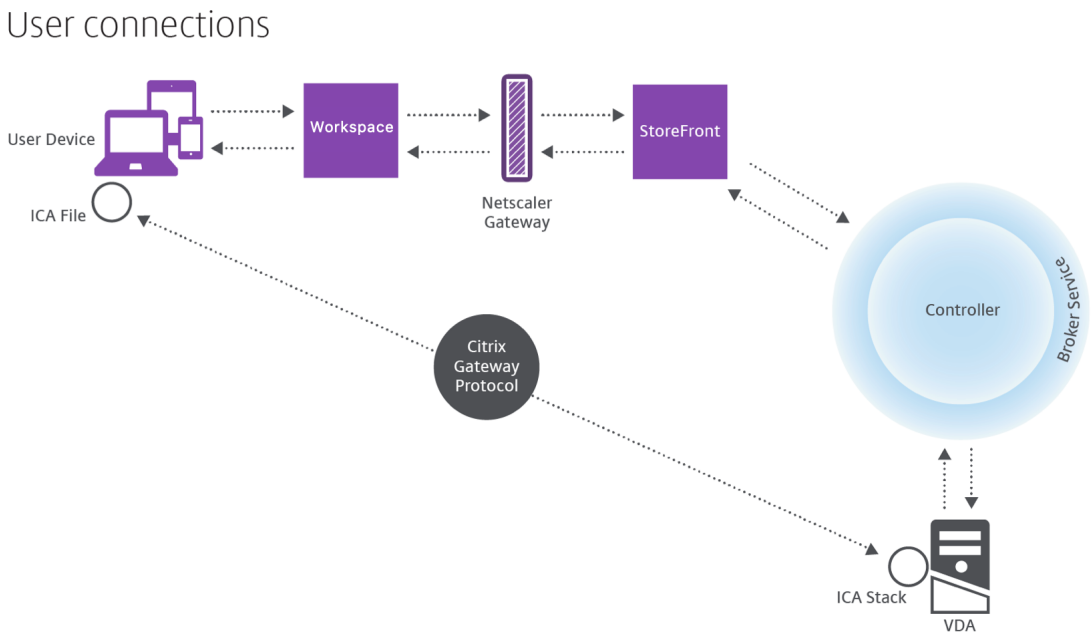
Los usuarios nunca acceden directamente al Controller. El VDA funciona como intermediario entre los usuarios y el Controller. Cuando los usuarios inician sesión mediante StoreFront, sus credenciales pasan al servicio Broker Service presente en el Controller. A continuación, el Broker Service obtiene 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.



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.

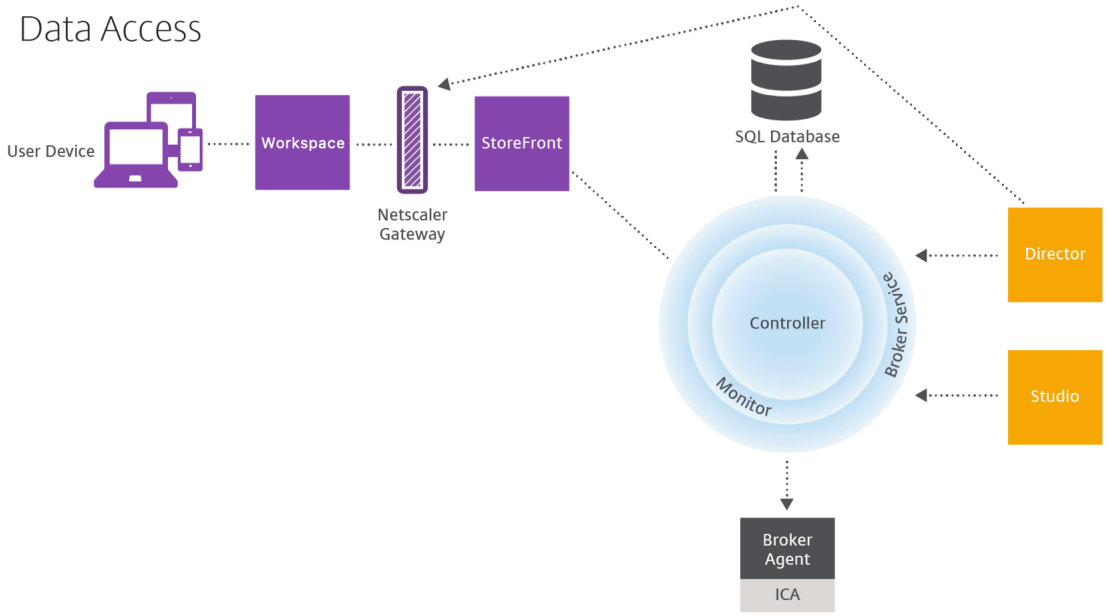
El archivo ICA se copia al dispositivo del usuario y establece una conexión directa entre el dispositivo y la pila ICA que se ejecuta en el VDA. Esta conexión omite la infraestructura de administración (aplicación Citrix Workspace, StoreFront y Controller).

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 servicio Broker. Por lo que accede solo a los datos en tiempo real. Director se comunica con el Broker Service (a través de un plug-in 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 entregan 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 escritorios y en qué máquinas pueden hacerlo. 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 distribuirlas 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 más máquinas. 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
- Puertos de red
- Bases de datos
- Hipervisores y otros servicios compatibles

Bases de datos

August 17, 2024

> **Nota:**
>
> Puede administrar la implementación de Citrix Virtual Apps and Desktops mediante dos consolas de administración: Web Studio (basada en la web) y Citrix Studio (basada en Windows). Este artículo se refiere únicamente a Web Studio. Para obtener información sobre Citrix Studio, consulte el artículo equivalente en Citrix Virtual Apps and Desktops 7 2212 o versiones anteriores.

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.
- **Registros:** También conocida como Registro de configuración, 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 lo siguiente respecto a las bases de datos:

- **Realice copias de reserva con regularidad.** Haga una copia de reserva 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 más información, consulte CTX135207; sin embargo, tenga en cuenta que hace referencia a CitrixXenDesktopDB, que ya no se desarrolla ni está disponible para los clientes.
- **Realice copias de reserva y restaure las bases de datos de SQL Server del sitio, de supervisión y de registros con regularidad.** Para obtener información específica sobre las bases de datos de SQL Server, consulte Creating Full and Differential Backups of a SQL Server Database.

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 Clústeres de conmutación por error de Windows Server con SQL Server.
- **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. Este método es más costoso que las otras dos soluciones debido a que se requieren licencias de SQL Server completas en cada servidor de la base de datos. No se puede usar la edición 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 disponibilidad 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 para alta disponibilidad de SQL Server. La Caché de host local permite a los usuarios conectarse y reconectarse con las aplicaciones y los escritorios 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 a sus escritorios y aplicaciones y utilizándolos. 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 las raras ocasiones en que falle la comunicación con todos los Controllers. La función 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. Normalmente, 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 Web 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, para la mayoría de las implementaciones de producción y cualquier implementación que use funciones de alta disponibilidad de Microsoft, se recomienda utilizar solo ediciones de SQL Server admitidas (que no sean Express). Instale SQL Server en equipos distintos del servidor donde está instalado el primer Controller. En 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 Web Studio y administrador de 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, Web 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 dispone de los derechos necesarios para las bases de datos, solicite ayuda a alguien que los tenga, como un administrador de bases de datos. Aquí se presenta el orden de pasos a seguir:

1. En la página **Bases de datos** del asistente para la creación de sitios, seleccione la opción **Generar scripts para configurar bases de datos manualmente**. Esta acción genera los siguientes tres tipos de scripts para cada una de las siguientes bases de datos principales y de réplica: bases de datos de sitios, supervisión y registros.

    - *Script que contiene "SysAdmin" en el nombre*. Un script que crea las bases de datos y las credenciales de Delivery Controller. Estas tareas requieren derechos de tipo "securityadmin".
    - *Script que contiene "DbOwner" en el nombre*. 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`.
    - *Script que contiene "Mixed" en el nombre*. Todas las tareas en un script, independientemente de los derechos necesarios.

    Puede indicar dónde almacenar los scripts.

    > **Nota:**
    >
    > En entornos empresariales, la configuración de la base de datos incluye scripts que pueden gestionar diferentes equipos de personas con diferentes roles (derechos): `securityadmin` o `db_owner`. Si corresponde, primero tiene scripts de tipo "SysAdmin" ejecutados por administradores con el rol `securityadmin` y, a continuación, scripts "DbOwner" ejecutados por administradores con derechos de tipo `db_owner`

> . Para generar esos scripts, también puede utilizar PowerShell. Para obtener más información, consulte Scripts de derechos preferidos sobre bases de datos.

2. Facilite esos scripts al administrador de base de datos. El asistente para la creación de sitios se detiene automáticamente en este punto. Cuando regrese más tarde, se le pedirá que continúe la creación del sitio.

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`. Se 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 procede.
- 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. A continuación, restaure el archivo de copia de seguridad en el servidor reflejado. Por último, inicie la creación de reflejo en el servidor principal.

El Administrador de base de datos utiliza la línea de comandos de SQLCMD o SQL Server Management Studio en modo SQLCMD para:

- Ejecutar cada uno de los scripts de `xxx_Replica.sql` en las instancias de base de datos de alta disponibilidad de SQL Server (si está configurada la opción de alta disponibilidad)
- Ejecutar cada uno de los scripts de `xxx\\_Principal.sql` en las instancias de base de datos principales 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.

Web Studio le preguntará si quiere continuar con la creación del sitio. Volverá a aparecer 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 Web 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 técnicamente sea más restrictivo, en la práctica, puede tratar el rol `securityadmin` de servidor como equivalente al rol `sysadmin` de servidor.

** Cuando se quita un Controller de un sitio, no se quita el inicio de sesión del Controller en el servidor de la base de datos. De esta forma, se evita el riesgo potencial de quitar un inicio de sesión que utilizan otros servicios en la misma máquina. Si ya no es necesario, el inicio de sesión debe quitarse manualmente. Esta acción requiere la pertenencia a un rol `securityadmin` de servidor.

Cuando utilice Web Studio para realizar estas operaciones, el usuario de Web Studio debe tener una cuenta de servidor de base de datos que sea explícitamente miembro de los roles de servidor adecuados, o bien, debe poder proporcionar credenciales de una cuenta que lo sea.

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, puede especificar los derechos preferidos sobre bases de datos. Si se especifica un valor no predeterminado, se crearán scripts independientes. Un script contiene tareas que requieren el rol `securityadmin`. El otro script requiere solamente los derechos de tipo `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. Inicie sesión en Web Studio y, a continuación, seleccione **Parámetros** en el panel de la izquierda.
3. Busque el mosaico de **Base de datos** y seleccione **Modificar**.
4. En la página **Administrar base de datos**, seleccione la base de datos para la que quiere especificar una nueva ubicación y, a continuación, seleccione **Cambiar base de datos** en la barra de acciones.
5. Especifique la nueva ubicación y el nombre de la base de datos.
6. Si quiere que Web Studio cree la base de datos y si tiene los permisos adecuados, haga clic en **Listo**. Cuando se le solicite, haga clic en **Listo** y Web Studio creará automáticamente la base de datos. Web 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. Web 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.
7. Si no quiere que Web Studio cree la base de datos o no dispone de los permisos necesarios, haga clic en **Generar script de base de datos**. 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.
- Establecer el 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

August 17, 2024

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 información detallada, consulte Implementar y entregar aplicaciones de 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 información detallada, 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.

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 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.

Acceso con Remote PC

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.

Para obtener más información, consulte Acceso con Remote PC.

Puertos de red

August 17, 2024

Se ofrece información completa sobre los puertos de red en Communication Ports Used by Citrix Technologies.

Cuando se instalan los componentes de Citrix, el firewall host del sistema operativo también se actualiza, de manera predeterminada, para coincidir con los puertos de red predeterminados.

Es posible que necesite información sobre los puertos:

- Para el cumplimiento de normativas.
- Si hay un firewall de red entre los componentes de Citrix Virtual Apps and Desktops y otros productos o componentes de Citrix, para poder configurar el firewall como es debido.
- 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 funciones de los componentes para que utilicen otro puerto o intervalo de puertos y, luego, quiere inhabilitar o bloquear puertos no utilizados en su configuración.

Algunos de los 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.

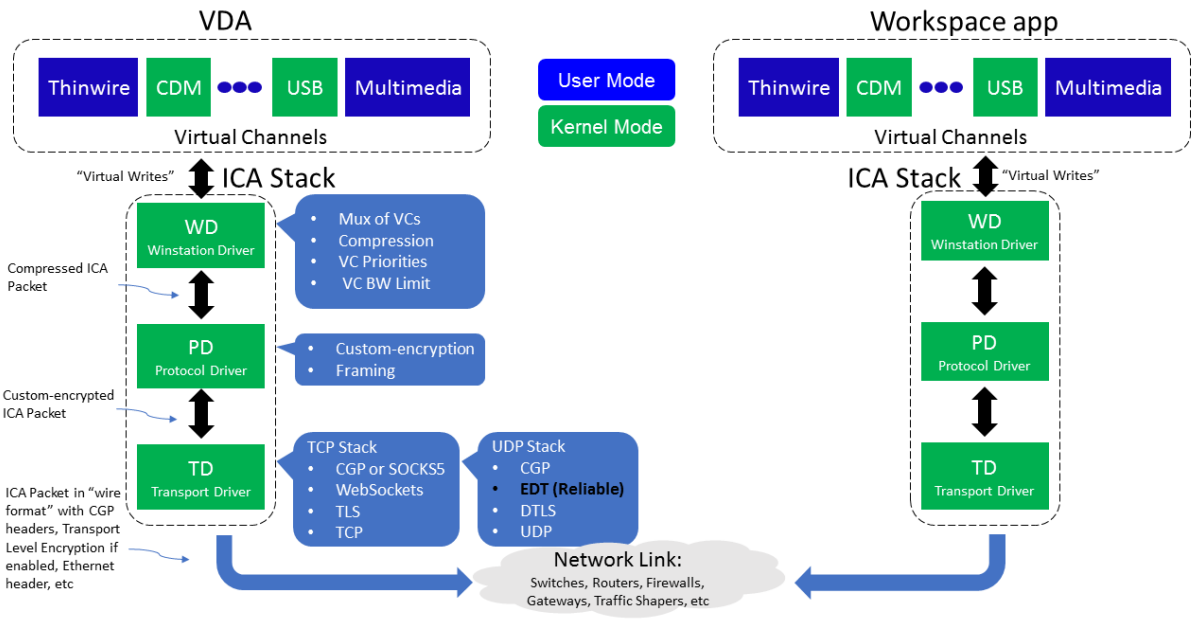
Además, los sistemas operativos del VDA y Delivery Controller requieren puertos entrantes para su propio uso. Para obtener información más detallada, consulte la documentación de Microsoft Windows.

HDX

August 17, 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 usa 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.

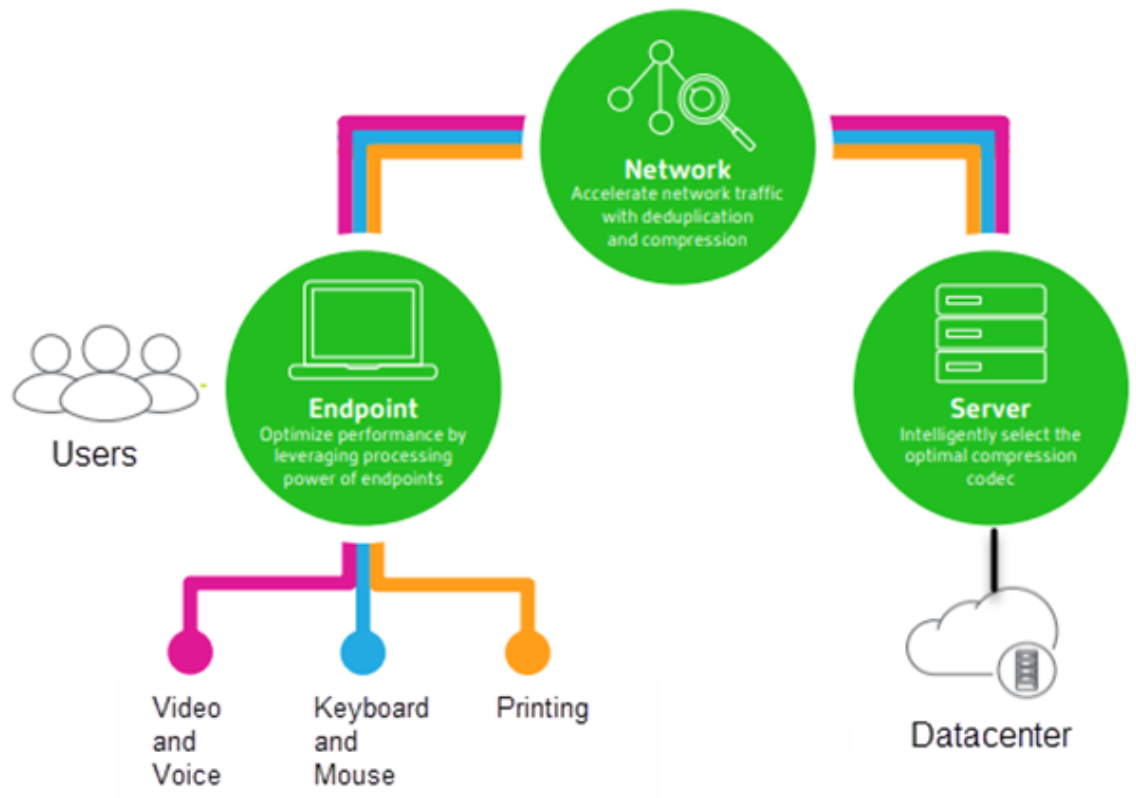


El diseño de HDX responde a tres principios técnicos:

- 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 fluida 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 información 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.

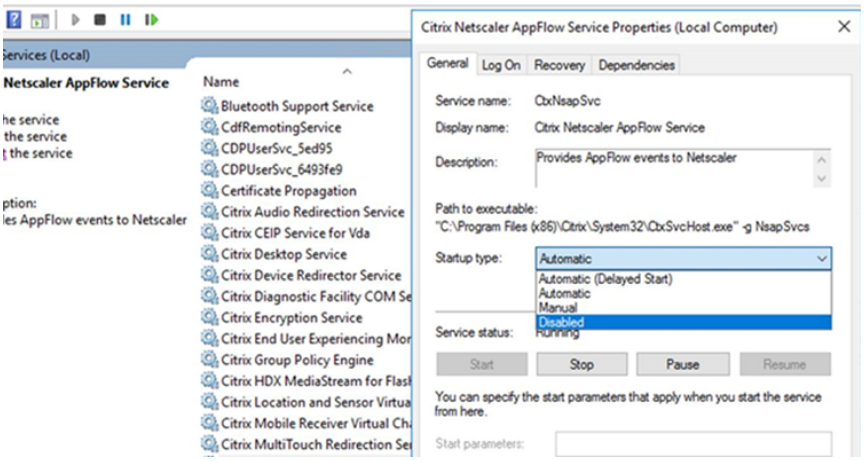
Puede habilitar NetScaler para usar el canal virtual HDX Insight y mover todos los puntos de datos requeridos en un formato sin comprimir. Si inhabilita esta función, el dispositivo NetScaler descifrará y descomprimirá el tráfico ICA que haya en varios canales virtuales. Usar el canal virtual único disminuye la complejidad, mejora la escalabilidad y es más rentable.

Requisitos mínimos:

- 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 di-

rectivas 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 usa 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 trascurrido 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 Multisecuencia 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.

> **Nota:**
>
> El parámetro de **Límite de memoria de presentación** se retiró. Con este cambio, Citrix ya no limita la memoria de presentación. En su lugar, se asigna la cantidad mínima de memoria requerida para garantizar que el diseño de presentación del cliente se adapte por completo.

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 Micró-

fono 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

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 multisecuencia 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 multisecuencia. Dentro de una red interna de la empresa, no se

> admiten las conexiones multisecuencia con TLS.

Para establecer la calidad de servicio en conexiones de multisecuencia, agregue las siguientes configuraciones de directiva Citrix (consulte Configuraciones de directiva de Conexiones de multisecuencia 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 multisecuencia: Esta configuración está inhabilitada de forma predeterminada. Si usa Citrix NetScaler SD-WAN con la funcionalidad de multisecuencia en el entorno, no es necesario definir esta configuración. Defina esta configuración de directiva cuando esté utilizando enrutadores externos o versiones antiguas de NetScaler SD-WAN para conseguir el nivel de Calidad de servicio (QoS) que necesite.
- Configuración de usuario para multisecuencia: 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. Agregue la siguiente clave del Registro:

KEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

Nombre: EnableKlMap

Tipo: DWORD

Valor: 1

Para inhabilitar esta función, establezca **EnableKlMap** en 0 o elimine la clave **CtxKlMap**.

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. Agregue la siguiente clave del Registro:

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

Nombre: DisableWindowHook

Tipo: DWORD

Valor: 1

Para usar la asignación de distribución de teclado Unicode normal, establezca **DisableWindowHook** en 0.

Canales virtuales ICA de Citrix

August 17, 2024

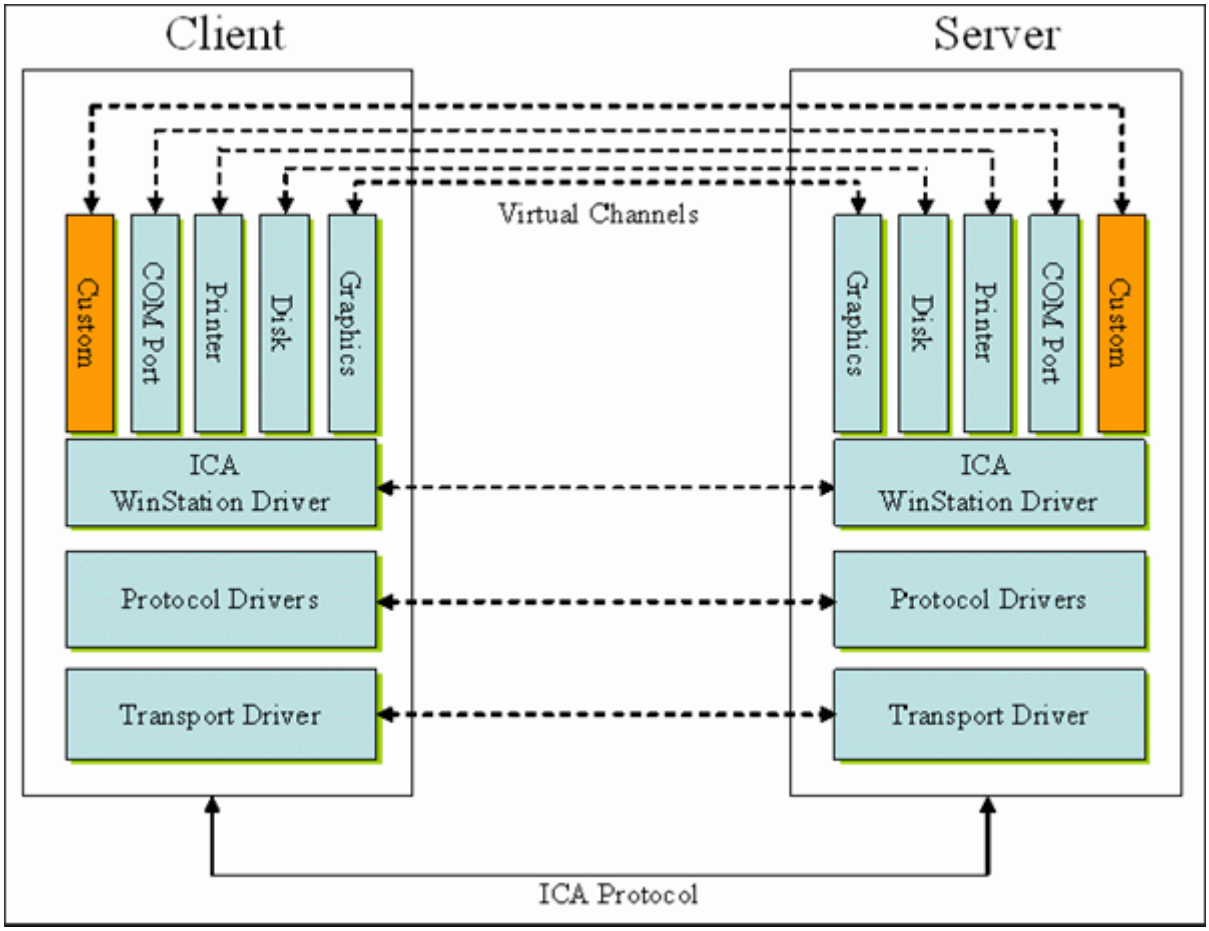
> **Advertencia:**
>
> Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si usa el Editor del 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.

- vdmmn.dll: Compatibilidad multimedia.
- vdmrvc.dll: Canal virtual de Mobile Receiver.
- vdmtchn.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.
- Icausbb.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

`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

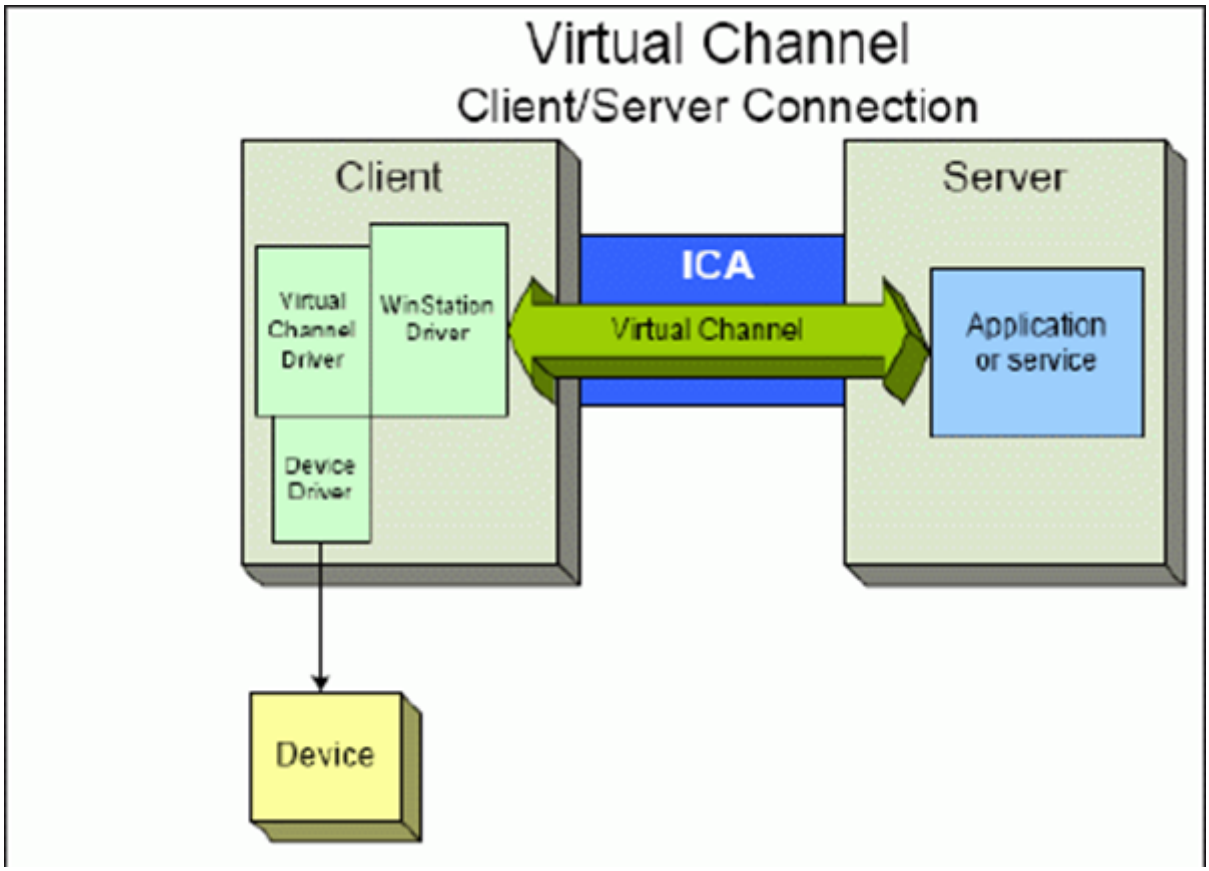
En los servidores de Citrix Virtual Apps and Desktops, varios canales se alojan como servicios de Windows. Este alojamiento ofrece una semántica del tipo “uno a varios”para múltiples aplicaciones en una sesión y múltiples sesiones en el servidor. He aquí algunos ejemplos de tales servicios:

- 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)
- Servicio Citrix ICA Status Channel

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

> **Nota:**
>
> Los SDK de Citrix están disponibles en el portal de Citrix Developer, en https://developer.cloud.com.

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.

> **Nota:**
>
> - 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 para Citrix Virtual Apps and Desktops, debe especificar qué canales virtuales pueden abrirse en una sesión ICA. Para obtener más información, consulte Configuraciones de la directiva Lista de canales virtuales permitidos.

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.

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 **picaPassthruHook**. 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 del 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

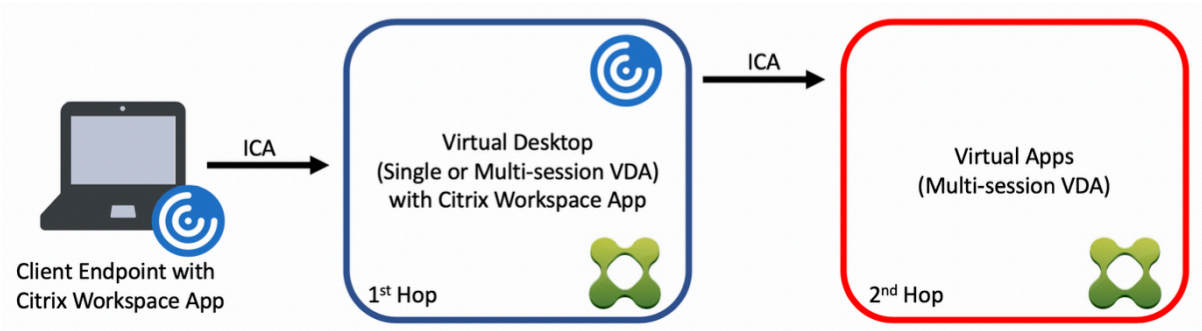
También puede consultar

- 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

August 17, 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

El doble salto está disponible en todas las ediciones de Citrix Virtual Apps and Desktops, incluido Citrix Cloud Services.

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 recodifi-

cación 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 compatible

> **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 del explorador web
- Acceso a aplicaciones locales
- RealTime Optimization Pack para Skype Empresarial
- Optimización para Microsoft Teams

Instalación y configuración

August 17, 2024

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 el Delivery Controller, Web Studio, Citrix Director y Citrix License Server. También puede instalar 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 pedirá 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 sesión única en cada PC de 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 o ESD (Antes de la instalación describe 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.

Creación de 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 u otro servicio 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 Web 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 (opcional)

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.

Limitación conocida

Cuando usa la versión 1912 o anterior de la aplicación Citrix Workspace para Windows, la sesión se interrumpe al cabo de un rato. Este problema se ha solucionado en las versiones LTSR y CR más recientes de la aplicación Citrix Workspace.
Para obtener más información sobre las versiones compatibles, consulte versiones de la aplicación Citrix Workspace para Windows o Citrix Receiver para Windows Long Term Service Release.

Identidades de las máquinas

August 17, 2024

Cada máquina debe tener una identidad de máquina única, también conocida como cuenta de equipo. Las identidades de máquina se pueden crear y administrar en las máquinas de forma local o en un directorio, como Active Directory (AD) local o Azure AD. Citrix permite alojar aplicaciones y escritorios virtuales en máquinas que estén unidas a Active Directory, Azure Active Directory, Azure Active Directory híbrido o que no estén unidas a ningún dominio.

Tipos de identidad de máquina

Se admiten estos tipos de identidad de máquina.

Tipo de identidad de máquina	Descripción
Unida a AD	Las identidades se crean y se administran en Active Directory local. Las máquinas aprovisionadas se unen a Active Directory local mediante las identidades de máquina asignadas.
Unida a Azure AD híbrido	Las identidades se crean en Active Directory local y se sincronizan con Azure AD a través de Azure AD Connect. Las máquinas aprovisionadas se unen a Active Directory local. Luego, las máquinas se unen a Azure AD híbrido. Para importar una máquina virtual unida a Azure AD híbrido, Citrix Virtual Apps and Desktops la trata como una máquina virtual unida a Active Directory.

Configuraciones compatibles

A continuación, se muestran los detalles de las configuraciones admitidas para cada caso.

Infraestructura admitida

Identidad de la máquina	Citrix Virtual Apps and Desktops	Citrix Workspace	Citrix StoreFront	Citrix Gateway Service	Citrix Gateway
Unida a AD	Sí	Sí	Sí	Sí	Sí
Unida a Azure AD	No	Sí	No	Sí	No
Unida a Azure AD híbrido	Sí	Sí	Sí	Sí	Sí
No unida a ningún dominio	No	Sí	No	Sí	No

Proveedores de identidades para autenticación en espacios de trabajo admitidos

Identidad de la máquina	Azure Active Directory	Active Directory	Active Directory y token	Okta	SAML	Citrix Gateway	Autenticación adaptable
Unida a AD	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Unida a Azure AD	Sí	No	No	No	No	No	No
Unida a Azure AD híbrido	Sí	Sí	Sí	Sí	Sí	Sí	Sí
No unida a ningún dominio	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Unidos a Azure Active Directory

August 17, 2024

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. Para usar el modelado de directivas, el controlador de dominio debe ejecutarse en todos los sistemas operativos de servidor compatibles. Esto no afecta al nivel funcional del dominio.

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

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. Utilice la siguiente información para agregar la clave del Registro al VDA y a los Delivery Controllers:

> **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 usa 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.

Se ha agregado una entrada del Registro para evitar la habilitación no deseada de la autenticación NTLM en los VDA, que es menos segura que Kerberos. Esta entrada se puede utilizar en lugar de la entrada `SupportMultipleForest`, que se puede seguir utilizando para garantizar la compatibilidad con versiones anteriores.

En el VDA, configure: `HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`.

- Nombre: `SupportMultipleForestDdcLookup`
- Tipo: `REG_DWORD`
- Datos: `0x00000001 (1)`

Esta clave de Registro realiza una búsqueda de DDC en un entorno de confianza bidireccional de varios bosques que le permite quitar la autenticación basada en NTLM durante el proceso de registro inicial.

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 `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.

Unidos a Azure Active Directory híbrido

August 17, 2024

> **Nota:**
>
> Desde julio de 2023, Microsoft cambió el nombre de Azure Active Directory (Azure AD) a Microsoft Entra ID. En este documento, cualquier referencia a Azure Active Directory, Azure AD o AAD ahora se refiere a Microsoft Entra ID.

Este artículo describe los requisitos para crear catálogos unidos de Azure Active Directory híbrido (HAAD) mediante Citrix DaaS, además de los requisitos descritos en la sección de requisitos del sistema de Citrix DaaS.

Las máquinas unidas a Azure AD híbrido utilizan AD local como el proveedor de autenticación. Puede asignarlas a usuarios o a grupos de dominio en AD local. Para habilitar la experiencia integrada de SSO para Azure AD, debe tener los usuarios del dominio sincronizados con Azure AD.

> **Nota:**
>
> Las máquinas virtuales unidas a Azure AD híbrido se admiten en infraestructuras de identidades tanto federadas como administradas.

Requisitos

- Tipo de VDA: Sesión única (solo escritorios) o multisesión (aplicaciones y escritorios)
- Versión de VDA: 2212 o posterior
- Tipo de aprovisionamiento: Persistente y No persistente de Machine Creation Services (MCS)
- Tipo de asignación: Dedicada y agrupada
- Plataforma de alojamiento: Cualquier hipervisor o servicio de la nube

Limitaciones

- Si se utiliza Servicio de autenticación federada (FAS) de Citrix, el inicio de sesión único (SSO) se dirige a AD local en lugar de Azure AD. En este caso, se recomienda configurar la autenticación basada en certificados de Azure AD para que el token de actualización principal (PRT) se genere al iniciar sesión el usuario, lo que facilita el inicio Single Sign-On en recursos de Azure AD dentro de la sesión. De lo contrario, el token PRT no estará presente, y el inicio SSO en recursos de Azure AD no funcionará. Para obtener información sobre cómo implementar el inicio de sesión único (SSO) de Azure AD en los VDA unidos de forma híbrida mediante el Servicio de autenticación federada (FAS) de Citrix, consulte VDA unidos de forma híbrida.

- No omita la preparación de imágenes al crear o actualizar catálogos de máquinas. Si quiere omitir la preparación de la imagen, asegúrese de que las máquinas virtuales maestras no estén unidas a Azure AD ni a Azure AD híbrido.

Consideraciones

- La creación de máquinas unidas a Azure Active Directory híbrido requiere el permiso `Write userCertificate` en el dominio de destino. Asegúrese de introducir las credenciales de un administrador con ese permiso durante la creación del catálogo.
- Citrix administra el proceso de unión a Azure AD híbrido. Debe inhabilitar `autoWorkplaceJoin` controlado por Windows en las máquinas virtuales maestras de esta manera. La tarea de inhabilitar manualmente `autoWorkplaceJoin` solo es necesaria para los VDA de la versión 2212 o anterior.

  1. Ejecute `gpedit.msc`.
  2. Vaya a **Configuración del equipo > Plantillas administrativas > Componentes de Windows > Registro de dispositivos**.
  3. **Inhabilite** la opción **Registrar los equipos asociados a un dominio como dispositivos**.

- Seleccione la unidad organizativa (OU) configurada para sincronizarse con Azure AD al crear las identidades de las máquinas.
- Para la VM maestra basada en Windows 11 22H2, cree una tarea programada en la VM maestra que ejecute los siguientes comandos al iniciarse el sistema con la cuenta SYSTEM. Esta actividad de programar una tarea en la VM maestra solo es necesaria para los VDA de la versión 2212 o anterior.

```
$VirtualDesktopKeyPath = 'HKLM:\Software\AzureAD\VirtualDesktop'
$WorkplaceJoinKeyPath = 'HKLM:\SOFTWARE\Policies\Microsoft\
   Windows\WorkplaceJoin'
$MaxCount = 60

for ($count = 1; $count -le $MaxCount; $count++)
{

  if ((Test-Path -Path $VirtualDesktopKeyPath) -eq $true)
  {

    $provider = (Get-Item -Path $VirtualDesktopKeyPath).GetValue(
       "Provider", $null)
    if ($provider -eq 'Citrix')
    {

        break;
     }

```



```
18
19      if ($provider -eq 1)
20      {
21
22          Set-ItemProperty -Path $VirtualDesktopKeyPath -Name "
                Provider" -Value "Citrix" -Force
23          Set-ItemProperty -Path $WorkplaceJoinKeyPath -Name "
                autoWorkplaceJoin" -Value 1 -Force
24          Start-Sleep 5
25          dsregcmd /join
26          break
27       }
28
29     }
30
31
32    Start-Sleep 1
33   }
```

Qué hacer a continuación

Para obtener más información sobre la creación de catálogos unidos a Azure Active Directory híbrido, consulte Crear catálogos unidos a Azure Active Directory híbrido.

Antes de la instalación

August 17, 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 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.

> **Nota:**
>
> Asegúrese de que se cumplen los siguientes requisitos previos de Microsoft en el sistema operativo del servidor y en el sistema operativo de la estación de trabajo:
>
> - Se están ejecutando los servicios **Instantáneas de volumen** y **Proveedor de instantáneas de software de Microsoft**. Para obtener más información, consulte Volume Shadow Copy Service.
> - La versión de **MS-Defender** debe ser posterior a 4.18.2105.5. Para obtener más información, consulte Microsoft Defender Antivirus security intelligence and product updates.

Si su implementación incluye cargas de trabajo de Windows Server, configure un servidor de licencias RDS de Microsoft.

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. Los instaladores independientes de VDA están disponibles en el sitio de descargas de Citrix. 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 que utilicen Machine Creation Services (MCS) y Citrix Provisioning (antes Provisioning Services). Para obtener más información, consulte Instalar agentes VDA mediante scripts.

Información que revisar antes de la instalación

- Descripción técnica: Para familiarizarse con el producto y sus componentes.
- Seguridad: Al planificar el entorno de la implementación.
- Problemas conocidos: Problemas que pueden surgir 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 u otro servicio 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.

- **Conexiones de host de nube pública:** Si tiene una licencia de derechos híbridos, puede crear conexiones de host a la nube pública. Para obtener información relacionada con la licencia de derechos híbridos, consulte Renovaciones de derechos híbridos. Para obtener información relacionada con los derechos de nube pública y los motivos de este cambio, consulte CTX270373.

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.

  Instale Citrix License Server y las licencias antes de instalar otros componentes en otros servidores.
- Para instalar un componente compatible en un Server CoreOS (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.

Asegúrese de que cada sistema operativo tiene las actualizaciones más recientes.

Asegúrese de que todas las máquinas tengan los relojes del sistema sincronizados. La infraestructura Kerberos que protege la comunicación entre las máquinas requiere sincronización.

Con XenServer, es posible que el estado de energía de la máquina virtual aparezca como desconocido, aunque parezca haberse registrado. 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.

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.

Si intenta instalar o actualizar un VDA en un sistema operativo Windows que esta versión del producto no admite, aparecerá un mensaje que le guiará a un artículo en el que se describen las opciones disponibles.

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 un 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. Unido a Active Directory contiene más información.
- 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 Citrix License Server se configura automáticamente como una cuenta de administrador total de Administración delegada.

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 la versión de un Delivery Controller, Studio, el Servidor de licencias o Director de los medios de un 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 Microsoft Print Spooler Service debe estar habilitado. No se puede instalar correctamente un VDA si ese servicio está inhabilitado.
- La mayoría de las ediciones Windows admitidas ya tienen Microsoft Media Foundation instalado. Si la máquina no tiene Media Foundation (como las ediciones N), varias funciones multimedia no se instalan y no funcionarán.

  - Redirección de Windows Media
  - Redirección de vídeo HTML5
  - Redirección de cámaras web de HDX RealTime

  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 la opción `/no_mediafoundation_ack` para aceptar la limitación.
- 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. Para obtener más información, consulte Registro de VDA.

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.

Se produce un reinicio al actualizar un VDA a la versión 7.17 (o una versión posterior compatible). Ese reinicio no se puede evitar.

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.

Al actualizar la versión de un VDA, tiene lugar un reinicio. Ese reinicio no se puede evitar.

Restaurar en caso de error al instalar o actualizar

> **Nota:**
>
> Esta función está disponible para los VDA de sesión única y multisesión.

Si una instalación o actualización de VDA de sesión única falla y está habilitada la funcionalidad "restaurar en caso de error", la máquina vuelve a un punto de restauración establecido anterior al comienzo del proceso de instalación o actualización.

Si una instalación o actualización de VDA multisesión falla y está habilitada la función de restauración en caso de error, la máquina regresa a una copia de seguridad realizada antes del comienzo del proceso de instalación o actualización.

Cuando se inicia una instalación o actualización de VDA de sesión única con esta funcionalidad habilitada, el instalador crea un punto de restauración del sistema anterior al comienzo del proceso de instalación o actualización. Si el proceso de instalación o actualización del VDA falla, la máquina vuelve al estado del punto de restauración. La carpeta `%temp%/Citrix` contiene registros de implementación y otra información acerca de la restauración.

Cuando comienza una instalación o actualización de VDA multisesión con esta función habilitada, el instalador crea una copia de seguridad del servidor antes del comienzo del proceso de instalación o actualización. Si el proceso de instalación o actualización del VDA falla, la máquina regresa al estado de la copia de seguridad. La carpeta `%temp%/Citrix` contiene registros de implementación y otra información acerca de la restauración. El tiempo necesario para crear la copia de seguridad del servidor se basa en el tamaño de la copia de seguridad necesaria y en la cantidad de recursos disponibles para el servidor. La copia de seguridad se almacena en *C:\WindowsImageBackup\servername*.

De forma predeterminada, esta función está inhabilitada.

Si tiene previsto habilitar esta función, compruebe que la restauración del sistema no esté inhabilitada a través de una configuración de objeto de directiva de grupo (`Computer Configuration` > `Administrative Templates` > `System` > `System Restore`).

> **Nota:**
>
> Este parámetro de GPO no se aplica a la restauración de VDA multisesión.

Para habilitar esta función al instalar o actualizar un VDA de sesión única o multisesión:

- Cuando utilice la interfaz gráfica de un instalador de VDA (como **Inicio automático** o el comando `XenDesktopVDASetup.exe` sin ninguna opción de restauración o silenciosa), active la casilla para **habilitar la restauración automática si la actualización falla** en la página **Resumen**.

  Si la instalación o actualización se completa correctamente, el punto de restauración o la copia de seguridad no se utilizan, pero se conservan.

- Ejecute un instalador de VDA con las opciones /`enablerestore` o /`enablerestorecleanup` mediante la línea de comandos.
  - Si utiliza la opción /`enablerestorecleanup` y la instalación o actualización se completa correctamente, el punto de restauración o la copia de seguridad se quitan automáticamente.
  - Si utiliza la opción /`enablerestore` y la instalación o actualización se completa correctamente, el punto de restauración no se utiliza, pero se conserva.

Instaladores

Instalador de producto completo

Con el instalador de producto completo, incluido en la imagen ISO del producto, puede:

- Instalar, actualizar versiones o quitar componentes principales: Delivery Controller, Studio, Director y el Servidor de licencias.
- Instalar o actualizar la versión de StoreFront.
- Instalar o actualizar la versión de agentes Windows VDA para sistemas operativos de sesión única o multisesión.
- Instalar el componente `UpsServer` de Universal Print Server en los servidores de impresión.
- Instalar el Servicio de autenticación federada.
- Instalar Grabación de sesiones.
- Instalar Workspace Environment Management

  > **Nota:**
  >
  > El instalador del agente de Workspace Environment Management no está traducido. Solo está disponible en inglés.

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. (No están disponibles en los medios de instalación del producto). 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 autoextraíbles que contiene el paquete independiente de VDA se extraen a 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.

VDAServerSetup.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.

VDAWorkstationSetup.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.

VDAWorkstationCoreSetup.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. 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 `VDAWorkstationSetup.exe`.

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.
- Citrix Supportability Tools.
- Citrix Files para Windows.
- Citrix Files para Outlook.

Este instalador `VDAWorkstationCoreSetup.exe` no instala ni contiene ninguna aplicación Citrix Workspace para Windows.

Utilizar `VDAWorkstationCoreSetup.exe` equivale a usar el instalador `VDAWorkstationSetup` 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` además de la opción /`exclude` que enumera todos los nombres de componentes adicionales válidos.

Puede instalar los componentes y las funciones omitidas más adelante. Para ello, vuelva a ejecutar el instalador del producto. Esta acción le permite instalar todos los componentes que faltan.

El instalador `VDAWorkstationCoreSetup.exe` instala automáticamente el MSI de redirección de contenido del explorador. Esta instalación automática es aplicable a la versión 2003 y versiones posteriores compatibles de VDA.

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 = BadCommandLineArgument
- 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 RDS 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.

Configurar un servidor de licencias RDS de Microsoft para cargas de trabajo de Windows Server

Este producto accede a las funciones de sesión remota de Windows Server al entregar una carga de trabajo de Windows Server, como Windows 2016. Normalmente, esto requiere una licencia de acceso de cliente de Servicios de Escritorio remoto (CAL de RDS). El VDA debe poder comunicarse con un servidor de licencias RDS para solicitar licencias CAL de RDS. Instale y active el servidor de licencias. Para obtener más información, consulte el documento Activate the Remote Desktop Services License Server de Microsoft. Para entornos de prueba de concepto, puede utilizar el período de gracia que ofrece Microsoft.

Con este método, puede hacer que este servicio aplique los parámetros del servidor de licencias. Puede configurar el servidor de licencias y el modo por usuario en la consola RDS de la imagen. También puede configurar el servidor de licencias mediante la configuración de directivas de grupo de Microsoft. Para obtener más información, consulte el documento License your RDS deployment with client access licenses (CALs) de Microsoft.

Para configurar el servidor de licencias RDS mediante configuraciones de la directiva de grupo:

1. Instale un servidor de licencias de Servicios de Escritorio remoto en una de las máquinas disponibles. La máquina debe estar siempre disponible. Las cargas de trabajo del producto Citrix deben poder establecer conexión con este servidor de licencias.
2. Especifique la dirección del servidor de licencias y el modo de licencia por usuario mediante la directiva de grupo de Microsoft. Para obtener más detalles, consulte el documento Specify the Remote Desktop Licensing Mode for an RD Session Host Server de Microsoft.

Las cargas de trabajo de Windows 10 requieren la activación de la licencia correcta de Windows 10. Se recomienda seguir la documentación de Microsoft para activar las cargas de trabajo de Windows 10.

Más información

Para configurar una ubicación de recursos para tipos de host específicos:

- Entornos en la nube de AWS
- Entornos de virtualización de XenServer

- Entornos de Google Cloud
- Entornos en la nube de Microsoft Azure Resource Manager
- Entornos de Microsoft System Center Configuration Manager
- Entornos de virtualización de Microsoft System Center Virtual Machine Manager
- Entornos de virtualización de Nutanix
- Soluciones de Nutanix Cloud y de partners
- Entornos de virtualización de VMware
- Soluciones de VMware Cloud y de partners

Entornos en la nube de AWS

August 17, 2024

En este artículo se describe cómo configurar su cuenta de AWS en calidad de ubicación de recursos que pueda utilizar con Citrix Virtual Apps and Desktops. La ubicación de recursos contiene un conjunto básico de componentes; es ideal para una prueba de concepto u otra implementación que no requiera recursos repartidos por varias zonas de disponibilidad. Después de completar estas tareas, puede instalar agentes VDA, aprovisionar máquinas, crear catálogos de máquinas y crear grupos de entrega.

Tras completarse las tareas indicadas en este artículo, la ubicación de recursos contendrá los siguientes componentes:

- Una nube privada virtual (VPC) con subredes públicas y privadas dentro de una única zona de disponibilidad.
- Una instancia que se ejecuta como un controlador de dominio de Active Directory y un servidor DNS, ubicados en la subred privada de la nube VPC.
- Una instancia que actúa como host bastión en la subred pública de la nube VPC. Esta instancia se utiliza para iniciar conexiones RDP a las instancias en la subred privada durante las tareas de administración. Después de finalizar la configuración de la ubicación de recursos, puede apagar esta instancia (para que no se pueda acceder fácilmente a ella). Cuando necesite administrar otras instancias en la subred privada, como instancias VDA, puede reiniciar la instancia del host bastión.

Descripción general de tareas

Configurar una nube privada virtual (VPC) con subredes públicas y privadas. Una vez completada esta tarea, AWS implementa una puerta de enlace NAT con una dirección IP elástica en la subred

pública. Esta acción permite que las instancias de la subred privada accedan a Internet. Las instancias en la subred pública están accesibles para el tráfico público entrante, mientras que las instancias en la subred privada no lo están.

Configurar grupos de seguridad. Los grupos de seguridad actúan como firewalls virtuales que controlan el tráfico de las instancias en su nube VPC. Debe agregar reglas a los grupos de seguridad que permitan que las instancias en la subred pública se comuniquen con instancias en la subred privada. También puede asociar estos grupos de seguridad a cada instancia ubicada en la nube VPC.

Crear un conjunto de opciones de DHCP. Con una nube Amazon VPC, los servicios DNS y DHCP se suministran de forma predeterminada, lo que afecta a la configuración del DNS en el controlador de dominio de Active Directory. El DHCP de Amazon no se puede inhabilitar, y el DNS de Amazon se puede usar solo para la resolución de DNS públicos, no para la resolución de nombres de Active Directory. Para especificar los servidores de nombre y dominio que entregar a las instancias por DHCP, cree un conjunto de opciones de DHCP. El conjunto asigna el sufijo de dominio de Active Directory y especifica el servidor DNS para todas las instancias en la nube VPC. Para que los registros de Host (A) y Reverse Lookup (PTR) se registren automáticamente cuando las instancias se unen al dominio, debe configurar las propiedades del adaptador de red para cada instancia que agregue a la subred privada.

Agregar un host bastión y un controlador de dominio a la nube VPC. A través del host bastión, puede iniciar sesión en las instancias de la subred privada para configurar el dominio y unir instancias al dominio.

Tarea 1: Configurar la nube VPC

1. En la consola de administración de AWS, seleccione **VPC**.
2. En el panel de mandos de la nube VPC, seleccione **Create VPC**.
3. Seleccione **VPC and more**.
4. En NAT gateways ($), seleccione **In 1 AZ** o **1 per AZ**.
5. En DNS options, deje seleccionada la opción **Enable DNS hostnames**.
6. Seleccione **Create VPC**. AWS crea las subredes pública y privada, la puerta de enlace de Internet, las tablas de redirección y el grupo de seguridad predeterminado.

Tarea 2: Configurar grupos de seguridad

Esta tarea crea y configura los siguientes grupos de seguridad para la nube VPC:

- Un grupo de seguridad público para asociarlo a las instancias de la subred pública.
- Un grupo de seguridad privado para asociarlo a las instancias de la subred privada.

Para crear los grupos de seguridad:

1. En el panel de mandos de la nube VPC, seleccione **Security Groups**.
2. Cree un grupo de seguridad para el grupo de seguridad pública. Seleccione **Create Security Group** e introduzca una etiqueta de nombre y una descripción del grupo. En la nube VPC, seleccione la nube VPC que ha creado. Seleccione **Yes, Create**.

Configurar el grupo de seguridad público

1. En la lista de grupos de seguridad, seleccione el grupo de seguridad público.
2. Seleccione la ficha **Inbound Rules** y seleccione **Edit** para crear estas reglas:

Tipo	Origen
ALL Traffic	Seleccione el grupo de seguridad privado.
ALL Traffic	Seleccione el grupo de seguridad público.
ICMP	0.0.0.0/0
22 (SSH)	0.0.0.0/0
80 (HTTP)	0.0.0.0/0
443 (HTTPS)	0.0.0.0/0
1494 (ICA/HDX)	0.0.0.0/0
2598 (Fiabilidad de la sesión)	0.0.0.0/0
3389 (RDP)	0.0.0.0/0

3. Cuando haya terminado, seleccione **Save**.
4. Seleccione la ficha **Outbound Rules** y seleccione **Edit** para crear estas reglas:

Tipo	Destino
ALL Traffic	Seleccione el grupo de seguridad privado.
ALL Traffic	0.0.0.0/0
ICMP	0.0.0.0/0

5. Cuando haya terminado, seleccione **Save**.

Configurar el grupo de seguridad privado

1. En la lista de grupos de seguridad, seleccione el grupo de seguridad privado.

2. Si no ha configurado el tráfico del grupo de seguridad público, deberá configurar puertos TCP; seleccione la ficha **Inbound Rules** y, a continuación, **Edit** para crear las siguientes reglas:

Tipo	Origen
ALL Traffic	Seleccione el grupo de seguridad privado.
ALL Traffic	Seleccione el grupo de seguridad público.
ICMP	Seleccione el grupo de seguridad público.
TCP 53 (DNS)	Seleccione el grupo de seguridad público.
UDP 53 (DNS)	Seleccione el grupo de seguridad público.
80 (HTTP)	Seleccione el grupo de seguridad público.
TCP 135	Seleccione el grupo de seguridad público.
TCP 389	Seleccione el grupo de seguridad público.
UDP 389	Seleccione el grupo de seguridad público.
443 (HTTPS)	Seleccione el grupo de seguridad público.
TCP 1494 (ICA/HDX)	Seleccione el grupo de seguridad público.
TCP 2598 (Fiabilidad de la sesión)	Seleccione el grupo de seguridad público.
3389 (RDP)	Seleccione el grupo de seguridad público.
TCP 49152–65535	Seleccione el grupo de seguridad público.

3. Cuando haya terminado, seleccione **Save.**
4. Seleccione la ficha **Outbound Rules** y seleccione **Edit** para crear estas reglas:

Tipo	Destino
ALL Traffic	Seleccione el grupo de seguridad privado.
ALL Traffic	0.0.0.0/0
ICMP	0.0.0.0/0
UDP 53 (DNS)	0.0.0.0/0

5. Cuando haya terminado, seleccione **Save**.

Tarea 3: Iniciar instancias

Siga estos pasos para crear dos instancias EC2 y descifrar la contraseña de administrador predeterminado que genera Amazon:

1. En la consola de administración de AWS, seleccione **EC2**.
2. Desde el panel de mandos de EC2, seleccione **Launch Instance**.
3. Seleccione un tipo de instancia y una imagen de máquina de servidor Windows.
4. En la página **Configure Instance Details**, escriba un nombre para la instancia y seleccione la nube VPC que ha configurado.
5. En **Subnet**, seleccione los siguientes elementos para cada instancia:
   - Para el host bastión, seleccione la subred pública
   - Controlador de dominio: seleccione la subred privada
6. En **Auto-assign Public IP address**, seleccione los siguientes elementos para cada instancia:
   - Para el host bastión, seleccione **Enable**.
   - Controlador de dominio: seleccione **Use default setting** o **Disable**.
7. En **Network Interfaces**, introduzca una dirección IP principal que se encuentre dentro del intervalo IP de la subred privada para el controlador de dominio.
8. En la página **Add Storage**, modifique el tamaño del disco, si es necesario.
9. En la página **Tag Instance**, escriba un nombre descriptivo para cada instancia.
10. En la página **Configure Security Groups**, seleccione **Select an existing security group** y, a continuación, seleccione los siguientes elementos para cada instancia:
    - Para el host bastión, seleccione el grupo de seguridad público.
    - Para el controlador de dominio, seleccione el grupo de seguridad privado.
11. Revise las selecciones y, a continuación, seleccione **Launch**.
12. Cree un nuevo par de claves o seleccione uno existente. Si crea un nuevo par de claves, descargue el archivo de clave privada (.pem) y guárdela en un lugar seguro. Deberá suministrar la clave privada cuando obtenga la contraseña predeterminada de administrador de la instancia.
13. Seleccione **Launch Instances**. Seleccione **View Instances** para mostrar una lista de las instancias. Espere hasta que la instancia que acaba de iniciar haya pasado por todas las comprobaciones de estado antes de acceder a ella.
14. Obtenga la contraseña del administrador predeterminado de cada instancia:
    a) En la lista de instancias, seleccione la instancia y, a continuación, seleccione **Connect**.

b) Vaya a la ficha **RDP client**, seleccione **Get Password** y cargue el archivo de clave privada (`.pem`) cuando se le indique.
c) Seleccione **Decrypt Password** para obtener una contraseña legible en lenguaje humano. AWS muestra la contraseña predeterminada.

15. Repita los pasos desde el paso 2 hasta que haya creado dos instancias:

- Una instancia de host bastión en la subred pública
- Una instancia en su subred privada que se va a usar como controlador de dominio.

Tarea 4: Crear un conjunto de opciones de DHCP

1. En el panel de mandos de la nube VPC, seleccione **DHCP Options Sets**.
2. Introduzca la siguiente información:

- Name tag. Introduzca un nombre descriptivo para el conjunto.
- Domain name. Escriba el nombre de dominio completo que usará cuando configure la instancia del controlador de dominio.
- Domain name servers. Escriba la dirección IP privada que asignó a la instancia del controlador de dominio y la cadena **AmazonProvidedDNS**, separadas con comas.
- NTP servers. Deje este campo en blanco.
- NetBIOS name servers. Introduzca la dirección IP privada de la instancia del controlador de dominio.
- NetBIOS node type. Escriba **2**.

3. Seleccione **Yes, Create.**
4. Asocie el nuevo conjunto a la nube VPC:

a) En el panel de mandos de la nube VPC, seleccione **Your VPCs** y, a continuación, seleccione la nube VPC que ha configurado.
b) Seleccione **Actions > Edit DHCP Options Set**.
c) Cuando se le solicite, seleccione el nuevo conjunto que ha creado y, a continuación, seleccione **Save**.

Tarea 5: Configurar las instancias

1. A través de un cliente RDP, conéctese a la dirección IP pública de la instancia del host bastión. Cuando se le solicite, introduzca las credenciales de la cuenta de administrador.
2. Desde la instancia del host bastión, inicie una Conexión a Escritorio remoto (RDC) y conéctese a la dirección IP privada de la instancia que quiere configurar. Cuando se le solicite, introduzca las credenciales del administrador de la instancia.

3. Configure los parámetros de DNS para todas las instancias en la subred privada:

    a) Seleccione **Inicio > Panel de control > Redes e Internet > Centro de redes y recursos compartidos > Cambiar configuración del adaptador**. Haga doble clic en la conexión de red que aparece.

    b) Seleccione **Propiedades > Protocolo de Internet versión 4 (TCP/IPv4) > Propiedades**.

    c) Seleccione **Avanzado > DNS**. Compruebe que los siguientes parámetros están habilitados y seleccione **Aceptar**:

    - Registrar en DNS las direcciones de esta conexión
    - Use el sufijo DNS de esta conexión en el registro de DNS

4. Para configurar el controlador de dominio:

    a) Mediante el Administrador de servidores, agregue el rol Servicios de dominio de Active Directory con todas las funciones predeterminadas.

    b) Promueva la instancia a un controlador de dominio. Durante la promoción, habilite el DNS y use el nombre de dominio que especificó al crear el conjunto de opciones de DHCP. Reinicie la instancia cuando lo pida el sistema.

Qué hacer a continuación

- Instalar componentes principales
- Instalar VDA
- Crear un sitio
- Para crear y administrar una conexión en AWS, consulte Conexión con AWS.

Más información

- Crear y administrar conexiones y recursos
- Crear catálogos de máquinas

Entornos de virtualización de XenServer

August 17, 2024

XenServer simplifica la administración de las operaciones y garantiza una experiencia de usuario de alta definición con cargas de trabajo elevadas.

Para configurar XenServer, consulte Preparar la instalación.

Qué hacer a continuación

- Instalar componentes principales
- Instalar VDA
- Crear un sitio
- Para crear y administrar una conexión en XenServer, consulte Conexión con XenServer

Más información

- Crear y administrar conexiones y recursos
- Crear catálogos de máquinas

Entornos de Google Cloud

August 17, 2024

Citrix Virtual Apps and Desktops le permite aprovisionar y administrar máquinas en Google Cloud.

Requisitos

- Cuenta de Citrix Cloud. La función descrita en este artículo solo está disponible en Citrix Cloud.
- Un proyecto de Google Cloud. El proyecto almacena todos los recursos de procesamiento asociados al catálogo de máquinas. Puede ser un proyecto existente o uno nuevo.
- Habilite cuatro API en su proyecto de Google Cloud. Para obtener información más detallada, consulte Habilitar las API de Google Cloud.
- Cuenta de servicio de Google Cloud. La cuenta de servicio se autentica en Google Cloud para permitir el acceso al proyecto. Para obtener información detallada, consulte Configurar y actualizar cuentas de servicio.
- Habilitar el acceso privado a Google. Para obtener información detallada, consulte Habilitar el acceso privado a Google.

Habilitar las API de Google Cloud

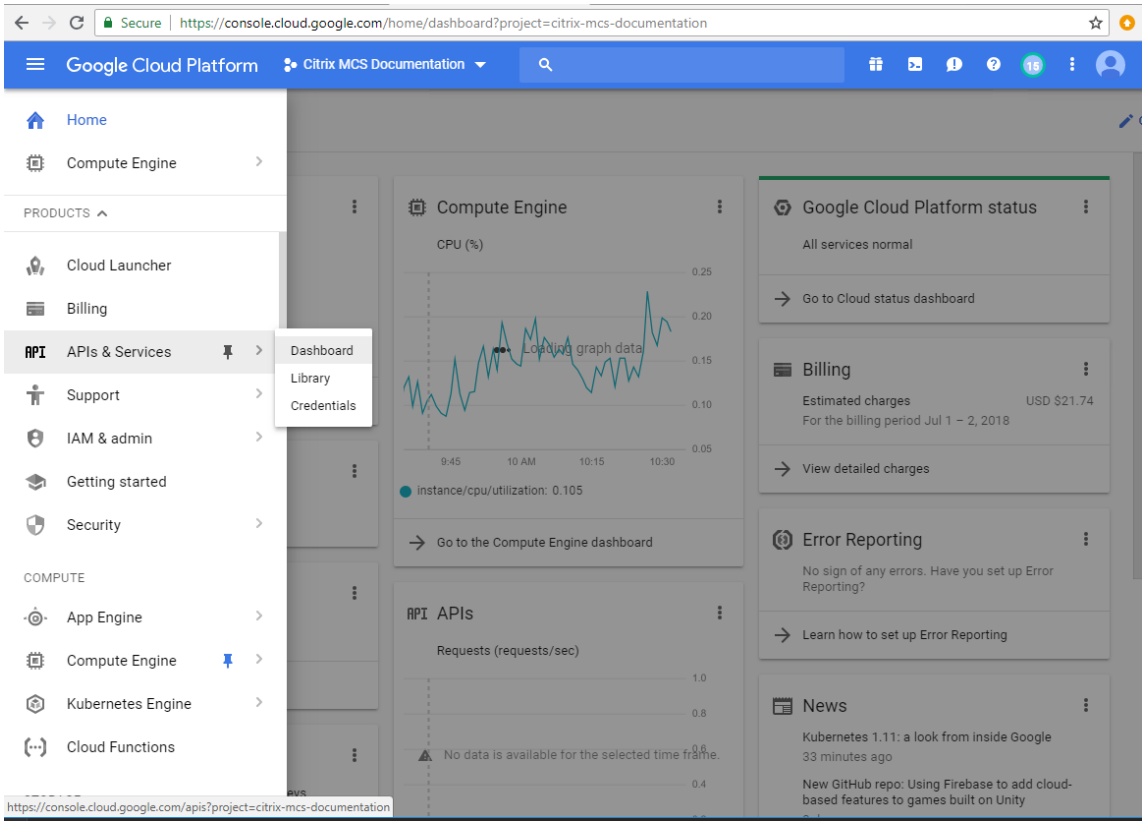
Para utilizar la funcionalidad de Google Cloud a través de Web Studio, habilite estas API en su proyecto de Google Cloud:

- API de Compute Engine
- API de Cloud Resource Manager

- API de Identity and Access Management (IAM)
- API de Cloud Build
- Servicio de administración de claves (KMS) en la nube

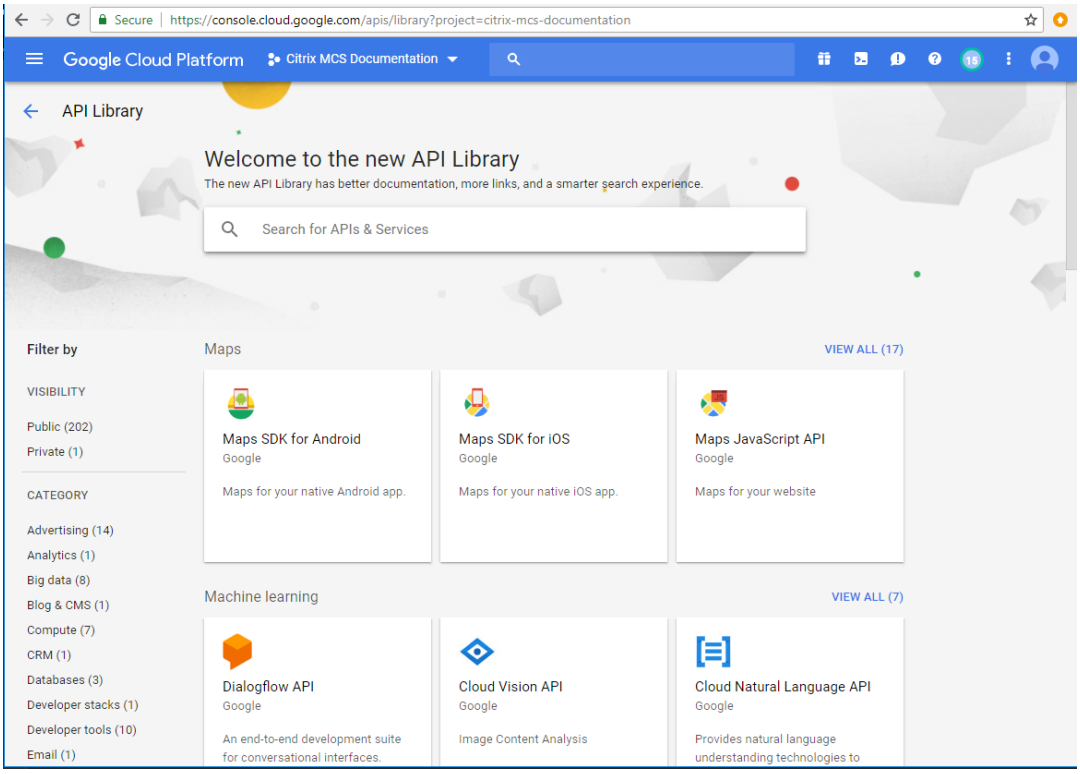
En la consola de Google Cloud, siga estos pasos:

1. En el menú superior izquierdo, seleccione **APIs and Services > Dashboard**.



2. En la pantalla **Dashboard**, compruebe que la API de Compute Engine esté habilitada. Si no es el caso, siga estos pasos:

    a) Vaya a **APIs and Services > Library**.



b) En el cuadro de búsqueda, escriba *Compute Engine*.

c) En los resultados de la búsqueda, seleccione **Compute Engine API**.

d) En la página **Compute Engine API**, seleccione **Enable**.

3. Habilite la API de Cloud Resource Manager.

   a) Vaya a **APIs and Services > Library**.

   b) En el cuadro de búsqueda, escriba *Cloud Resource Manager*.

   c) En los resultados de búsqueda, seleccione **Cloud Resource Manager API**.

   d) En la página **Cloud Resource Manager API**, seleccione **Enable**. Aparece el estado de la API.

4. Del mismo modo, habilite la **API de Identity and Access Management (IAM)** y la **API de Cloud Build**.

También puede usar Google Cloud Shell para habilitar las API. Para hacerlo:

1. Abra la consola de Google y cargue Cloud Shell.
2. Ejecute estos cuatro comandos en Cloud Shell:

   - gcloud services enable compute.googleapis.com
   - gcloud services enable cloudresourcemanager.googleapis.com

- gcloud services enable iam.googleapis.com
- gcloud services enable cloudbuild.googleapis.com

3. Haga clic en **Authorize** si Cloud Shell lo solicita.

Configurar y actualizar cuentas de servicio

> **Nota:**
>
> GCP presentará cambios en el comportamiento predeterminado de los servicios de Cloud Build y en el uso de las cuentas de servicio a partir del 29 de abril de 2024. Para obtener más información, consulte Cambio de la cuenta de servicio de Cloud Build. Los proyectos de Google existentes con la API de Cloud Build habilitada antes del 29 de abril de 2024 no se ven afectados por este cambio. No obstante, si quiere mantener el comportamiento actual del servicio de Cloud Build a partir del 29 de abril, puede crear o aplicar una directiva de organización para inhabilitar la aplicación de restricciones antes de habilitar la API de Cloud Build. Como resultado, el siguiente contenido se divide en dos: Antes del 29 de abril de 2024 y A partir del 29 de abril de 2024. Si establece la nueva directiva de la organización, vaya a la sección Antes del 29 de abril de 2024.

Antes del 29 de abril de 2024

Citrix Cloud usa tres cuentas de servicio independientes en el proyecto de Google Cloud:

- *Cuenta de servicio de Citrix Cloud*: Esta cuenta de servicio permite a Citrix Cloud acceder al proyecto de Google y aprovisionar y administrar máquinas. Esta cuenta de servicio se autentica en Google Cloud mediante una clave generada por Google Cloud.

  Debe crear esta cuenta de servicio manualmente, tal y como se describe aquí. Para obtener más información, consulte Crear una cuenta de Citrix Cloud Service.

  Puede identificar esta cuenta de servicio con una dirección de correo electrónico. Por ejemplo, `<my-service-account>@<project-id>.iam.gserviceaccount.com`.

- *Cuenta de servicio de Cloud Build*: Esta cuenta de servicio se aprovisiona automáticamente después de habilitar todas las API mencionadas en Habilitar las API de Google Cloud. Para ver todas las cuentas de servicio creadas automáticamente, vaya a **IAM y Admin > IAM** en la consola de **Google Cloud** y seleccione la casilla de verificación **Incluir asignaciones de funciones proporcionadas por Google**.

  Puede identificar esta cuenta de servicio mediante una dirección de correo electrónico que comience por el **ID del proyecto** y la palabra **cloudbuild**. Por ejemplo, `<project-id>@cloudbuild.gserviceaccount.com`

  Verifique si a la cuenta de servicio se le han concedido los siguientes roles. Si debe agregar roles, siga los pasos descritos en Agregar roles a la cuenta de servicio de Cloud Build.

  - Cuenta de servicio de Cloud Build
  - Administrador de instancias de proceso
  - Usuario de cuenta de servicio

- *Cuenta de servicio de Cloud Compute*: Google Cloud agrega esta cuenta de servicio a las instancias creadas en Google Cloud una vez que se activa la API de Compute. Esta cuenta tiene el rol de editor básico de IAM para realizar las operaciones. Sin embargo, si elimina el permiso predeterminado para tener un control más granular, deberá agregar el rol **Administrador de almacenamiento** que requiere los siguientes permisos:

  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

Puede identificar esta cuenta de servicio mediante una dirección de correo electrónico que comience por el **ID del proyecto** y la palabra **compute**. Por ejemplo, `<project-id>-compute@developer.gserviceaccount.com`.

Crear una cuenta de servicio de Citrix Cloud Para crear una cuenta de servicio de Citrix Cloud, siga estos pasos:

1. En la consola de Google Cloud, vaya a **IAM & Admin > Service accounts**.
2. En la página **Service accounts**, seleccione **CREATE SERVICE ACCOUNT**.
3. En la página **Create service account**, introduzca la información necesaria y, a continuación, seleccione **CREATE AND CONTINUE**.
4. En la página **Grant this service account access to project**, haga clic en el menú desplegable **Select a role** y seleccione los roles necesarios. Haga clic en **+ADD ANOTHER ROLE** si quiere agregar más roles.

   Cada cuenta (personal o de servicio) tiene varios roles que definen la gestión del proyecto. Otorgue estos roles a esta cuenta de servicio:

   - Administrador de procesos
   - Administrador de almacenamiento
   - Editor de compilaciones en la nube
   - Usuario de cuenta de servicio
   - Usuario de almacén de datos en la nube
   - Operador criptográfico de Cloud KMS

   El operador criptográfico de Cloud KMS requiere los siguientes permisos:

- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.get
- cloudkms.keyRings.list

> **Nota:**
>
> Habilite todas las API para obtener la lista completa de roles disponibles al crear una cuenta de servicio.

5. Haga clic en **CONTINUE**
6. En la página **Grant users access to this service account**, agregue usuarios o grupos para permitirles realizar acciones en esta cuenta de servicio.
7. Haga clic en **DONE**.
8. Vaya a la consola principal de IAM.
9. Identifique la cuenta de servicio creada.
10. Compruebe que los roles se hayan asignado correctamente.

Consideraciones:

Al crear la cuenta de servicio, tenga en cuenta lo siguiente:

- Los pasos **Grant this service account access to project** y **Grant users access to this service account** son opcionales. Si opta por omitir estos pasos de configuración opcionales, la cuenta de servicio recién creada no se mostrará en la página **IAM & Admin > IAM**.
- Para mostrar los roles asociados a una cuenta de servicio, agregue los roles sin omitir los pasos opcionales. Este proceso garantiza que aparezcan roles para la cuenta de servicio configurada.

Clave de la cuenta de servicio de Citrix Cloud La clave de la cuenta de Citrix Cloud Service es necesaria para crear una conexión en Citrix DaaS. La clave se halla en un archivo de credenciales (JSON). El archivo se descarga automáticamente y se guarda en la carpeta **Descargas** después de crear la clave. Al crear la clave, establezca el tipo de clave en JSON. De lo contrario, la interfaz de Configuración completa de Citrix no puede analizarla.

Para crear una clave de cuenta de servicio, vaya a **IAM y Admin > Cuentas de servicio** y haga clic en la dirección de correo electrónico de la cuenta de servicio de Citrix Cloud. Cambie a la ficha **Teclas** y seleccione **Agregar clave > Crear nueva clave**. Asegúrese de seleccionar **JSON** como tipo de clave.

> **Sugerencia:**
>
> Cree claves mediante la página **Service accounts** de la consola de Google Cloud. Le recomendamos cambiar las claves con frecuencia por motivos de seguridad. Para proporcionar claves

> nuevas a la aplicación de Citrix Virtual Apps and Desktops, modifique una conexión de Google Cloud existente.

Agregar roles a la cuenta de servicio de Citrix Cloud Para agregar roles a la cuenta de servicio de Citrix Cloud:

1. En la consola de Google Cloud, vaya a **IAM & Admin > IAM**.
2. En la página **IAM > PERMISSIONS**, busque la cuenta de servicio que creó, identificable con una dirección de correo electrónico.

   Por ejemplo, `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. Seleccione el icono del lápiz para modificar el acceso a la entidad principal de la cuenta de servicio.
4. En la página **Edit access to "project-id"** para la opción de la entidad principal seleccionada, seleccione **ADD ANOTHER ROLE** para agregar los roles necesarios a su cuenta de servicio uno por uno y, a continuación, seleccione **SAVE**.

Agregar roles a la cuenta de servicio de Cloud Build Para agregar roles a la cuenta de servicio de Cloud Build:

1. En la consola de Google Cloud, vaya a **IAM & Admin > IAM**.
2. En la página **IAM**, busque la cuenta de servicio de Cloud Build, identificable con una dirección de correo electrónico que comience por el **ID del proyecto** y la palabra **cloudbuild**.

   Por ejemplo, `<project-id>@cloudbuild.gserviceaccount.com`
3. Seleccione el icono del lápiz para modificar los roles de la cuenta de Cloud Build.
4. En la **página Edit access to "project-id"** para la opción de la entidad principal seleccionada, seleccione **ADD ANOTHER ROLE** para agregar los roles necesarios a su cuenta de servicio de Cloud Build uno por uno y, a continuación, seleccione **SAVE**.

   > **Nota:**
   >
   > Habilite todas las API para obtener la lista completa de roles.

A partir del 29 de abril de 2024

Citrix Cloud usa dos cuentas de servicio independientes en el proyecto de Google Cloud:

- *Cuenta de servicio de Citrix Cloud*: Esta cuenta de servicio permite a Citrix Cloud acceder al proyecto de Google y aprovisionar y administrar máquinas. Esta cuenta de servicio se autentica en Google Cloud mediante una clave generada por Google Cloud.

  Debe crear esta cuenta de servicio manualmente.

  Puede identificar esta cuenta de servicio con una dirección de correo electrónico. Por ejemplo, `<my-service-account>@<project-id>.iam.gserviceaccount.com`.

- *Cuenta de servicio de Cloud Compute*: Esta cuenta de servicio se aprovisiona automáticamente después de habilitar todas las API mencionadas en Habilitar las API de Google Cloud. Para ver todas las cuentas de servicio creadas automáticamente, vaya a **IAM y Admin > IAM** en la consola de **Google Cloud** y seleccione la casilla de verificación **Incluir asignaciones de funciones proporcionadas por Google**. Esta cuenta tiene el rol de editor básico de IAM para realizar las operaciones. Sin embargo, si elimina el permiso predeterminado para tener un control más granular, deberá agregar el rol **Administrador de almacenamiento** que requiere los siguientes permisos:

  - resourcemanager.projects.get
  - storage.objects.create
  - storage.objects.get
  - storage.objects.list

  Puede identificar esta cuenta de servicio mediante una dirección de correo electrónico que comience por el **ID del proyecto** y la palabra **compute**. Por ejemplo, `<project-id>-compute@developer.gserviceaccount.com`.

  Verifique si a la cuenta de servicio se le han concedido los siguientes roles.

  - Cuenta de servicio de Cloud Build
  - Administrador de instancias de proceso
  - Usuario de cuenta de servicio

Crear una cuenta de servicio de Citrix Cloud Para crear una cuenta de servicio de Citrix Cloud, siga estos pasos:

1. En la consola de Google Cloud, vaya a **IAM & Admin > Service accounts**.
2. En la página **Service accounts**, seleccione **CREATE SERVICE ACCOUNT**.
3. En la página **Create service account**, introduzca la información necesaria y, a continuación, seleccione **CREATE AND CONTINUE**.
4. En la página **Grant this service account access to project**, haga clic en el menú desplegable **Select a role** y seleccione los roles necesarios. Haga clic en **+ADD ANOTHER ROLE** si quiere agregar más roles.

Cada cuenta (personal o de servicio) tiene varios roles que definen la gestión del proyecto. Otorgue estos roles a esta cuenta de servicio:

- Administrador de procesos
- Administrador de almacenamiento
- Editor de compilaciones en la nube
- Usuario de cuenta de servicio
- Usuario de almacén de datos en la nube
- Operador criptográfico de Cloud KMS

El operador criptográfico de Cloud KMS requiere los siguientes permisos:

- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.get
- cloudkms.keyRings.list

> **Nota:**
>
> Habilite todas las API para obtener la lista completa de roles disponibles al crear una cuenta de servicio.

5. Haga clic en **CONTINUE**
6. En la página **Grant users access to this service account**, agregue usuarios o grupos para permitirles realizar acciones en esta cuenta de servicio.
7. Haga clic en **DONE**.
8. Vaya a la consola principal de IAM.
9. Identifique la cuenta de servicio creada.
10. Compruebe que los roles se hayan asignado correctamente.

Consideraciones:

Al crear la cuenta de servicio, tenga en cuenta lo siguiente:

- Los pasos **Grant this service account access to project** y **Grant users access to this service account** son opcionales. Si opta por omitir estos pasos de configuración opcionales, la cuenta de servicio recién creada no se mostrará en la página **IAM & Admin > IAM**.
- Para mostrar los roles asociados a una cuenta de servicio, agregue los roles sin omitir los pasos opcionales. Este proceso garantiza que aparezcan roles para la cuenta de servicio configurada.

Clave de la cuenta de servicio de Citrix Cloud La clave de la cuenta de Citrix Cloud Service es necesaria para crear una conexión en Citrix DaaS. La clave se halla en un archivo de credenciales (JSON). El

archivo se descarga automáticamente y se guarda en la carpeta **Descargas** después de crear la clave. Al crear la clave, establezca el tipo de clave en JSON. De lo contrario, la interfaz de Configuración completa de Citrix no puede analizarla.

Para crear una clave de cuenta de servicio, vaya a **IAM y Admin > Cuentas de servicio** y haga clic en la dirección de correo electrónico de la cuenta de servicio de Citrix Cloud. Cambie a la ficha **Teclas** y seleccione **Agregar clave > Crear nueva clave**. Asegúrese de seleccionar **JSON** como tipo de clave.

> **Sugerencia:**
>
> Cree claves mediante la página **Service accounts** de la consola de Google Cloud. Le recomendamos cambiar las claves con frecuencia por motivos de seguridad. Para proporcionar claves nuevas a la aplicación de Citrix Virtual Apps and Desktops, modifique una conexión de Google Cloud existente.

Agregar roles a la cuenta de servicio de Citrix Cloud Para agregar roles a la cuenta de servicio de Citrix Cloud:

1. En la consola de Google Cloud, vaya a **IAM & Admin > IAM**.
2. En la página **IAM > PERMISSIONS**, busque la cuenta de servicio que creó, identificable con una dirección de correo electrónico.

   Por ejemplo, `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. Seleccione el icono del lápiz para modificar el acceso a la entidad principal de la cuenta de servicio.
4. En la página **Edit access to "project-id"** para la opción de la entidad principal seleccionada, seleccione **ADD ANOTHER ROLE** para agregar los roles necesarios a su cuenta de servicio uno por uno y, a continuación, seleccione **SAVE**.

Agregar roles a la cuenta de servicio de Cloud Compute Para agregar roles a la cuenta de servicio de Cloud Compute:

1. En la consola de Google Cloud, vaya a **IAM & Admin > IAM**.
2. En la página **IAM**, busque la cuenta de servicio de Cloud Compute, identificable con una dirección de correo electrónico que comience por el **ID del proyecto** y la palabra **compute**.

   Por ejemplo, `<project-id>-compute@developer.gserviceaccount.com`
3. Seleccione el icono del lápiz para modificar los roles de la cuenta de Cloud Build.

4. En la **página Edit access to "project-id"** para la opción de la entidad principal seleccionada, seleccione **ADD ANOTHER ROLE** para agregar los roles necesarios a su cuenta de servicio de Cloud Build uno por uno y, a continuación, seleccione **SAVE**.

   > **Nota:**
   >
   > Habilite todas las API para obtener la lista completa de roles.

Permisos de almacenamiento y administración de depósitos

Citrix Virtual Apps and Desktops mejora el proceso de notificación de errores de compilación en la nube para el servicio de Google Cloud. Este servicio ejecuta compilaciones en Google Cloud. Citrix Virtual Apps and Desktops crea un depósito de almacenamiento denominado `citrix-mcs-cloud-build-logs-{ region } -{ 5 random characters }` donde los servicios de Google Cloud capturan la información del registro de compilación. Se establece una opción en este depósito que elimina el contenido tras un período de 30 días. Este proceso requiere que la cuenta de servicio utilizada para la conexión tenga establecidos los permisos `storage.buckets.update` en Google Cloud. Si la cuenta de servicio no tiene este permiso, Citrix Virtual Apps and Desktops ignora los errores y continúa con el proceso de creación del catálogo. Sin este permiso, el tamaño de los registros de compilación aumenta y se requiere una limpieza manual.

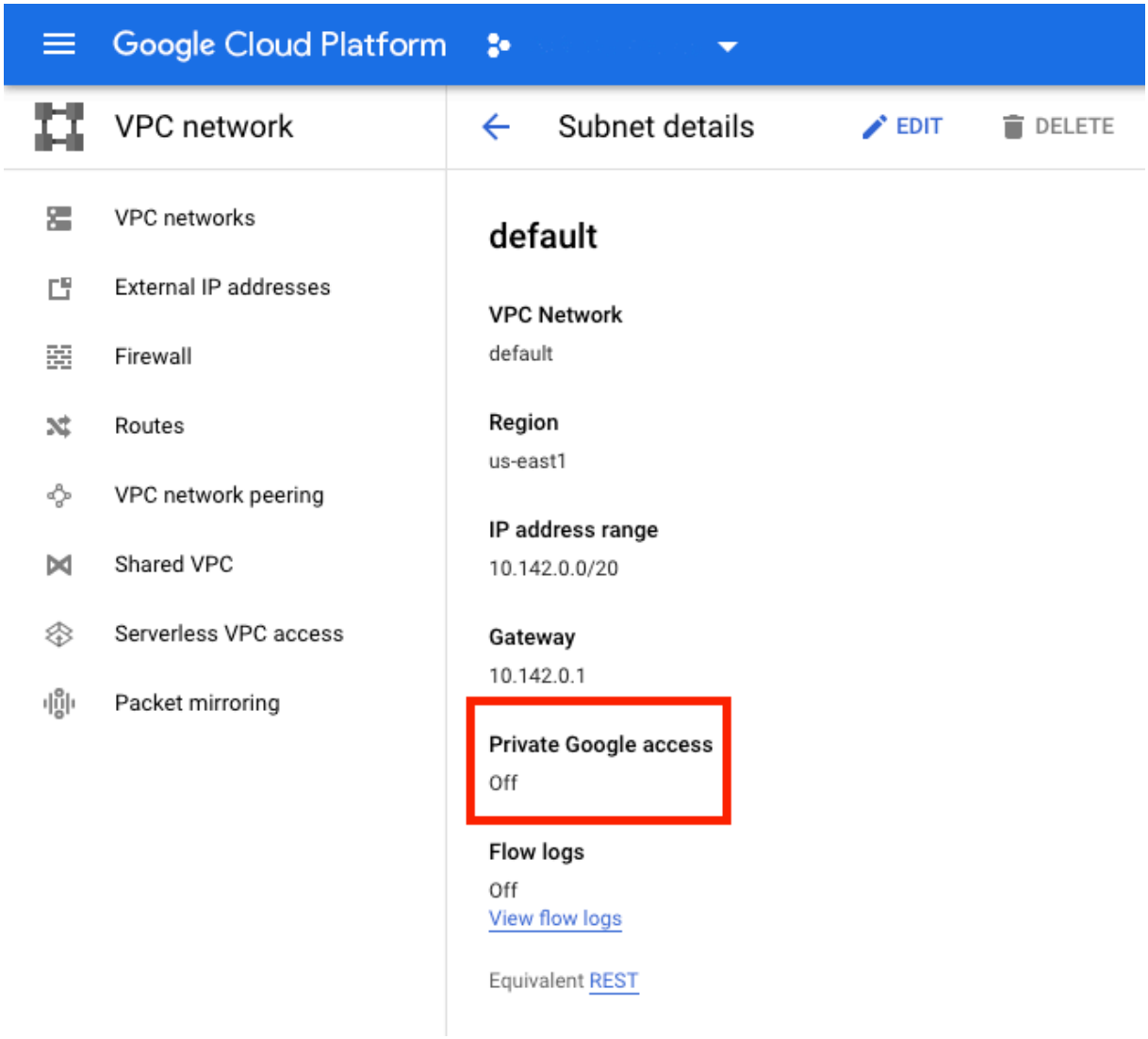
Habilitar el acceso privado a Google

Cuando una máquina virtual carece de una dirección IP externa asignada a su interfaz de red, los paquetes solo se envían a otros destinos de direcciones IP internas. Cuando habilita el acceso privado, la máquina virtual se conecta al conjunto de direcciones IP externas utilizadas por la API de Google y los servicios asociados.

> **Nota:**
>
> Independientemente de si el acceso privado a Google está habilitado, todas las máquinas virtuales con y sin direcciones IP públicas deben poder acceder a las API públicas de Google, especialmente si se han instalado dispositivos de red de terceros en el entorno.

Para asegurarse de que una máquina virtual de la subred pueda acceder a las API de Google sin una dirección IP pública para el aprovisionamiento de MCS:

1. En Google Cloud, acceda a la **configuración de red de VPC**.
2. En la pantalla Detalles de subred, active **Acceso privado a Google**.



Para obtener más información, consulte Configura el Acceso privado a Google.

> **Importante:**
>
> Si la red está configurada para impedir el acceso de la máquina virtual a Internet, asegúrese de que su organización asume los riesgos asociados con la habilitación del acceso privado a Google para la subred a la que está conectada la máquina virtual.

Qué hacer a continuación

- Instalar componentes principales
- Instalar VDA
- Crear un sitio
- Para crear y administrar una conexión en entornos de Google Cloud, consulte Conexión con entornos de Google Cloud

Más información

- Crear y administrar conexiones y recursos
- Crear catálogos de máquinas

Entornos de virtualización de HPE Moonshot

August 17, 2024

Citrix Virtual Apps and Desktops administra las cargas de trabajo de HPE Moonshot a través de un plug-in HPE Moonshot administrado por Citrix presente. Con este plug-in, puede crear conexiones a su chasis HPE Moonshot, crear catálogos y administrar la energía de las máquinas del catálogo.

Requisito

Instale el plug-in HPE Moonshot administrado por Citrix en el Delivery Controller.

> **Nota:**
>
> - Si están instalados los plug-ins HPE Moonshot gestionados por Citrix y HPE, el Delivery Controller usa el plug-in HPE Moonshot gestionado por Citrix.
> - Si los plug-ins HPE Moonshot gestionados por Citrix y HPE están instalados y quiere usar el plug-in Moonshot gestionado por HPE, desinstale el plug-in HPE Moonshot gestionado por Citrix y actualice la caché de `RegisterPlugin`.

Instale el plug-in HPE Moonshot administrado por Citrix

Para instalar el plug-in HPE Moonshot administrado por Citrix, haga lo siguiente:

1. Instale `E:\x64\Citrix Desktop Delivery Controller\MoonshotPlugin`.msi. `E:\`, es la ISO.
2. Abra PowerShell como administrador y ejecute el siguiente comando.

```
C:\Program Files\Common Files\Citrix\HCLPlugins> .\RegisterPlugins
    .exe -pluginsroot .\CitrixMachineCreation\v1.0.0.0\
```

3. Una vez registrado correctamente el plug-in, reinicie los siguientes servicios desde el **Administrador de tareas**:

    a) CitrixBrokerService

b) CitrixHostService
c) CitrixMachineCreationService

4. Ejecute `Get-HypHypervisorPlugins` para comprobar si el plug-in está instalado en el Delivery Controller. El campo **DisplayName** de la salida debe mostrarse como **HPE Moonshot**.

Desinstale el plug-in HPE Moonshot administrado por Citrix y actualice la caché de RegisterPlugin

Si los plug-ins HPE Moonshot gestionados por Citrix y HPE están instalados y quiere usar el plug-in Moonshot gestionado por HPE; luego debe desinstalar el plug-in HPE Moonshot gestionado por Citrix y actualizar la caché de `RegisterPlugin`. Para ello:

1. Desinstale el plug-in HPE Moonshot administrado por Citrix.
2. Abra PowerShell como administrador y ejecute el siguiente comando:

```
cd `C:\Program Files\Common Files\Citrix\HCLPlugins`
C:\Program Files\Common Files\Citrix\HCLPlugins> .\RegisterPlugins
    .exe -PluginsRoot ` C:\Program Files\Common Files\Citrix\
    HCLPlugins\ManagedMachine\v2.5.0.0`
```

3. Una vez registrado correctamente el plug-in, reinicie los siguientes servicios desde el **Administrador de tareas**:

a) CitrixBrokerService
b) CitrixHostService
c) CitrixMachineCreationService

4. Ejecute `Get-HypHypervisorPlugins` para comprobar si el plug-in está instalado en el Delivery Controller. El campo **DisplayName** de la salida debe mostrarse como **HPE Moonshot Machine Manager**.

Pasos clave

1. Configure sus entornos de HPE.
2. Cree una conexión con el chasis HPE Moonshot.
3. Cree un catálogo de máquinas.

> **Nota:**
>
> Antes de crear un catálogo, asegúrese de tener uno o más nodos de cartuchos HPE Moon-

> shot e instale los VDA en esos nodos. Puede considerar el chasis HPE Moonshot como el hipervisor y los nodos de cartuchos como máquinas virtuales.

4. Cree un grupo de entrega.
5. Migre el resto de los nodos de HPE Moonshot no administrados al catálogo administrado o al grupo de entrega.

Qué hacer a continuación

- Instalar componentes principales
- Instalar VDA
- Crear un sitio
- Para crear y administrar una conexión en HPE Moonshot, consulte Conexión con HPE Moonshot

Más información

- Crear y administrar conexiones y recursos
- Crear catálogos de máquinas

Entornos en la nube de Microsoft Azure Resource Manager

August 17, 2024

Cuando utilice el Administrador de recursos de Microsoft Azure para aprovisionar máquinas virtuales en la implementación de Citrix Virtual Apps and Desktops, familiarícese con lo siguiente:

- Azure Active Directory: https://docs.microsoft.com/en-in/azure/active-directory/fundamentals/active-directory-whatis/
- Marco de consentimiento: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/plan-an-application-integration
- Entidad principal de servicio: https://docs.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals/

Para configurar Microsoft Azure Resource Manager, consulte Antes de la instalación.

Qué hacer a continuación

- Instalar componentes principales

- Instalar VDA
- Crear un sitio
- Para crear y administrar una conexión en entornos de Azure, consulte Conexión con Microsoft Azure

Más información

- Crear y administrar 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 Microsoft System Center Configuration Manager

August 17, 2024

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.
- **Función Proxy de reactivación de Configuration Manager:** La función Wake on LAN de Acceso con Remote PC está disponible con Configuration Manager. Para obtener más información, consulte Función Wake on LAN integrada en SCCM.
- **Propiedades de Citrix Virtual Apps and Desktops:** Las Propiedades 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 aparecen 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
`AssignmentType`	Establece el valor de IsAssigned. Los valores válidos son `ClientIP`, `ClientName`, `None` y `User` (se establece `IsAssigned` en `True`)
`BrokerSiteName`	Devuelve el mismo valor que `HostIdentifier`
`DesktopCatalogName`	Catálogo de máquinas asociado al escritorio.
`DesktopGroupName`	Grupo de entrega asociado al escritorio.
`HostIdentifier`	Devuelve el mismo valor que `BrokerSiteName`.
`IsAssigned`	`True` para asignar el escritorio a un usuario y `False` para un escritorio aleatorio
`IsMasterImage`	Permite tomar decisiones sobre el entorno. Por ejemplo: puede instalar aplicaciones en la imagen y no en las máquinas aprovisionadas. El valor válido es `True` en una máquina virtual que se utiliza como imagen. Este valor se establece durante la instalación basada en una selección. También se puede dejar el valor vació en una máquina virtual que se aprovisiona desde esa imagen.
`IsVirtualMachine`	`True` para una máquina virtual y **`false`** para una máquina física.
`OSChangesPersist`	`False` si la imagen del sistema operativo del escritorio vuelve a un estado limpio cada vez que se reinicia; de lo contrario, el valor es **`true`**.
`PersistentDataLocation`	La ubicación donde Configuration Manager almacena datos persistentes. Los usuarios no pueden acceder a ella.
`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, los nombres incluyen espacios o varían ligeramente con respecto a los nombres de propiedades. Por ejemplo: `BrokerSiteName` aparece 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 Microsoft System Center Virtual Machine Manager

August 17, 2024

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.

> **Nota:**
>
> No se admiten clústeres mixtos de Hyper-V (que contienen servidores que ejecutan diferentes versiones de Hyper-V).

Puede utilizar Machine Creation Services y Citrix Provisioning (antes llamado Provisioning Services) para aprovisionar:

- Máquinas virtuales con SO de servidor o escritorio compatibles de la 1.ª generación.
- Máquinas virtuales con SO de servidor o escritorio compatibles de la 2.ª generación, incluida compatibilidad con arranque seguro.

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 servidor de Hyper-V. Esta configuración permite ofrecer la administración del ciclo de vida de las máquinas virtuales (la creación, actualización y eliminación de VM).

   No se admite la instalación de Controller en un servidor que ejecuta Hyper-V.

En implementaciones grandes en las que un solo SCVMM administra varios clústeres en diferentes centros de datos, puede limitar el ámbito de los grupos de hosts de los administradores delegados.

Para limitar el ámbito de los grupos de hosts, use el rol de administrador delegado en la consola de Microsoft System Center Virtual Machine Manager (VMM):

1. En el **asistente para crear roles de usuario**, seleccione Fabric Administrator (administrador delegado) como rol de usuario.
2. En **Miembros**, agregue la cuenta de usuario en Active Directory que quiera usar como administrador delegado.
3. En **Ámbito**, seleccione los grupos de hosts a los que quiere que tenga acceso el administrador delegado.
4. Cree otra **cuenta de ejecución** con las credenciales de usuario del administrador delegado. Use estas credenciales para crear una conexión de hipervisor más adelante. No use las cuentas del rol de administrador principal.

Aprovisionar Azure Stack HCI mediante SCVMM

Azure Stack HCI es una solución de clústeres de infraestructura hiperconvergente (HCI) que aloja cargas de trabajo virtualizadas de Windows y Linux y su almacenamiento en un entorno híbrido local.

Los servicios híbridos de Azure mejoran el clúster con funciones como la supervisión en la nube, la recuperación de sitios y las copias de seguridad de VM. También puede obtener una vista centralizada de todas las implementaciones de Azure Stack HCI en Azure Portal.

Consideraciones

Se deben tener en cuenta las siguientes cuestiones:

- No se admiten las cargas de trabajo multisesión de Windows 10 Enterprise y Windows 11 Enterprise.
- La compatibilidad con la administración del clúster Azure Stack HCI 23H2 vendrá con SCVMM 2025.

Integrar Azure Stack HCI en SCVMM

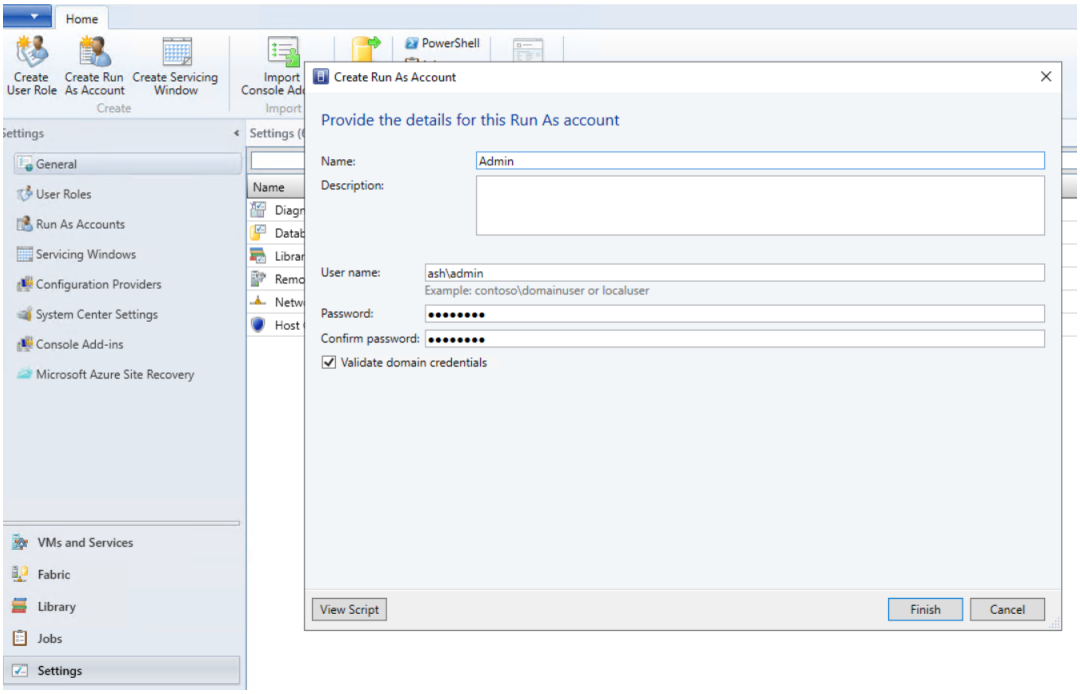
Para integrar Azure Stack HCI en SCVMM, primero debe crear un clúster de Azure Stack HCI y, a continuación, integrar ese clúster en SCVMM.

1. Para crear el clúster de Azure Stack HCI, consulte el documento de Microsoft Conexión de Azure Stack HCI a Azure.
2. Para integrar el clúster de Azure Stack HCI en SCVMM, haga lo siguiente:

    a) Inicie sesión en la máquina preparada para alojar el servidor de SCVMM e instale SCVMM 2019 UR3 o una versión posterior.

    > **Nota:**
    >
    > Instale la consola de administrador SCVMM 2019 UR3 o una versión posterior en todos los controladores.

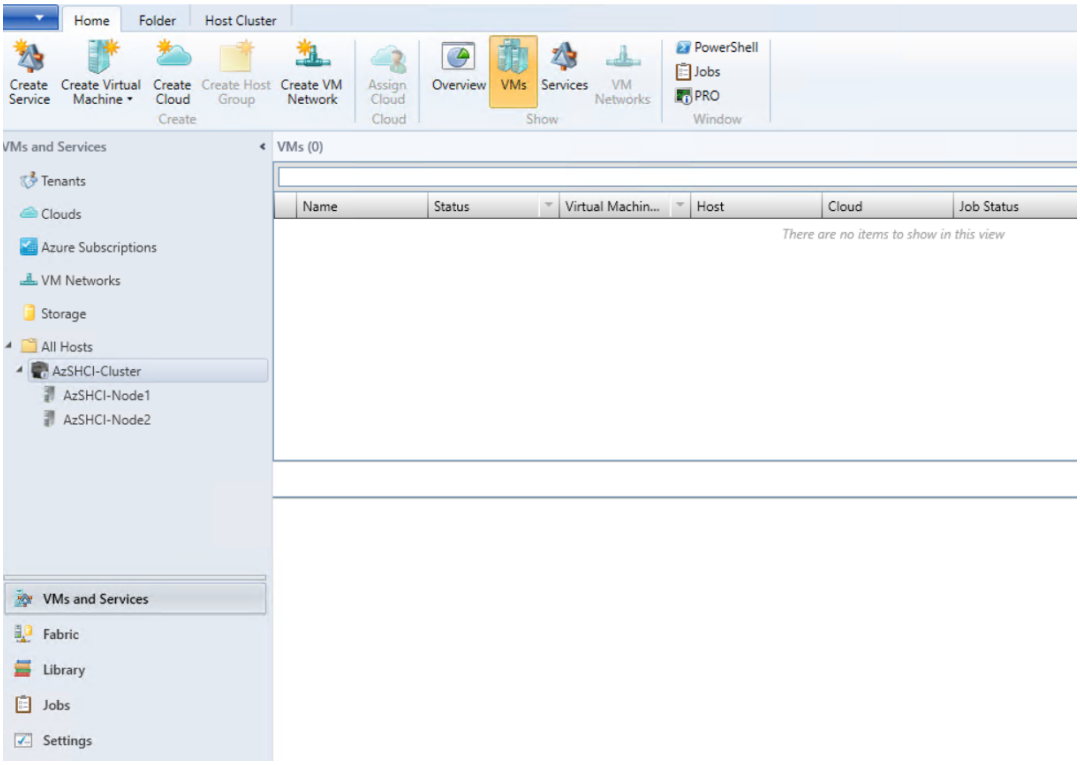
    b) En la página **Settings** de la consola de VMM, cree una cuenta de ejecución.



c) Ejecute estos comandos de PowerShell con privilegios de administrador en el servidor de SCVMM para agregar el clúster de Azure Stack HCI como host:

```
$runAsAccountName = 'Admin'
$runAsAccount = Get-SCRunAsAccount -Name $runAsAccountName
$hostGroupName = 'All Hosts'
$hostGroup = Get-SCVMHostGroup -Name $hostGroupName
$hostCluster = 'FQDN of Azure Stack HCI cluster'
Add-SCVMHostCluster -Name $hostCluster -RunAsynchronously -
    VMHostGroup
$hostGroup -Credential $runAsAccount -RemoteConnectEnabled
    $true
```

d) Ahora podrá ver el clúster de Azure Stack HCI junto con los nodos en la consola de VMM.



e) Cree la conexión de host de SCVMM en la Web Studio y, a continuación, cree un catálogo de máquinas de MCS.

Qué hacer a continuación

- Instalar componentes principales
- Instalar VDA
- Crear un sitio
- Para crear y administrar una conexión en SCVMM, consulte Conexión con Microsoft System Center Virtual Machine Manager

Más información

- Crear y administrar conexiones y recursos
- Crear catálogos de máquinas

Entornos de virtualización de Nutanix

August 17, 2024

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.

Instalar y registrar el plug-in de Nutanix

Complete el procedimiento siguiente para instalar y registrar el plug-in de Nutanix en todos los Delivery Controllers. Use Citrix Studio para crear una conexión con Nutanix. A continuación, cree un catálogo de máquinas que utilice una instantánea de una imagen maestra creada en el entorno de Nutanix.

> **Sugerencia:**
>
> Le recomendamos que detenga y, a continuación, reinicie Citrix Host Service, Citrix Broker Service y Machine Creation Services cuando instale o actualice el plug-in de Nutanix.

Para obtener más información sobre cómo instalar el plug-in de Nutanix, consulte el sitio de la documentación de Nutanix.

Qué hacer a continuación

- Instalar componentes principales
- Instalar VDA
- Crear un sitio
- Para crear y administrar una conexión en entornos de Nutanix, consulte Conexión con Nutanix

Más información

- Crear y administrar conexiones y recursos
- Crear catálogos de máquinas

Soluciones de Nutanix Cloud y de partners

August 17, 2024

Citrix Virtual Apps and Desktops admite estas soluciones de Nutanix Cloud y de partners:

- Nutanix Cloud Clusters en AWS

Nutanix Cloud Clusters en AWS

Citrix Virtual Apps and Desktops admite Nutanix Cloud Clusters en AWS. Los clústeres de Nutanix simplifican la forma en que las aplicaciones se ejecutan en nubes privadas o en varias nubes públicas. Para obtener más información sobre Nutanix Cloud Clusters en AWS, consulte Nutanix Cloud Clusters on AWS Deployment and User Guide.

> **Sugerencia:**
>
> Esto proporciona la misma funcionalidad que un clúster local de Nutanix. Solo se admite un clúster único, *Prism Element*. Para obtener más información, consulte esto.

Requisitos

Necesita lo siguiente para utilizar Nutanix Clusters en AWS:

- Una cuenta de Nutanix.
- Una cuenta de AWS con estos permisos:
  - IAMFullAccess
  - AWSConfigRole
  - AWSCloudFormationFullAccess

Crear un Nutanix Cluster

Para crear un Nutanix Cluster:

1. Inicie sesión en su cuenta de Nutanix.
2. Busque la opción **Nutanix cluster** y haga clic en **Launch**. Se abre la **consola de Nutanix**. Para obtener más información, consulte Get Started with Nutanix Cluster on AWS.
3. Elija **Create a new VPC**.

El proceso de creación de clústeres puede fallar por estos errores:

- No se pudo crear el clúster en un tiempo determinado. Clúster en proceso de eliminación.
- Clúster de Nutanix del host: Nodo `XXXXXXXXXXX: Instance i-xxxxxxxxxxxxx: disable network interface source/dest check error.`
- Clúster de Nutanix del host: Nodo `XXXXXXXXXXX: Unable to obtain instance i-xxxxxxxxxxxxxx network interface info.`

Si el clúster no se pudo crear:

- Intente recrear uno en otra región.
- Asegúrese de eliminar Nutanix CloudFormation Stack (CFS) antes de intentarlo de nuevo.

Además de otros recursos, Nutanix CFS crea:

- 1 nube VPC denominada *Nutanix Cluster xxxxxxxxxxxx* 10.0.0.0/16
- 2 subredes: 10.0.128.0/24 y 10.0.129.0/24
- 1 puerta de enlace de Internet
- 1 puerta de enlace NAT

Una vez creado el clúster, obtenga la dirección de **Nutanix Prism**:

1. Vaya a la **consola de Nutanix**.
2. En la esquina superior derecha de la consola, pase el cursor sobre el enlace **Launch Prism Element** y copie la URL.

Qué hacer a continuación

- Instalar componentes principales
- Instalar VDA
- Crear un sitio
- Para crear y administrar una conexión con soluciones de Nutanix Cloud y de partners, consulte Conexión con soluciones de Nutanix Cloud y de partners

Más información

- Crear y administrar conexiones y recursos
- Crear catálogos de máquinas

Entornos de virtualización de VMware

August 17, 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). Al inhabilitar esta función, MCS no funciona correctamente.

Qué hacer a continuación

- Instalar componentes principales
- Instalar VDA
- Crear un sitio
- Para crear y administrar una conexión en entornos VMware, consulte Conexión con VMware

Más información

- Crear y administrar conexiones y recursos
- Crear catálogos de máquinas

Soluciones de VMware Cloud y de partners

August 17, 2024

Citrix Virtual Apps and Desktops admite estas soluciones de VMware Cloud y de partners:

- Azure VMware Solution (AVS)
- Google Cloud VMware Engine
- VMware Cloud en Amazon Web Services (AWS)

Integración de Azure VMware Solution (AVS)

Citrix Virtual Apps and Desktops Service es compatible con AVS. AVS proporciona una infraestructura de la nube que contiene clústeres de vSphere creados por la infraestructura de Azure. Aproveche Citrix Virtual Apps and Desktop Service para usar AVS en el aprovisionamiento de la carga de trabajo de VDA del mismo modo que utilizaría vSphere en entornos locales.

Configurar el clúster de AVS

Para permitir que Citrix Virtual Apps and Desktop Service use AVS, siga estos pasos en Azure:

- Solicitar una cuota del host
- Registrar el proveedor de recursos Microsoft.AVS
- Lista de comprobación para la red
- Crear una nube privada de Azure VMware Solution
- Acceder a una nube privada de Azure VMware Solution
- Configurar redes para la nube privada de VMware en Azure
- Configurar DHCP para Azure VMware Solution
- Agregar un segmento de red en Azure VMware Solution
- Comprobar el entorno de Azure VMware Solution

Solicitar una cuota del host para clientes del Contrato Enterprise de Azure En la página **Help + Support** de Azure Portal, seleccione **New support request** e incluya esta información:

- Issue type: Technical
- Subscription: Seleccione su suscripción
- Service:All services > Azure VMware Solution
- Resource: General question
- Summary: Need capacity
- Problem type: Capacity Management Issues
- Problem subtype: Customer Request for Additional Host Quota/Capacity

En el campo **Description** del tíquet de asistencia, incluya esta información en la ficha **Details**:

- POC or Production
- Region Name
- Number of hosts
- Cualquier otro detalle

> **Nota:**
>
> AVS requiere un mínimo de tres hosts y recomienda utilizar una redundancia de N+1 hosts.

Después de especificar los detalles del tíquet de asistencia, seleccione **Review + Create** para enviar la solicitud a Azure.

Registrar el proveedor de recursos Microsoft.AVS Después de solicitar la cuota del host, registre el proveedor de recursos:

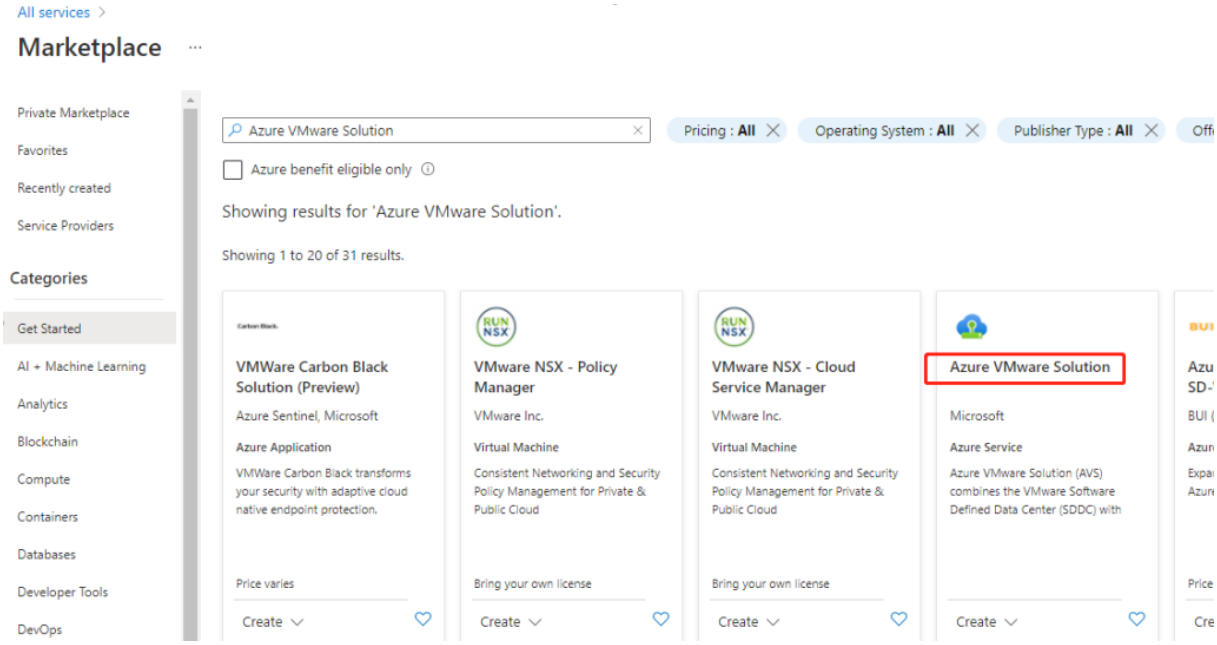
1. Inicie sesión en Azure Portal.

2. En el menú de Azure Portal, seleccione **All services**.
3. En el menú **All services**, introduzca la suscripción y seleccione **Subscriptions**.
4. Seleccione la suscripción de la lista de suscripciones.
5. Seleccione **Resource providers** e introduzca **Microsoft.AVS** en la barra de búsqueda.
6. Si el proveedor de recursos no está registrado, seleccione **Register**.

Consideraciones sobre las redes AVS ofrece servicios de red que requieren intervalos específicos de direcciones de red y puertos de firewall. Consulte Lista de comprobación del planeamiento de red para Azure VMware Solution para obtener más información.

Crear una nube privada de Azure VMware Solution Después de considerar los requisitos de red de su entorno, cree una nube privada de AVS:

1. Inicie sesión en Azure Portal.
2. Seleccione **Create a new resource**.
3. En el cuadro de texto **Search the Marketplace**, escriba *Azure VMware Solution* y seleccione **Azure VMware Solution** en la lista.



imagen

En la ventana **Azure VMware Solution**:

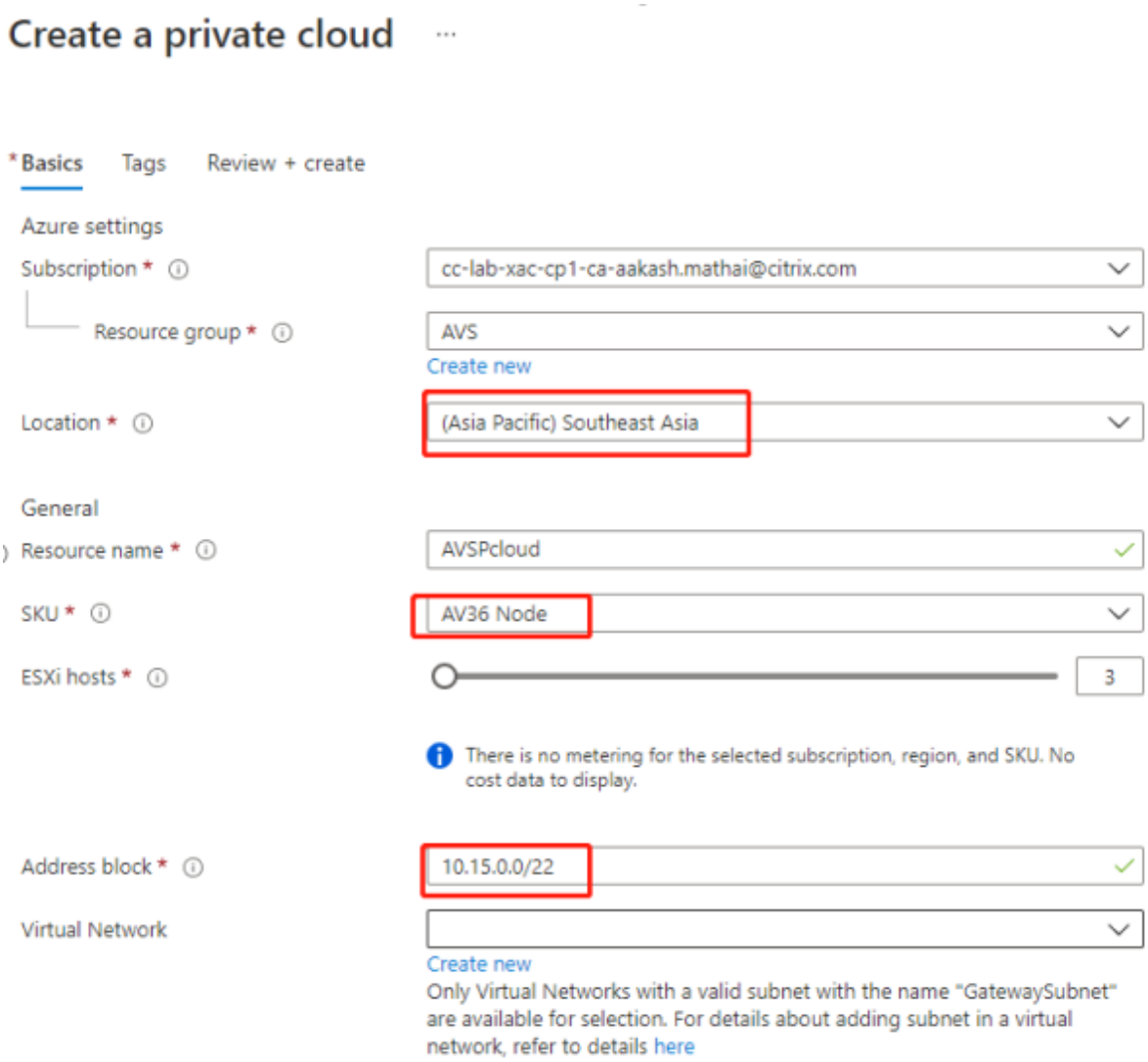
1. Seleccione **Create**.
2. Haga clic en la ficha **Basics**.
3. Introduzca valores para los campos mediante la información de esta tabla:

Campo	Valor
Subscription	Seleccione la suscripción que piensa utilizar para la implementación. Todos los recursos de una suscripción de Azure se facturan juntos.
Resource group	Seleccione el grupo de recursos de su nube privada. Un grupo de recursos de Azure es un contenedor lógico en el que se implementan y administran recursos de Azure. Si no, también puede crear otro grupo de recursos para su nube privada.
Location	Seleccione una ubicación, como East US. Esta es la región definida durante la fase de planificación.
Resource name	Proporcione el nombre de su nube privada de Azure VMware Solution.
SKU	Seleccione AV36.
Hosts	Muestra la cantidad de hosts asignados al clúster de nubes privadas. El valor predeterminado es 3, que se puede aumentar o reducir después de la implementación.
Address block	Proporciona un bloque de direcciones IP para la nube privada. La redirección CIDR representa la red de administración de nubes privadas y se utilizará para los servicios de administración de clústeres, como vCenter Server y NSX-T Manager. Utilice el espacio de direcciones /22; por ejemplo, 10.175.0.0/22. La dirección debe ser única y no solaparse con otras redes virtuales de Azure ni con redes locales.
Virtual Network	Deje esto en blanco porque el circuito ExpressRoute de Azure VMware Solution se establece como un paso posterior a la implementación.

En la pantalla **Create a private cloud**:

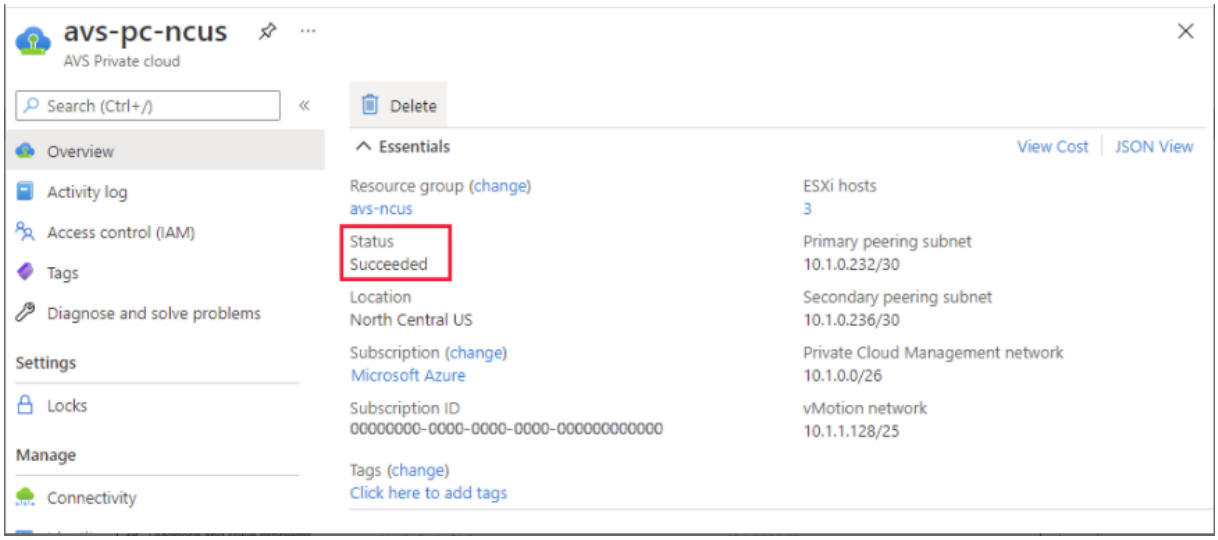
1. En el campo **Location**, seleccione la región que tiene el AVS; la región del grupo de recursos es la misma que la región de AVS.

2. En el campo **SKU**, seleccione **AV36 Node**.
3. Especifique una dirección IP en el campo **Address Block**. Por ejemplo, 10.15.0.0/22.
4. Seleccione **Review + Create**.
5. Tras revisar la información, haga clic en **Create**.



> **Sugerencia:**
>
> La creación de una nube privada puede tardar entre 3 y 4 horas. Agregar un único host al clúster puede tardar entre 30 y 45 minutos.

Compruebe que la implementación se haya realizado correctamente. Vaya al grupo de recursos que creó y seleccione su nube privada. Cuando **Status** pasa a **Succeeded**, la implementación se ha completado.



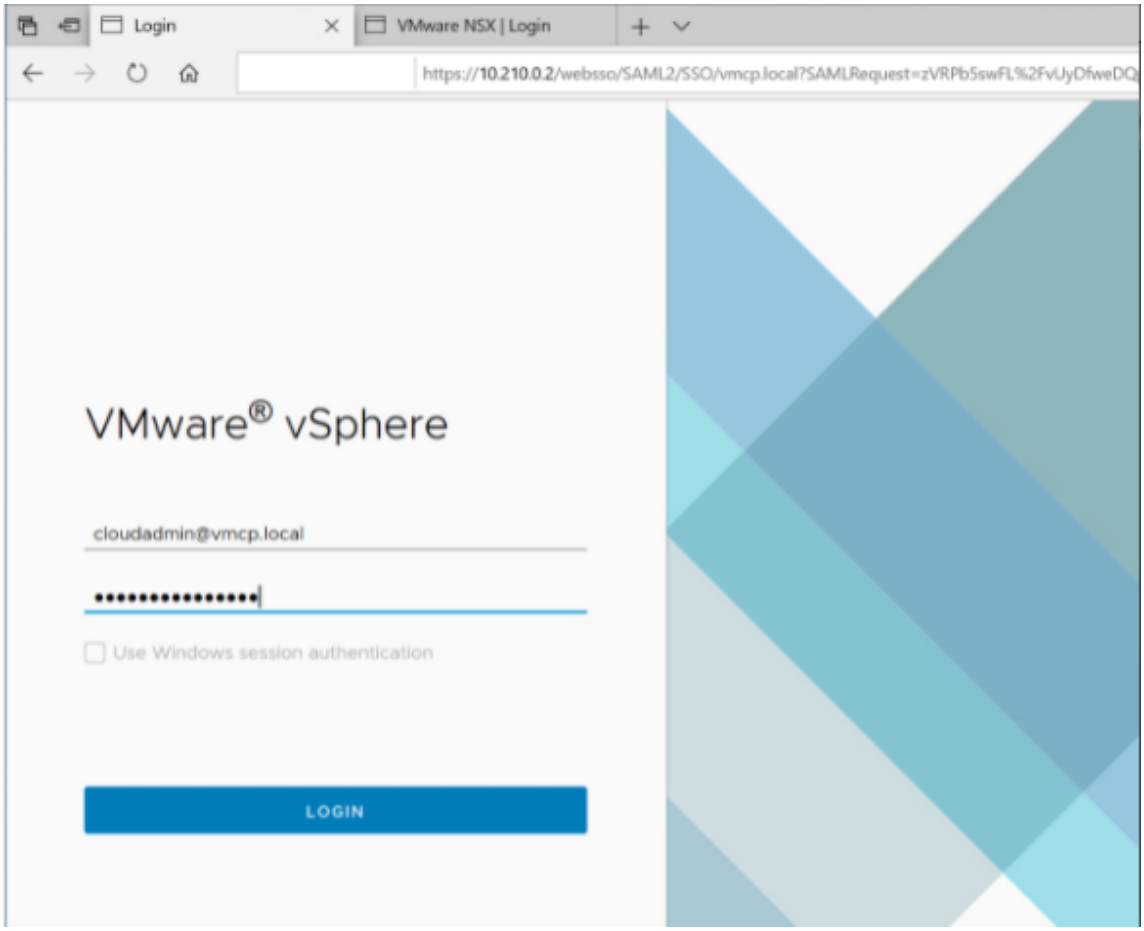
Acceder a una nube privada de Azure VMware Solution Una vez que haya creado una nube privada, cree una máquina virtual de Windows y conéctese al vCenter local de su nube privada.

Crear una máquina virtual de Windows

1. En el grupo de recursos, seleccione **+ Add**, busque **Microsoft Windows 10/2016/2019** y seleccione esa opción.
2. Haga clic en **Crear**.
3. Introduzca la información necesaria y, a continuación, seleccione **Review + Create**.
4. Una vez superada la validación, seleccione **Create** para iniciar el proceso de creación de máquinas virtuales.

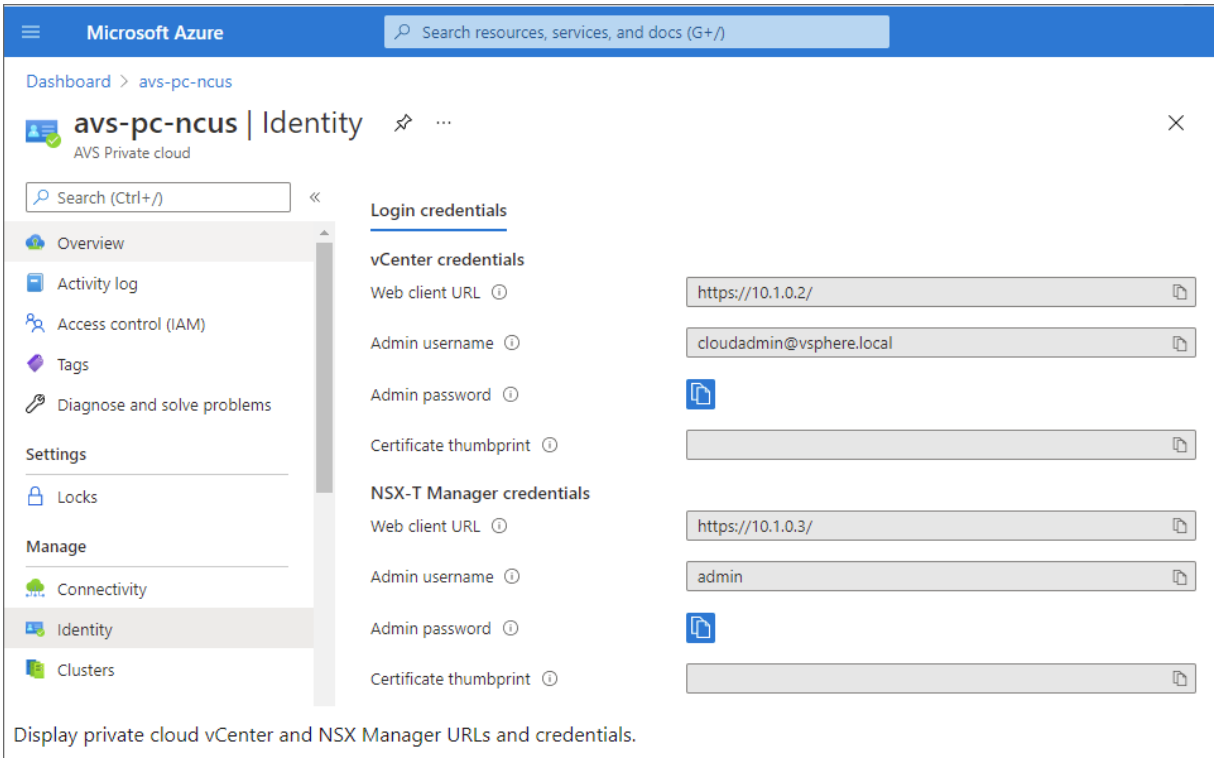
Conectarse al vCenter local de su nube privada

1. Inicie sesión en **vSphere Client con VMware vCenter SSO** como administrador de la nube.



2. En Azure Portal, seleccione su nube privada y, a continuación, **Manage > Identity**.

Aparecen las direcciones URL y las credenciales de usuario de vCenter y NSX-T Manager de la nube privada:



Display private cloud vCenter and NSX Manager URLs and credentials.

Tras confirmar las URL y las credenciales de usuario:

1. Vaya a la máquina virtual que creó en el paso anterior y conéctese a la máquina virtual.
2. En la máquina virtual de Windows, abra un explorador web y vaya a las URL de vCenter y NSX-T Manager en dos fichas del explorador. En la ficha de vCenter, introduzca las credenciales de usuario *cloudadmin@vmcp.local* del paso anterior.

Configurar redes para la nube privada de VMware en Azure Después de acceder a una nube privada de AVS, configure la red mediante la creación de una red virtual y una puerta de enlace.

Crear una red virtual

1. Inicie sesión en Azure Portal.
2. Vaya al grupo de recursos creado anteriormente.
3. Seleccione **+ Add** para definir un nuevo recurso.
4. En el cuadro de texto **Search the Marketplace**, escriba *virtual network*. Busque el recurso de red virtual y selecciónelo.
5. En la página **Virtual Network**, seleccione **Create** para configurar la red virtual de su nube privada.
6. En la página **Create Virtual Network**, introduzca los detalles de su red virtual.
7. En la ficha **Basics**, introduzca un nombre para la red virtual, seleccione la región adecuada y haga clic en **Next: IP Addresses**.

8. En la ficha **IP Addresses**, en el espacio de las direcciones IPv4, introduzca la dirección creada anteriormente.

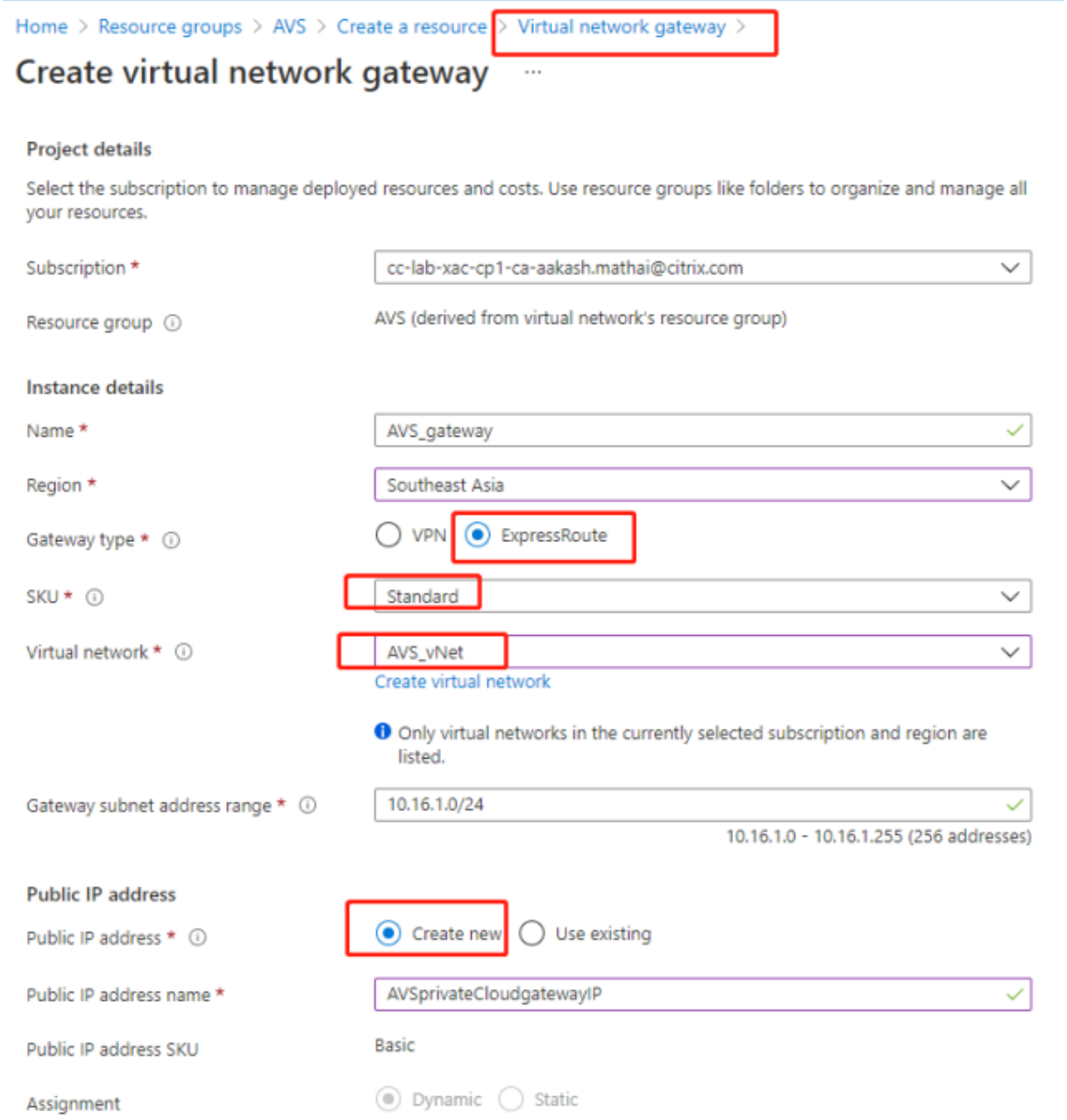
> **Importante:**
>
> Utilice una dirección que no se superponga con el espacio de direcciones que utilizó al crear su nube privada.

Después de introducir el espacio de direcciones:

1. Seleccione **+ Add subnet**.
2. En la página **Add subnet**, asigne a la subred un nombre y a un intervalo de direcciones adecuado.
3. Haga clic en **Add.**
4. Seleccione **Review + Create**.
5. Compruebe la información y haga clic en **Create**. Una vez finalizada la implementación, la red virtual aparece en el grupo de recursos.

Crear una puerta de enlace de red virtual Después de crear una red virtual, cree una puerta de enlace de red virtual.

1. En el grupo de recursos, seleccione **+ Add** para agregar un nuevo recurso.
2. En el cuadro de texto **Search the Marketplace**, escriba *virtual network gateway*. Busque el recurso de red virtual y selecciónelo.
3. En la página **Virtual Network Gateway**, haga clic en **Create**.
4. En la ficha **Basics** de la página **Create virtual network gateway**, proporcione valores en cada campo.
5. Haga clic en **Review + Create**.

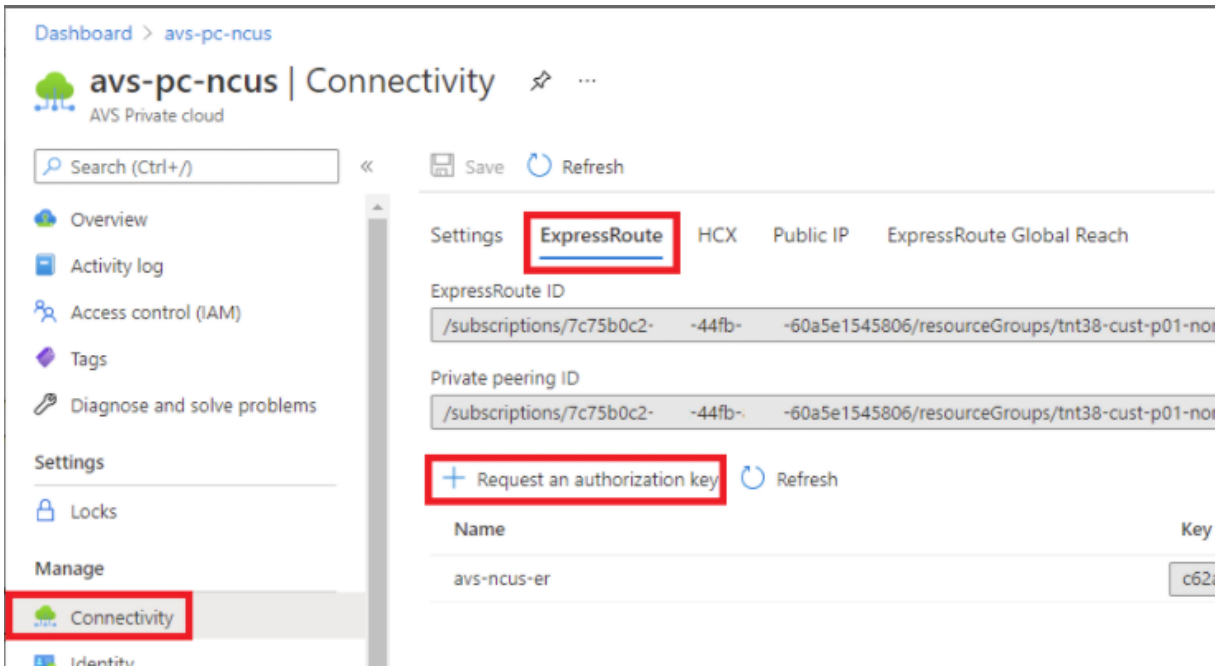


Tras revisar la configuración de la puerta de enlace de red virtual, haga clic en **Create** para implementar la puerta de enlace de red virtual.
Una vez finalizada la implementación, conecte su conexión de **ExpressRoute** a la puerta de enlace de red virtual que contiene la nube privada de AVS.

Conectar ExpressRoute a la puerta de enlace de red virtual Después de implementar una puerta de enlace de red virtual, agregue una conexión entre esta y la nube privada de AVS:

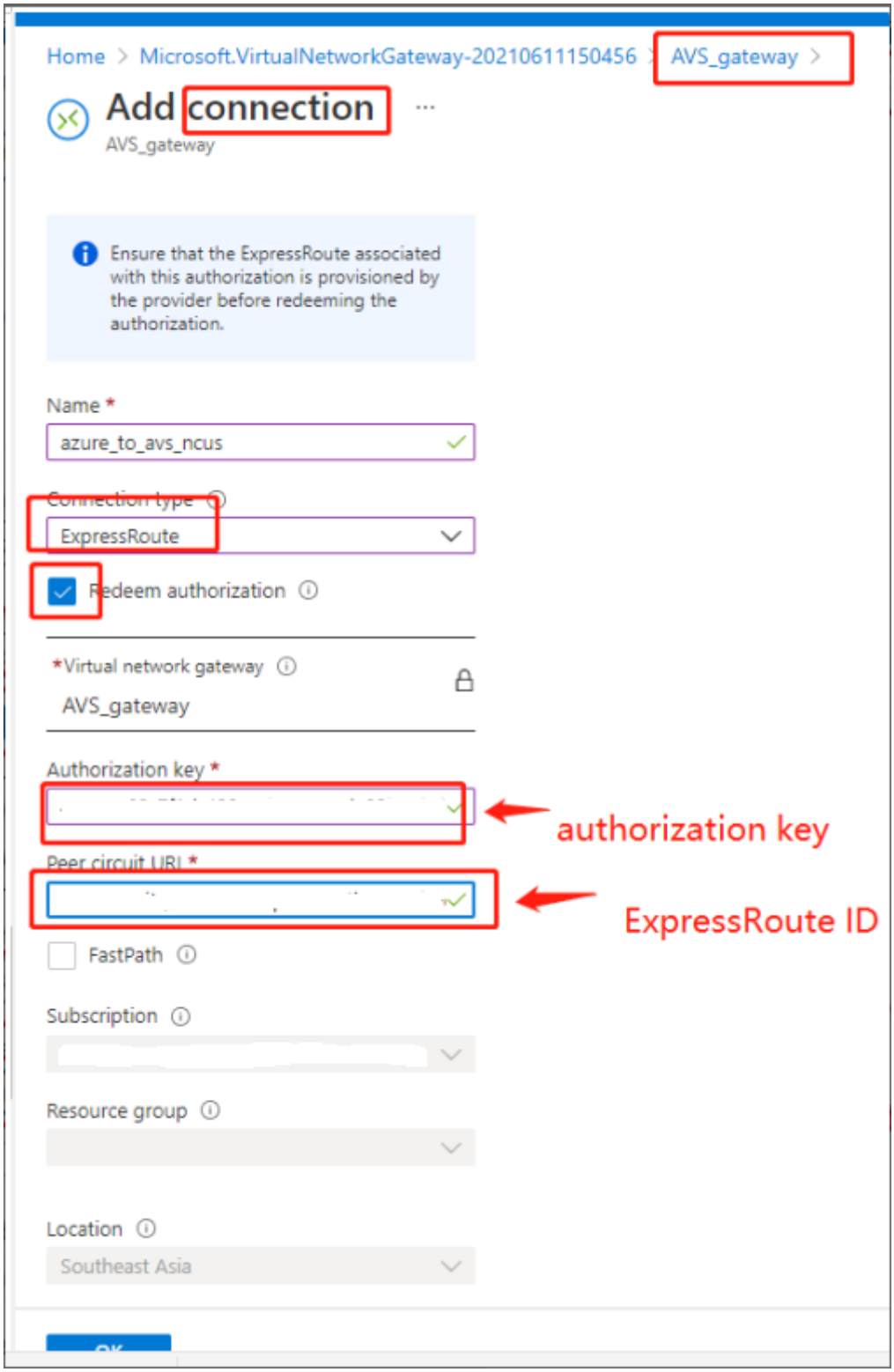
1. Solicite una clave de autorización de ExpressRoute.

2. En Azure Portal, vaya a la **nube privada de Azure VMware Solution**. Seleccione **Manage > Connectivity > ExpressRoute** y, a continuación, seleccione **+ Request an authorization key**.

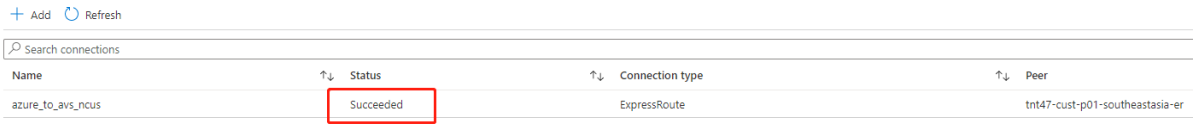


Después de solicitar una clave de autorización:

1. Introduzca un nombre para la clave y haga clic en **Create**. La creación de la clave puede tardar unos 30 segundos. Una vez creada, la nueva clave aparece en la lista de claves de autorización de la nube privada.
2. Copie la **clave de autorización** y el **ID de ExpressRoute**. Los necesitará para completar el proceso de emparejamiento. La clave de autorización desaparece después de un tiempo, así que cópiela en cuanto aparezca.
3. Vaya a la **puerta de enlace de red virtual** que piensa utilizar y seleccione **Connections > + Add**.
4. En la página **Add connection**, proporcione valores en cada campo y seleccione **OK**.



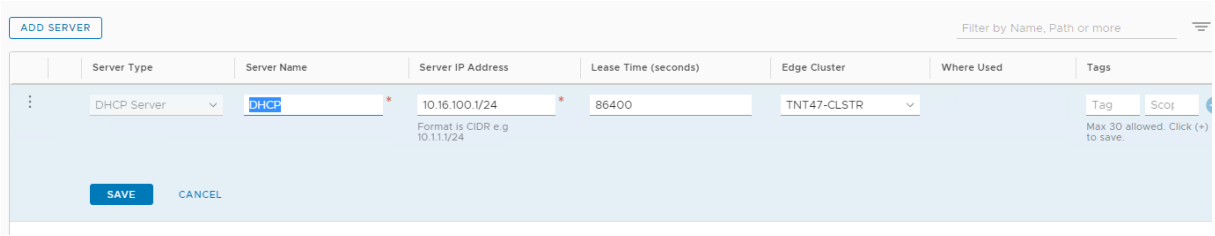
La conexión se establece entre el circuito de ExpressRoute y la red virtual:



Configurar DHCP para Azure VMware Solution Después de conectar ExpressRoute a la puerta de enlace virtual, configure DHCP.

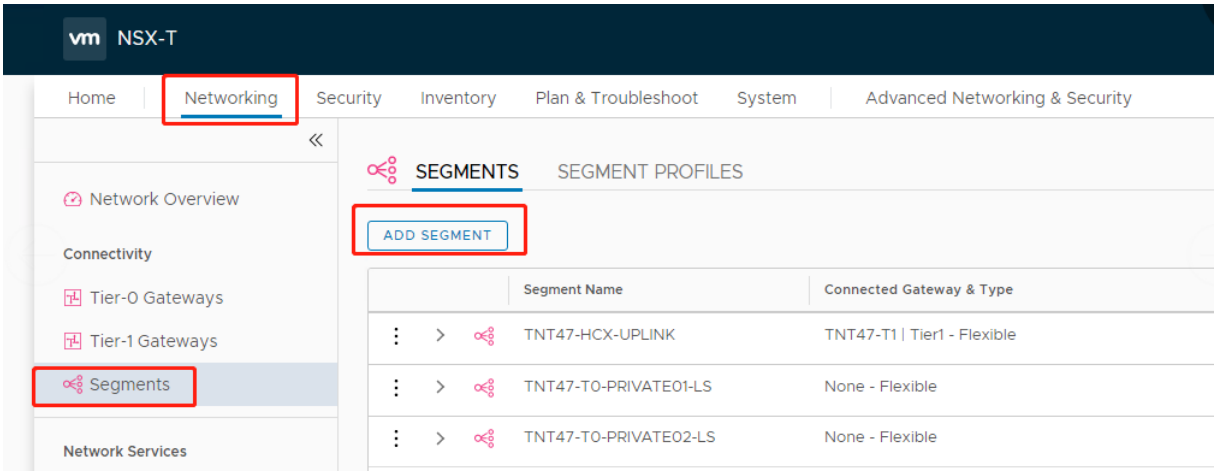
Usar NSX-T para alojar el servidor DHCP En NSX-T Manager:

1. Seleccione **Networking > DHCP** y, a continuación, seleccione **Add Server**.
2. Seleccione **DHCP** para **Server Type**, proporcione el nombre del servidor y la dirección IP.
3. Haga clic en **Guardar**.
4. Seleccione **Tier 1 Gateways**, seleccione los puntos suspensivos en vertical de la puerta de enlace de nivel 1 y, a continuación, seleccione **Edit**.
5. Seleccione **No IP Allocation Set** para agregar una subred.
6. Seleccione **DHCP Local Server** para **Type**.
7. Para **DHCP Server**, seleccione **Default DHCP** y, a continuación, haga clic en **Save**.
8. Haga clic en **Save** de nuevo y seleccione **Close Editing**.



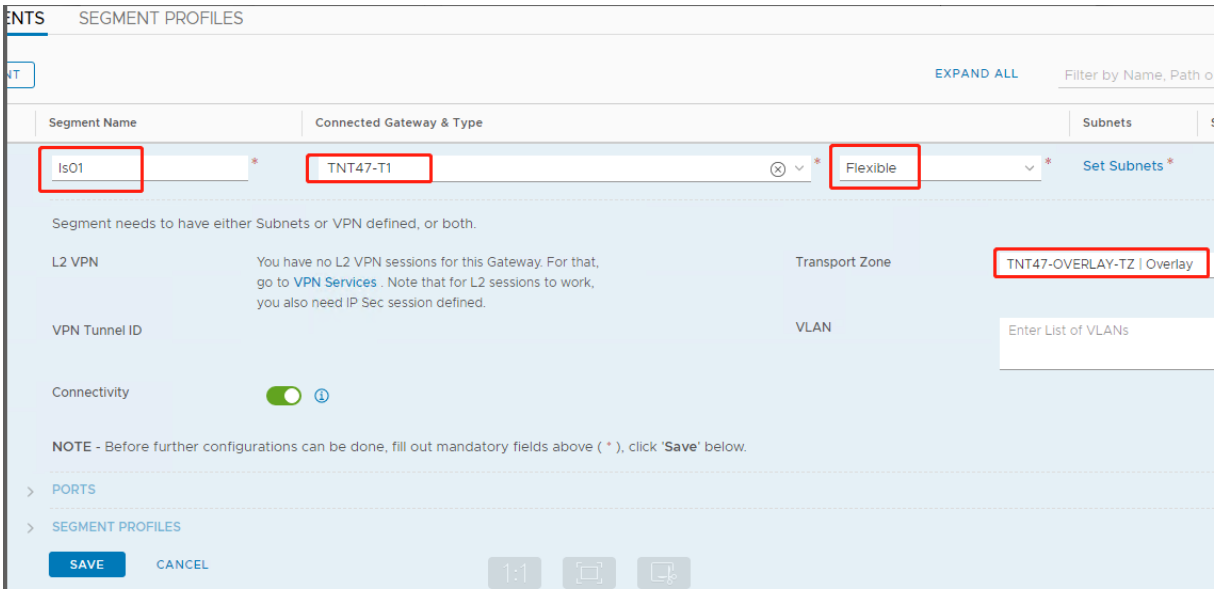
Agregar un segmento de red en Azure VMware Solution Después de configurar DHCP, agregue un segmento de red.

Para agregar un segmento de red, en NSX-T Manager, seleccione **Networking > Segments** y, a continuación, haga clic en **Add Segment**.



En la pantalla **Segments profile**:

1. Introduzca un **nombre** para el segmento.
2. Seleccione **Tier-1 Gateway (TNTxx-T1)** como **Connected Gateway** y deje **Type** como **Flexible**.
3. Seleccione la superposición preconfigurada **Transport Zone(TNTxx-OVERLAY-TZ)**.
4. Haga clic en **Set Subnets**.



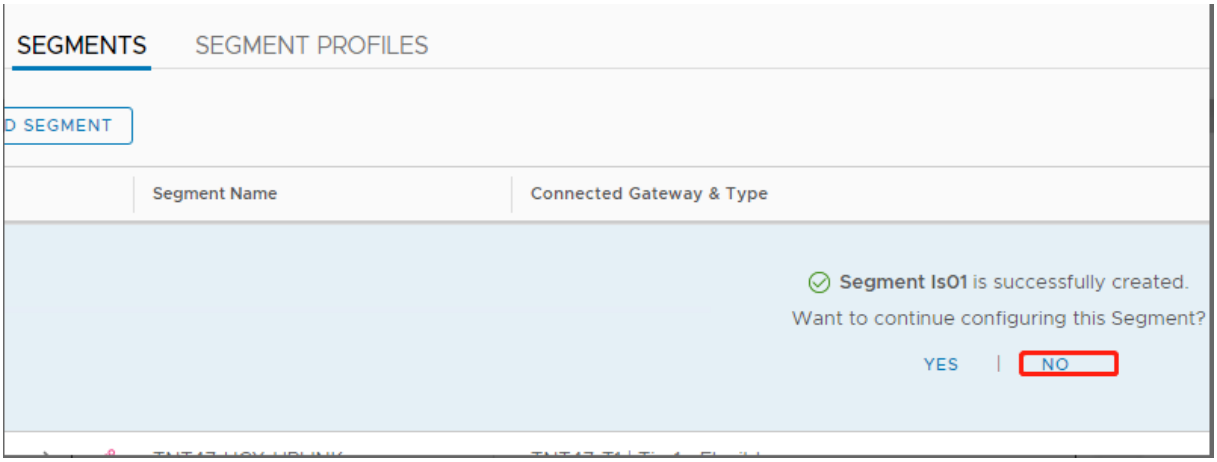
En la sección **Subnets**:

1. Introduzca la dirección IP de la puerta de enlace.
2. Seleccione **Add**.

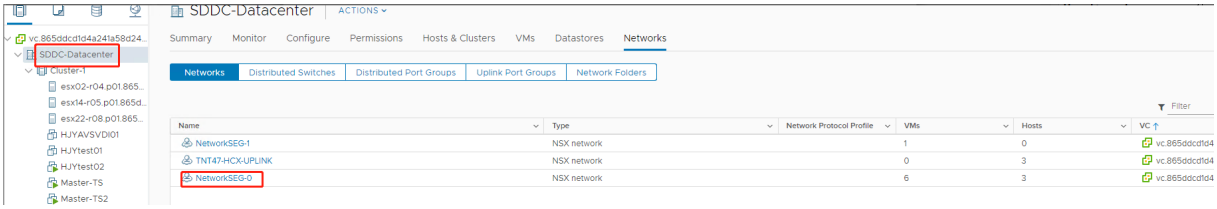
> **Importante:**
>
> La dirección IP de este segmento debe pertenecer a la dirección IP de la puerta de enlace de Azure, 10.15.0.0/22.

El intervalo de DHCP debe pertenecer a la dirección IP del segmento:

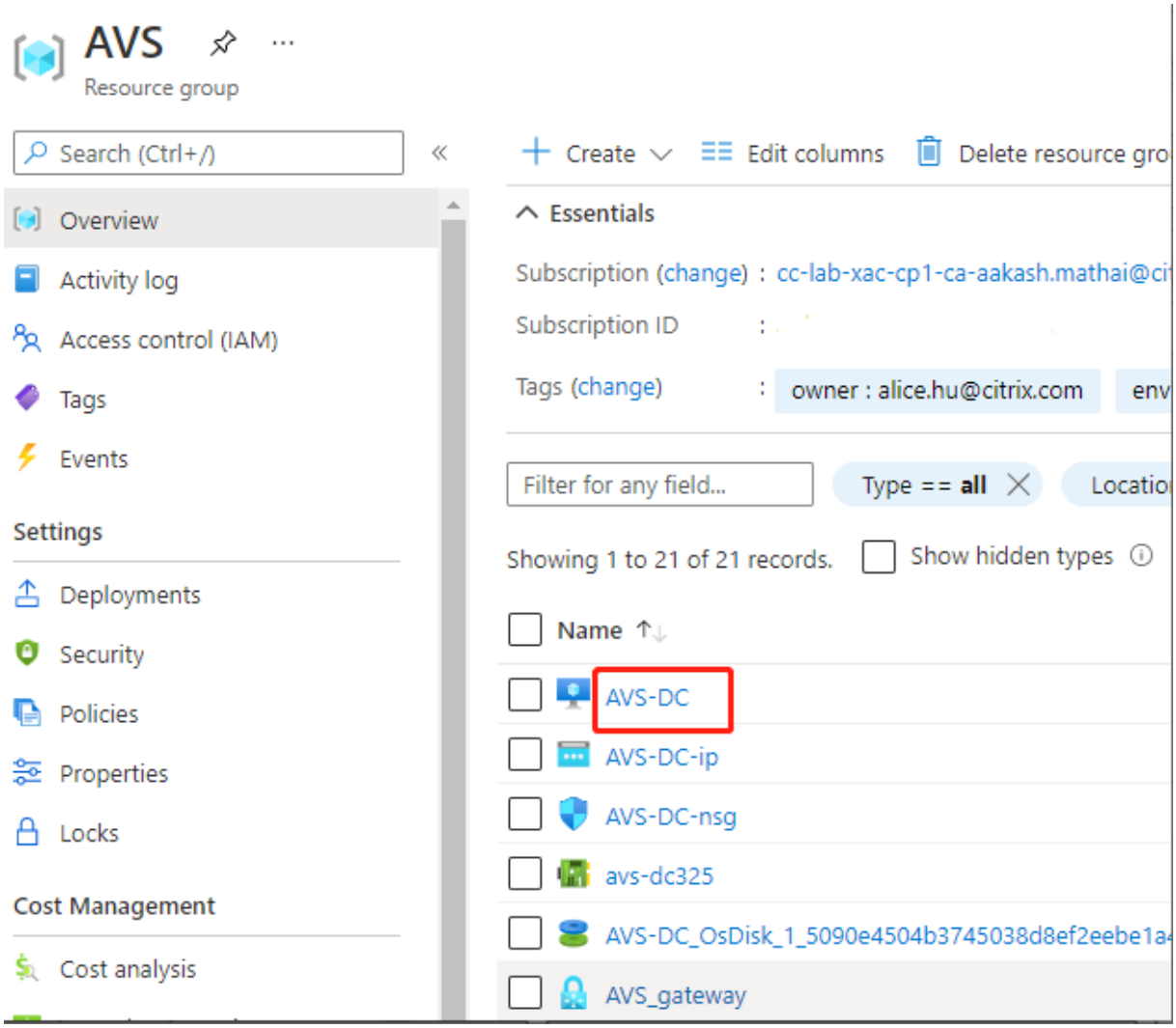
Seleccione **No** para no seguir configurando el segmento:



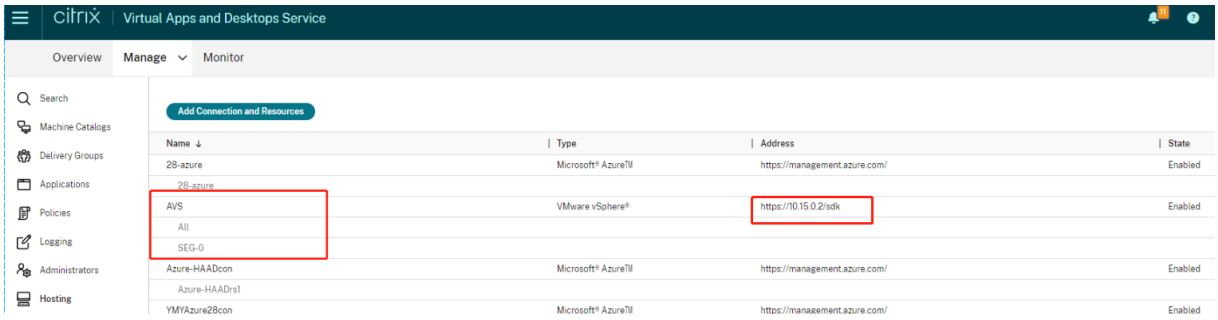
En vCenter, seleccione **Networking > SDDC-Datacenter**:



Verificar el entorno de AVS Configure una conexión directa y un conector en el grupo de recursos de Azure:



Compruebe la conexión con las credenciales de vCenter:



Google Cloud VMware Engine

Citrix Virtual Apps and Desktops le permite migrar cargas de trabajo de Citrix locales basadas en VMware a VMware Engine de Google Cloud.

Configurar Google Cloud VMware Engine

En el siguiente procedimiento, se describe cómo adquirir y configurar un clúster en Google Cloud VMware Engine.

Acceder al portal de VMware Engine

1. En la **consola de Google Cloud**, haga clic en el menú de navegación.
2. En la sección **Compute**, haga clic en **VMware Engine** para abrir VMware Engine en una nueva ficha de explorador.

Requisitos para crear la primera nube privada Debe tener acceso a Google Cloud VMware Engine, a la cuota de nodos de VMware Engine disponible y a un rol de IAM apropiado. Prepare los siguientes requisitos antes de seguir creando su nube privada:

1. Solicite acceso a la API y a la cuota de nodos. Para obtener más información, consulte Requesting API access and quota.
2. Anote los rangos de direcciones que quiere usar con los dispositivos de administración de VMware y la red de implementación de HCX. Para obtener más información, consulte Networking requirements.
3. Obtenga el rol de "administrador de servicios de VMware Engine"de IAM.

Crear la primera nube privada

1. Acceda al portal de VMware Engine.
2. En la página de inicio de VMware Engine, haga clic en **Create a private cloud**. Se indican la ubicación de alojamiento y los tipos de nodos de hardware.
3. Seleccione el número de nodos para la nube privada. Se requieren al menos tres nodos.
4. Introduzca un rango de enrutamiento CIDR para la red de administración de VMware.
5. Introduzca un rango de enrutamiento CIDR para la red de implementación de HCX.

   > **Importante:**
   >
   > El rango de enrutamiento CIDR no debe superponerse con ninguna de sus subredes locales o en la nube. El rango de enrutamiento CIDR debe ser /27 o superior.

6. Seleccione **Review and create**.
7. Revise la configuración. Para cambiar cualquier parámetro, haga clic en **Back**.
8. Haga clic en **Create** para empezar a crear la nube privada.

A medida que VMware Engine crea su nueva nube privada, implementa varios componentes de VMware y establece directivas de Autoscale iniciales para los clústeres de la nube privada. La creación de una nube privada puede tardar entre 30 minutos y 2 horas. Cuando se complete el aprovisionamiento, recibirá un correo electrónico.

Configurar la puerta de enlace de VPN de Google Cloud VMware Engine Para establecer una conectividad inicial con Google Cloud VMware Engine, puede usar una puerta de enlace de VPN. Se trata de una VPN cliente basada en OpenVPN con la que puede conectarse a su vCenter SDDC (centro de datos definido por software) de VMware y realizar cualquier configuración inicial necesaria.

Antes de implementar la puerta de enlace de VPN, configure el rango de **servicios perimetrales** para la región en la que se implementa el SDDC. Para hacerlo:

1. Inicie sesión en el portal de **Google Cloud VMware Engine** y vaya a **Network > Regional Settings**. Haga clic en **Add Region**.
2. Elija la región en la que se implementa el SDDC y habilite el **acceso a Internet** y el **servicio de IP pública**.
3. Suministre la gama de servicios perimetrales indicada durante la planificación y haga clic en **Submit**. La activación de estos servicios tarda entre 10 y 15 minutos.

   Una vez completado el proceso, los servicios perimetrales se muestran como **habilitados** en la página Regional Settings. La habilitación de estos parámetros permite asignar direcciones IP públicas al SDDC, que es un requisito para implementar una puerta de enlace de VPN.

Para implementar una puerta de enlace de VPN:

1. En el portal de **Google Cloud VMware Engine**, vaya a **Network > VPN Gateways**. Haga clic en **Create New VPN Gateway**.
2. Proporcione el nombre de la puerta de enlace de VPN y la subred del cliente reservadas durante la planificación. Haga clic en **Siguiente**.
3. Seleccione usuarios a los que conceder acceso a la VPN. Haga clic en **Siguiente**.
4. Especifique las redes que deben ser accesibles a través de VPN. Haga clic en **Siguiente**.
5. Se muestra una pantalla de resumen. Verifique las opciones seleccionadas y haga clic en **Submit** para crear la puerta de enlace de VPN. Se muestra la página VPN Gateways con la nueva puerta de enlace VPN con el estado **Creating**.
6. Cuando el estado cambie a **Operational**, haga clic en la nueva puerta de enlace de VPN.
7. Haga clic en **Download my VPN configuration** para descargar un archivo ZIP que contiene perfiles OpenVPN preconfigurados para la puerta de enlace de VPN. Hay disponibles perfiles para conectarse a través de UDP/1194 y TCP/443. Elija su preferencia e impórtela en Open VPN. A continuación, conéctese.
8. Vaya a **Resources** y seleccione su SDDC.

Conectar la VPN

1. Establezca una conexión de punto a sitio entre su red local y la nube privada mediante la configuración de VPN Gateway. Consulte Configurar la puerta de enlace de VPN de Google Cloud VMware Engine.
2. Cargue la configuración de VPN descargada en Configurar la puerta de enlace de VPN de Google Cloud VMware Engine.
3. Importe a su cliente VPN, por ejemplo, OpenVPN Connect.

Para obtener más información, consulte Connecting using VPN.

Crear la primera subred

Acceder a NSX-T Manager desde el portal de VMware Engine El proceso de creación de una subred se produce en NSX-T, al que se accede a través de VMware Engine. Haga lo siguiente para acceder a NSX-T Manager.

1. Inicie sesión en el portal de **Google Cloud VMware Engine**.
2. En el menú de navegación principal, vaya a **Resources**.
3. Haga clic en el **nombre de la nube privada** en la que quiere crear la subred.
4. En la página de detalles de la nube privada, haga clic en la ficha **vSphere Management Network**.
5. Haga clic en el **nombre de dominio completo** correspondiente a NSX-T Manager.
6. Cuando se le indique, introduzca sus credenciales de inicio de sesión. Si ha configurado vIDM y lo ha conectado a un origen de identidad, como Active Directory, use sus credenciales de origen de identidad en su lugar.

   > **Aviso:**
   >
   > Puede recuperar las credenciales generadas en la página de detalles de la nube privada.

Configurar el servicio DHCP para la subred Antes de crear una subred, configure un servicio DHCP:

En NSX-T Manager:

1. Vaya a **Networking > DHCP**. El panel de mandos de redes muestra que el servicio DHCP crea una puerta de enlace de nivel 0 y una de nivel 1.
2. Para comenzar a aprovisionar un servidor DHCP, haga clic en **Add Server**.
3. Seleccione **DHCP** para **Server Type**, proporcione el nombre del servidor y la dirección IP.

4. Haga clic en **Save** para crear el servicio DHCP.

Haga lo siguiente para conectar este servicio DHCP a la puerta de enlace de nivel 1 correspondiente. El servicio DHCP ya ha aprovisionado una puerta de enlace de nivel 1 predeterminada:

1. Seleccione **Tier 1 Gateways**, seleccione los puntos suspensivos en vertical de la puerta de enlace de nivel 1 y, a continuación, seleccione **Edit**.
2. En el campo **IP Address Management**, seleccione **No IP Allocation Set**.
3. Seleccione **DHCP Local Server** para **Type**.
4. Seleccione el servidor DHCP que creó para **DHCP Server**.
5. Haga clic en **Guardar**.
6. Haga clic en **Close Editing**.

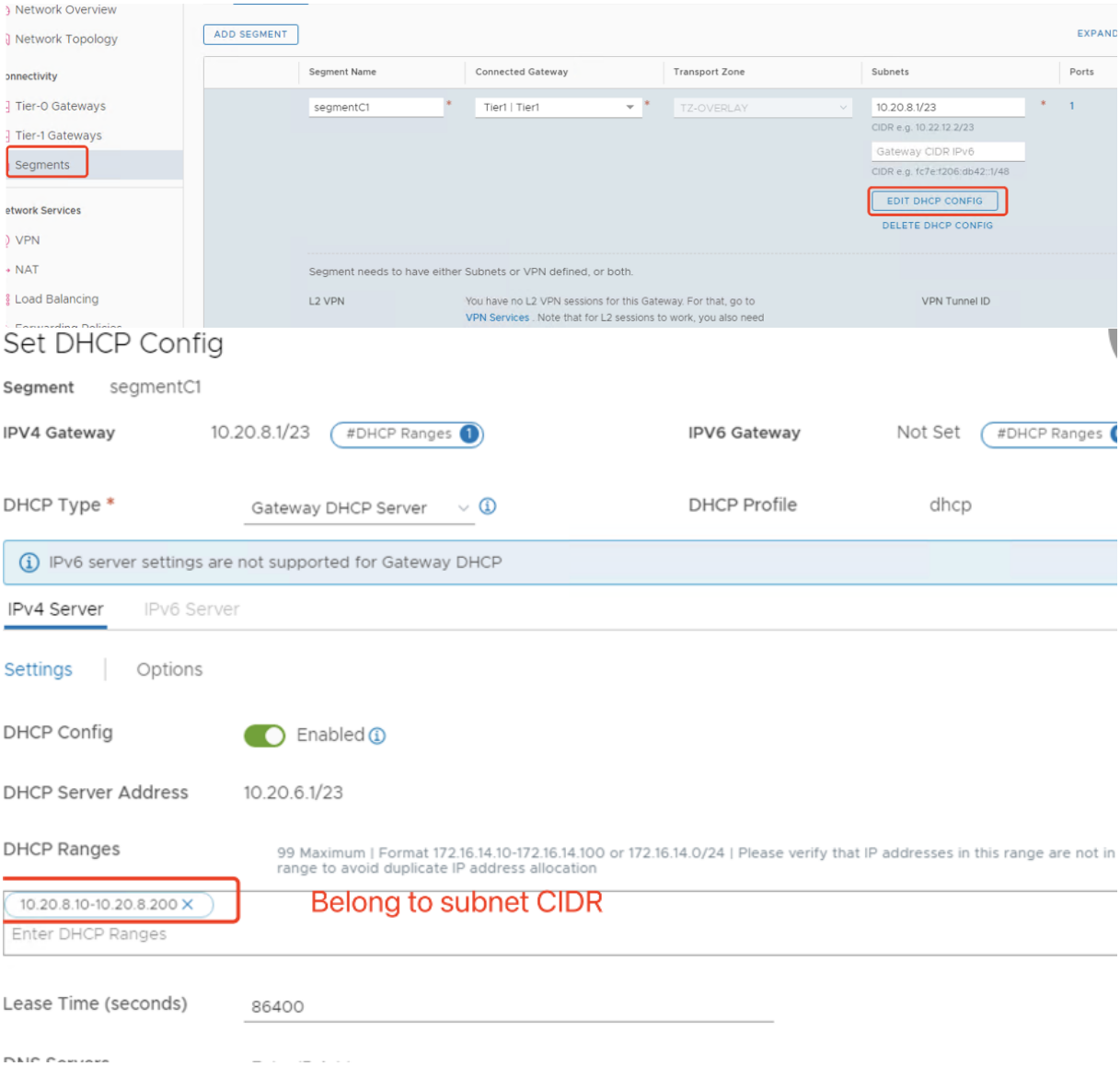
Ahora puede crear un segmento de red en NSX-T. Para obtener más información sobre DHCP en NSX-T, consulte la documentación de VMware para DHCP.

Crear un segmento de red en NSX-T Para las VM de carga de trabajo, cree subredes como segmentos de red de NSX-T para su nube privada:

1. En NSX-T Manager, vaya a **Networking > Segments**.
2. Haga clic en **Add Segment**.
3. Introduzca un nombre para el segmento.
4. Seleccione **Tier -1** como **Connected Gateway** y deje Type como **Flexible**.
5. Haga clic en **Set Subnets**.
6. Haga clic en **Add Subnets**.
7. En **Gateway IP/Prefix Length**, introduzca el rango de subredes. Especifique el rango de subredes con **.1** como último octeto. Por ejemplo, **10.12.2.1/24**.
8. Especifique los rangos de DHCP y haga clic en **ADD**.
9. En **Transport Zone**, seleccione **TZ-OVERLAY** en la lista desplegable.
10. Haga clic en **Guardar**. Ahora puede seleccionar este segmento de red en vCenter al crear una VM.

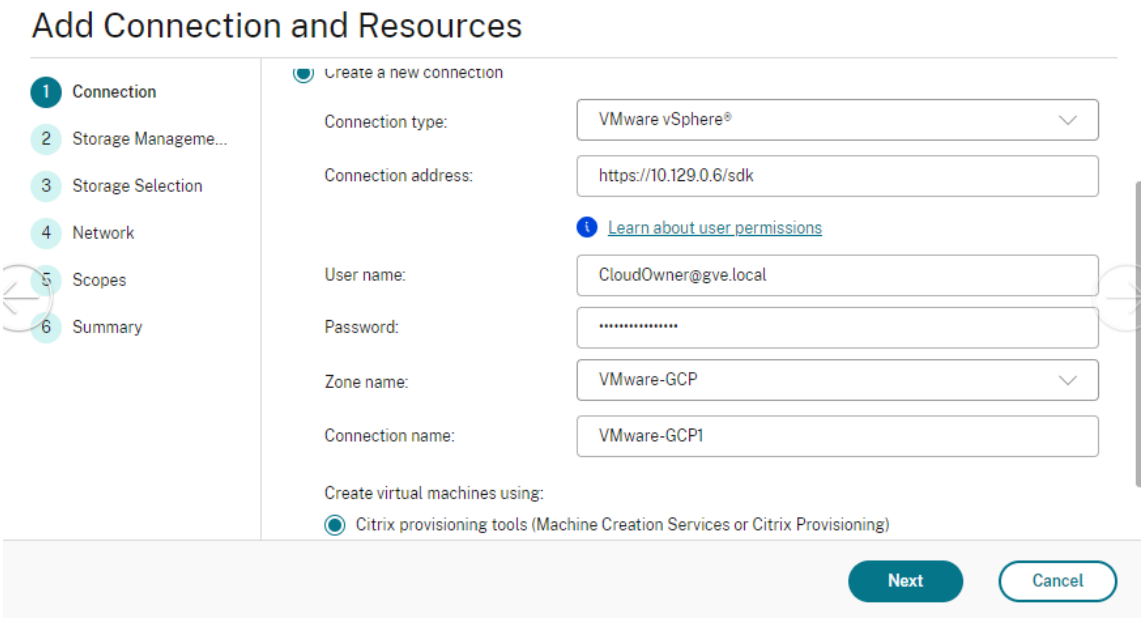
En una región determinada, puede configurar como máximo 100 rutas únicas desde VMware Engine a su red de VPC mediante el acceso a servicios privados. Esto incluye, por ejemplo, rangos de direcciones IP de administración de nube privada, segmentos de red de carga de trabajo de NSX-T y rangos de direcciones IP de red HCX. Este límite incluye todas las nubes privadas de la región.

> **Nota:**
>
> Existe un problema de configuración de Google Cloud por el que debe configurar el rango DHCP varias veces. Por lo tanto, asegúrese de configurar el rango DHCP después de la configuración de Google Cloud. Haga clic en **EDIT DHCP CONFIG** para configurar los rangos DHCP.



Crear la conexión de VMware de Google Cloud en Citrix Studio

1. Cree una máquina en vCenter.
2. Abra Citrix Studio.
3. Seleccione el nodo de alojamiento y haga clic en **Agregar conexión y recursos**.
4. En la pantalla **Conexión**, seleccione **Crear una nueva conexión** y los siguientes detalles:



a) Seleccione el **Tipo de conexión VMware vSphere**.
b) En **Dirección de la conexión**, introduzca la dirección IP privada de vCenter.
c) Introduzca las credenciales de vCenter.
d) Escriba un nombre para la conexión.
e) Elija la herramienta para crear máquinas virtuales.

5. En la pantalla **Red**, seleccione la subred creada en el servidor NSX-T.
6. Complete el asistente.

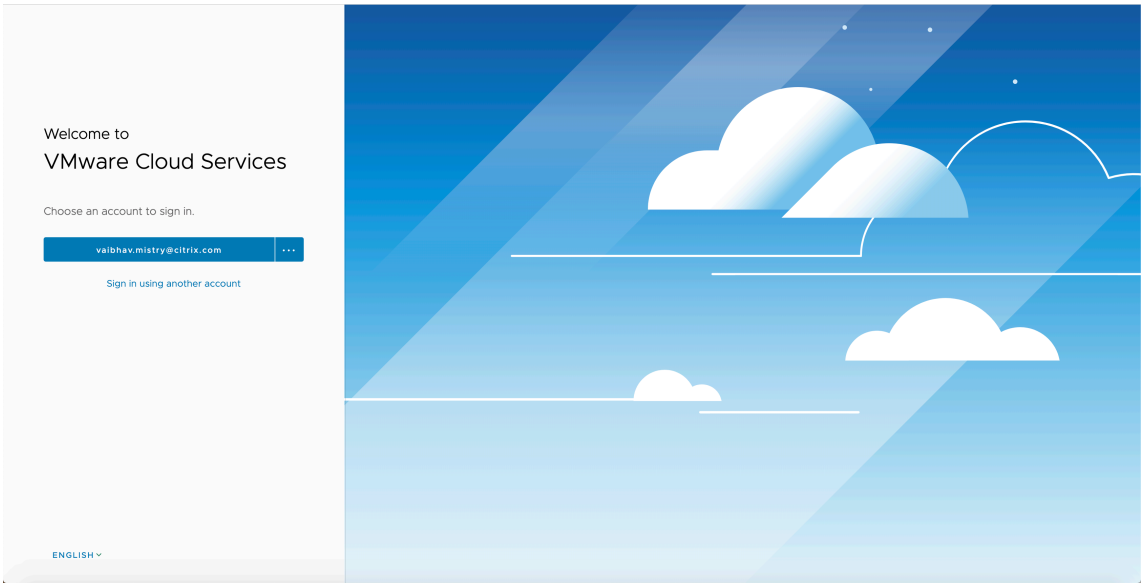
VMware Cloud en Amazon Web Services (AWS)

La nube de VMware en Amazon Web Services (AWS) le permite migrar las cargas de trabajo Citrix locales basadas en VMware a la nube de AWS.

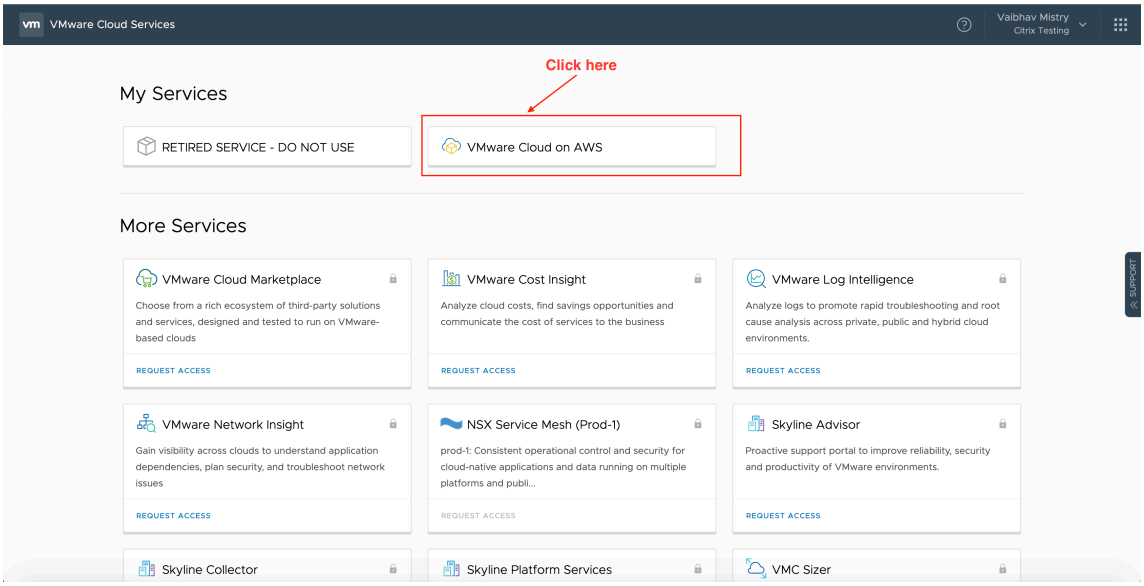
En este artículo se describe el procedimiento para configurar VMware Cloud en AWS.

Acceder al entorno de VMware Cloud

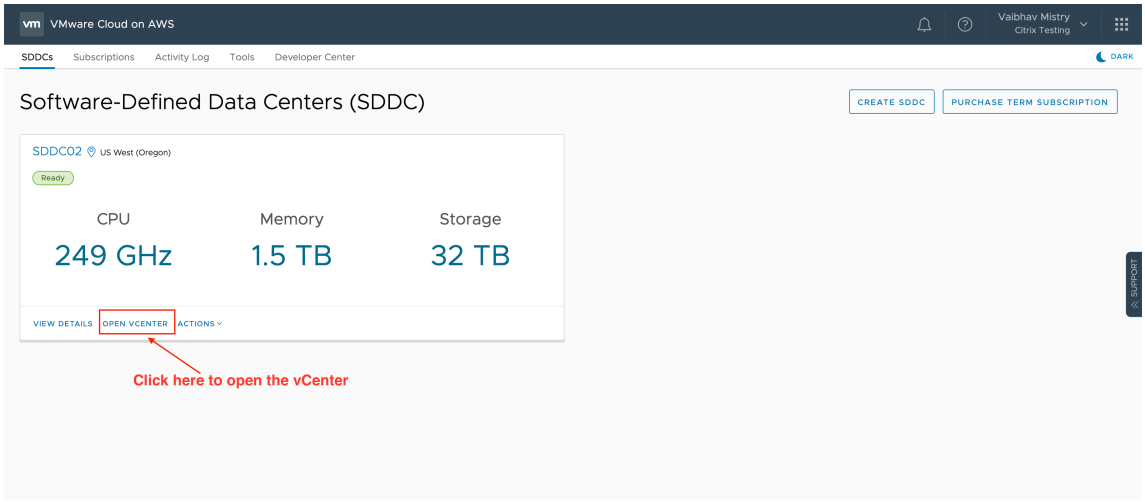
1. Inicie sesión en los servicios de VMware Cloud mediante la URL https://console.cloud.vmware.com/.

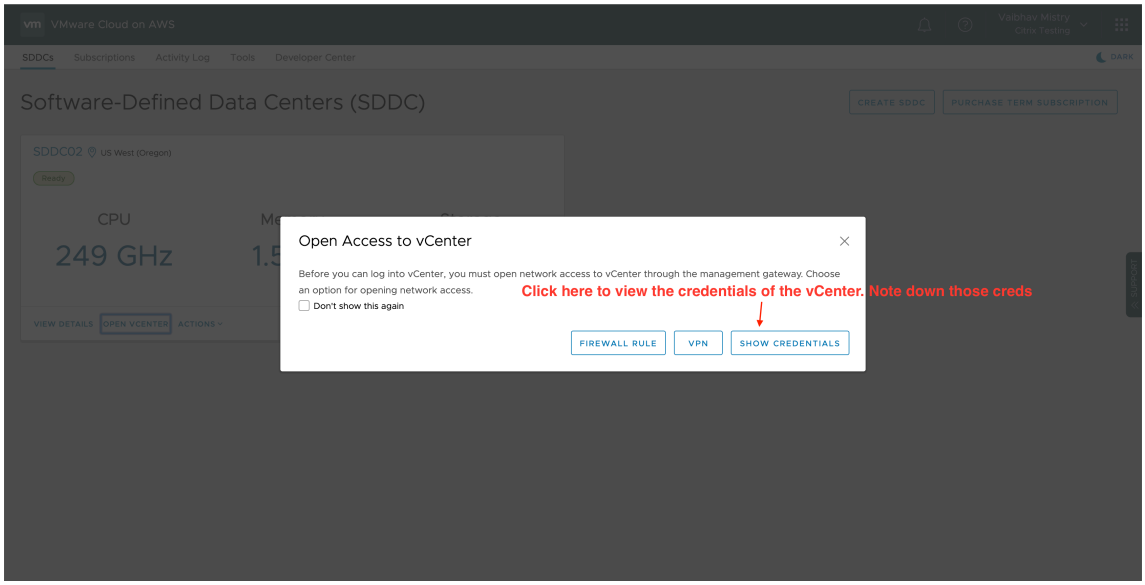


2. Haga clic en **VMware Cloud on AWS**. Aparecerá la página Software-Defined Data Centers (SDDC).

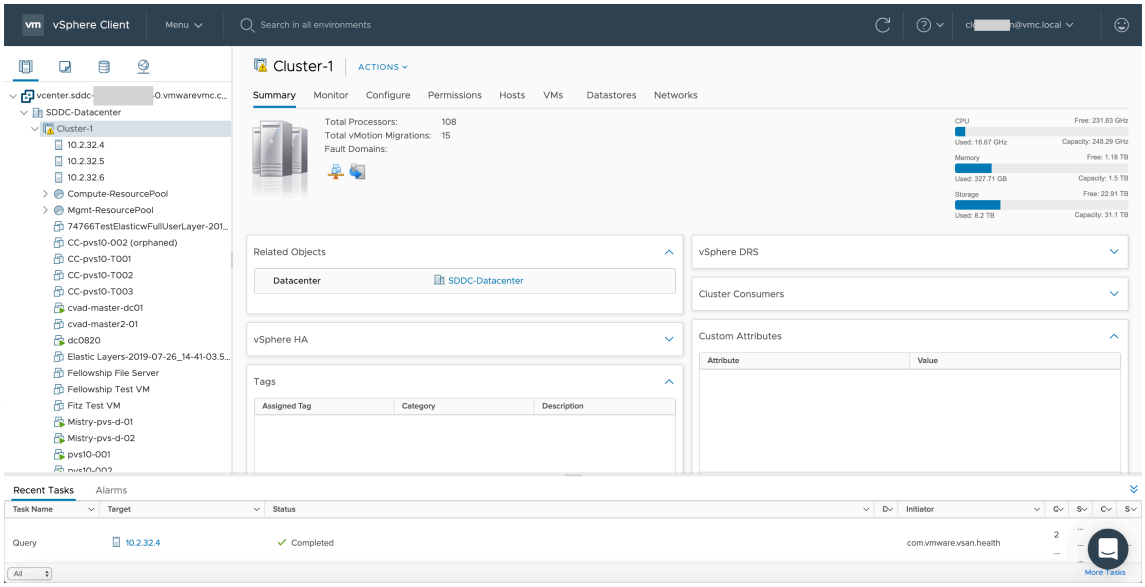


3. Haga clic en **OPEN VCENTER** y, a continuación, en **SHOW CREDENTIALS**. Anote las credenciales para usarlas más adelante.





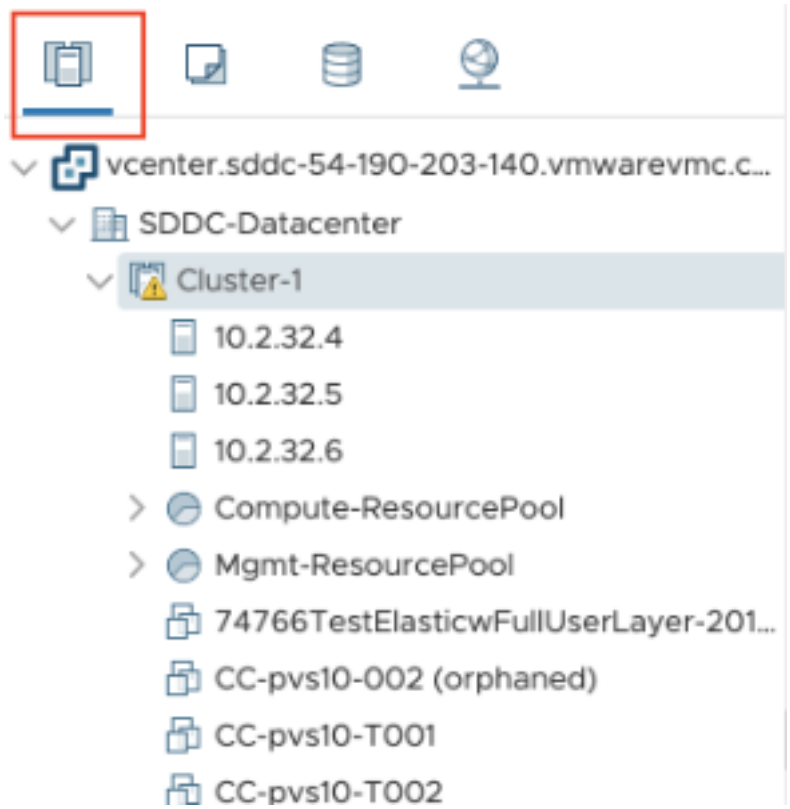
4. Abra un explorador web e introduzca la URL de vSphere Web Client.
5. Introduzca las credenciales anotadas y haga clic en **Login**. La página web del cliente de vSphere es similar al entorno local.



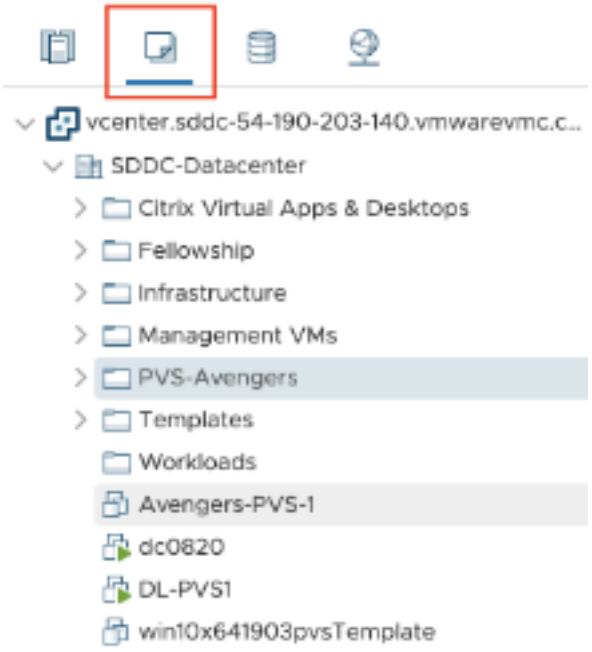
Acerca del entorno de VMware Cloud

Hay cuatro vistas en la página web del cliente de vSphere.

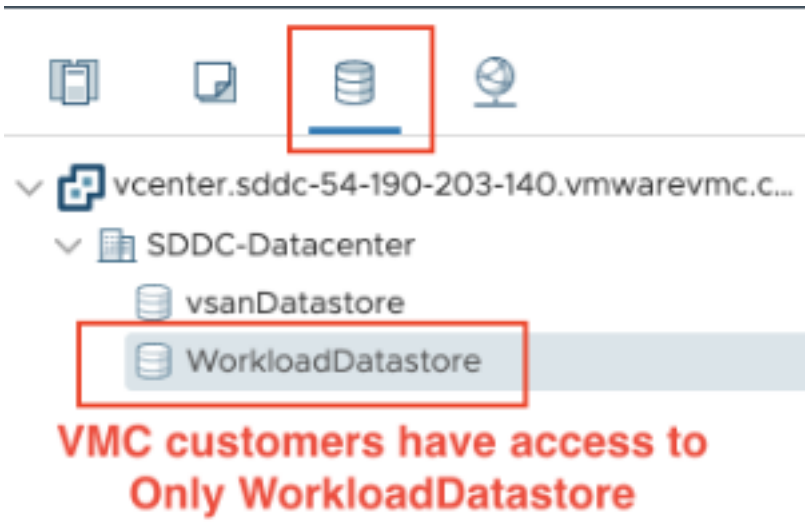
- Vista Host y Cluster: No puede crear clústeres, pero el administrador de la nube puede crear varios grupos de recursos.



- Vista VM y Template: El administrador de la nube puede crear muchas carpetas.



- Vista Storage: Seleccione el almacenamiento **WorkloadDatastore** cuando agregue la unidad de alojamiento en Citrix Studio porque tiene acceso a Workload Datastore solamente.



- Vista Network: Los iconos son diferentes para las redes de la nube de VMware y las redes opacas.

Después de configurar el clúster, consulte Entornos de virtualización de VMware para agregar conexiones y recursos.

Qué hacer a continuación

- Instalar componentes principales
- Instalar VDA
- Crear un sitio

- Para crear y administrar una conexión, consulte Conexión con soluciones de VMware Cloud y de partners

Más información

- Crear y administrar conexiones y recursos
- Crear catálogos de máquinas

Instalar componentes principales

August 17, 2024

> **Importante:**
>
> Citrix recopila datos básicos de licencias según sea necesario para sus intereses legítimos, incluida la conformidad de uso de las licencias. Para obtener más información, consulte Datos de Citrix Licensing.

Los componentes principales son Citrix Delivery Controller, Citrix Studio, Web Studio, Citrix Director y Citrix License Server.

> **Nota:**
>
> Citrix Studio es una consola de administración basada en Windows que le permite configurar y administrar su implementación local de Citrix Virtual Apps and Desktops. Web Studio es la próxima generación de Citrix Studio, una consola web de administración que ofrece las mismas funciones que Citrix Studio. Para obtener más información sobre Web Studio, consulte Instalar Web Studio.

(en versiones anteriores a 2003, los componentes principales incluían Citrix StoreFront; todavía puede instalar StoreFront si hace clic en el icono de **Citrix StoreFront** 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.

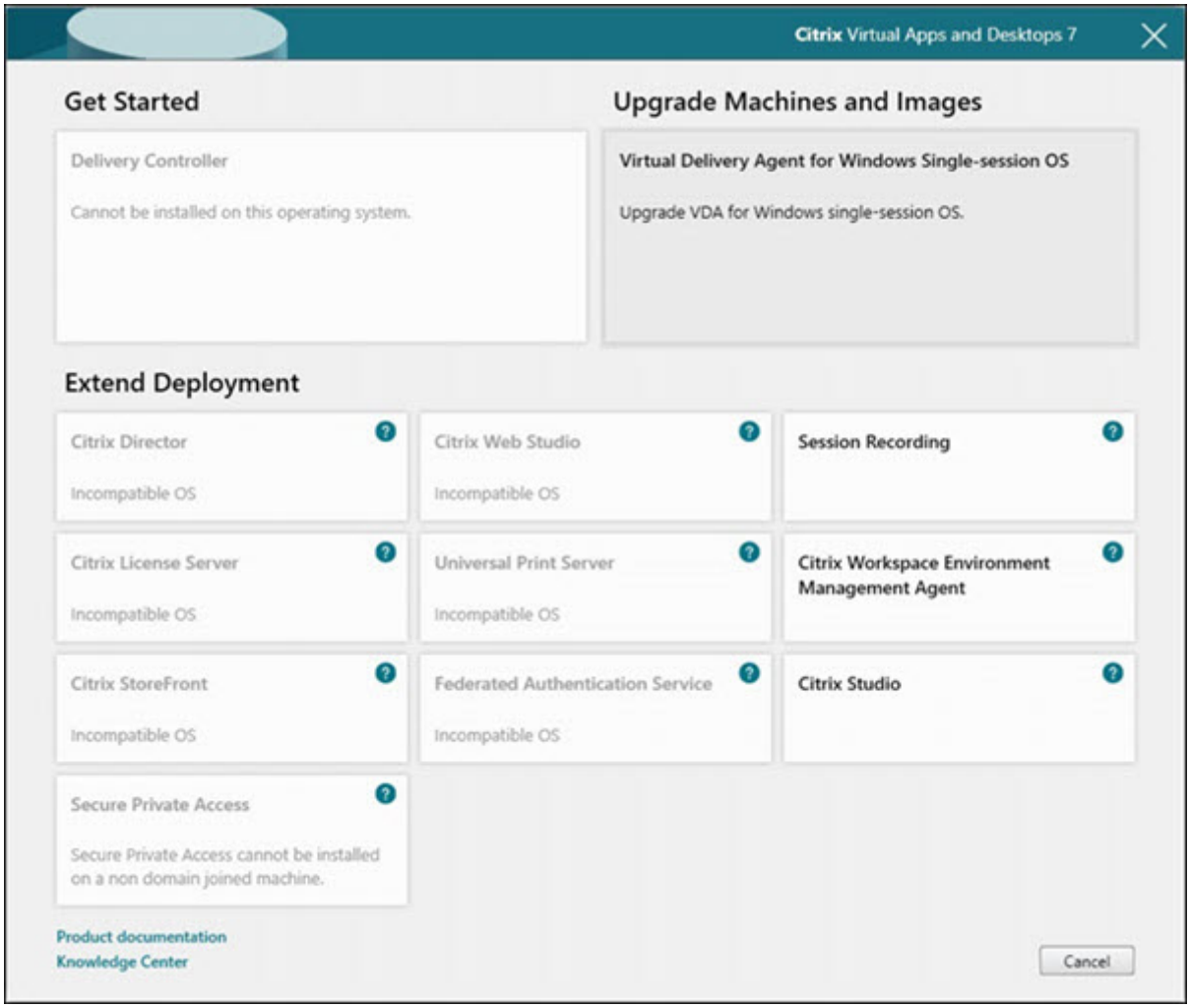
Paso 2. Elija el producto a instalar

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 línea de comandos: `/xenapp` para instalar Citrix Virtual Apps. Citrix Virtual Apps and Desktops se instala si se omite la opción.

Paso 3. Elija qué instalar

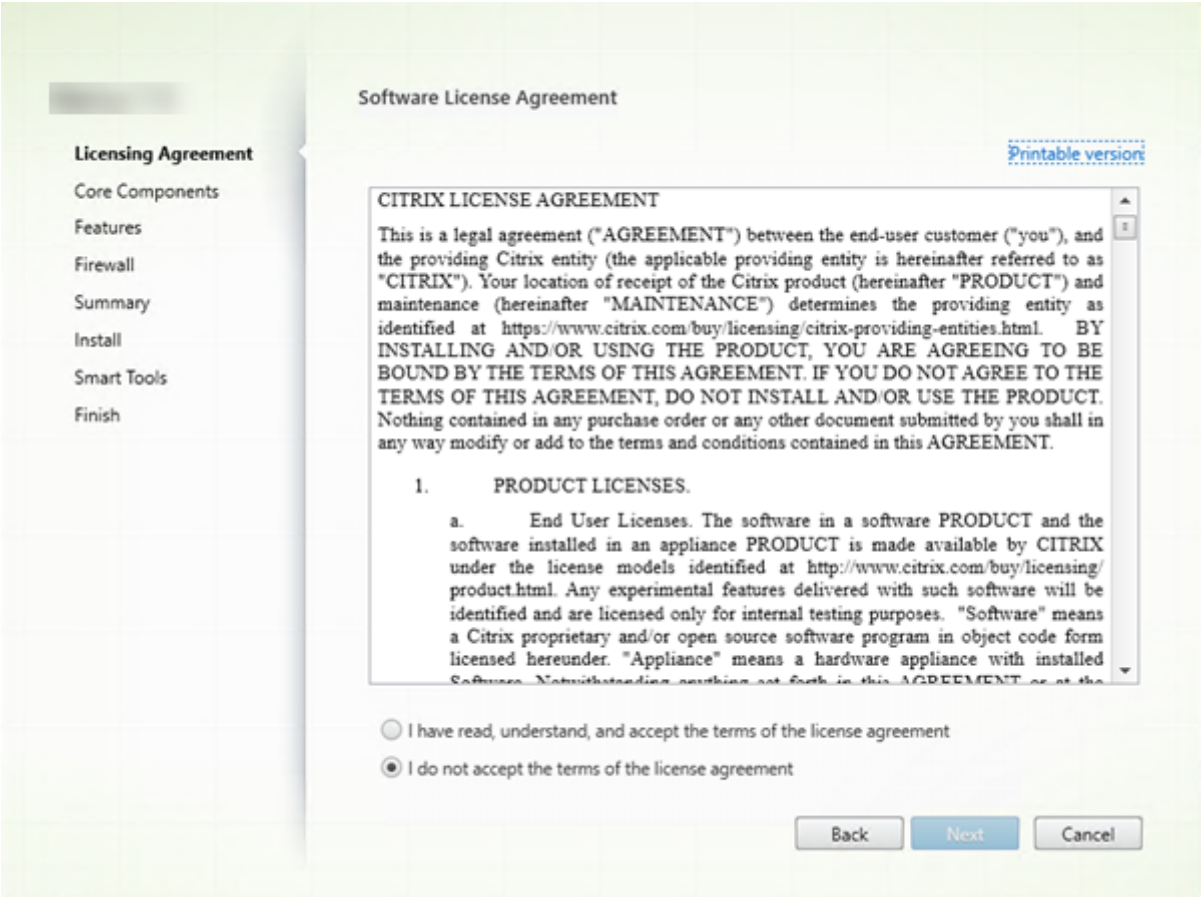


Si acaba de empezar, seleccione **Delivery Controller**. (En una página posterior, seleccionará los componentes concretos que se instalarán en esta máquina.)

Si ya ha instalado un Controller (en esta máquina o en otra) y quiere instalar otro componente, selecciónelo en la sección **Ampliar implementación**.

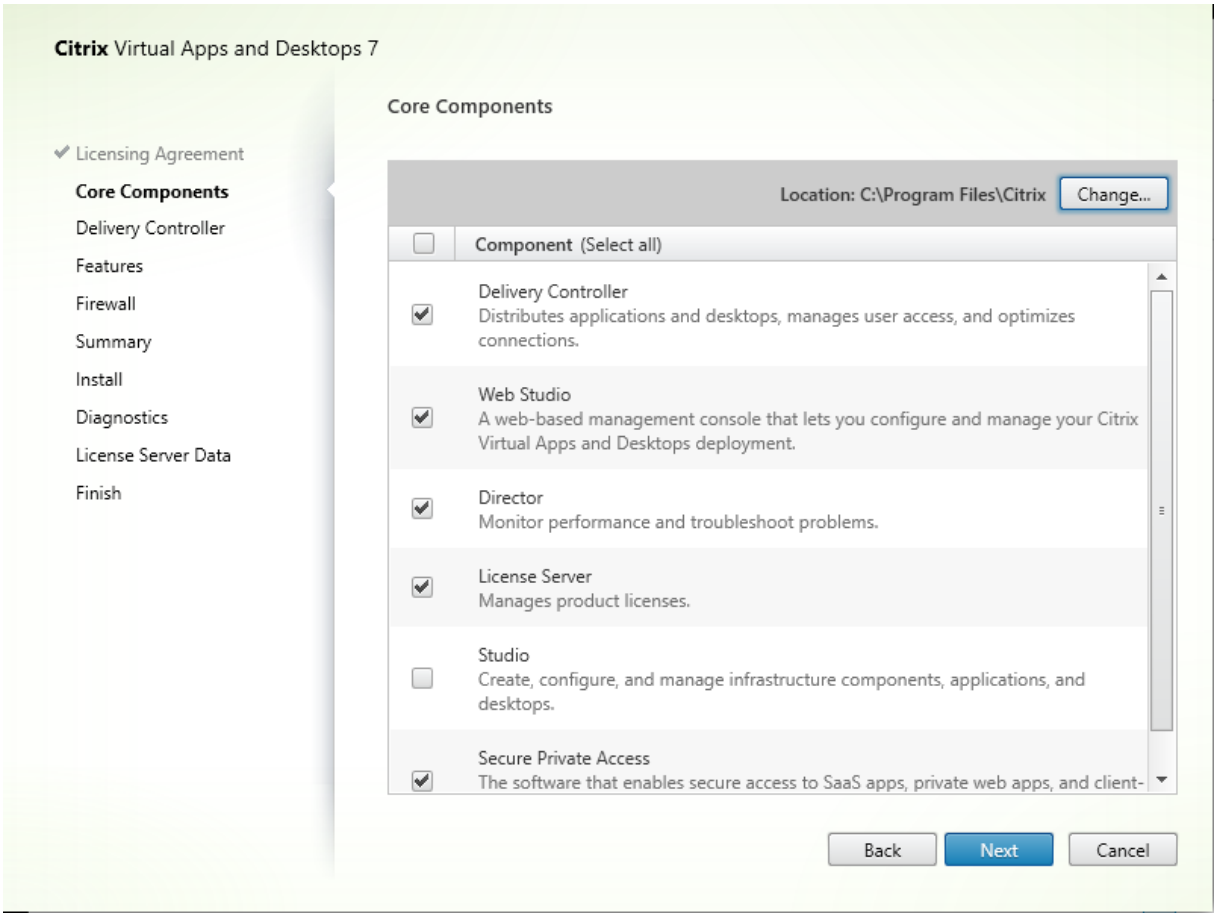
Opción de línea de comandos: `/components`

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. Seleccionar los componentes que instalar y la ubicación de la instalación



En la página **Componentes principales**:

- **Ubicación:** De forma predeterminada, los componentes se instalan en `C:\Program Files\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, Secure Private Access y el Servidor de licencias en servidores independientes.

  > **Nota:**
  >
  > Si va a instalar componentes en más de un servidor, primero instale Citrix License Server y las licencias antes de instalar otros componentes en otros servidores. Para obtener instrucciones, consulte la sección Instalación automática de la Guía sobre el sistema de licencias

> de Citrix Virtual Apps and Desktops.

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 necesariamente 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.

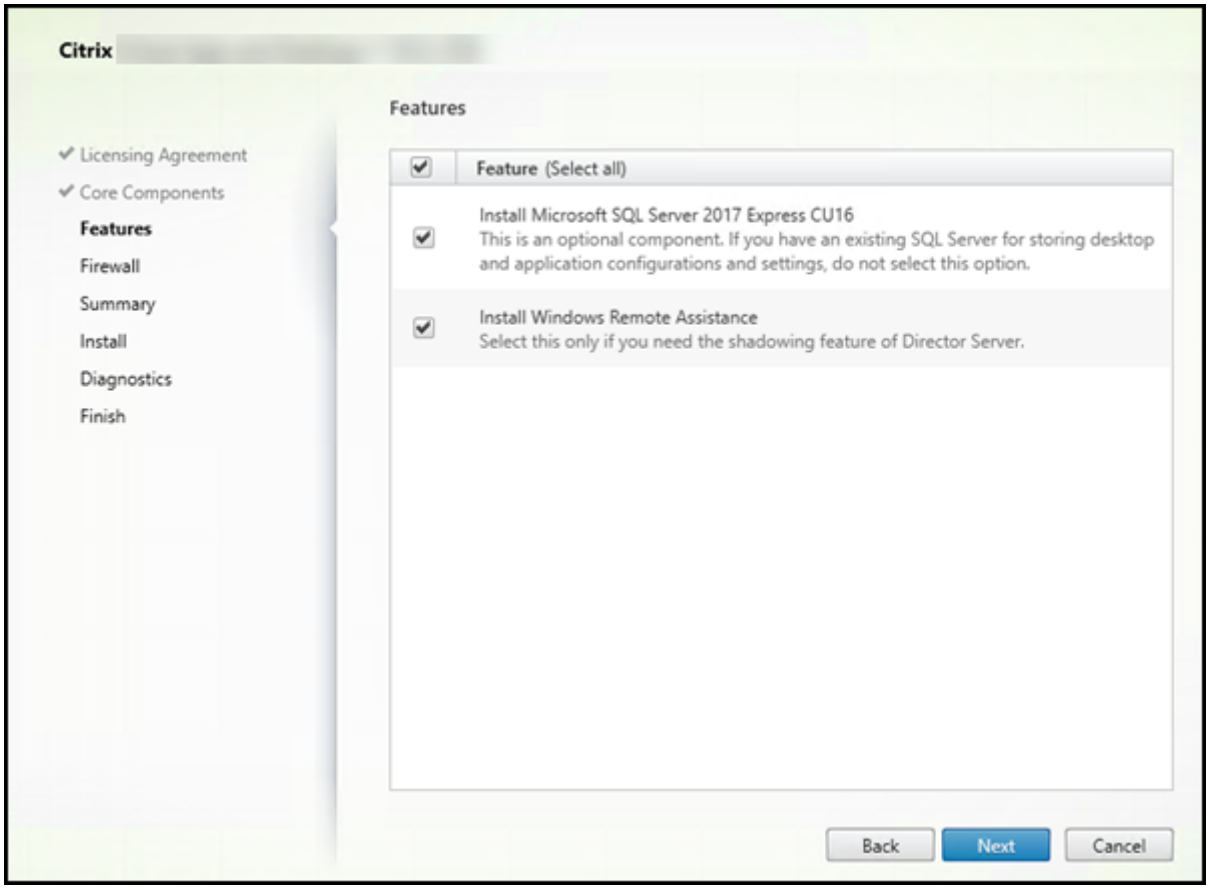
- Recomendación: Haga clic en **Cancelar** para detener la instalación. Agregue más RAM a la máquina y vuelva a iniciar la instalación.
- También puede hacer clic en **Siguiente** para continuar con la instalación. Es posible que el sitio tenga problemas de estabilidad.

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.

Al actualizar la versión, también se le notifica si la versión del SO o de SQL Server ya no es compatible. Consulte Actualizar la versión de una implementación.

Paso 6. Habilite o inhabilite las funciones



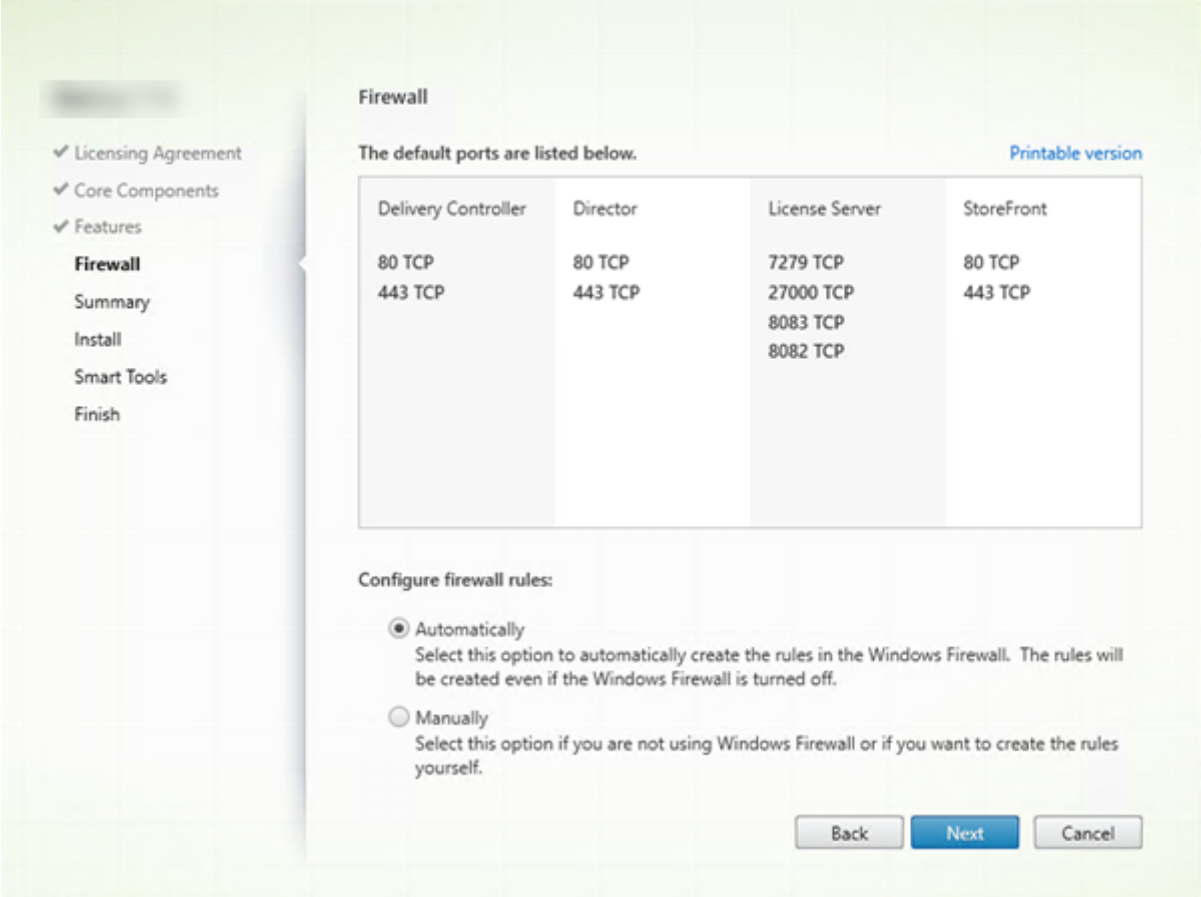
En la página **Funciones**:

- 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



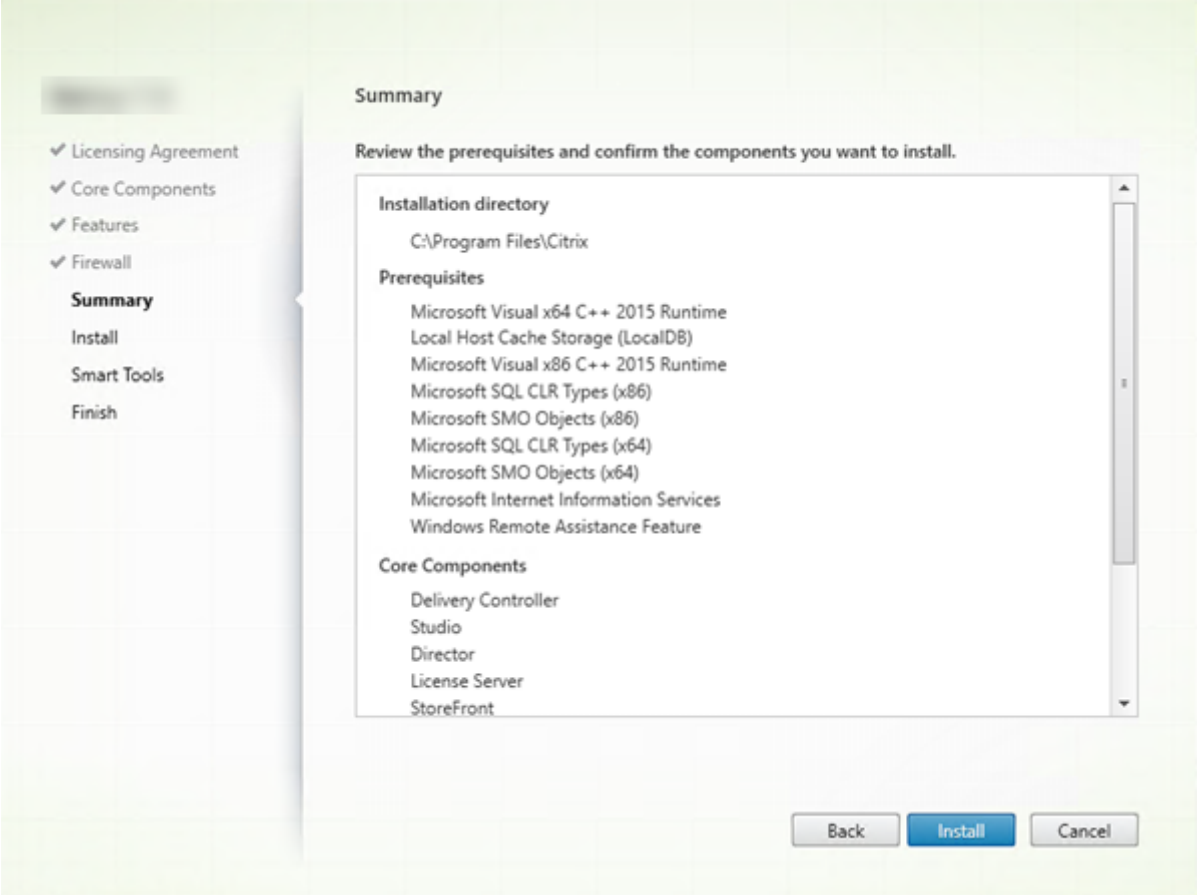
De forma predeterminada, los puertos que aparecen en la página **Firewall** se abren automáticamente si el servicio Firewall de Windows se está ejecutando, incluso aunque el firewall no esté habilitado. La opción predeterminada no presenta problemas para la mayoría de las implementaciones. Para obtener 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 es para las implementaciones de prueba).

Opción de línea de comandos: `/configure_firewall`

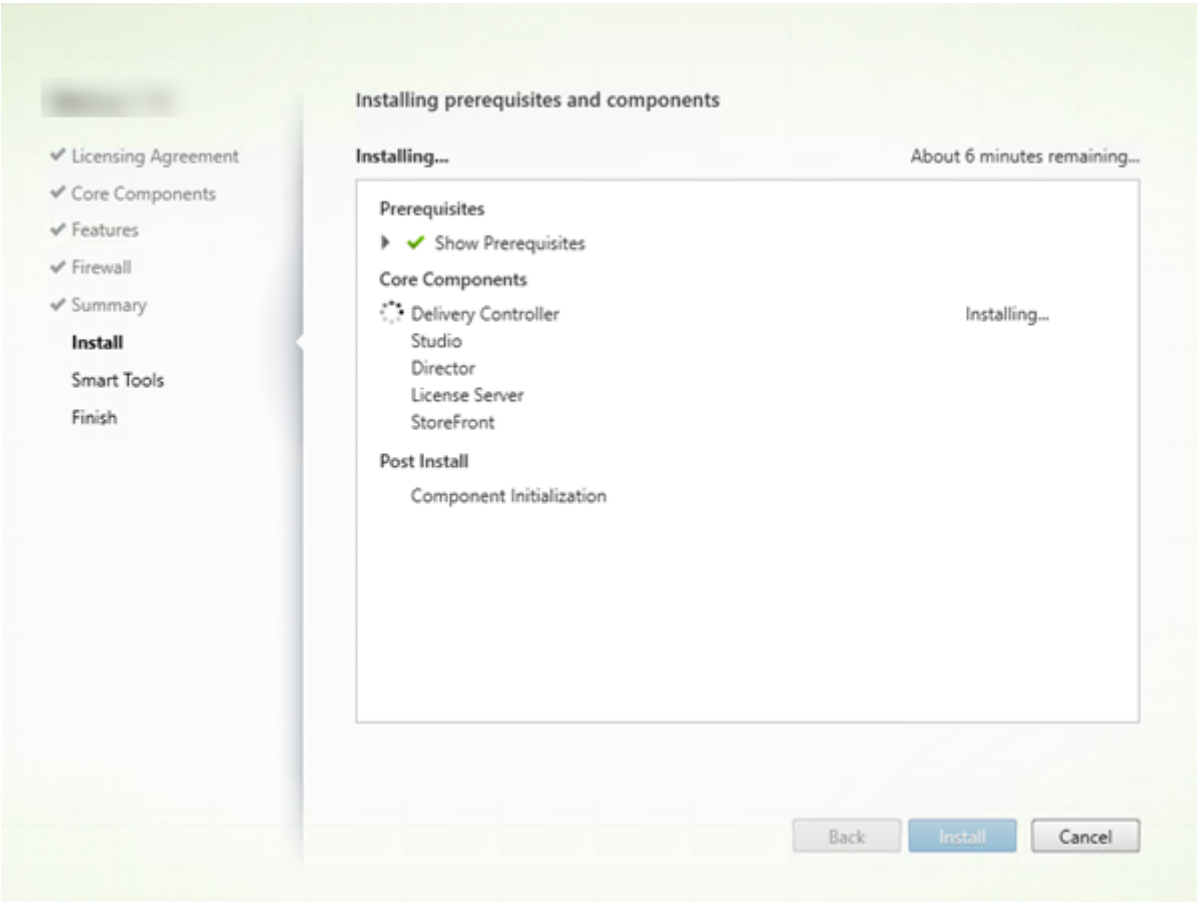
Paso 8. Revise los requisitos previos y confirme la instalación



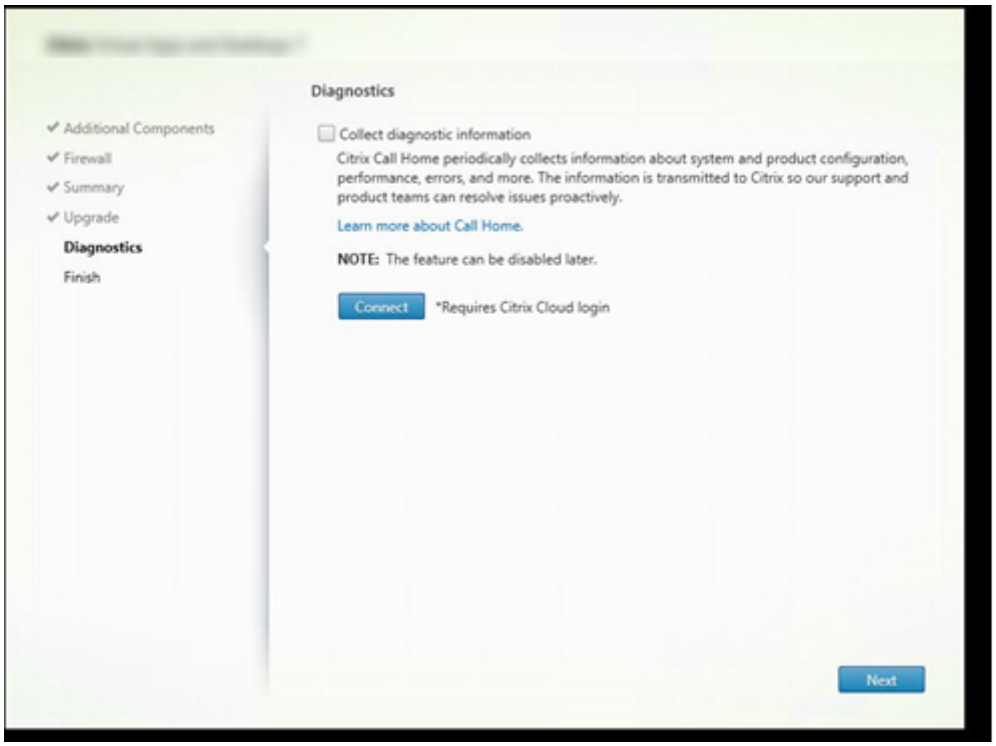
La página **Resumen** muestra lo que se instalará. Si fuera necesario, puede usar el botón **Atrás** para volver a las páginas anteriores del asistente y cambiar las opciones.

Cuando haya terminado, haga clic en **Instalar**.

La pantalla muestra el progreso de la instalación.



Paso 9. Compartir información de diagnóstico con Cloud Software Group



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.

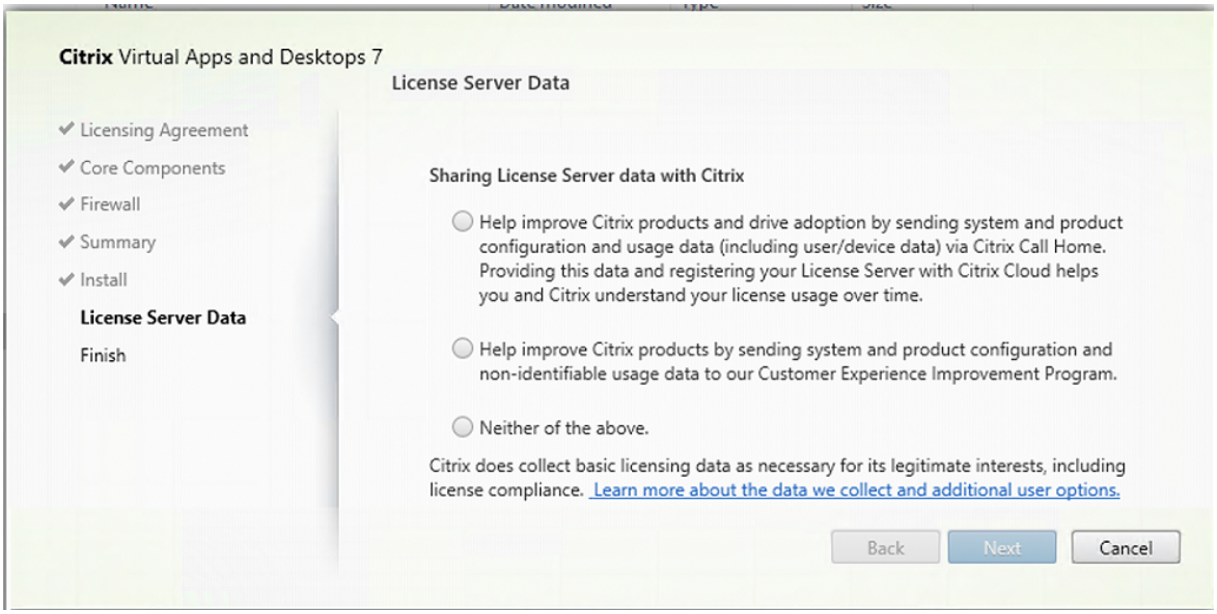
Si elige participar (opción predeterminada), haga clic en **Conectar**. Cuando se le solicite, introduzca las credenciales de su cuenta de Citrix Puede cambiar su opción de inscripción más tarde, después de la instalación.

Una vez validadas las credenciales (o si elige no participar), haga clic en **Siguiente**.

Si hace clic en **Conectar** en la página **Diagnósticos** sin seleccionar antes **Recopilar información de diagnóstico**, al cerrar el cuadro de diálogo **Conectar con Citrix Insight Services**, el botón **Siguiente** está inhabilitado. No puede pasar a la siguiente página. Para volver a habilitar el botón **Siguiente**, seleccione y desmarque inmediatamente **Recopilar información de diagnóstico**.

Para obtener más información, consulte Call Home.

Paso 10. Compartir datos del servidor de licencias con Cloud Software Group



En la página **Datos del servidor de licencias**, le pedimos que comparta los datos de Call Home o de Customer Experience Improvement Program (CEIP) para ayudarnos. Además, Cloud Software Group también exige la recopilación de datos básicos sobre licencias, incluido el cumplimiento de las licencias, según sea necesario para sus intereses legítimos.

La página **Datos del servidor de licencias** aparece cuando ha instalado el servidor de licencias:

- De forma independiente.
- Como componente principal, durante la instalación de un Delivery Controller.

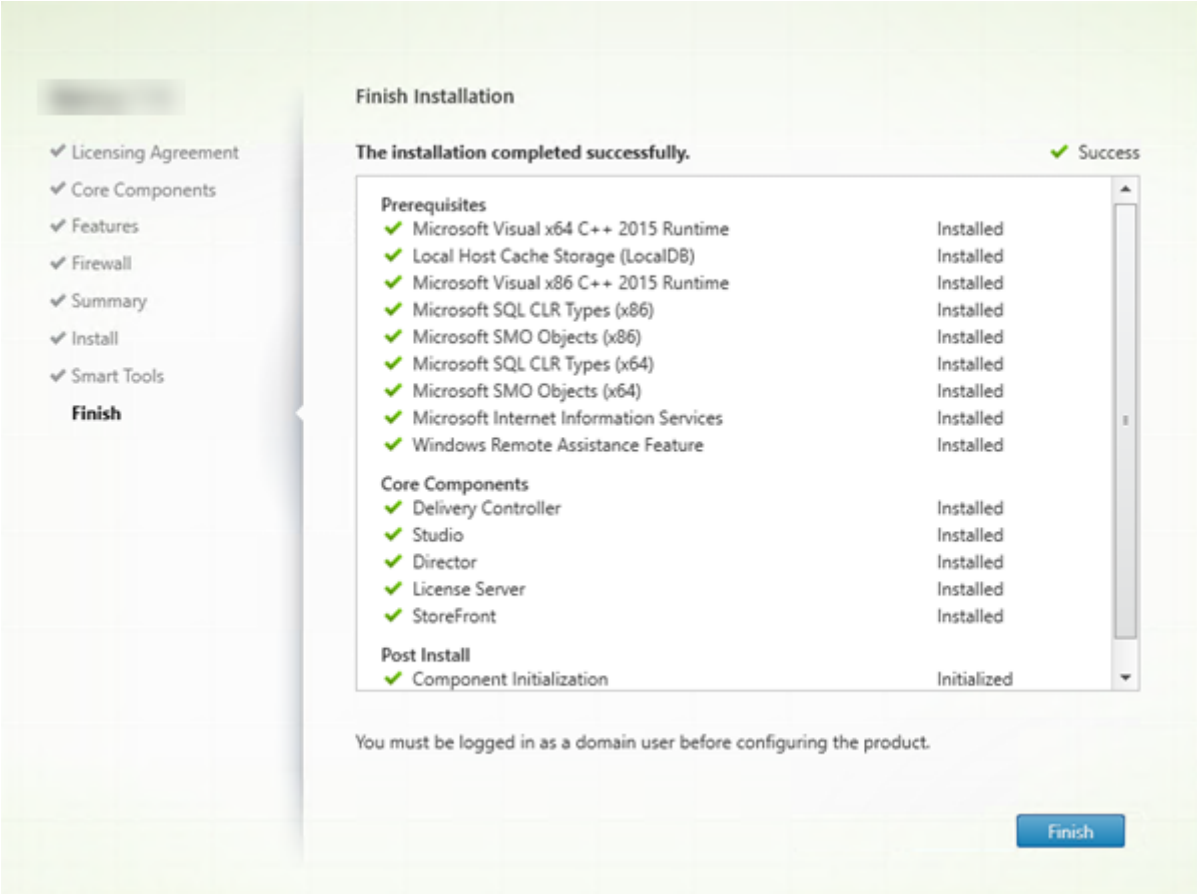
Durante la actualización de una versión, esta página no aparece si la configuración ya está definida en el archivo `/CITRIX.opt:`.

El servidor de licencias supervisa varios tipos de datos de usuario, como los datos de licencias, los datos de Call Home y los datos de CEIP. Para habilitar la recopilación de datos de Call Home y de CEIP, debe optar por participar (apuntarse).

Para obtener más información sobre cómo habilitar Call Home y la recopilación de datos de CEIP durante la instalación mediante la línea de comandos, consulte Opciones de línea de comandos para instalar los componentes principales.

Para obtener más información sobre la recopilación de datos de licencias de Cloud Software Group, consulte Programas de recopilación de datos de Citrix Licensing.

Paso 11. 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 12: Instale los componentes principales restantes en otras máquinas

Si ha instalado todos los componentes principales en una máquina, continúe con Siguientes pasos. De lo contrario, ejecute el instalador en las demás máquinas para instalar otros componentes. También puede instalar más Controllers en otros servidores.

Siguientes pasos

Después de instalar todos los componentes necesarios, 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 siguientes componentes:

- **Componente de servidor Universal Print Server:** Inicie el instalador en el servidor de impresión.

  1. Seleccione **Universal Print Server** en la sección **Ampliar implementación**.
  2. Acepte el contrato de licencia.
  3. 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 Opciones de línea de comandos para instalar Universal Print Server.

- Servicio de autenticación federada.
- Grabación de sesiones.
- Workspace Environment Management.

Instalación desde la línea de comandos

August 17, 2024

> **Importante:**
>
> - Si va a actualizar y su versión actual utiliza o tiene instalado el software Personal vDisk o AppDisks, consulte Quitar discos PvD, AppDisks y hosts no admitidos.
> - Citrix recopila datos básicos de licencias según sea necesario para sus intereses legítimos, incluida la conformidad de uso de las licencias. Para obtener más información, consulte Datos de Citrix Licensing.

Introducción

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 agentes VDA en máquinas de Active Directory. Para obtener más información, consulte Instalar agentes VDA mediante scripts.

Si intenta instalar o actualizar un SO Windows a una versión incompatible con esta versión de Citrix Virtual Apps and Desktops, aparece un mensaje que le lleva a la información sobre las opciones de que dispone. Consulte Sistemas operativos anteriores.

Para obtener información sobre cómo informa Citrix de los resultados de las instalaciones 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 apropiado.

   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 un VDA: Ejecute `XenDesktopVDASetup.exe` con las opciones que aparecen en Opciones de línea de comandos para instalar un VDA.

   Para instalar StoreFront: Ejecute `CitrixStoreFront-x64.exe` en la carpeta `x64 > StoreFront` de los medios de instalación.

   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 la Grabación de sesiones: Siga las instrucciones indicadas en Grabación de sesiones.

Para instalar Workspace Environment Management: Siga las instrucciones indicadas en Workspace Environment Management.

Para instalar Secure Private Access:ejecute `XenDesktopSPASetup.exe` en la carpeta de configuración de `x64 > XenDesktop` de los medios de instalación. Siga las instrucciones de las opciones de línea de comandos para instalar Secure Private Access.

Opciones de línea de comandos para instalar componentes principales

Las siguientes opciones de parámetros son válidas para instalar componentes principales con el comando `XenDesktopServerSetup.exe`. Para obtener más información acerca de las opciones, consulte Instalar componentes principales.

- **/ceipoptin** *ceipoptin* [,*ceipoptin*] …

  Permite la recopilación de datos de Call Home y del Customer Experience Improvement Program (CEIP). Los valores válidos son:

  - `DIAGNOSTIC`: Elija este valor para permitir que Citrix Licensing recopile datos de Call Home.
  - `ANONYMOUS`: Elija este valor para permitir que Citrix Licensing recopile datos de CEIP no identificados (que no identifican a los usuarios).
  - `NONE`: Elija este valor para inhabilitar la recopilación de datos de CEIP por parte de Citrix Licensing.

  Para obtener más información sobre la recopilación de datos de Call Home, consulte Call Home de Citrix Licensing.

  Para obtener más información sobre la recopilación de datos de CEIP, consulte Customer Experience Improvement Program de Citrix Licensing.

  Para obtener más información detallada sobre los datos de CEIP, consulte Elementos de datos de CEIP de Citrix Licensing.

  Para obtener más información sobre los datos de licencias del Servidor de licencias, consulte Datos de Citrix Licensing.

- **/components** *component* [, *component*]…

  Lista de los componentes, separados por comas, para instalar o quitar. Los valores válidos son:

  - `CONTROLLER`: Controller
  - `DESKTOPSTUDIO`: Studio

  - `WEBSTUDIO`: Web Studio
  - `DESKTOPDIRECTOR`: Director
  - `LICENSESERVER`: Citrix License Server
  - `SECUREPRIVATEACCESS`: Secure Private Access

  Si se omite esta opción, se instalarán todos los componentes o se quitarán si también se especifica la opción `/remove`.

  (en versiones anteriores a 2003, los valores válidos incluían `STOREFRONT`; a partir de la versión 2003, utilice el comando de instalación dedicado de StoreFront que se menciona en Usar el instalador de producto completo).

- **/onlyprereqs**

  Solo se instalarán los requisitos previos para los componentes seleccionados. No se instalará ningún componente del producto Citrix.

- **/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. Normalmente 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.

Durante una actualización de versión, esta opción se omite si se detecta una versión de SQL Server no compatible. Para obtener información detallada, consulte Comprobación de versión de SQL Server.

- **/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. Valor predeterminado = `TEMP%\Citrix\XenDesktop Installer`

- **/no_remote_assistance**

  Válido solamente cuando se instala Director. Inhabilita la funcionalidad de remedo 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).

- **/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.

- **/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 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.

- **/SKIPHDXDRIVERCHECK**

  Omite la comprobación de los controladores HDX en el metainstalador del VDA.

- **/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 Delivery Controller, 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
```

El siguiente comando instala un Delivery Controller, Secure Private Access 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 /xenapp /components
controller,secureprivateaccess /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_xxxx.exe`
   - Virtual Delivery Agent de SO de sesión única: `VDAWorkstationSetup_xxxx.exe`
   - Servicios principales de Virtual Delivery Agent para sistema operativo de sesión única: `VDAWorkstationCoreSetup_xxxx.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: `C:\YourExtractFolder\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 mediante las opciones válidas que se indican en este artículo.

   - Para `VDAServerSetup_XXXX.exe`, ejecute `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`
   - Para `VDAWorkstationCoreSetup_XXXX.exe`, ejecute `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopRemotePCSetup.exe`
   - Para `VDAWorkstationSetup_XXXX.exe`, ejecute `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`

   Para ejecutar el paquete descargado, ejecute su nombre: `VDAServerSetup.exe`, `VDAWorkstationSetup.exe` o `VDAWorkstationCoreSetup.exe`. Use las opciones válidas que aparecen a continuación.

Si conoce el instalador de producto completo:

- Ejecute el paquete independiente `VDAServerSetup.exe` o `VDAWorkstationSetup.exe` como si fuera el comando `XenDesktopVdaSetup.exe` en todo excepto el nombre.
- El instalador `VDAWorkstationCoreSetup.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): `VDAServerSetup_xxxx.exe`, `VDAWorkstationSetup_xxxx.exe` o `VDAWorkstationCoreSetup_xxxx.exe`.

Para obtener más información acerca de las opciones, consulte Instalar agentes VDA.

- **/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 ambos, el VDA y la aplicación Citrix Workspace para Windows, especifique `/components vda,plugins` o no especifique ningún componente. Si no se especifica ningún componente, solo se instalará el VDA de forma predeterminada.

  Para instalar solo el VDA y excluir la instalación de la aplicación Citrix Workspace, especifique `/components vda`.

  Esta opción no es válida cuando se utiliza el instalador `VDAWorkstationCoreSetup_xxxx.exe`. Ese instalador no puede instalar la aplicación Citrix Workspace.

- **/onlyprereqs**

  Solo se instalarán los requisitos previos para los componentes seleccionados. No se instalará ningún componente del producto Citrix.

- **/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_guid` y `/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_hdx_tls_dtls**

  Abre el puerto TCP y UDP 443 para HDX Direct V1.

- **/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 remedo 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.

- **/enablerestore** o **/enablerestorecleanup**

  (Válido solo para VDA de sesión única) Habilita el retorno automático al punto de restauración si falla la instalación o actualización del VDA.

  Si la instalación/actualización se completa correctamente:

  - `/enablerestorecleanup` indica al instalador que quite el punto de restauración.
  - `/enablerestore` indica al instalador que retenga el punto de restauración, aunque no se haya utilizado.

  Para obtener información más detallada, consulte Restaurar en caso de error al instalar o actualizar.

- **/ENABLE_SECURE_DEFAULTS**

  Cambia la configuración predeterminada de varias funciones de habilitadas a inhabilitadas para ofrecer una configuración lista para usar más segura. Las funciones relevantes son: redirección de unidades del cliente, redirección de carpetas especiales, arrastrar y colocar, redirección de dispositivos TWAIN del cliente, redirección de dispositivos Plug and Play USB del cliente, redirección de impresoras del cliente, redirección del portapapeles del cliente y redirección del micrófono del cliente.

- **/enable_ss_ports**

  Abre los puertos del firewall de Windows que se requieren para compartir la pantalla, si se detecta el servicio Firewall de Windows, incluso si el firewall no está habilitado. Si se utiliza un firewall distinto o no se utiliza ninguno, es necesario configurar el firewall manualmente.

- **/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 los siguientes:

SO multisesión	SO de sesión única	Servicios principales del SO de sesión única
Citrix Authentication Identity Assertion VDA Plug-in	Citrix Authentication Identity Assertion VDA Plug-in	Citrix Authentication Identity Assertion VDA Plug-in
Citrix Backup and Restore	Citrix Backup and Restore	Citrix Browser Content Redirection
Citrix Browser Content Redirection	Citrix Browser Content Redirection	Citrix Personalization **for** App-V - VDA
Citrix MCS IODriver	Citrix MCS IODriver	Citrix Telemetry Service
Citrix Personalization **for** App-V - VDA	Citrix Personalization **for** App-V - VDA	Citrix Universal Print Client
Citrix Profile Management	Citrix Profile Management	Citrix Vda Log Capture Service
Citrix Profile Management WMI Plug-in	Citrix Profile Management WMI Plug-in	CSE Component
Citrix Rendezvous V2	Citrix Rendezvous V2	Director VDA Plug-in
Citrix Telemetry Service	Citrix Telemetry Service	Machine Management Provider
Citrix Universal Print Client	Citrix Universal Print Client	VDA Monitor Plug-in

SO multisesión	SO de sesión única	Servicios principales del SO de sesión única
Citrix Vda Log Capture Service	Citrix Vda Log Capture Service	VDA WMI Proxy Plug-in
Citrix VDA Upgrade Agent	Citrix VDA Upgrade Agent	
CSE Component	CSE Component	
Director VDA Plug-in	Director VDA Plug-in	
Machine Identity Service	Machine Identity Service	
Machine Management Provider	Machine Management Provider	
VDA Monitor Plug-in	User Personalization Layer	
VDA WMI Proxy Plug-in	VDA Monitor Plug-in	
	VDA WMI Proxy Plug-in	
Citrix App Protection Component	Citrix App Protection Component	Citrix App Protection Component
Citrix HyperV Filter Driver	Citrix HyperV Filter Driver	
Citrix Personalization **for** App-V - VDA	Citrix Personalization **for** App-V - VDA	Citrix Personalization **for** App-V - VDA

Excluir Citrix Profile Management de la instalación (/exclude "Citrix Profile Management") 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 especifica /exclude e /includeadditional con el mismo nombre de componente, 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. Esta opción puede ser útil cuando está creando una implementación de acceso con Remote PC y quiere instalar otros componentes que no están incluidos de manera predeterminada. Los valores válidos son los siguientes:

SO multisesión	SO de sesión única
`Citrix Backup and Restore`	`Citrix Backup and Restore`
`Citrix MCS IODriver`	`Citrix MCS IODriver`
`Citrix Personalization for App-V - VDA`	`Citrix Personalization for App-V - VDA`
`Citrix Profile Management`	`Citrix Profile Management`
`Citrix Profile Management WMI Plug-in`	`Citrix Profile Management WMI Plug-in`
`Citrix Rendezvous V2`	`Citrix Rendezvous V2`
`Citrix VDA Upgrade Agent`	`Citrix VDA Upgrade Agent`
`Citrix Web Socket Vda Registration Tool`	`Citrix Web Socket Vda Registration Tool`
`Machine Identity Service`	`Machine Identity Service`
	`User Personalization Layer`

Si especifica /`exclude` e /`includeadditional` con el mismo nombre de componente, ese componente no se instala.

- **/installdir** *directorio*

  Directorio vacío existente donde se instalarán los componentes. Valor predeterminado = C:\Archivos de programa\Citrix.

- **/install_mcsio_driver**

No usar. En su lugar, use `/includeadditional "Citrix MCS IODriver"` o `/exclude "Citrix MCS IODriver"`

- **/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. Configura el VDA como una imagen que se utilizará para crear otras máquinas. Esta opción equivale a `/mastermcsimage`.

  Esta opción no es válida cuando se utiliza el instalador `VDAWorkstationCoreSetup_xxxx.exe`.

- **/mastermcsimage**

  Especifica que esta máquina se utilizará como imagen con Machine Creation Services. Esta opción equivale a `/masterimage`.

- **/masterpvsimage**

  Especifica que esta máquina se utilizará como imagen con Citrix Provisioning o una herramienta de aprovisionamiento de terceros (como Microsoft System Center Configuration Manager) para aprovisionar máquinas virtuales.

- **/websockettoken** *WebSocketToken*

  Crea un VDA de Web Socket. El WebSocketToken es para el token que se requiere.

- **/websockettokenfile** *FileContainingWebSockToken*

  Crea un VDA de Web Socket. *FileContainingWebSockToken* es para el archivo que contiene el token requerido.

- **/websockettokenstdin** <*WebSocketToken*

  Crea un VDA de Web Socket. <*WebSocketToken* es para el token requerido y que STDIN transfiere.

- **/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, la instalación del VDA se cierra porque no se cumplen las condiciones previas. La mayoría de las ediciones Windows admitidas vienen con Media Foundation ya instalado, a excepción de las ediciones N. Si habilita las funciones de Windows > Funciones multimedia de *forma manual*, es posible que la clave del Registro que busca el metainstalador de Citrix no

tenga un valor definido. Compruebe la clave del Registro `SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\Windows-Features\WindowsMediaVersion` antes de iniciar el proceso de instalación para confirmar que el valor existe y no está vacío.

- **/nodesktopexperience**

  La función Enhanced Desktop Experience (Experiencia de escritorio mejorada) ya no está disponible. Esta opción (y la configuración de directiva) se ignora, si se especifica.

  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.

- **/physicalmachine**

  Utilice este argumento junto con `/remotepc` para la instalación de Remote PC. De lo contrario, es posible que el VDA no se comporte de la manera prevista en determinados casos de usuario.

- **/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.

- **/proxyconfig** "*dirección o ruta del archivo PAC*"

  Si tiene previsto usar el protocolo Rendezvous con el servicio Gateway, el servicio de actualización de VDA, etc., en su entorno y tiene un proxy no transparente en la red para las conexiones salientes, especifique el proxy aquí. Solo se admiten proxies HTTP. La dirección o la ruta del archivo PAC del proxy para uso con el protocolo Rendezvous. Esta línea de comandos instalará automáticamente Citrix Rendezvous V2 como si se usara /includeadditional "Citrix Rendezvous V2". Para obtener más información sobre la funcionalidad, consulte Protocolo Rendezvous.

  - Formato de dirección de proxy: `http://<url-or-ip>:<port>`
  - Formato de archivo PAC: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

- **/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 cualquier componente adicional (consulte las listas de componentes con las opciones `/exclude` y `/includeadditional`).

  Esta opción no es válida cuando se utiliza el instalador `VDAWorkstationCoreSetup.exe`. El instalador excluye la instalación de estos componentes.

  `/remotepc` no es compatible con la opción `/servervdi`.

- **/remove**

  Quita los componentes especificados con la opción `/components`.

- **/remove_appdisk_ack**

  Autoriza al instalador de VDA a desinstalar el plug-in de VDA para AppDisks si está instalado.

- **/remove_pvd_ack**

  Autoriza al instalador de VDA a desinstalar el disco Personal vDisk si está instalado.

- **/removeall**

  Quita el VDA. No quita la aplicación Citrix Workspace (si está instalada).

- **/REMOVEALLWITHCWA**

  Quita CWA junto con el VDA.

- **/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 multisesión. 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.

Utilice esta opción solo con el instalador de VDA completo.

- **/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 detección 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.

- **/xendesktopcloud**

  Indica que el VDA está instalado en una implementación de Citrix DaaS (Citrix Cloud).

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 y usará MCS para aprovisionar 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 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"/mastermcsimage /
enable_remote_assistance
```

Instalar un VDA de SO de sesión única con el instalador independiente VDAWorkstationCoreSetup:

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`

Solucionar problemas de VDA

- 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 funciones de la máquina Windows muestra la versión real del VDA.
- Después de instalar un VDA, no se pueden entregar aplicaciones o escritorios a los usuarios hasta que el VDA se registre con un Delivery Controller.

  Para obtener información sobre los métodos de registro de VDA y cómo solucionar problemas de registro, consulte Registro de VDA.

Opciones de línea de comandos para instalar Universal Print Server

La siguiente opción es válida con el comando `XenDesktopPrintServerSetup.exe`.

- **/enable_upsserver_port**

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.

Opciones de línea de comandos para instalar un acceso privado seguro

Las siguientes opciones son válidas en ambos casos:

1. Instalador de CVAD: `XenDesktopSPASetup.exe`
2. Instalador local de SPA: `SecurePrivateAccessSetup_XXXX.exe`

- **/enable_spa_ports**

  Abre los puertos del Firewall de Windows requeridos por Secure Private Access, 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.

- **/nosql**

  Impide la instalación de Microsoft SQL Server Express en el servidor en el que está instalando Secure Private Access. Si se omite esta opción, se instalará SQL Server Express como la base de datos del sitio.

- **/help o /h o /?**

  Muestra la ayuda del comando

- **/noreboot**

  Impide que se reinicie el sistema después de la instalación. El acceso privado seguro no se puede usar hasta después de un reinicio.

- **/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.

- **/remove**

  Elimina el Secure Private Access.

Para obtener más información sobre las opciones, consulte el instalador de Secure Private Access.

Más información

Para obtener información sobre cómo informa Citrix del resultado de la instalación de un componente, consulte Códigos de retorno en la instalación de Citrix.

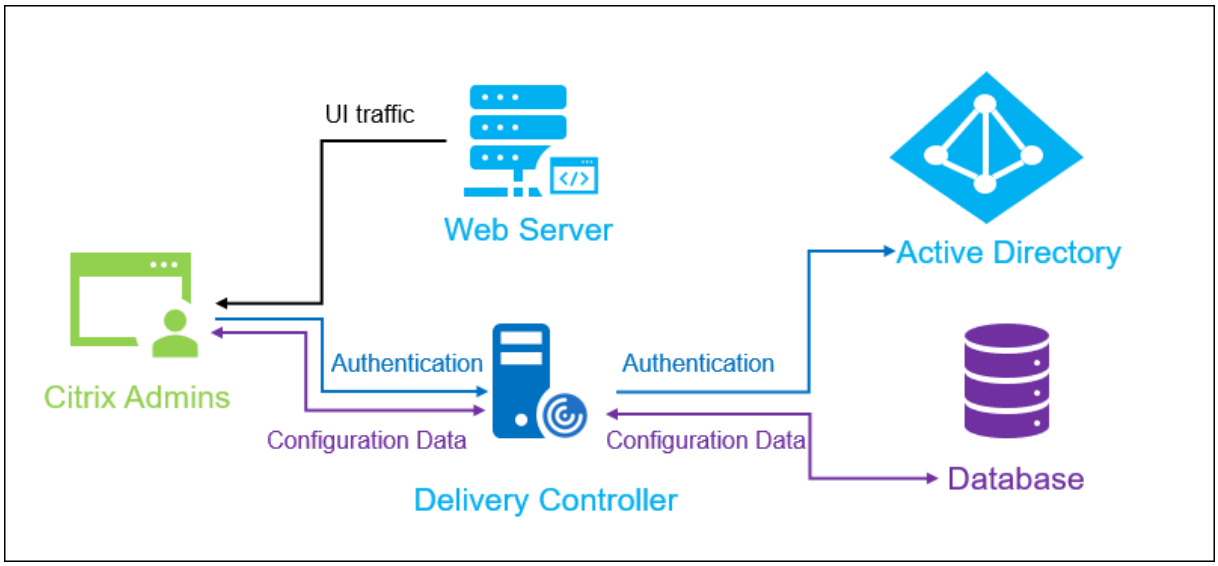
Instalar Web Studio

August 20, 2024

Introducción

Citrix Studio es una consola de administración basada en Windows que le permite configurar y administrar su implementación de Citrix Virtual Apps and Desktops. Web Studio es la próxima generación de Citrix Studio, una consola web de administración que ofrece las mismas funciones que Citrix Studio. Con el mismo aspecto que la interfaz de Configuración completa de Citrix DaaS, Web Studio moderniza su experiencia de administración al proporcionar una experiencia web nativa.

Puede implementar Web Studio en cualquier servidor de Windows que tenga instalado Internet Information Service (IIS). Para realizar una implementación rápida, le recomendamos que instale Web Studio junto con un Delivery Controller. En ese caso, Web Studio se instala como un sitio web en el Delivery Controller. Le recomendamos seguir esta configuración para tener una arquitectura sencilla y reducir el tiempo de administración. Este diagrama muestra la arquitectura de Web Studio:



El flujo de trabajo general para poner en marcha Web Studio es el siguiente:

1. Instalar Web Studio.

2. Configure un sitio.
3. Agregue Delivery Controllers a Web Studio para administrarlos.
4. Iniciar sesión en Web Studio.

Para configurar una implementación de Web Studio con equilibrio de carga, consulte este artículo.

Nuevas funciones disponibles en Web Studio

Consulte el artículo Novedades.

Requisitos del sistema

Sistemas operativos compatibles:

- Windows Server 2022
- 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

Exploradores web compatibles:

- Microsoft Edge 92
- Firefox ESR (Extended Support Release; versión de asistencia extendida) 90
- Google Chrome 92
- Safari 14

La resolución de pantalla recomendada para ver Web Studio es de 1440 x 1024.

Requisitos previos

Esta versión de Web Studio es compatible con las implementaciones de Citrix Virtual Apps and Desktops 2212 y versiones posteriores.

Para implementaciones anteriores a 2212, primero actualice la versión a 2212 y, a continuación, instale Web Studio.

Limitaciones conocidas

Si usa Web Studio y Citrix Studio indistintamente, tenga en cuenta la siguiente limitación: Una plantilla creada en Web Studio no se muestra en Citrix Studio, y viceversa. Esto se debe a que Web Studio usa una base de datos diferente de Citrix Studio para almacenar plantillas. Como solución temporal,

cree una directiva a partir de una plantilla en Web Studio y, a continuación, cree otra plantilla a partir de esta directiva en Citrix Studio y viceversa.

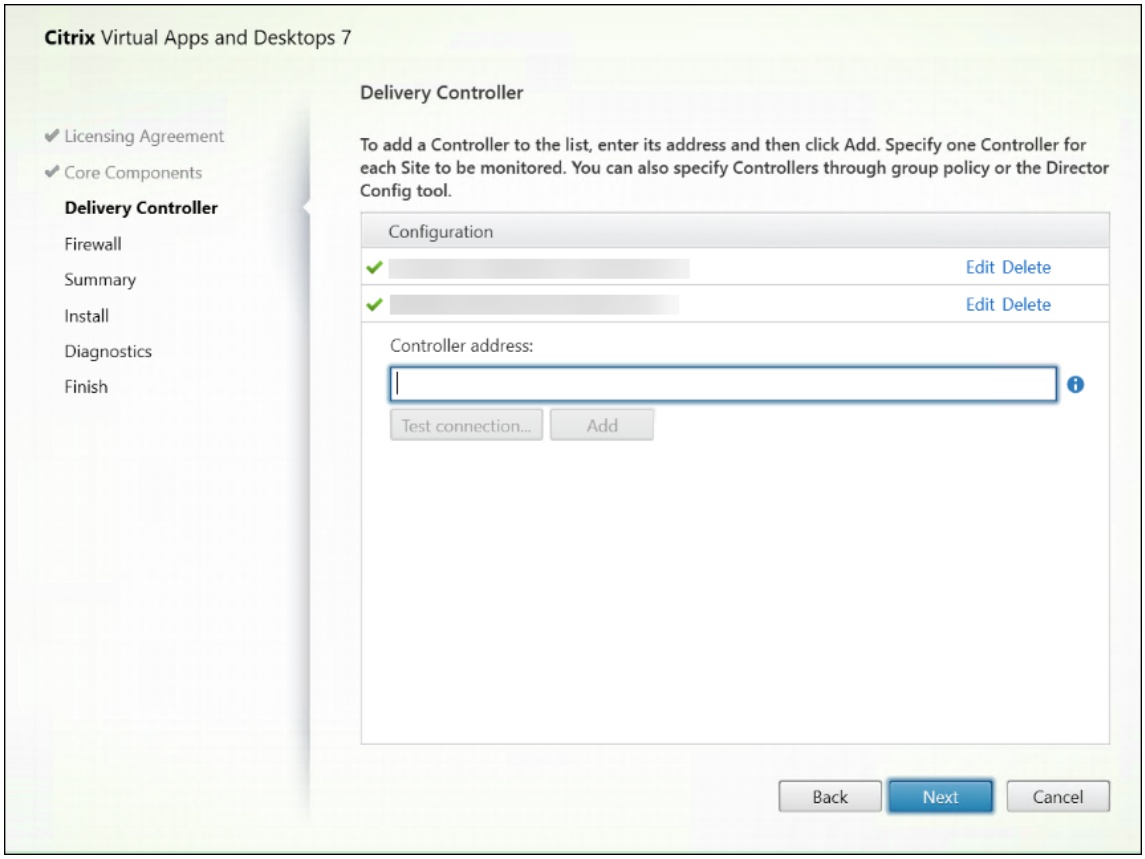
- Para garantizar la correcta instalación de Web Studio, no cambie el nombre del sitio predeterminado (**Sitio web predeterminado**) en Administrador de Internet Information Services (IIS). Cualquier cambio en el nombre del sitio predeterminado provoca errores de instalación.

Instalar Web Studio

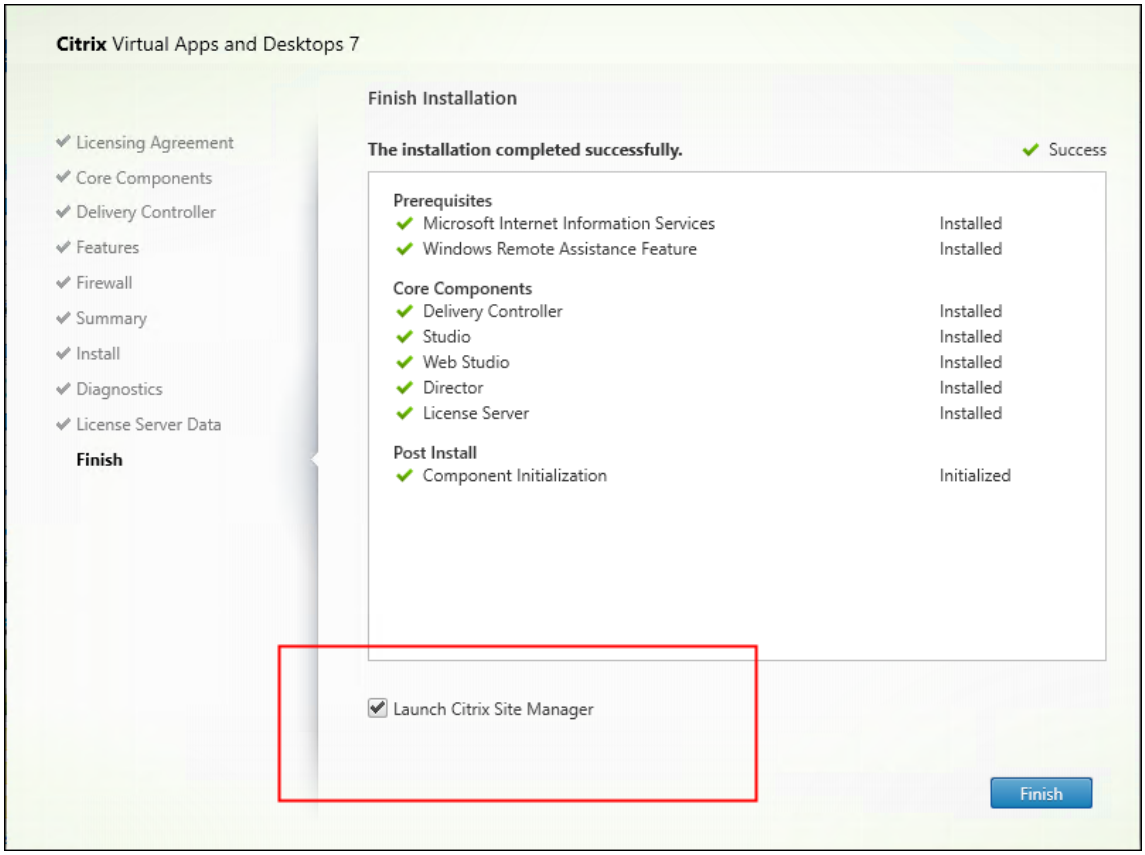
Esta información complementa la guía de Instalar componentes principales. Para instalar Web Studio:

- Instale Web Studio con el instalador ISO del producto completo para Citrix Virtual Apps and Desktops. El instalador ISO comprueba los requisitos previos, instala los componentes que falten, configura el sitio web de Web Studio (en el Delivery Controller si se incluye en la instalación de Delivery Controller) y realiza una configuración básica.
- Si Web Studio no se incluyó durante la instalación, utilice el instalador para agregar Web Studio.
- Al instalar Web Studio, se le pedirá que escriba la dirección de un Delivery Controller.

  > **Nota:**
  >
  > - Puede agregar más de un Delivery Controller. Web Studio intenta conectarse a ellos en orden aleatorio. Si no se puede acceder al Delivery Controller al que Web Studio intenta conectarse, Web Studio recurre automáticamente a otros Delivery Controllers.
  > - Si se seleccionó Director en **Componentes principales** y se instaló, los Delivery Controllers que agregue aquí se utilizarán tanto para Web Studio como para Director.
  > - Si no tiene configurado el certificado público de confianza externo y no quiere solicitarlo a una CA empresarial, solo tiene que configurar el FQDN de su Delivery Controller.
  > - Si tiene el certificado público de confianza externo y puede configurar el DNS público para su Delivery Controller, puede escribir el nombre DNS como la dirección de Delivery Controller.
  > - Si puede solicitar el certificado a la CA de su empresa y puede especificar su DNS personal, puede agregar su DNS personal como la dirección del Delivery Controller.



- Para proteger las comunicaciones entre el explorador web y el servidor web, y entre el explorador web y el Delivery Controller, el cifrado TLS debe estar habilitado en el sitio web de IIS que aloja Web Studio y en el Delivery Controller. Si no hay ningún certificado TLS configurado para el Delivery Controller, el instalador crea un certificado autofirmado con el FQDN del Delivery Controller y localhost como certificado del nombre DNS. Si se configura un certificado TLS, el instalador no realiza ningún cambio. Para obtener más información sobre el cifrado TLS, consulte Proteger un entorno de Web Studio (opcional).
- En la página **Finalizar**, la casilla **Iniciar Site Manager** está marcada de forma predeterminada para que Citrix Site Manager se abra automáticamente. Para iniciarlo más tarde, abra el menú Inicio del escritorio y seleccione **Citrix > Citrix Site Manager**. Antes de iniciar Web Studio, debe usar Citrix Site Manager para crear un sitio o unirse a un sitio existente. Para obtener más información, consulte Configurar un sitio.



> **Nota:**
>
> También puede utilizar la línea de comandos para instalar Web Studio. Ejemplo: `.\XenDesktopServerSetup.exe /components webstudio /controllers "ddc1.studio.local"/configure_firewall /quiet`. Para obtener más información, consulte Instalación desde la línea de comandos.

Configurar un sitio

Para configurar la implementación de Citrix Virtual Apps and Desktops (también conocida como sitio), utilice la herramienta Citrix Site Manager. La herramienta se instala automáticamente con un Delivery Controller.

Para configurar un sitio, siga estos pasos:

1. En un Delivery Controller, abra el menú Inicio del escritorio y, a continuación, seleccione **Citrix > Citrix Site Manager**.
2. En Citrix Site Manager, seleccione **Crear un sitio**. Aparece el asistente de configuración de sitios.
3. Cree un sitio y configure sus parámetros de esta manera:
    - En la página **Introducción**, escriba el nombre del sitio.

- 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, consulte el paso 3. Bases de datos.
- En la página **Licencias**, especifique la dirección del servidor de licencias y, a continuación, indique la licencia que utilizar (instalar). Para obtener más información, consulte el paso 4. Licencias.

4. En la página **Resumen**, compruebe todos los parámetros y haga clic en **Enviar**.

   La dirección IP de este Controller se agrega automáticamente al sitio.

   > **Nota:**
   >
   > El usuario que crea un sitio pasa a ser su administrador total. Para obtener más información, consulte Administración delegada.

Si instala un Controller nuevo después de crear un sitio, debe agregarlo al sitio. Estos son los pasos detallados:

1. Ejecute Citrix Site Manager en este nuevo Controller.
2. Seleccione **Unirse a un sitio existente**.
3. Escriba la dirección de un Controller que ya esté agregado al sitio.
4. Haga clic en **Submit**.

Agregar Delivery Controllers a Web Studio para administrarlos

Utilice la herramienta de configuración de Studio para agregar los Delivery Controllers a Web Studio para administrarlos. Esta herramienta está disponible en la carpeta de instalación de Web Studio.

De forma predeterminada, la herramienta se instala en esta carpeta predeterminada.

- `C:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe`

Supongamos que quiere configurar estos dos Delivery Controllers para el sitio que quiere administrar con Web Studio: `ddc1.studio.local` y `ddc2.studio.local`. Ejecute este comando de PowerShell:

- `.\StudioConfig.exe --server "ddc1.studio.local,ddc2.studio.local"`

> **Nota:**
>
> - La herramienta requiere permisos de administrador del equipo.
> - Es posible que los cambios en la configuración del Delivery Controller no surtan efecto inmediatamente debido a los parámetros de caché del servidor IIS. Para que surta efecto inmediato, vaya al servidor de Web Studio, abra Administrador de Internet Information Ser-

> vices (IIS), vaya a Start Page > Sites > Default Web Site y seleccione **Restart** en el panel Manage Website.
> - Para ver todos los parámetros compatibles, ejecute `StudioConfig.exe --help`.

Configurar Web Studio como proxy para Delivery Controllers (opcional)

De forma predeterminada, al administrar la implementación mediante la consola de Web Studio, se conecta al servidor de Web Studio y a los Delivery Controllers a través del explorador web. Le ofrecemos la opción de configurar el servidor de Web Studio como proxy para Delivery Controllers. Como resultado, solo se conecta al servidor de Web Studio cuando administra la implementación.

Esta sección le guía para configurar un servidor de Web Studio como proxy para Delivery Controllers. Suponemos que Web Studio y Delivery Controllers están instalados en servidores diferentes.

Antes de empezar, compruebe que tiene todos los componentes principales necesarios instalados en la implementación. Para obtener más información, consulte Instalar componentes principales.

Para habilitar el modo proxy para Web Studio, siga estos pasos:

1. En el servidor de Web Studio, ejecute Windows PowerShell como administrador.
2. Ejecute el siguiente comando, donde `fqdn_of_webstudio_machine` se sustituye por el nombre de dominio completo de su servidor de Web Studio.

   ```
   & "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe"--enableproxy --proxyserver "fqdn_of_webstudio_machine"
   ```

   > **Nota:**
   >
   > Si tiene una implementación de Web Studio con equilibrio de carga, sustituya `fqdn_of_webstudio_machine` por el FQDN del servidor del equilibrador de carga (también conocido como servidor virtual). Para obtener más información, consulte Configurar una implementación de Web Studio con equilibrio de carga.

Para inhabilitar el modo proxy para Web Studio, ejecute este comando de PowerShell:

```
1 `& "c:\Program Files\Citrix\Web Studio\Tool\StudioConfig.exe" --disableproxy`
```

> **Nota:**
>
> Como práctica recomendada, le recomendamos proteger su implementación de Web Studio mediante un certificado público de confianza externo o un certificado de una entidad de certificación (CA) empresarial. Para obtener más información, consulte Proteger una implementación de Web Studio.

Iniciar sesión en Web Studio

El sitio web de Web Studio se encuentra en `https://<address of the server hosting Web Studio>/Citrix/Studio`.

Para iniciar sesión en Web Studio, abra el menú Inicio del escritorio y seleccione **Citrix > Citrix Web Studio**. Los administradores con permisos para Web Studio deben ser usuarios del dominio de Active Directory. Al iniciar sesión en Web Studio, tenga en cuenta estos casos:

- Si aún no ha especificado Delivery Controllers para el sitio. Se le pedirá que especifique un Delivery Controller para que tenga acceso temporal a Web Studio.
- Si los Delivery Controllers especificados no están disponibles actualmente, no puede iniciar sesión en Web Studio. Pruebe sus conexiones para asegurarse de que se puede acceder a esos Delivery Controllers. O bien especifique otro Delivery Controller para que tenga acceso temporal a Web Studio.

Siguientes pasos

1. Instalar VDA
2. Utilice Web Studio para ofrecer aplicaciones y escritorios virtuales a sus usuarios mediante:
   a) La creación de un catálogo de máquinas
   b) La creación de un grupo de entrega
   c) La creación de un grupo de aplicaciones (opcional)

Instalar VDA

August 17, 2024

> **Importante:**
>
> - Si va a actualizar y su versión actual tiene instalado el software Personal vDisk o AppDisks, consulte Quitar discos PvD, AppDisks y hosts no admitidos.
> - Los archivos binarios distribuidos por Citrix ahora están firmados. Los archivos binarios firmados indican que están validados por certificados generados por Citrix o por certificados auténticos de terceros.

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 los VDA, instale 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** en 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_2308.exe`: *Versión* del VDA de SO multisesión
   - `VDAWorkstationSetup_2308.exe`: *Versión* del VDA de SO de sesión única
   - `VDAWorkstationCoreSetup_2308.exe`: *Versión* de VDA de los servicios principales de SO de sesión única
2. Haga clic con el botón secundario en el paquete que ha descargado y seleccione **Ejecutar como administrador**.

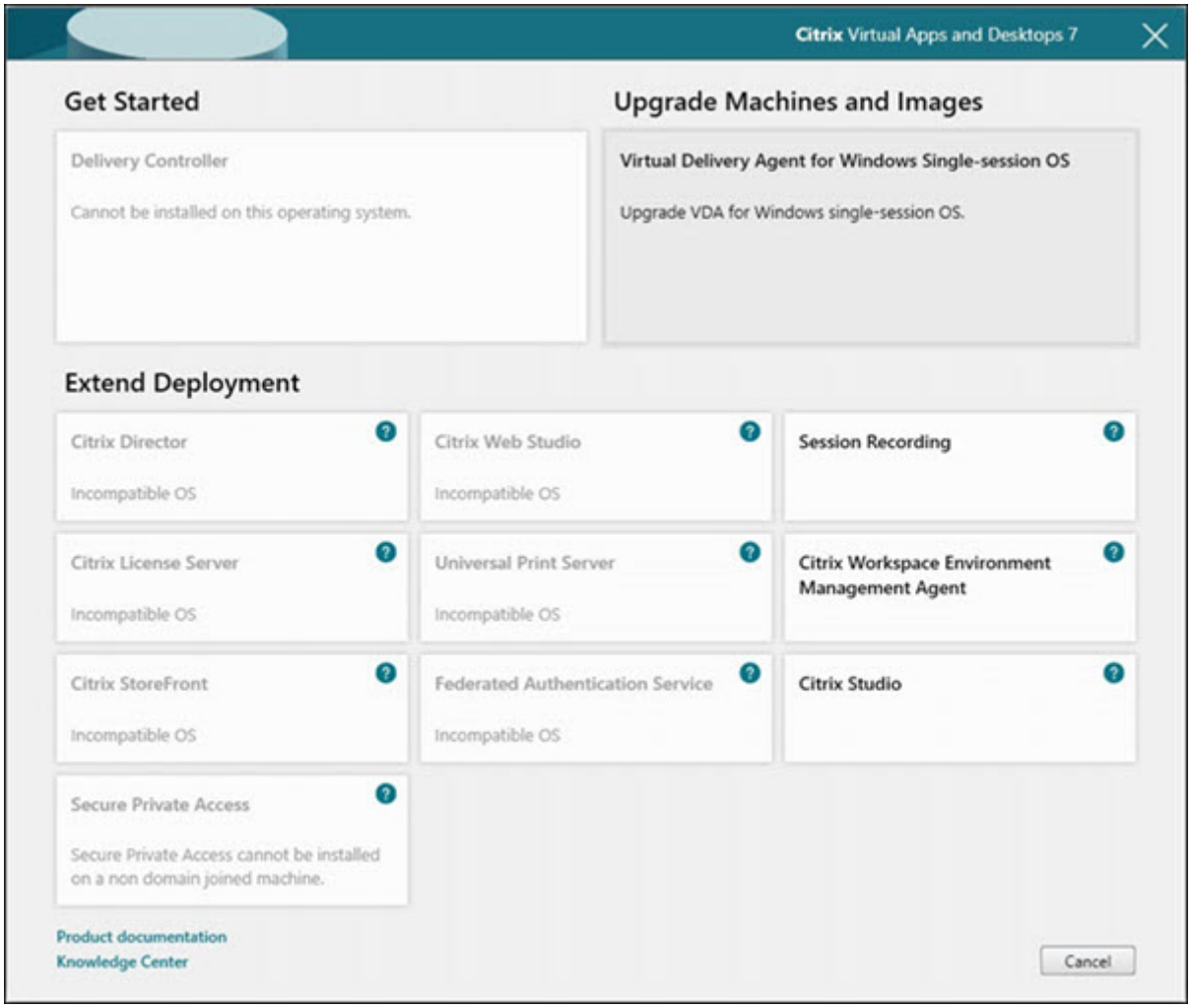
   Se iniciará el asistente de instalación.

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 esta opción.

Paso 3. Seleccione el VDA

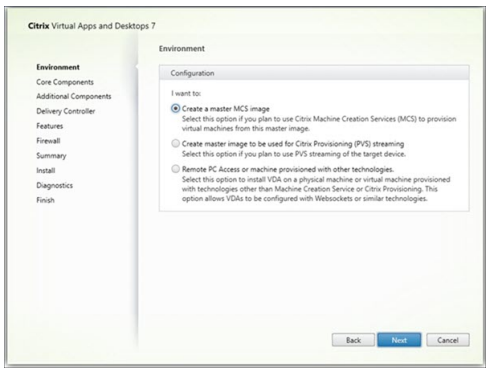


Seleccione la entrada **Virtual Delivery Agent**. El instalador sabe si se está ejecutando en un sistema operativo de sesión única o multisesión, por lo que solo ofrece el tipo de VDA apropiado.

Por ejemplo: si ejecuta el instalador en una máquina Windows Server 2019, 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 para aprovisionar más máquinas.

La opción que elija afecta a las herramientas de Citrix Provisioning 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.

Elija una de las siguientes opciones:

- **Crear una imagen maestra de MCS:** Seleccione esta opción para instalar un VDA en la imagen de una VM si va a usar Machine Creation Services para aprovisionar máquinas virtuales. Esta opción instala Machine Identity Service. Esta es la opción predeterminada.

  Opción de la línea de comandos: `/mastermcsimage` o `/masterimage`

> **Importante:**
>
> Los medios de instalación o la imagen ISO deben montarse localmente. No se admite el montaje de una imagen ISO en una unidad de red para instalar software.

- **Crear una imagen maestra con Citrix Provisioning o herramientas de aprovisionamiento de terceros:** Seleccione esta opción para instalar un VDA en la imagen de una VM o si va a usar Citrix Provisioning o herramientas de aprovisionamiento de terceros (como Microsoft System Center Configuration Manager) para aprovisionar 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 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.

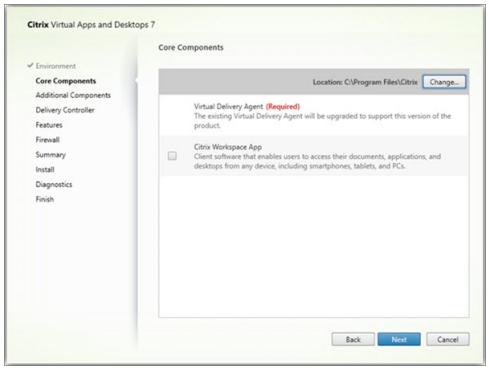
  Opción de línea de comandos: `/remotepc`

Haga clic en **Siguiente**.

Esta página no aparecerá:

- Si actualiza la versión de un VDA
- Si usa el instalador `VDAWorkstationCoreSetup_2308.exe`, `VDAServerSetup_2308.exe` o `VDAWorkstationSetup_2308.exe`

Paso 5. Seleccionar los componentes que instalar y la ubicación de la instalación



En la página **Componentes principales**:

- **Ubicación:** De forma predeterminada, los componentes se instalan en `C:\Program Files\Citrix`. Esta opción predeterminada no presenta problemas para la mayoría de las implementaciones. Si indica otra ubicación, esta debe tener permisos de `execute` 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.

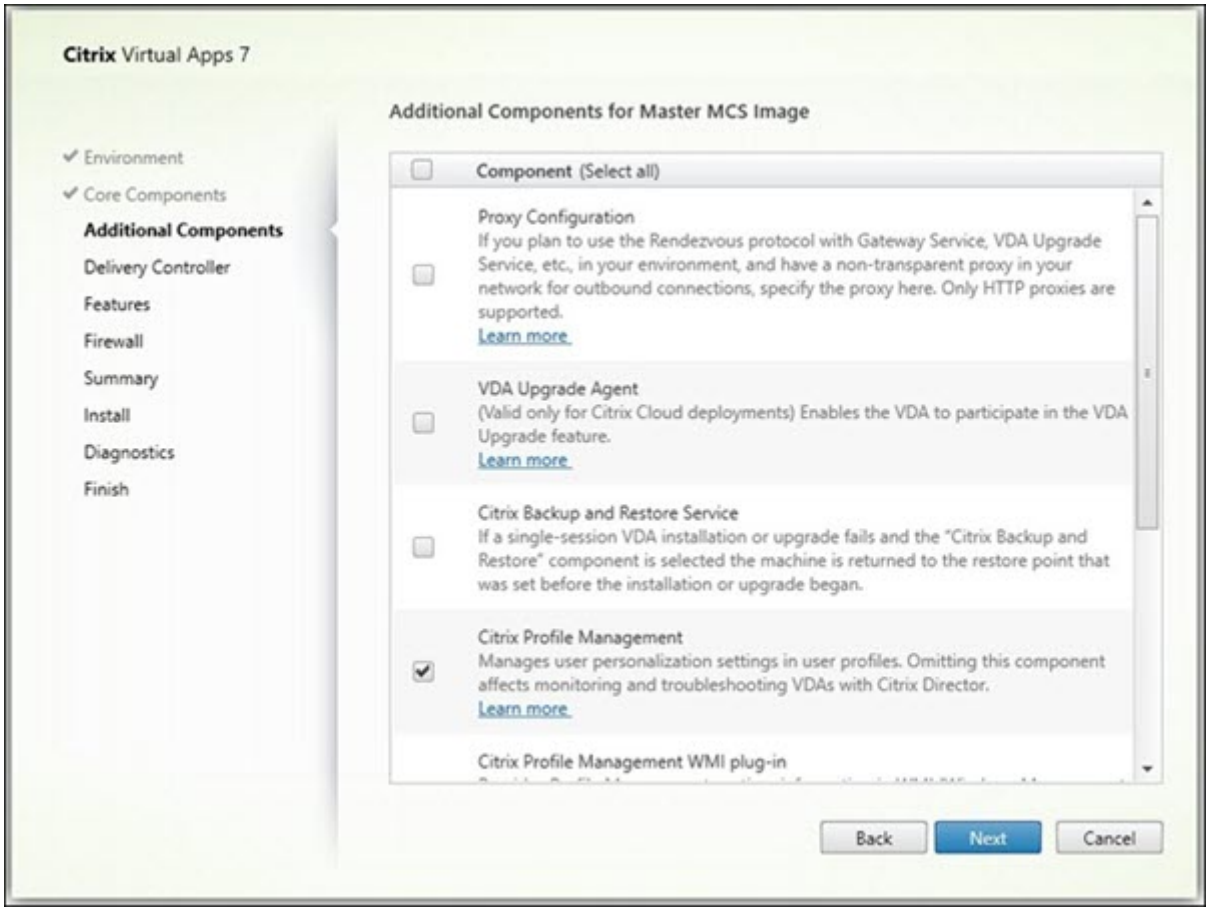
Haga clic en **Siguiente**.

Opciones de línea de comandos: `/installdir`, `/components vda,plugin` para instalar el VDA y la aplicación Citrix Workspace para Windows

> **Nota:**
>
> Puede optar por instalar, actualizar o desinstalar la aplicación Citrix Workspace durante la instalación, actualización o desinstalación de un VDA en los siguientes casos:

- Durante la instalación de un VDA, puede optar por instalar la aplicación Citrix Workspace. De forma predeterminada, la aplicación Citrix Workspace no se instala durante la instalación del VDA.
- Durante una actualización de versión de un VDA, si la aplicación Citrix Workspace aún no está instalada en el VDA, puede optar por instalar la aplicación Citrix Workspace.
- Durante una actualización de versión de un VDA, si se puede actualizar la versión de la aplicación Citrix Workspace, aparece la opción para hacerlo.
- Durante la desinstalación de un VDA, puede optar por no desinstalar la aplicación Citrix Workspace. De forma predeterminada, la aplicación Citrix Workspace se desinstala durante la desinstalación del VDA.

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 - VDA	No seleccionado	No seleccionado
Capa de personalización de usuarios	No seleccionado	No se muestra porque no es válido para este caso de uso.
Citrix Profile Management	Seleccionado	No seleccionado
Citrix Profile Management WMI Plug-in	Seleccionado	No seleccionado
Citrix VDA Upgrade Agent	No seleccionado	No seleccionado
Copia de seguridad y restauración de Citrix	No seleccionado	No seleccionado
Citrix MCS IODriver	No seleccionado	No seleccionado
Citrix Rendezvous V2	No seleccionado	No seleccionado

Esta página no aparecerá si:

- Utiliza 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. (Los componentes pueden aparecer en un orden diferente en el instalador).

- **Personalización de Citrix para App-V:** Instale este componente si va a usar aplicaciones provenientes de paquetes de Microsoft App-V. Para obtener información detallada, consulte Implementar y entregar aplicaciones de 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 de Citrix:** 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.

  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 Profile Management:** 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**, 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 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 Profile Management "` para habilitar la instalación del componente, `/exclude "Citrix Profile Management"` para impedir la instalación del componente.

- **Plug-in WMI de Citrix Profile Management:** 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 Profile Management WMI Plug-in"` para habilitar la instalación del componente, `/exclude "Citrix Profile Management WMI Plug-in"` para impedir la instalación del componente.

- **Agente de actualización de VDA:** Aplicable solamente a las implementaciones de Citrix DaaS (antes, Citrix Virtual Apps and Desktops Service). Permite que los VDA participen en la función de actualización de VDA. Puede utilizar esta función para actualizar la versión de los VDA de un catálogo desde la consola de administración de forma inmediata o a una hora programada. Si este agente no está instalado, puede actualizar un VDA mediante el instalador de VDA en la máquina.

  Opciones de línea de comandos: `/includeadditional "Citrix VDA Upgrade Agent"` para habilitar la instalación del componente, `/exclude "Citrix VDA Upgrade Agent"` para impedir la instalación del componente.

- **Memoria caché de escritura de E/S de MCS para optimizar el almacenamiento:** Instala el controlador de E/S de Citrix MCS. Para obtener más información, consulte Almacenamiento compartido por los hipervisores y Configurar caché para datos temporales.

  Opciones de línea de comandos: `/includeadditional "Citrix MCS IODriver"` para habilitar la instalación del componente, `/exclude "Citrix MCS IODriver"` para impedir la instalación del componente.

- **Configuración de proxy:** Si tiene previsto usar el protocolo Rendezvous con Gateway Service, el servicio de actualización de versión de VDA, etc., en su entorno y tiene un proxy no transparente en la red para las conexiones salientes, especifique el proxy aquí. Solo se admiten proxies HTTP.

  Si instala este componente, especifique la dirección del proxy o la ruta del archivo PAC en la página **Configuración del proxy de Rendezvous**. Para obtener más información sobre la funcionalidad, consulte Protocolo Rendezvous.

  Opción de línea de comandos: `/includeadditional "Citrix Rendezvous V2"` para habilitar la instalación del componente, `/exclude "Citrix Rendezvous V2"` para impedir la instalación del componente.

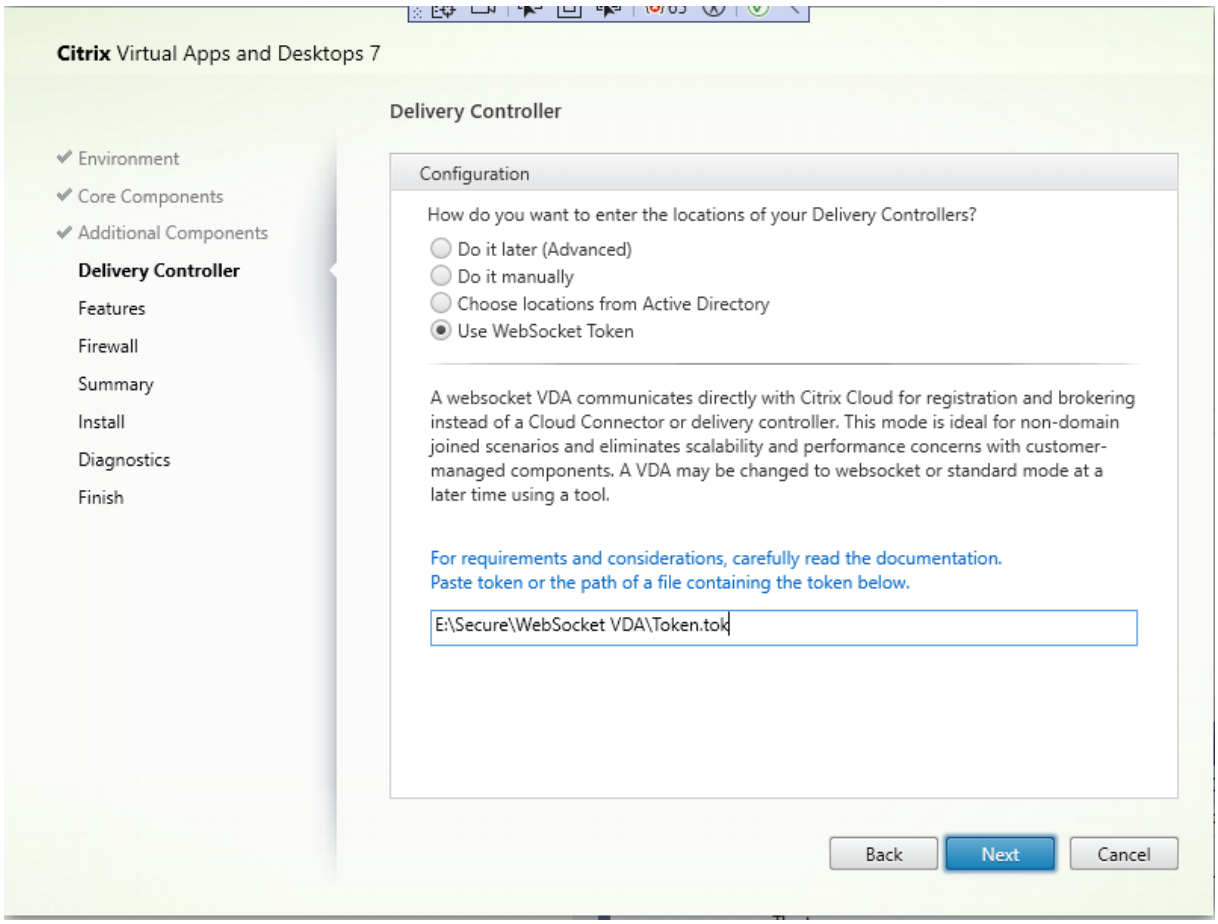
- **Copia de seguridad y restauración de Citrix:** Si se produce un error al instalar o actualizar la versión de un VDA, este componente puede devolver la máquina a una copia de seguridad que se realizó antes de la instalación o la actualización.

  Asegúrese de que se cumplen los requisitos previos de Microsoft, tal y como se indica en Antes de la instalación.

  Opción de línea de comandos: `/includeadditional "Citrix Backup and Restore"` para habilitar la instalación del componente, `/exclude "Citrix Backup and Restore"` para impedir la instalación del componente.

  > **Nota:**
  >
  > Si la optimización del almacenamiento MCS está habilitada, es posible que se produzca un error en la copia de seguridad o restauración del sistema operativo de escritorio o servidor Windows. Para resolver este problema, inhabilite la opción de optimización del almacenamiento de MCS en el metainstalador.

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 mientras instala el VDA (**Hacerlo manualmente**). 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 más Controllers, 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.
- **Usar token de WebSocket (Technical Preview):** Crea un VDA de WebSocket. El WebSocketToken es para el token que se requiere.
- **Dejar que Machine Creation Services lo haga automáticamente:** Esta opción es válida sola-

mente si utiliza Machine Creation Services (MCS) para aprovisionar máquinas.

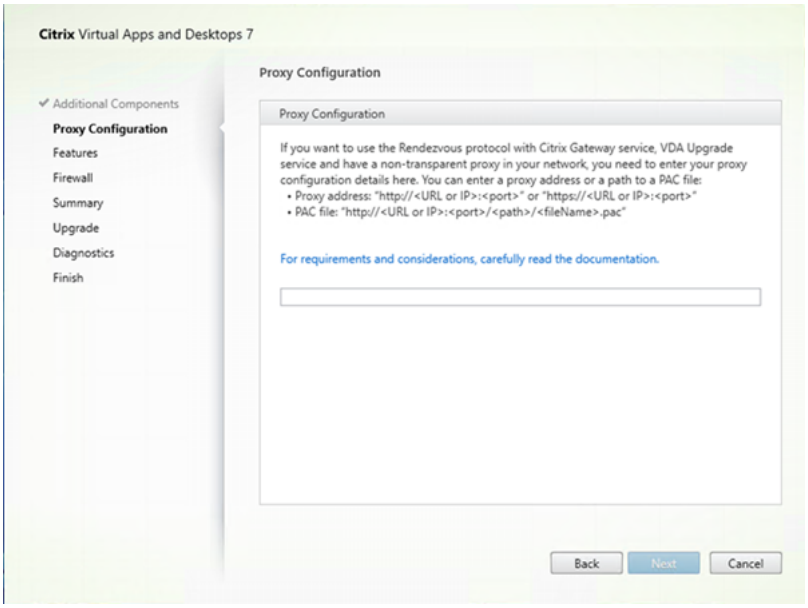
Haga clic en **Siguiente**. Si ha seleccionado la opción **Hacerlo más tarde (avanzado)**, se le pedirá una confirmación de que especificará las direcciones de Controller más adelante.

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. Configuración de proxy



La página **Configuración del proxy** aparece solo si ha habilitado la casilla de verificación **Configuración del proxy** en la página **Componentes adicionales**.

1. Seleccione si va a especificar el origen de proxy por dirección de proxy o por ruta de archivo PAC.

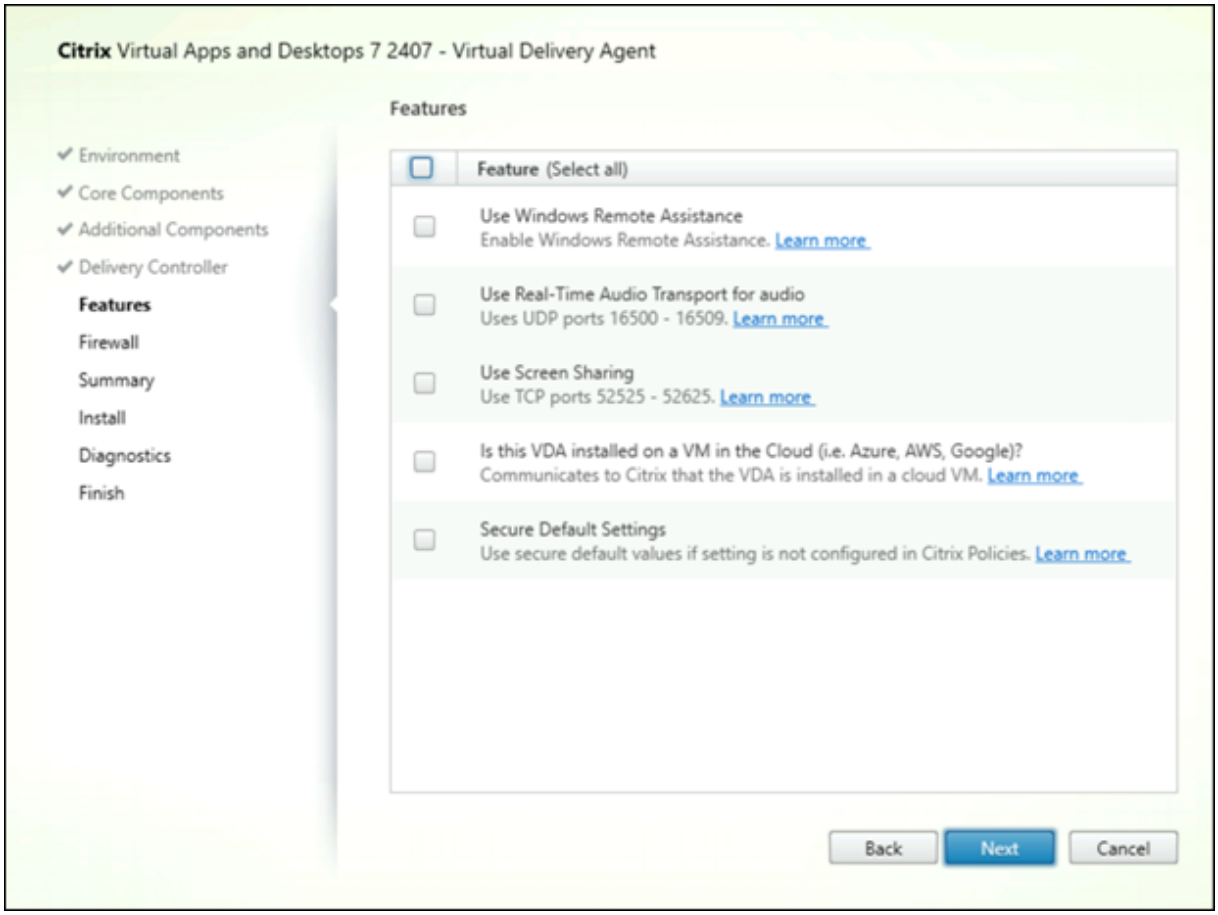
2. Especifique la dirección del proxy o la ruta del archivo PAC.

   - Formato de dirección de proxy: `http://<url-or-ip>:<port>`
   - Formato de archivo PAC: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

El firewall del puerto de proxy debe estar abierto para que la prueba de conexión se haga correctamente. Si no se puede establecer una conexión con el proxy, puede elegir si quiere continuar con la instalación del VDA.

Opción de línea de comandos: `/proxyconfig`

Paso 9. 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.

- **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`

- **Usar la pantalla compartida:** Cuando está habilitada, los puertos usados para compartir pantalla se abren en el firewall de Windows. Opción inhabilitada de forma predeterminada.

  Opción de línea de comandos: `/enable_ss_ports`

- **¿El VDA está instalado en una máquina virtual en una nube?** Este parámetro ayuda a Citrix a identificar correctamente ubicaciones de recursos para implementaciones de VDA locales y de servicio (Citrix Cloud) con el fin de obtener telemetría. Esta función no afecta a la utilización por parte del cliente. Habilite este parámetro si su implementación usa Citrix DaaS (valor predeterminado = inhabilitado).

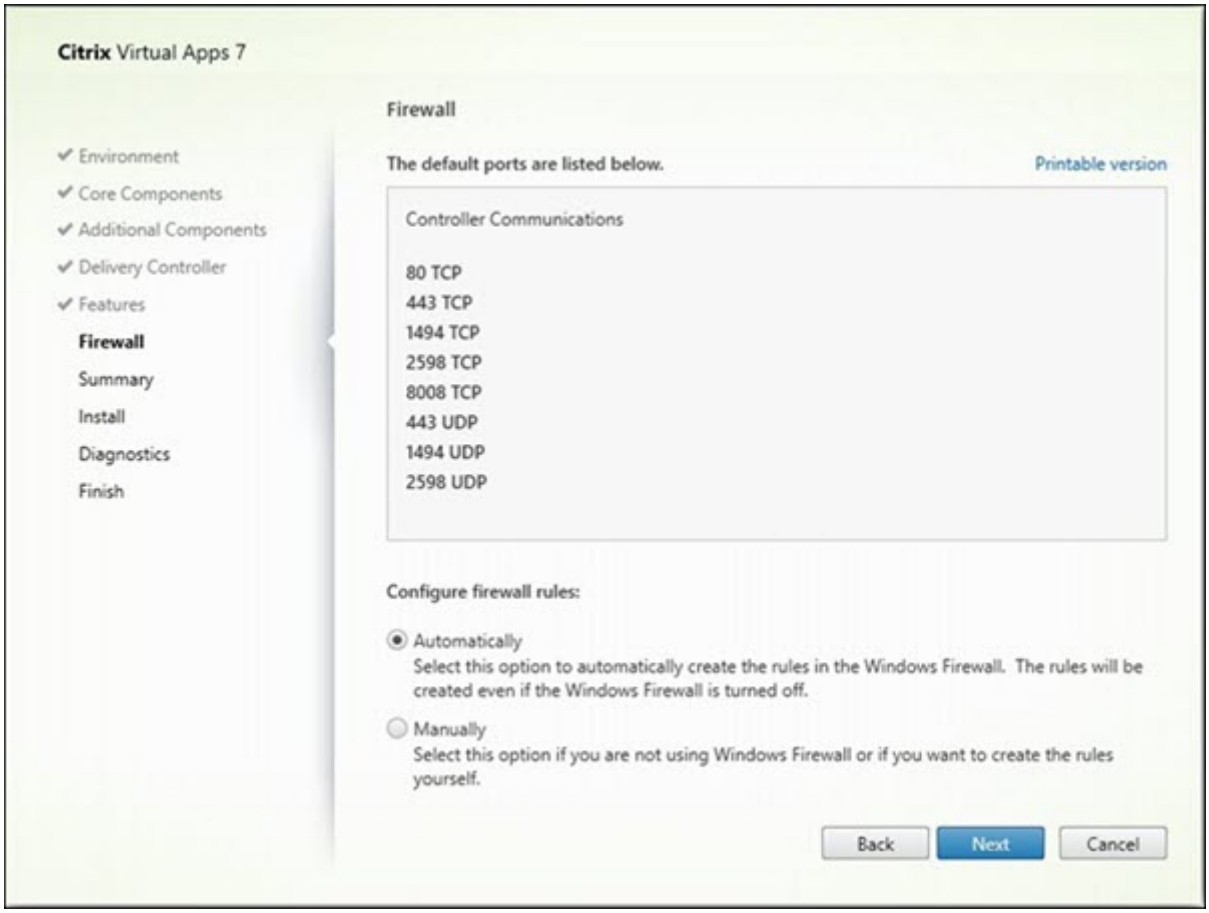
  Opción de línea de comandos: `/xendesktopcloud`

- **Parámetros predeterminados seguros:** Esta opción cambia la configuración predeterminada de varias funciones de habilitadas a inhabilitadas para ofrecer una configuración lista para usar más segura. Las funciones relevantes son: redirección de unidades del cliente, redirección de carpetas especiales, arrastrar y colocar, redirección de dispositivos TWAIN del cliente, redirección de dispositivos Plug and Play USB del cliente, redirección de impresoras del cliente, redirección del portapapeles del cliente y redirección del micrófono del cliente.

Opción de línea de comandos: `/ENABLE_SECURE_DEFAULTS`

Haga clic en **Siguiente**.

Paso 10. Puertos de firewall

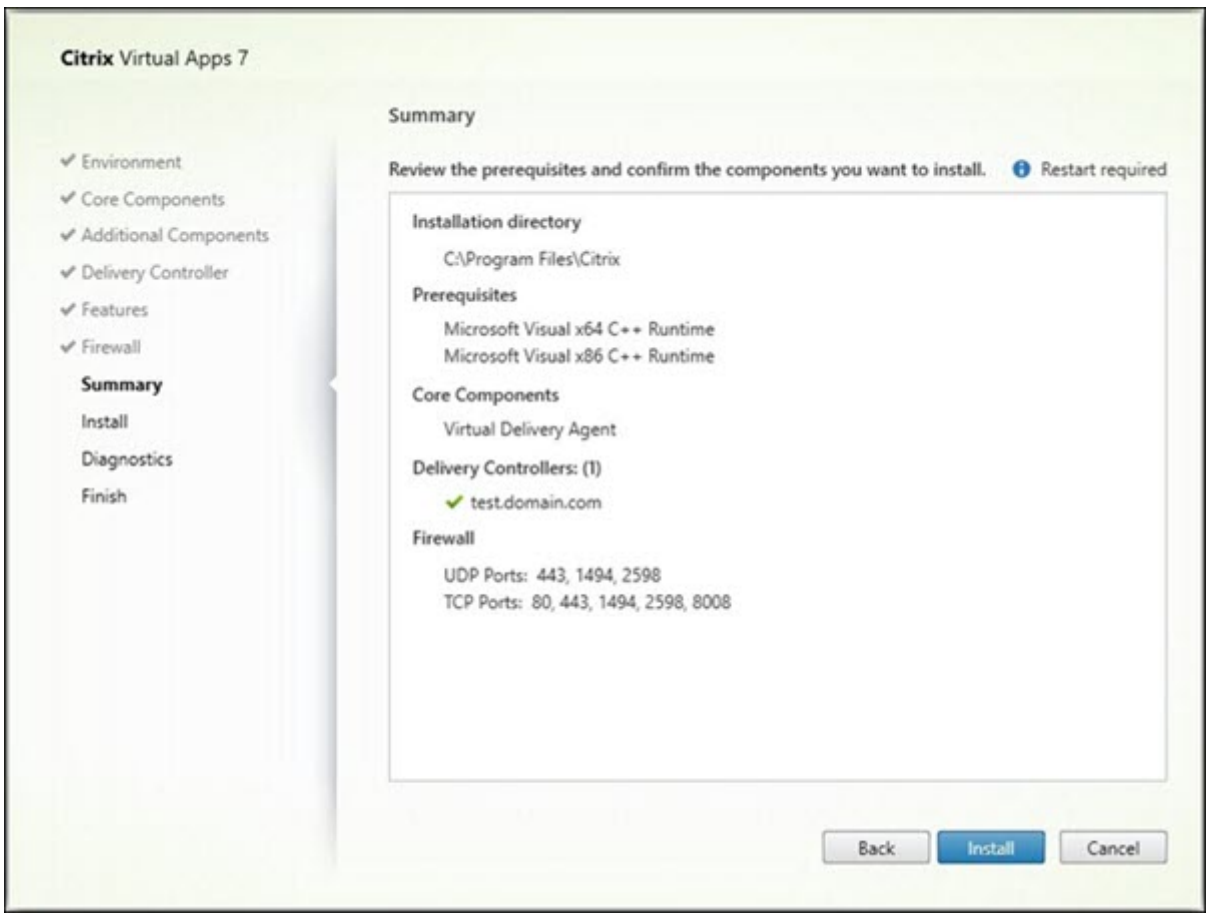


De forma predeterminada, los siguientes puertos se abren automáticamente en la página **Firewall** si el servicio Firewall de Windows se está ejecutando, incluso aunque no esté habilitado. Esta opción predeterminada no presenta problemas para la mayoría de las implementaciones. Para obtener información acerca de los puertos, consulte Puertos de red.

Haga clic en **Siguiente**.

Opción de línea de comandos: `/enable_hdx_ports`

Paso 11. Revise los requisitos previos y confirme la instalación

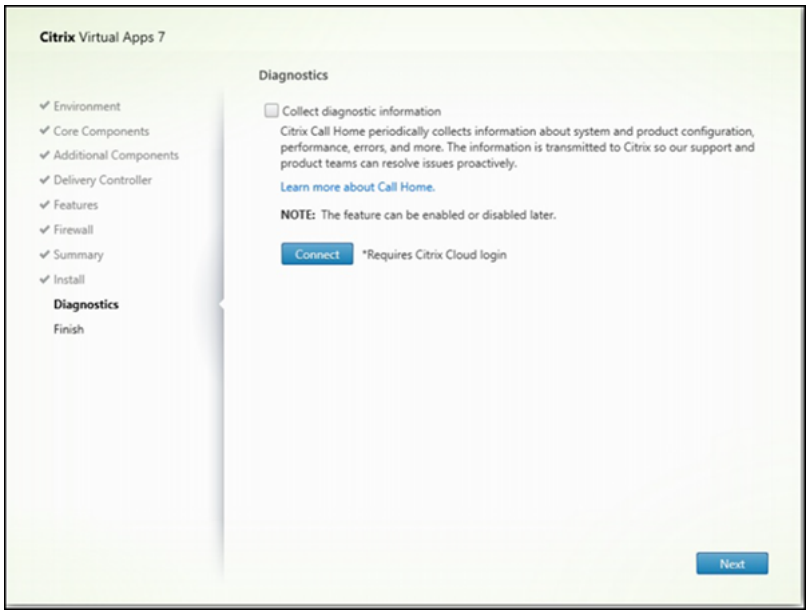


La página **Resumen** muestra lo que se instalará. Use el botón **Atrás** para volver a las páginas anteriores del asistente y cambiar las opciones.

Cuando haya terminado, haga clic en **Instalar**.

Es posible que la máquina se reinicie una o más veces si los requisitos previos todavía no están instalados o habilitados. Consulte Antes de la instalación.

Paso 12: Diagnóstico



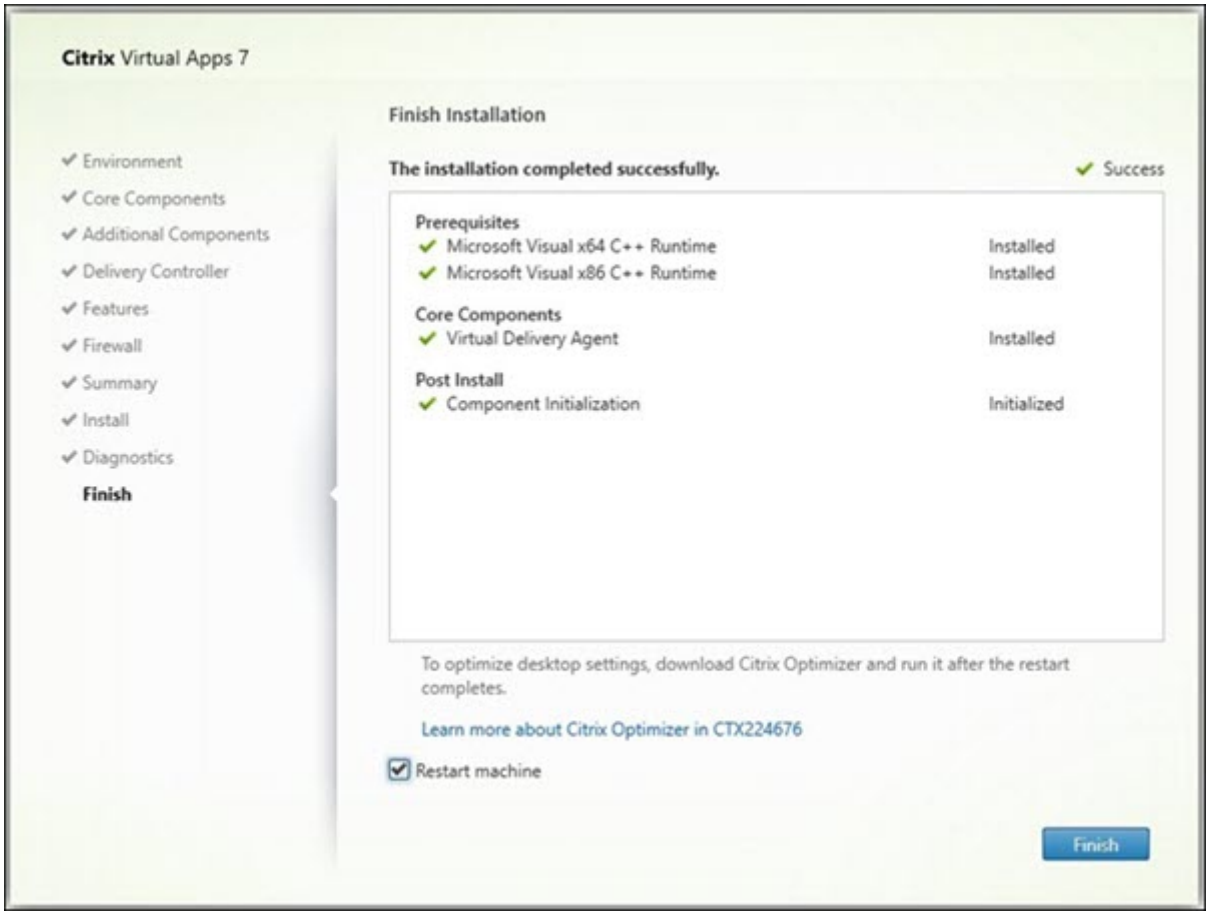
En la página **Diagnósticos**, elija si quiere participar en Citrix Call Home. Si elige participar (opción predeterminada), haga clic en **Conectar**. Cuando se le solicite, introduzca las credenciales de su cuenta de Citrix

Una vez validadas las credenciales (o si elige no participar), haga clic en **Siguiente**.

Cuando utiliza el instalador completo del producto, si hace clic en **Conectar** en la página **Diagnósticos** sin seleccionar antes **Recopilar información de diagnóstico**, al cerrar el cuadro de diálogo **Conectar con Citrix Insight Services**, el botón **Siguiente** está inhabilitado. No puede pasar a la siguiente página. Para volver a habilitar el botón **Siguiente**, seleccione y desmarque inmediatamente **Recopilar información de diagnóstico**.

Para obtener más información, consulte Call Home.

Paso 13: 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

Citrix Optimizer

Citrix Optimizer es una herramienta para el sistema operativo Windows que ayuda a los administradores de Citrix a eliminar y mejorar varios componentes para optimizar los VDA.

Una vez instalado un VDA y completado el reinicio final, descargue e instale Citrix Optimizer. Consulte CTX224676. El artículo de CTX contiene el paquete de descarga e instrucciones sobre la instalación y el uso de Citrix Optimizer.

Personalizar un VDA

Para 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

Solucionar problemas

- Para obtener información sobre cómo informa Citrix de los resultados de las instalaciones 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 funciones de la máquina Windows muestra la versión real del VDA.
- Después de instalar un VDA, no se pueden entregar aplicaciones o escritorios a los usuarios hasta que el VDA se registre con un Delivery Controller.

  Para obtener información sobre los métodos de registro de VDA y cómo solucionar problemas de registro, consulte Registro de VDA.

Limitación conocida

Cuando usa la versión 1912 o anterior de la aplicación Citrix Workspace para Windows, la sesión se interrumpe al cabo de un rato. Este problema se ha solucionado en las versiones LTSR y CR más recientes de la aplicación Citrix Workspace.
Para obtener más información sobre las versiones compatibles, consulte versiones de la aplicación Citrix Workspace para Windows o Citrix Receiver para Windows Long Term Service Release.

Configurar el control de acceso de Windows Defender relacionado con la instalación del VDA

August 17, 2024

Los clientes configuran los parámetros de Control de acceso de Windows Defender (WDAC) para prohibir la carga de archivos binarios sin firmar. Por lo tanto, se prohíben los archivos binarios no firmados que se distribuyen a través de los instaladores de VDA, lo que restringe la instalación del VDA.

Citrix ahora firma todos los archivos binarios que genera con un certificado de firma de código de Citrix. Además, Citrix también firma los archivos binarios de terceros que se distribuyen junto con nuestro producto con un certificado que autentica esos archivos binarios de terceros como archivos binarios de confianza.

> **Importante:**
>
> La actualización de un VDA antiguo con archivos binarios de terceros sin firmar a una versión más reciente de VDA con archivos binarios firmados puede no colocar siempre los archivos binarios firmados en la máquina actualizada.
> Esto se debe a un mecanismo del sistema operativo por el que la actualización del sistema no reemplaza los archivos binarios que tienen la misma versión.
> Aunque los archivos binarios de terceros están firmados, Citrix no puede actualizar sus versiones, que están controladas por terceros, por lo que estos archivos binarios no se actualizan. Para evitar esta limitación:
>
> 1. Incluya los archivos binarios en una lista de permitidos. Esto elimina la necesidad de firmar los archivos binarios.
> 2. Desinstale el VDA anterior e instale el nuevo. Es como una instalación nueva de un VDA y se instalarán las versiones firmadas.

Crear una nueva directiva base con el asistente

WDAC le permite agregar archivos binarios de confianza para que se ejecuten en su sistema. Tras la instalación de WDAC, se abre automáticamente el **Asistente para directivas de control de aplicaciones de Windows Defender**.

Para agregar los archivos binarios, se debe crear una nueva directiva WDAC base. En esta sección se proporcionan las directrices recomendadas por Citrix para crear una directiva base.

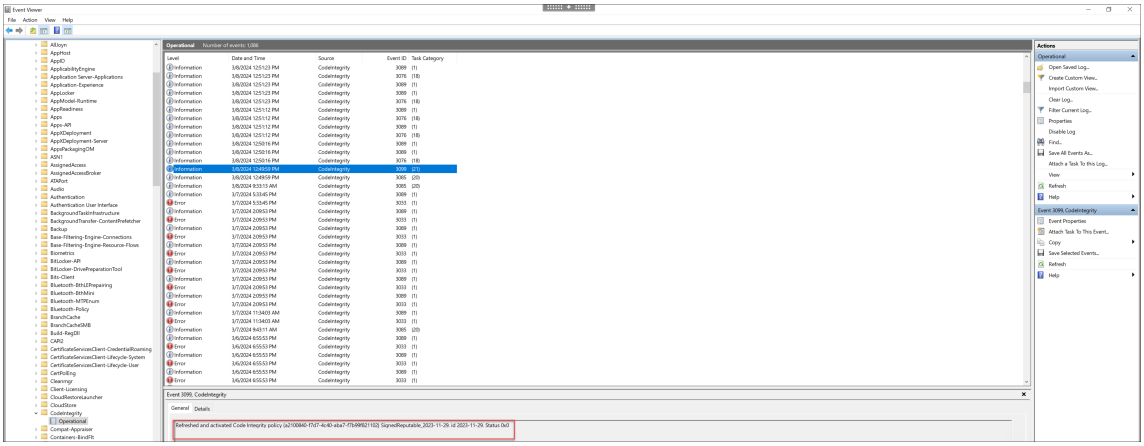
- Seleccione el **modo firmado y de confianza** como plantilla base, ya que autoriza los componentes operativos de Windows, las aplicaciones instaladas desde Microsoft Store, todo el software firmado por Microsoft y los controladores de terceros de hardware compatible con Windows.
- **Habilite el modo de auditoría**, puesto que le permite probar las nuevas directivas de control de aplicaciones de Windows Defender antes de aplicarlas.
- Agregue una **regla personalizada** para las **reglas de archivo** para especificar el nivel en el que se identifican las aplicaciones y se confía en ellas, y proporcione un archivo de referencia. Al seleccionar "Publicador"(Publisher) como tipo de regla, se puede seleccionar un archivo de referencia firmado por uno de los certificados de Citrix.
- Después de agregar las reglas, vaya a la carpeta en la que se guardan los archivos `.XML` y `.CIP`. El archivo `.XML` contiene todas las reglas definidas en la directiva. Se puede configurar para cambiar, agregar o quitar cualquier regla.
- Antes de implementar las directivas de WDAC, el archivo `.XML` debe convertirse a su formato binario. El archivo WDAC convierte el archivo `.XML` en un archivo `.CIP`.
- Copie el archivo `.CIP` y péguelo en: C:\WINDOWS\System32\CodeIntegrity\CiPolicies\Active y reinicie la máquina. La directiva generada se aplicará en modo de auditoría.
- Para ver un proceso paso a paso para crear una directiva base, consulte Creación de una nueva directiva base con el Asistente.

Cuando se aplica esta directiva, WDAC no emite advertencias sobre ningún archivo de Citrix que esté firmado por la entidad de certificación/publicación.

Del mismo modo, podemos crear una regla de nivel de publicador para los archivos que han sido firmados por un tercero.

Verificar la directiva aplicada

1. Una vez reiniciada la máquina, abra el **Visor de eventos** y vaya a **Registros de aplicaciones y servicios > Microsoft > Windows > CodeIntegrity > Operational**.
2. Asegúrese de que la directiva aplicada esté activada.



3. Busque los registros que hayan infringido la directiva y compruebe las propiedades de ese archivo. En primer lugar, confirme que se ha firmado. Si no es así y ha habido una actualización de versión de VDA en esta máquina, lo más probable es que se trate del caso descrito en la limitación anterior. Si tiene firma, es posible que este archivo se haya firmado con el certificado alternativo, como se describió anteriormente.

Un ejemplo de archivo generado por Citrix y firmado con un certificado de Citrix es `C:\Windows\System32\drivers\picadm.sys`.
Un ejemplo de archivo binario de terceros firmado con el certificado de terceros de Citrix es `C:\Program Files\Citrix\IcaConfigTool\Microsoft.Practices.Unity.dll`.

Instalar agentes VDA mediante scripts

August 17, 2024

> **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`. 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=\\fileserver1\share1`.
    - Si lo desea, puede especificar también una ubicación en el recurso compartido de red para guardar los registros centralizados. Por ejemplo: `SET LOGSHARE=\\fileserver1\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`. 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.

Solucionar 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_<DateTimeStamp>.log`
  - `VDA_Install_ProcessLog_<DateTimeStamp>.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 `ROOT` del recurso compartido `DEPLOYSHARE` (que contiene el archivo `AutoSelect.exe`).
  - Es capaz de autenticarse en los dos puntos compartidos `DEPLOYSHARE` y `LOG`.

- 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 muestra la versión real del VDA.
- Después de instalar un VDA, no se pueden entregar aplicaciones o escritorios a los usuarios hasta que el VDA se registre con un Delivery Controller.

  Para obtener información sobre los métodos de registro de VDA y cómo solucionar problemas de registro, consulte Registro de VDA.

Métodos de implementación de VDA de terceros

August 17, 2024

Para implementar correctamente un Virtual Delivery Agent (VDA) con Microsoft System Center Configuration Manager (SCCM) o herramientas de distribución de software similares, como Ansible and Microsoft Intune, Citrix recomienda usar el instalador de VDA a través de una serie de pasos.

> **Nota:**
>
> Los siguientes artículos describen solo recomendaciones basadas en la forma en que Citrix ha probado el entorno. Puede personalizar estos pasos según sus necesidades. Citrix no se hace responsable de las actualizaciones o ajustes necesarios para adaptarlo a las necesidades de los clientes.

- Instalar agentes VDA mediante SCCM
- Instalar agentes VDA mediante Ansible
- Instalar agentes VDA mediante Microsoft Intune

Instalar agentes VDA mediante SCCM

August 17, 2024

Información general

Microsoft Endpoint Configuration Manager, anteriormente System Center Configuration Manager (SCCM), es un producto de Windows que habilita la administración, implementación y protección de dispositivos y aplicaciones en toda la empresa.

> **Nota:**
>
> El siguiente artículo describe solo las recomendaciones basadas en la forma en que Citrix ha probado el entorno. Puede personalizar estos pasos según sus necesidades. Citrix no se hace responsable de las actualizaciones o ajustes necesarios para adaptarlo a las necesidades de los clientes.

Recomendaciones

- Para implementar correctamente un Virtual Delivery Agent (VDA) con 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.

Antes de comenzar

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.
- 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.
  Para obtener más información sobre la instalación de VDA, consulte Instaladores.

El **secuenciador de tareas de SCCM** administra todos los reinicios necesarios.

Pasos clave para implementar VDA con SCCM

En los pasos siguientes se describe cómo implementar el VDA mediante SCCM en la máquina virtual.

1. Instalar el VDA.
2. Crear una unidad organizativa (OU).
3. Verificar las máquinas.
4. Usar VDA para distribuir contenido.

Paso 1: Instalar el VDA

Después de identificar todos los requisitos previos, use el **secuenciador de tareas de SCCM** para completar las tareas siguientes:

1. Instale los VDA desde una copia accesible de los medios de instalación o desde uno de los instaladores independientes de VDA:

   - `VDAWorkstationSetup_XXXX.exe`
   - `VDAServerSetup_XXXX.exe`
   - `VDAWorkstationCoreSetup_XXXX.exe`

   Para obtener más información sobre los instaladores de VDA, consulte Instaladores.

   > **Nota:**
   >
   > Al actualizar la versión de un VDA, la máquina en la que está instalado debe estar en modo de mantenimiento, sin sesiones.

2. 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 usar un instalador de VDA que no sea `VDAWorkstationCoreSetup_XXXX.exe`, el instalador de VDA se copia en `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopVdaSetup.exe`.
   - Cuando se usa `VDAWorkstationCoreSetup_XXXX.exe`, el instalador del VDA se copia en `%ProgramData%\Citrix\XenDesktopSetup\XenDesktopRemotePCSetup.exe`.

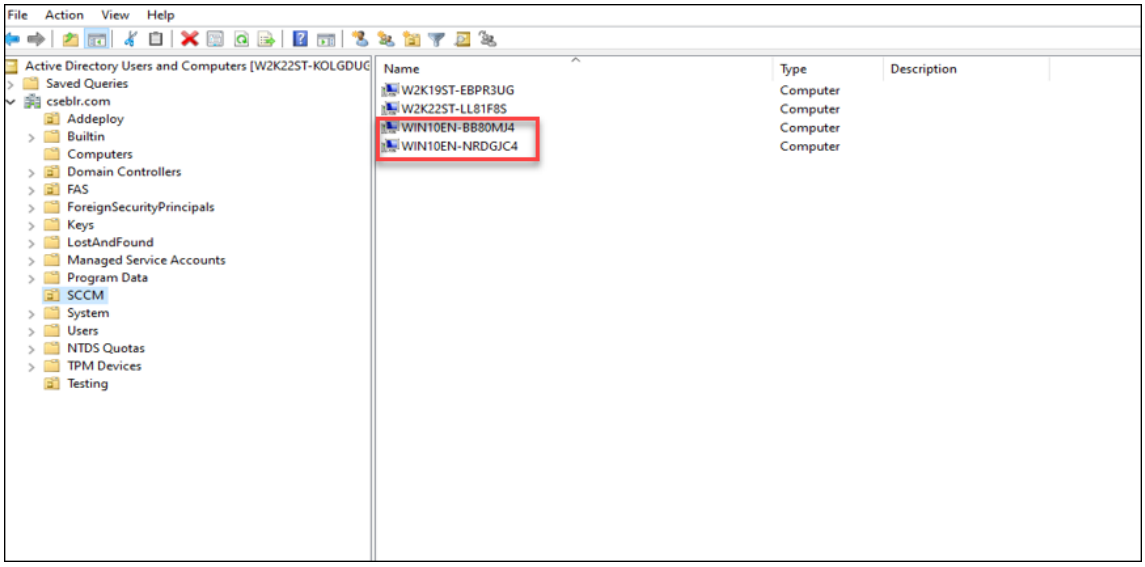
3. La ubicación del directorio del instalador de VDA también se almacena en el Registro `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaInstall" "MetaInstallerInstallLocat" "`.

4. Agregue las opciones de línea de comandos `/NOREBOOT`, `/NORESUME` y `/QUIET`.

- /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 de Registro RunOnce (\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce). Windows usa la clave para abrir el instalador del VDA cuando se reinicia la máquina. Esto es un problema para SCCM, ya que SCCM no puede supervisar la instalación ni capturar el código de salida.

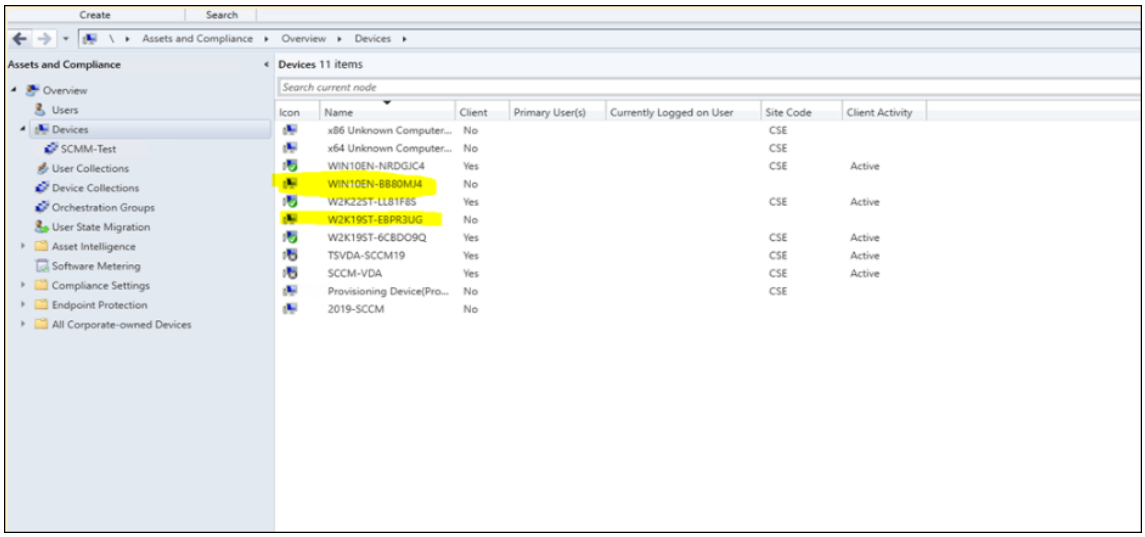
Paso 2: Crear una unidad organizativa (OU)

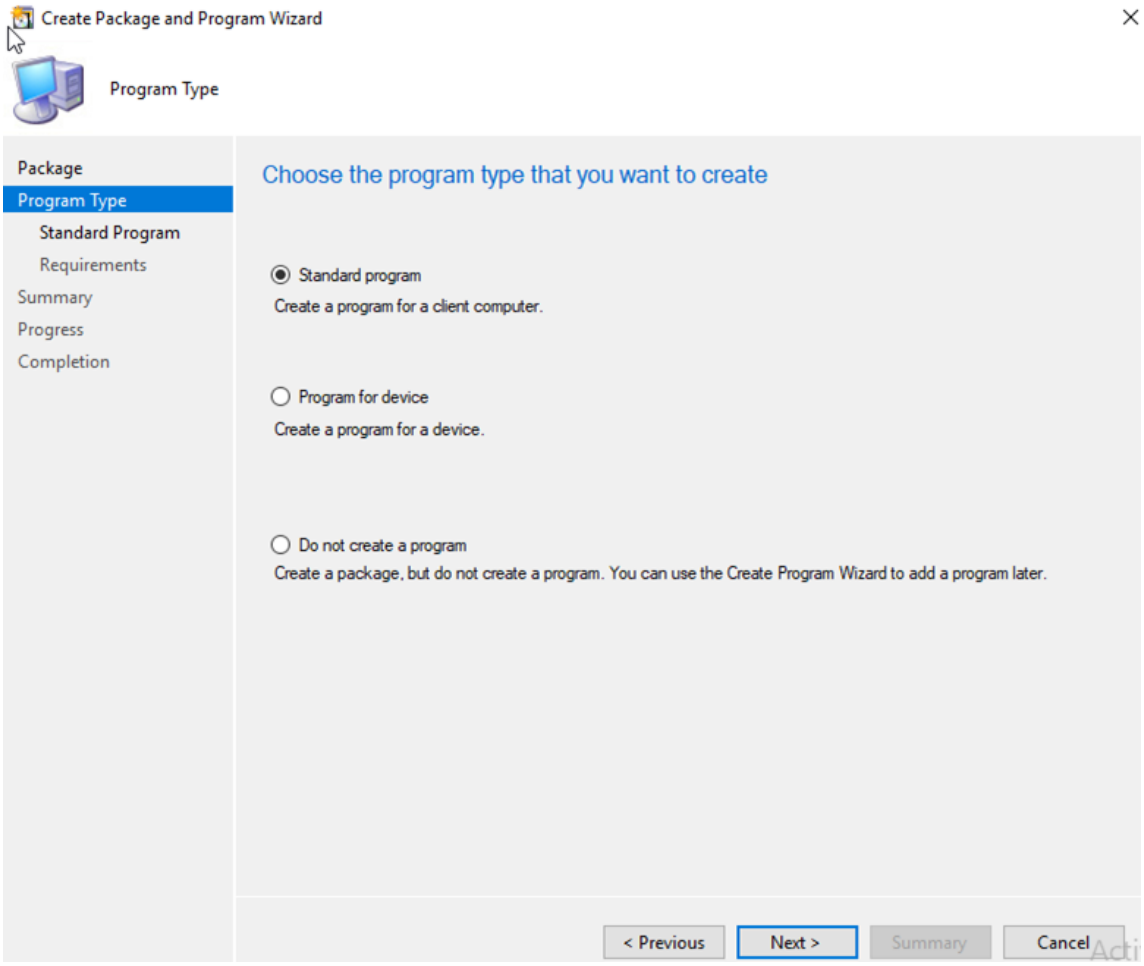
1. Cree dos máquinas virtuales unidas a un dominio que quiera agregar a la OU. Cuando las máquinas virtuales se crean inicialmente, se encuentran en la carpeta **Equipos**. Mueva las máquinas virtuales a la carpeta **SCCM**.
   Ejemplo: WIN10EN-BB80MJ4.cseblr.com
   W2K19ST-EBPR3UG.cseblr.com



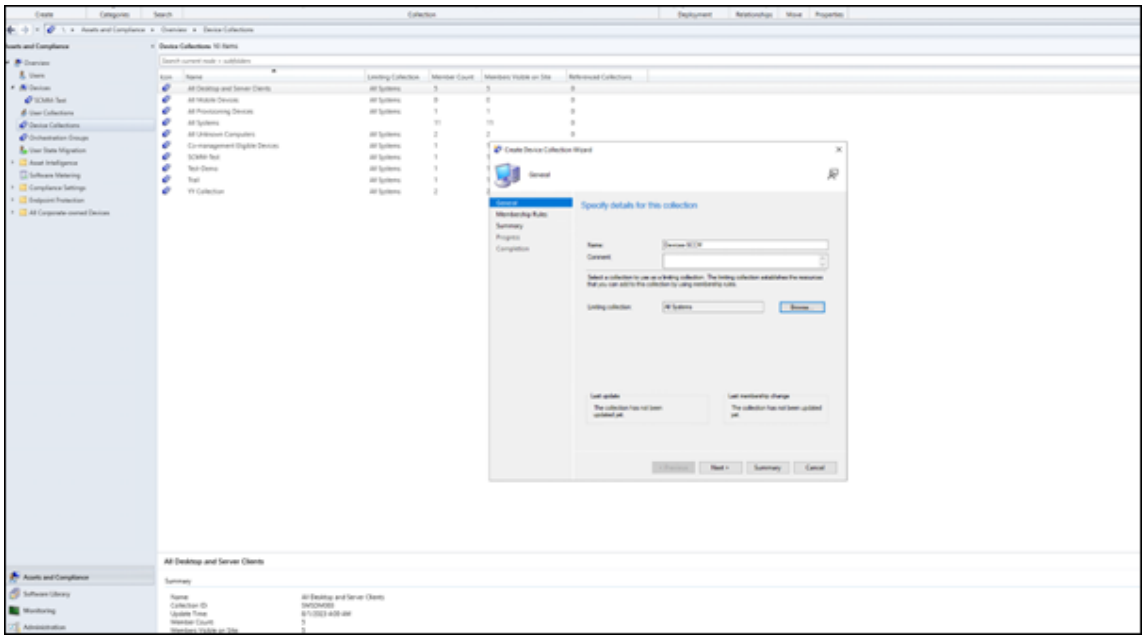
2. En Microsoft Configuration Manager, vaya a \Administration\Overview\Hierarchy Configuration\Discovery Methods\.
3. Haga clic en **Detección de sistemas de Active Directory** y seleccione la casilla de verificación **Habilitar detección de sistemas de Active Directory** para habilitar la detección automática de las máquinas virtuales recién creadas.
4. Haga clic en el  para seleccionar nuevos contenedores.

5. En la sección **Ubicación** , agregue la **ruta** en la que se encuentran las máquinas virtuales de SCCM.
6. Vaya a `\Administration\Overview\Site Configuration\Sites` y haga clic con el botón secundario en el VDA de SCCM.
7. Seleccione **Configuración de instalación de cliente > Instalación de inserción de cliente**. Se abre la ventana **Propiedades de la instalación de inserción de cliente**.
8. Una vez que las máquinas virtuales estén configuradas en `Enabled`, podrá ver la lista de máquinas virtuales como se muestra en las siguientes imágenes.

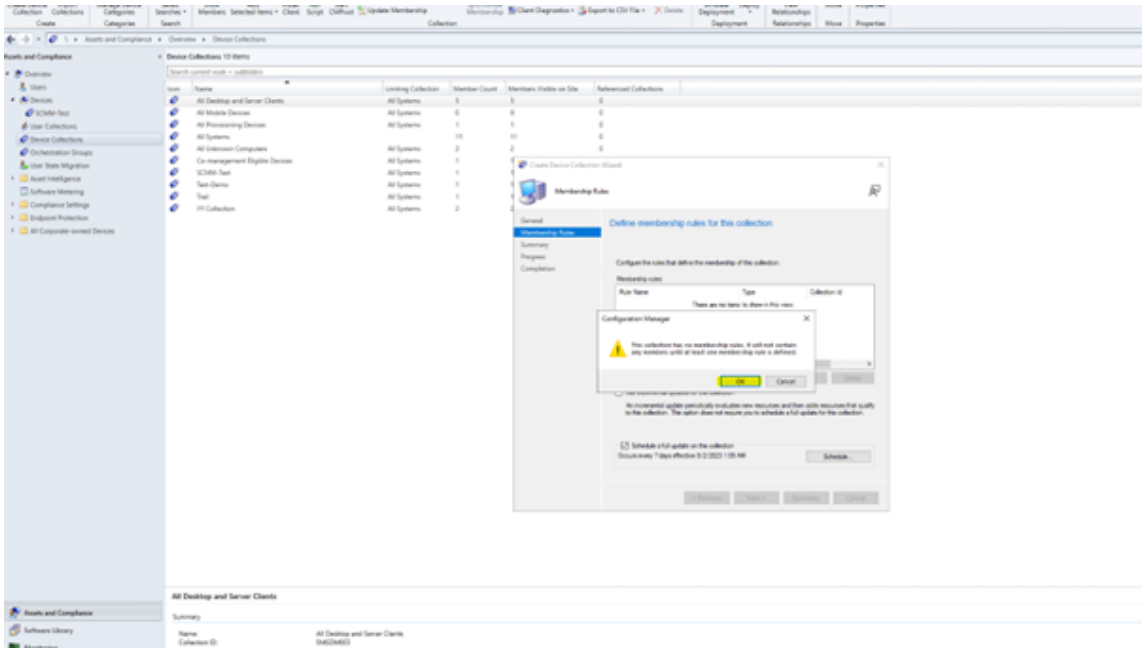




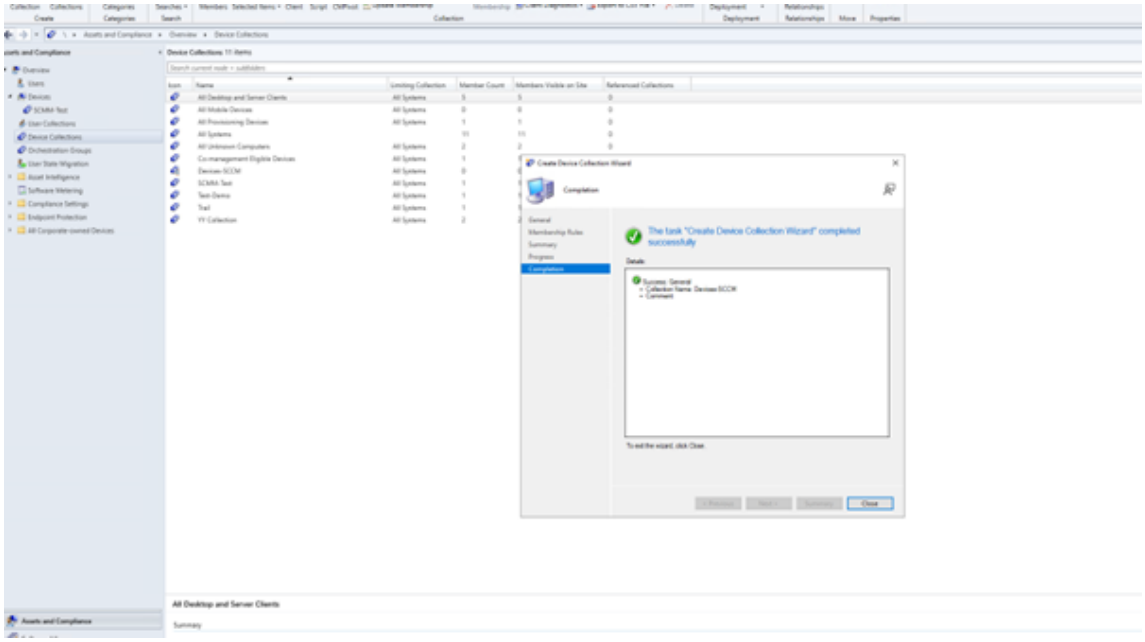
9. Cree una **Colección de dispositivos** para crear la unidad organizativa. Introduzca el **Nombre** de la colección.



10. Siga las instrucciones del asistente.

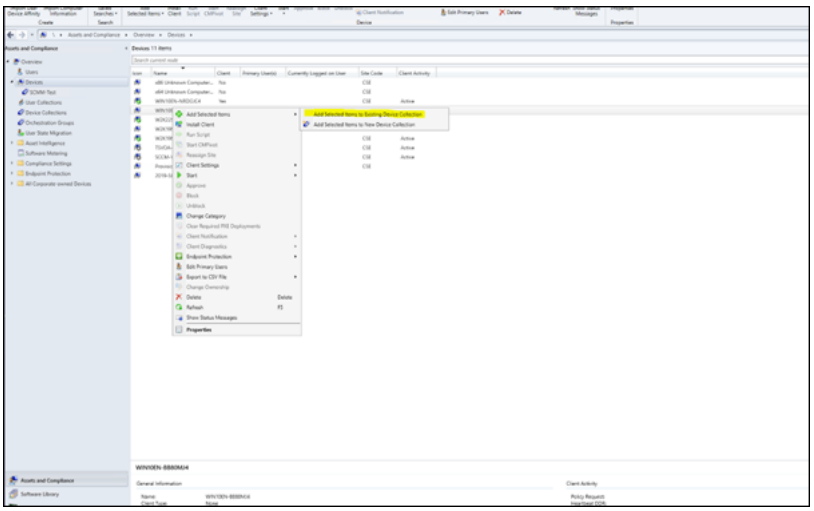


Se crea la OU.

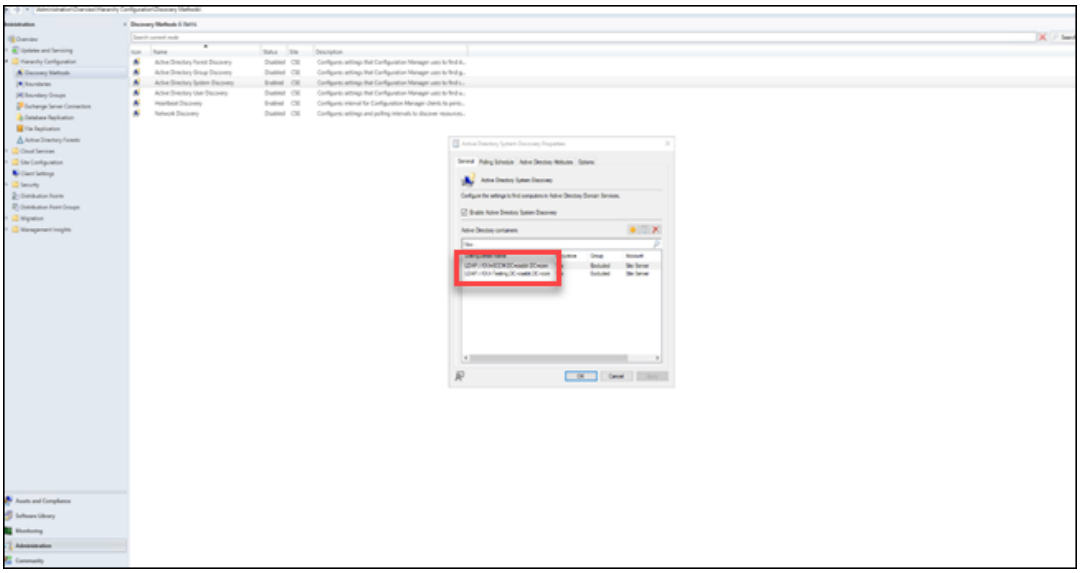


11. Agregue las máquinas virtuales creadas a la colección de dispositivos recién creada.

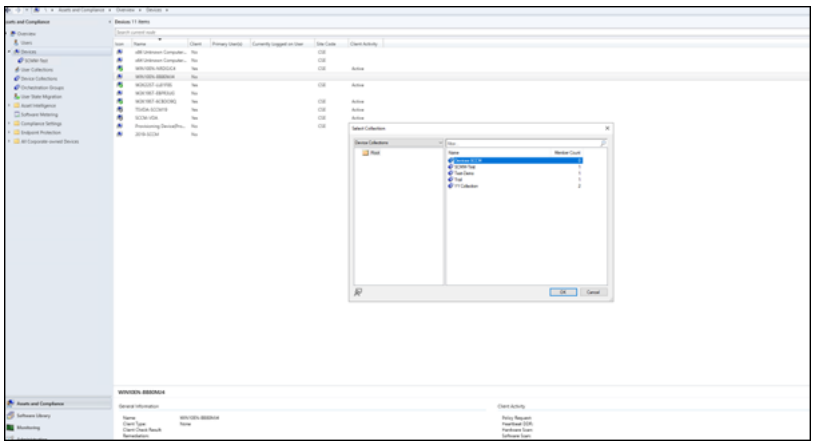
    a) Haga clic con el botón secundario en la VM. Seleccione **Agregar elementos seleccionados > Agregar elementos seleccionados a la colección de dispositivos existente**.



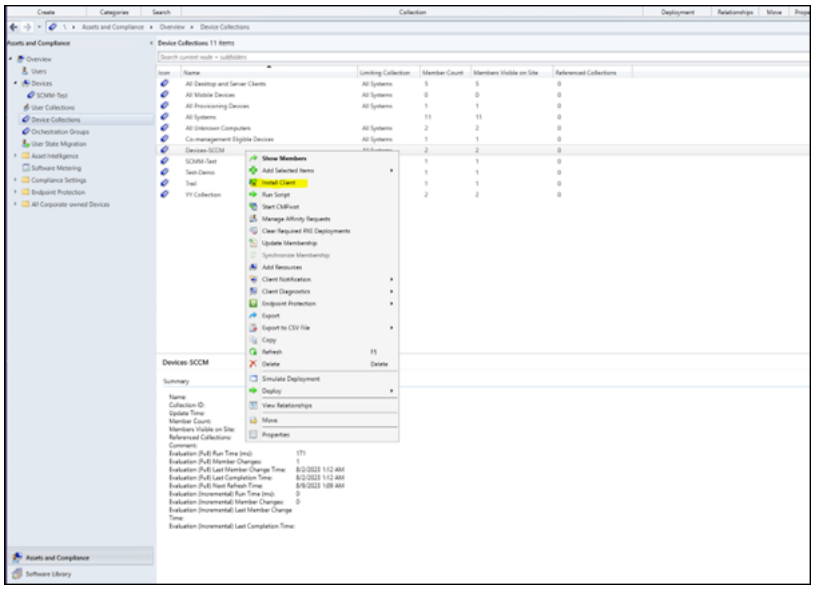
b) En la ventana **Seleccionar colección**, seleccione el nombre del dispositivo. En este ejemplo, es `Devices-SCCM`.



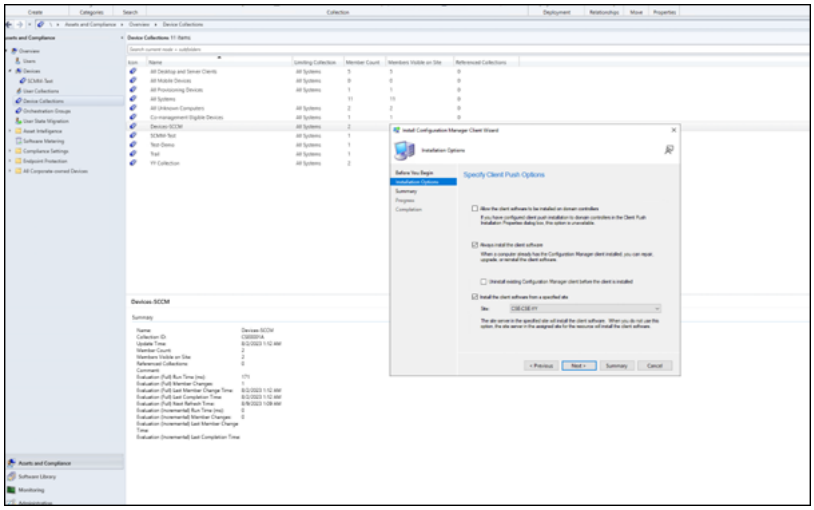
`Devices-SCCM` aparece en **Activos y compatibilidad > Información general > Recopilaciones de dispositivos**.



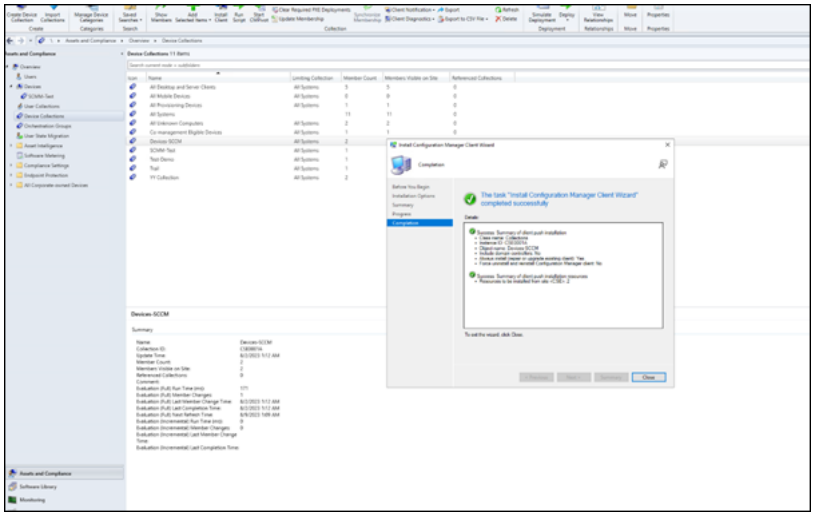
12. Seleccione **Instalar cliente** en el Recopilador de dispositivos.



13. Seleccione el **sitio** de instalación requerido.



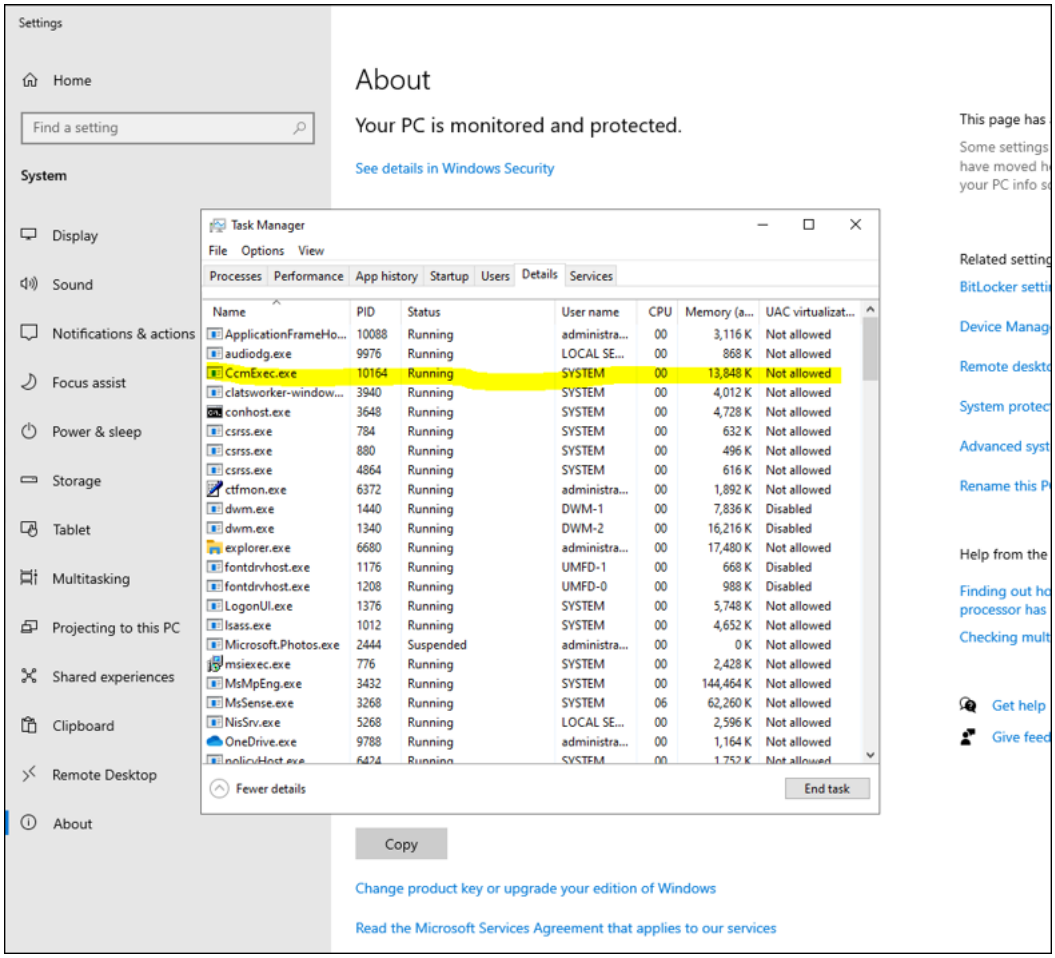
14. Siga las instrucciones del asistente. El **Asistente para instalar el cliente de Configuration Manager** se completa correctamente.



Para obtener información detallada, consulte Administrar colecciones en la documentación de Microsoft.

Paso 3: Verificar las máquinas

1. En la máquina cliente, verifique que el cliente esté instalado. Para ello, compruebe si el proceso `CCMExec` se está ejecutando.



2. Verifique si el cliente se está ejecutando para las máquinas virtuales de SCCM.

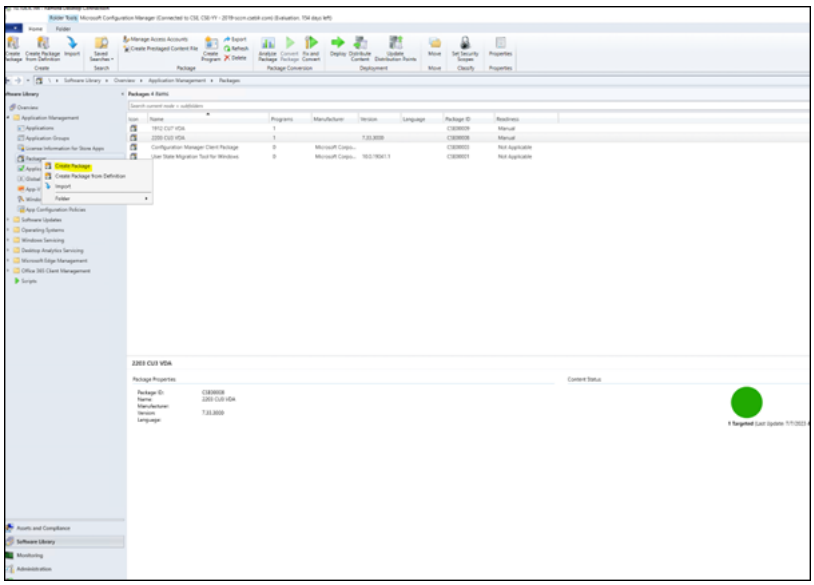
Paso 4: Usar VDA para distribuir contenido

Los pasos siguientes describen cómo puede usar el VDA implementado para distribuir contenido en las máquinas virtuales asociadas.

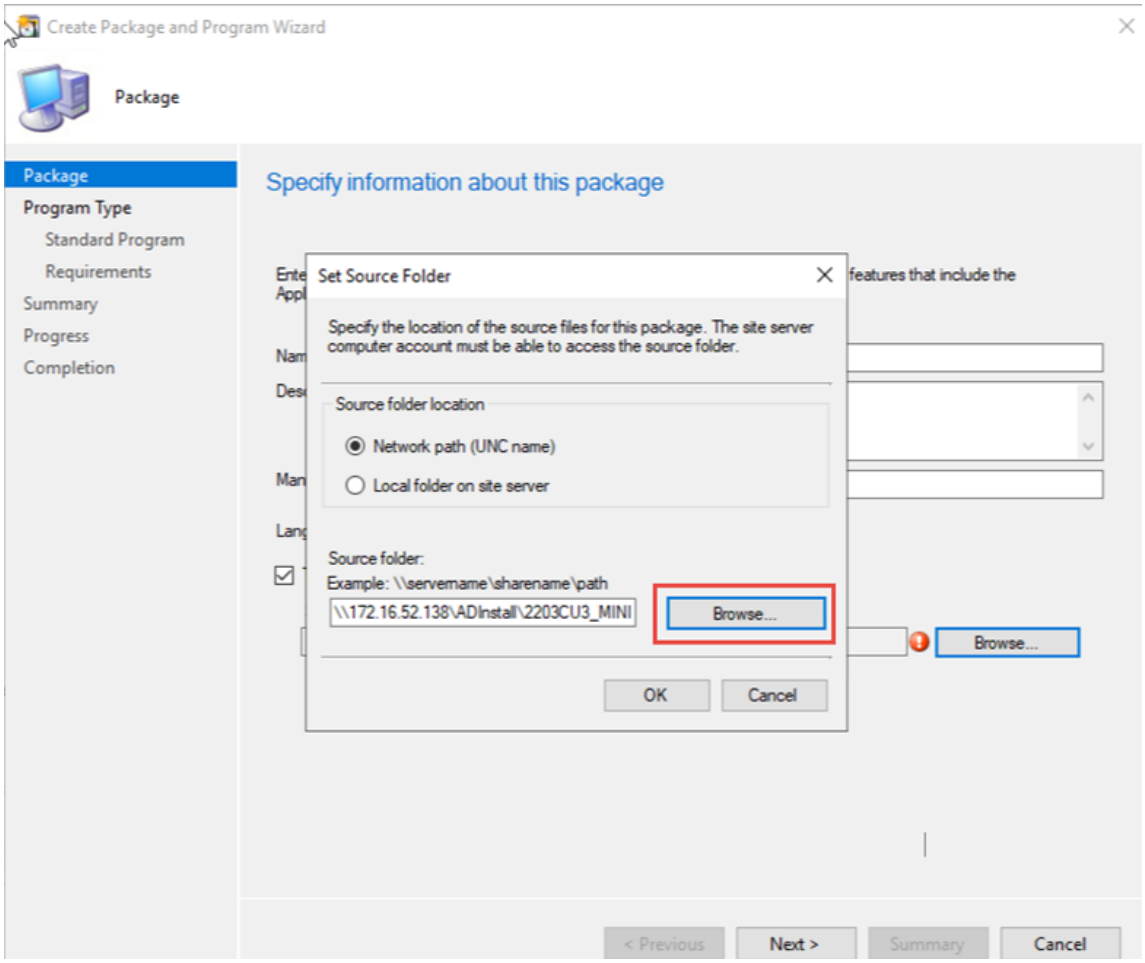
1. Crear un paquete
2. Distribuir contenido

Crear un paquete

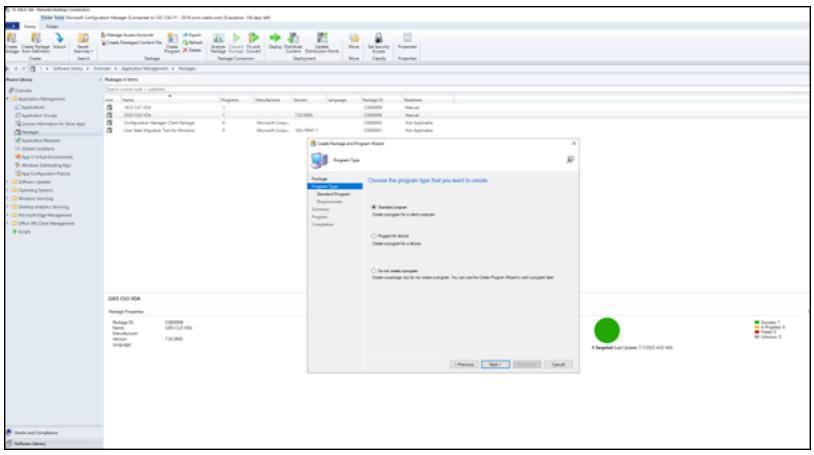
1. Para crear un paquete, haga clic con el botón secundario en el VDA que quiera y, a continuación, haga clic en **Crear paquete**.



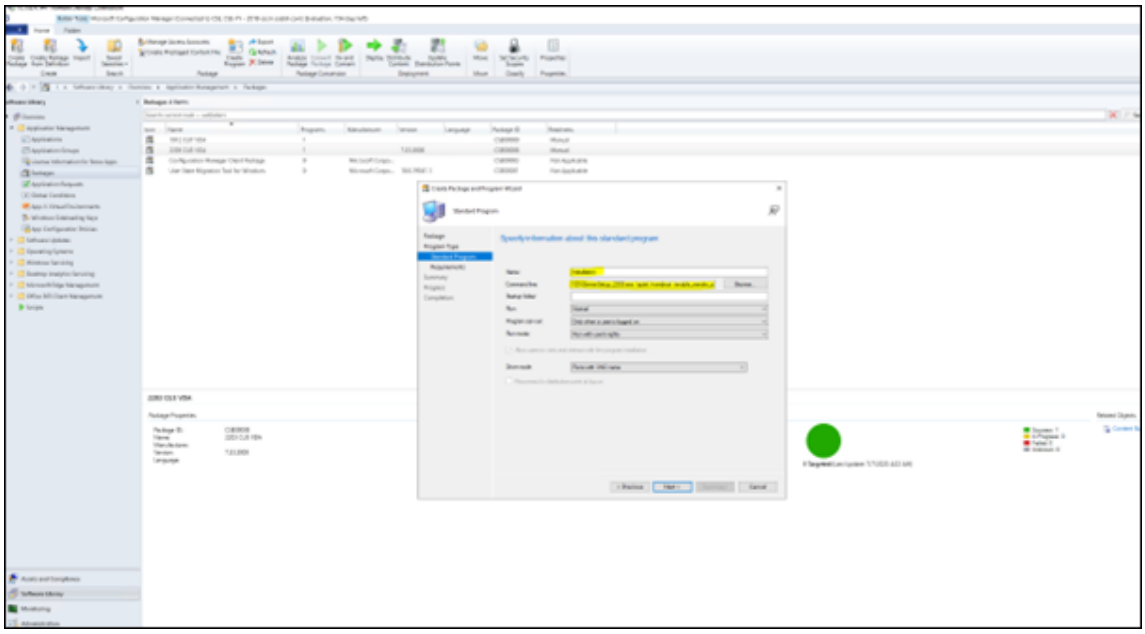
2. Especifique la ubicación de los archivos de origen de este paquete haciendo clic en **Examinar**.



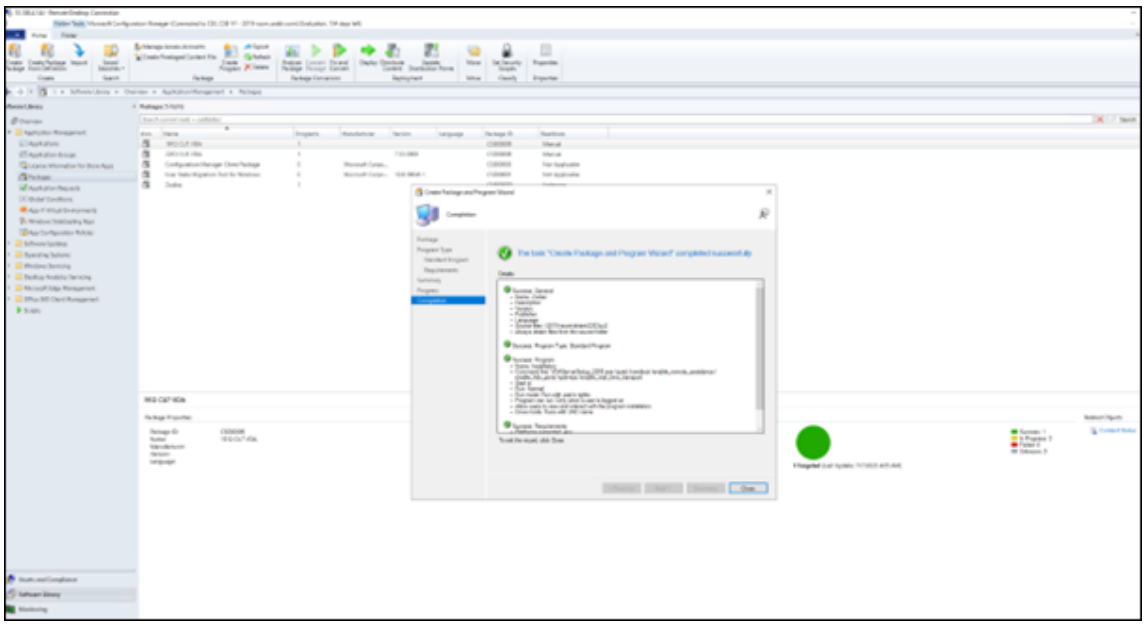
3. Seleccione un tipo de paquete.



4. Introduzca el **nombre** del paquete y la **línea de comandos**.



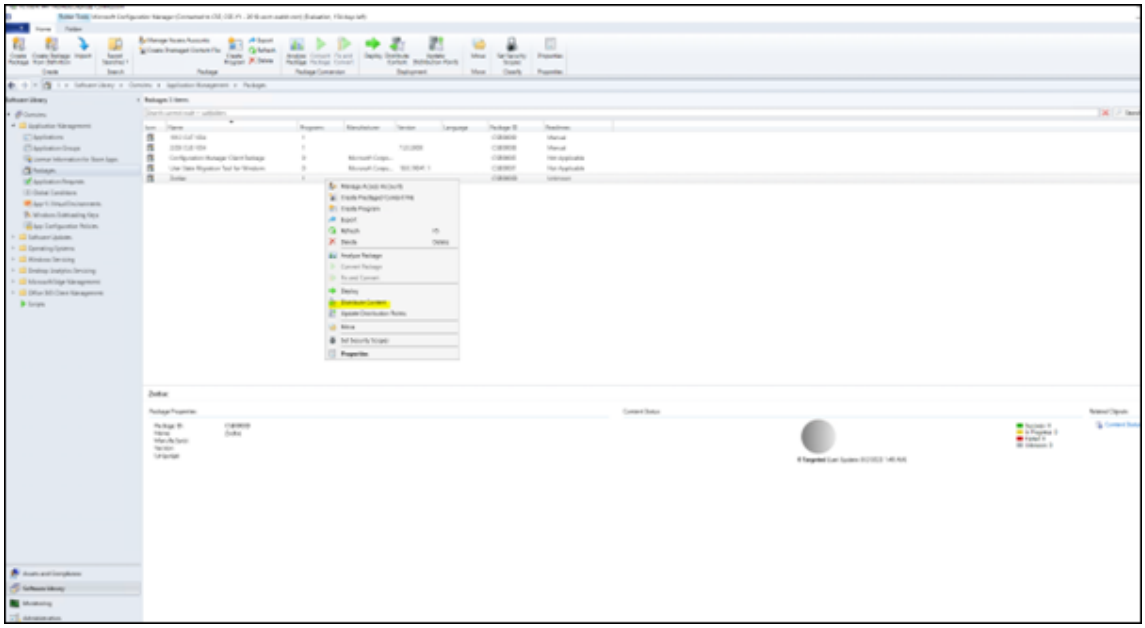
5. Haga clic en **Siguiente**.



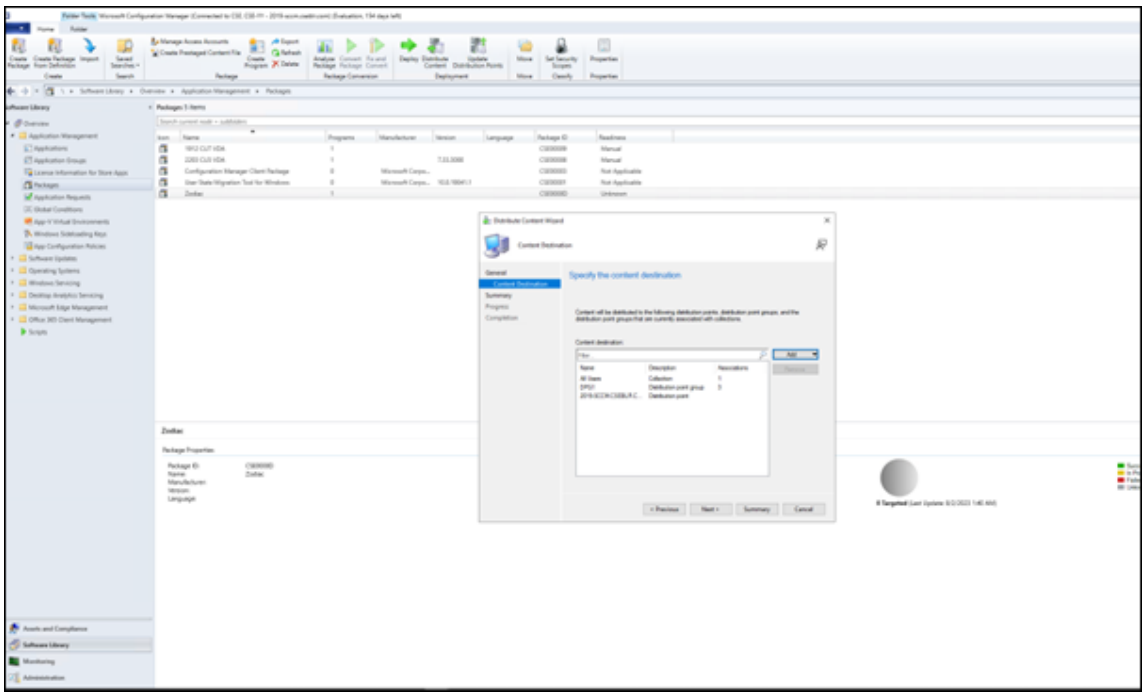
Para obtener información detallada, consulte los Paquetes y programas de Configuration Manager en la documentación de Microsoft.

Distribuir contenido

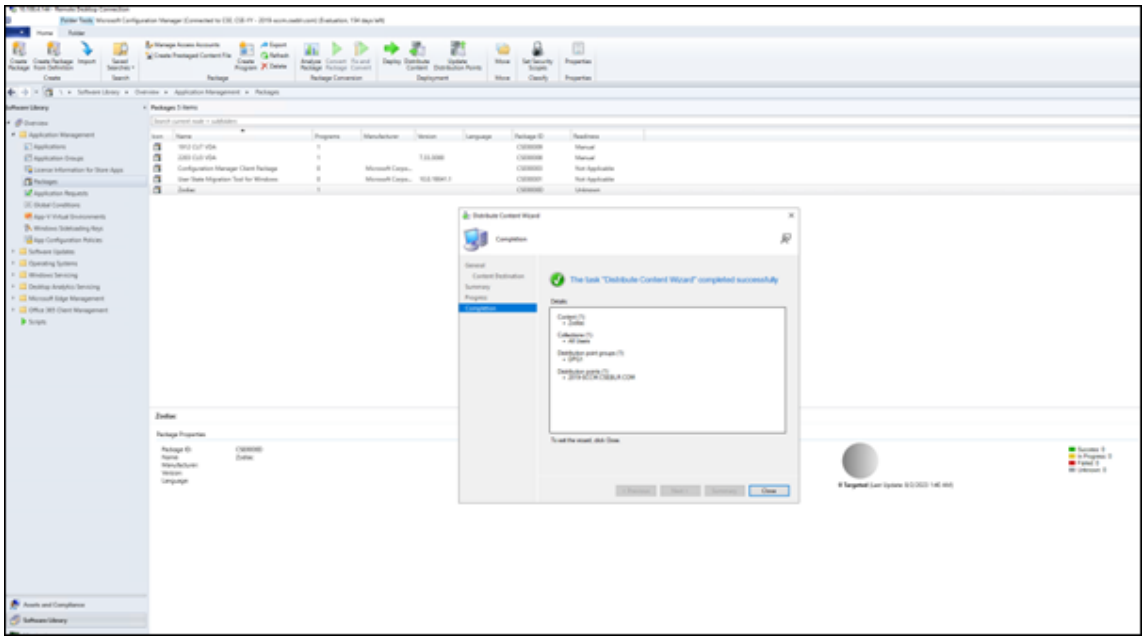
1. Haga clic con el botón secundario en el nombre del paquete que ha creado.
2. Seleccione **Distribuir contenido**.



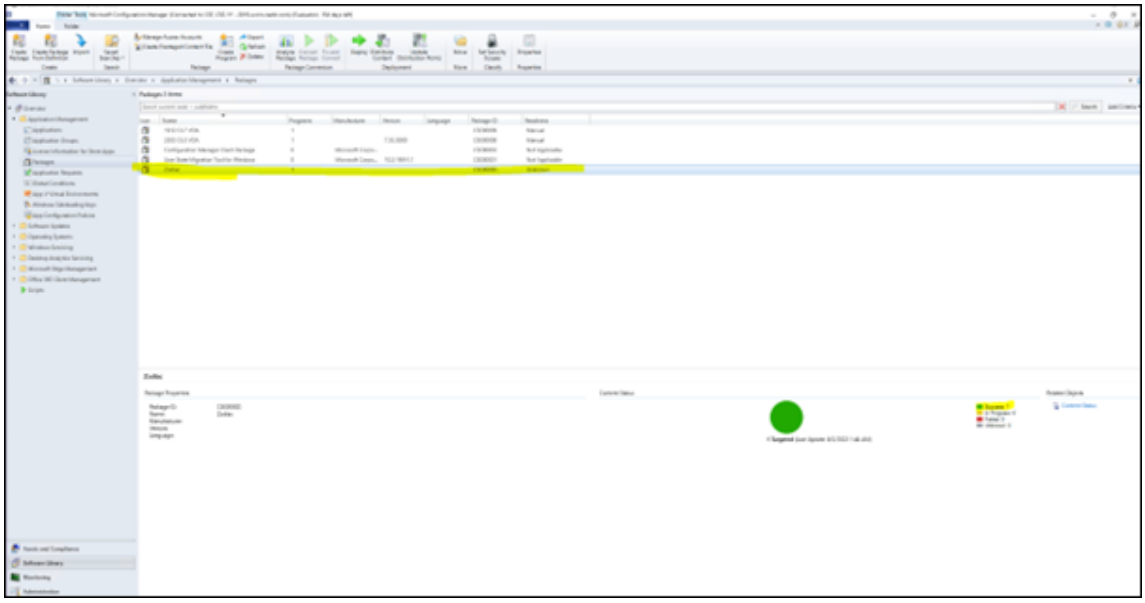
3. En la ventana del **Asistente para distribuir contenido**, seleccione la ubicación de los archivos de origen del paquete que ha creado. En este ejemplo, es `2019-SCCM`. Haga clic en **Siguiente**.



4. Verifique que el paquete (en este ejemplo `Zodiac`) esté disponible para su implementación.



La siguiente imagen muestra que el paquete está disponible para su implementación.

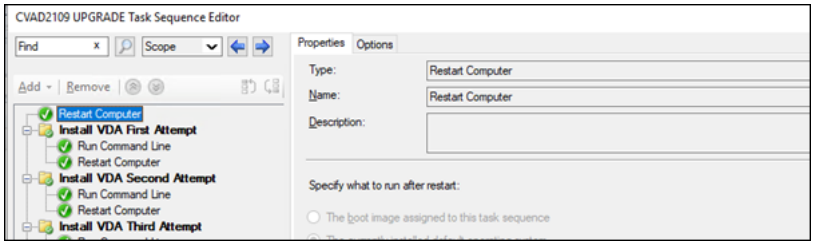


Para obtener información detallada, consulte Implementación y administración de contenido para Configuration Manager en la documentación de Microsoft.

Ejemplo de secuencia de instalación mediante SCCM

En este ejemplo se muestra la secuencia de instalación.

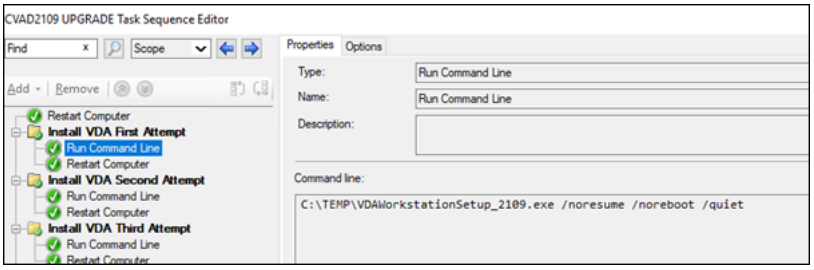
1. **Reiniciar el equipo:** Prepare el equipo reiniciándolo.



2. **Primer intento de instalación del VDA:** inicie la instalación del VDA.

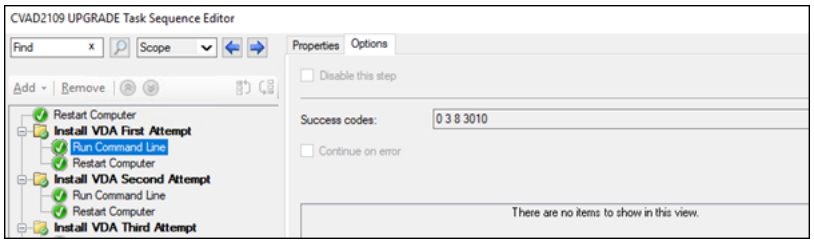
   a) Agregue las opciones de línea de comandos `/quiet`, `/noreboot` y `/noresume`.

   b) Ejecute el instalador de VDA que prefiera (imagen local o uno de los instaladores mínimos).

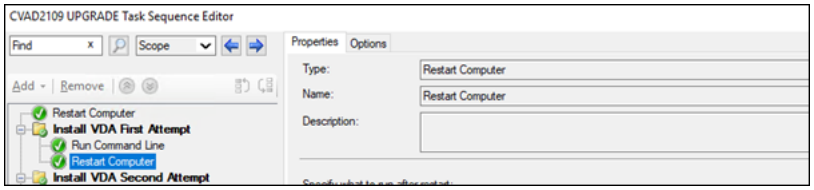


c) SCCM debe capturar el código de devolución.

- Si el código de devolución es 0 u 8, la instalación se ha completado y es necesario reiniciar.

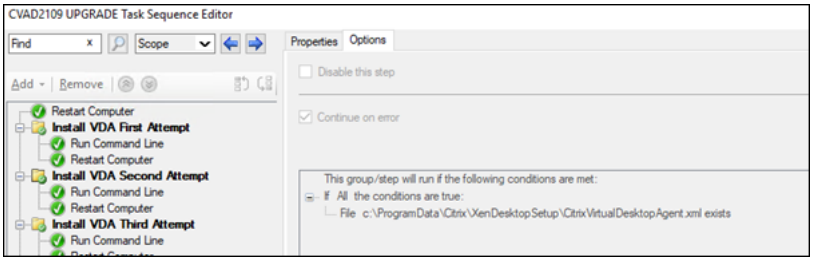


- Si el código de retorno es 3, reinicie la máquina y, a continuación, pase el control a **Segundo intento de instalación del VDA**.



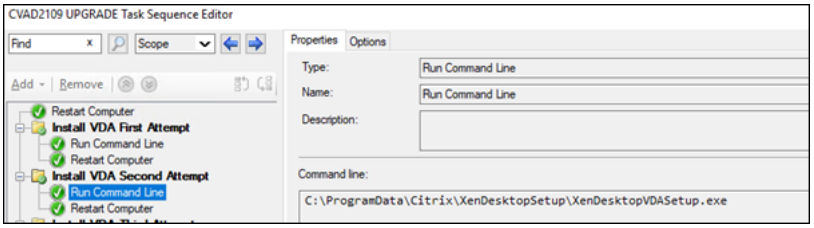
3. **Segundo intento de instalación del VDA:** continúe con la instalación del VDA.

a) Tras el **primer intento de instalación del VDA**, si el archivo `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` existe, la instalación no se completó correctamente y debe continuar una vez finalizado el reinicio.



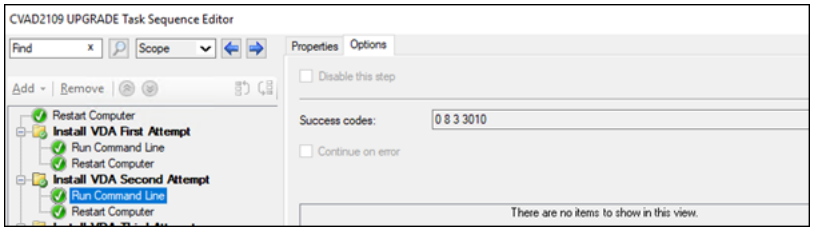
b) **El segundo intento de instalación de VDA** se repite hasta que no exista el archivo `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` o hasta que se devuelva un código de retorno distinto de 0 u 8. Trate los demás códigos de devolución como un error y SEGUNDO INTENTO DE INSTALCIÓN DEL VDA 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 el `%programdata%\Citrix\XenDesktopSetup\` directorio de archivos 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 SEGUNDO INTENTO DE INSTALACIÓN DEL VDA hasta que el archivo `%programdata%\Citrix\XenDesktopSetup\CitrixVirtualDesktopAgent.xml` no exista o hasta que se devuelva un 0 u 8. Trate los demás códigos de devolución como un error y SEGUNDO INTENTO DE INSTALCIÓN DEL VDA debería notificar un error y finalizar.

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 /physicalmachine /
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
```

Instalar agentes VDA mediante Microsoft Intune

August 17, 2024

Información general

En este artículo se describe cómo implementar los VDA mediante Microsoft Intune. Para obtener más información, consulte la documentación de Microsoft.

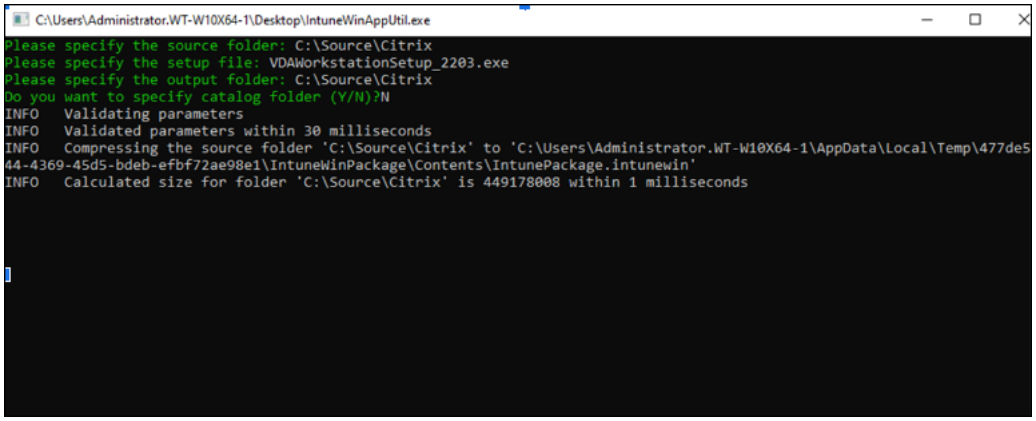
> **Nota:**
>
> El siguiente artículo describe solo las recomendaciones basadas en la forma en que Citrix ha probado el entorno. Puede personalizar estos pasos según sus necesidades. Citrix no se hace responsable de las actualizaciones o ajustes necesarios para adaptarlo a las necesidades de los clientes.

Pasos clave para implementar VDA con Microsoft Intune

1. Preparar la instalación de Citrix VDA.
2. Configurar la suscripción al programa para desarrolladores de Microsoft 365.
3. Agregar y asignar una aplicación.
4. Instala la aplicación en el dispositivo inscrito.

Paso 1: Preparar la instalación de Citrix VDA

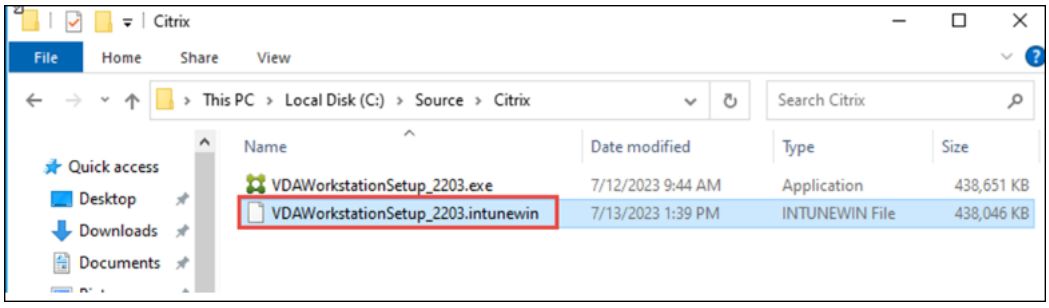
1. Descargue el archivo IntuneWinAppUtil.exe actualizado de GitHub.
2. Ejecute el archivo `IntuneWinAppUtil.exe` con la opción **Ejecutar como administrador**.
3. Introduzca los siguientes datos:



   a) **Especifique la carpeta de origen**: Introduzca la carpeta que contiene los archivos de configuración de la aplicación. Por ejemplo, C:\source\Citrix.
   b) **Especifique el archivo de instalación**: Introduzca el nombre del archivo de instalación (por ejemplo, setup.exe o setup.msi). Por ejemplo, VDAWorkstationSetup_2203.exe.
   c) **Especifique la carpeta de salida**: Introduzca la ruta de la carpeta de salida para generar el archivo .intunewin. Por ejemplo, C:\source\Citrix.
   d) **¿Desea especificar una carpeta de catálogo (S/N)?** Escriba N.

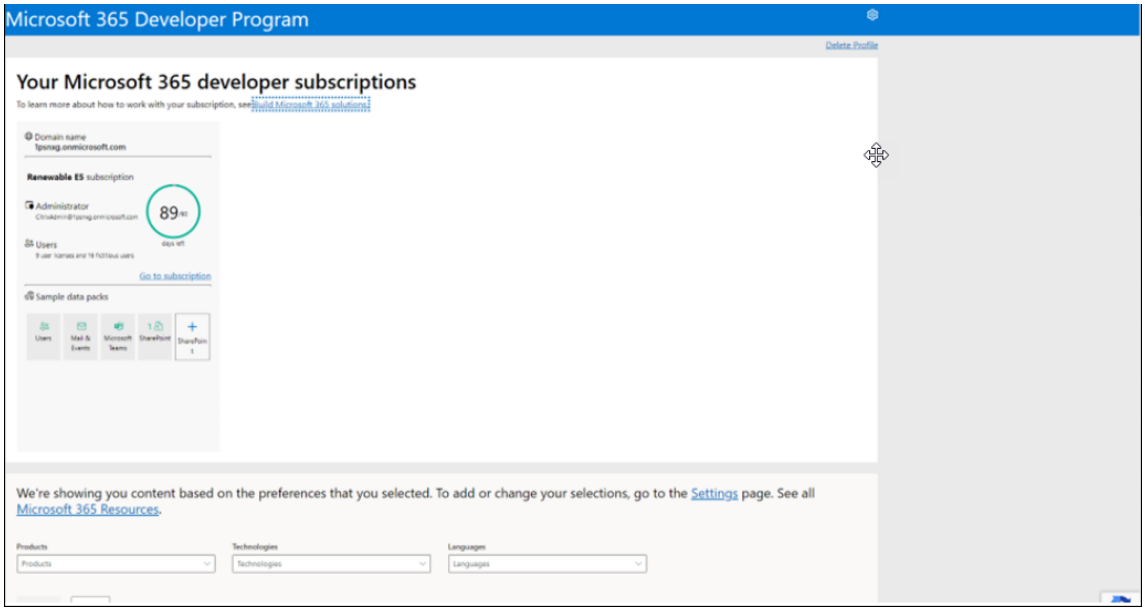
> **Nota:**
>
> Espere unos minutos mientras se ejecuta la **herramienta Win32 Content Prep**. Una vez generado el archivo `.intunewin`, el estado indica 100% en la parte inferior de la línea de comando.

4. Cuando finalice el proceso, vaya a la carpeta de salida (en este ejemplo `C:\source\Citrix`) para obtener el archivo de implementación de Microsoft Intune.
5. Regístrate para obtener una prueba gratuita de Microsoft Intune.

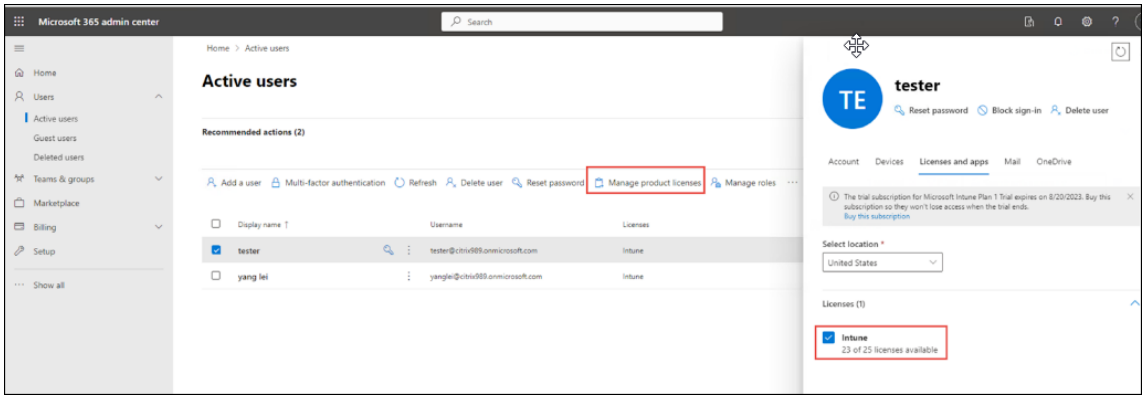


Paso 2: Configurar la suscripción al programa para desarrolladores de Microsoft 365

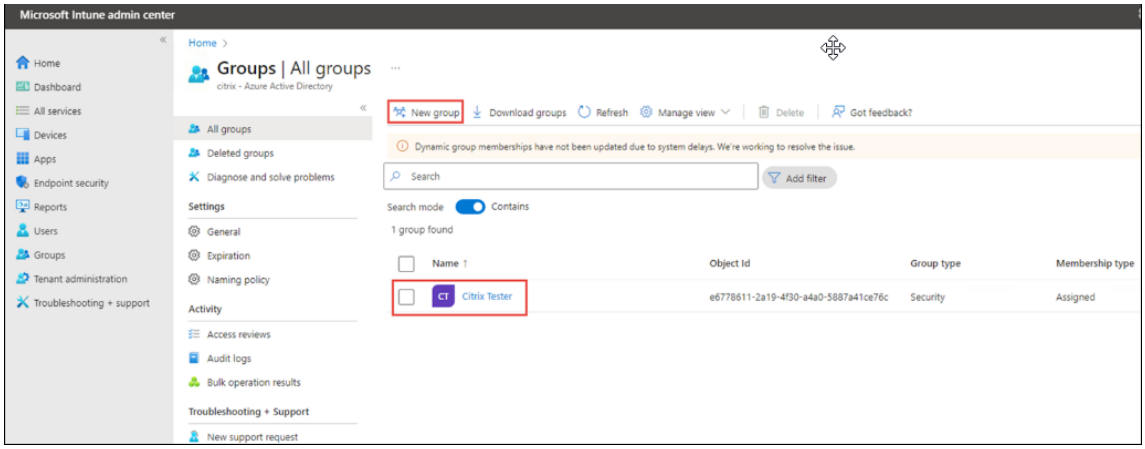
1. Cree el sandbox instantáneo para activar su suscripción.
   Para obtener su espacio aislado (sandbox) para desarrolladores, vaya al panel del Programa para desarrolladores de Microsoft 365 y seleccione **Agregar una nueva suscripción**.



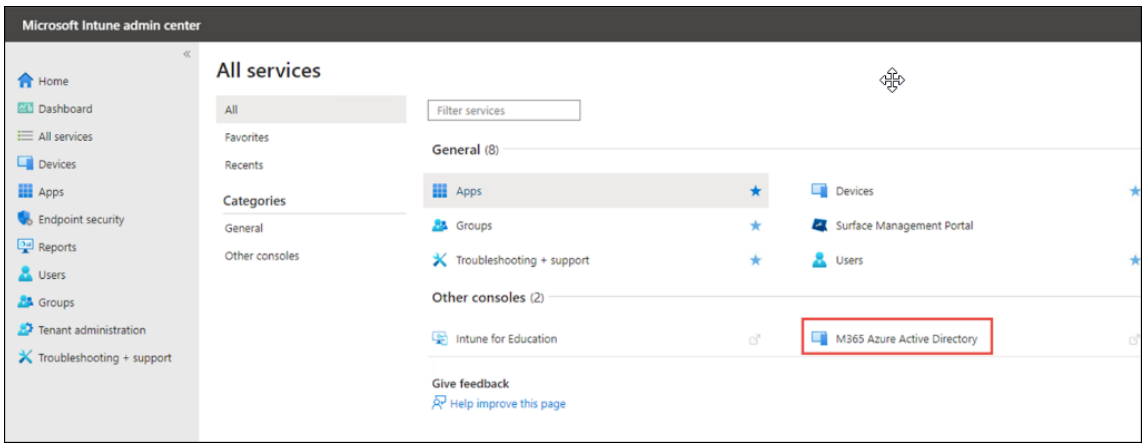
2. Cree un usuario en el Centro de administración de Microsoft 365 y asígnele una licencia.



3. Cree un grupo.

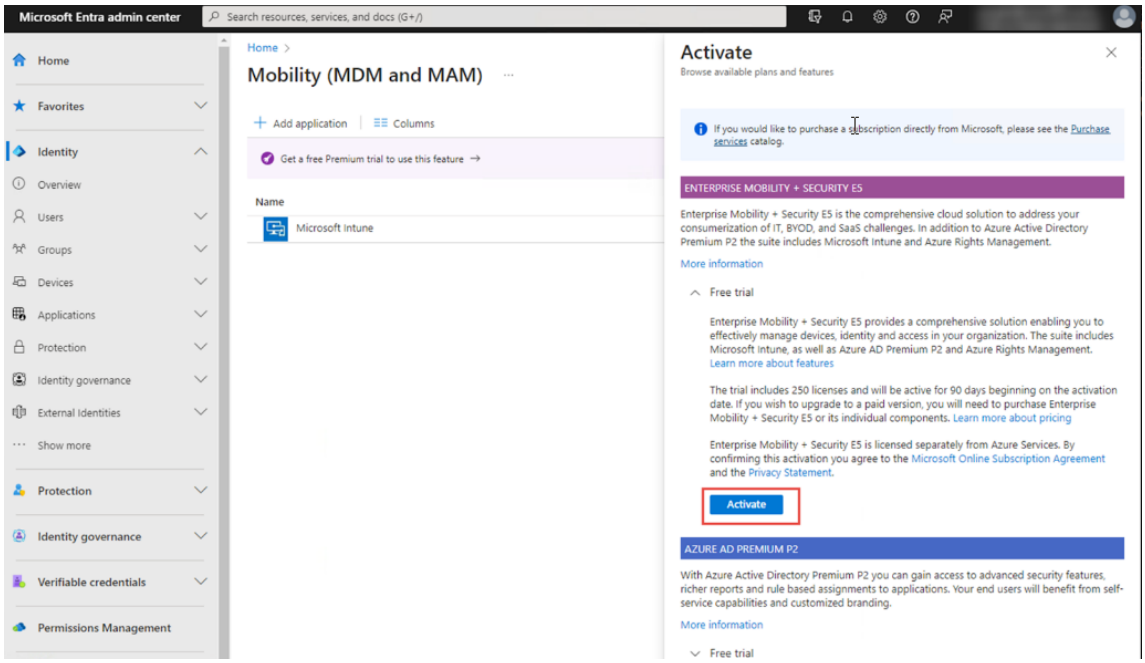


4. Una vez creado el grupo, debe proporcionarle la autoridad de MDM. Configure la inscripción automática. La activación puede tardar un minuto.
   O puedes agregar manualmente la autoridad de MDM al grupo siguiendo estos pasos:
   1. Vaya a **Todos los servicios > Microsoft Entra**.
   1. Vaya a **Configuración > Movilidad** y seleccione **Microsoft Intune**.
   1. Seleccione el grupo que acabas de crear. Se abrirá una página con el ámbito de usuario de MDM.
   1. Haga clic en **Guardar**.
5. En la ficha **Todos los servicios**, haga clic en **M365 Azure Active Directory**.

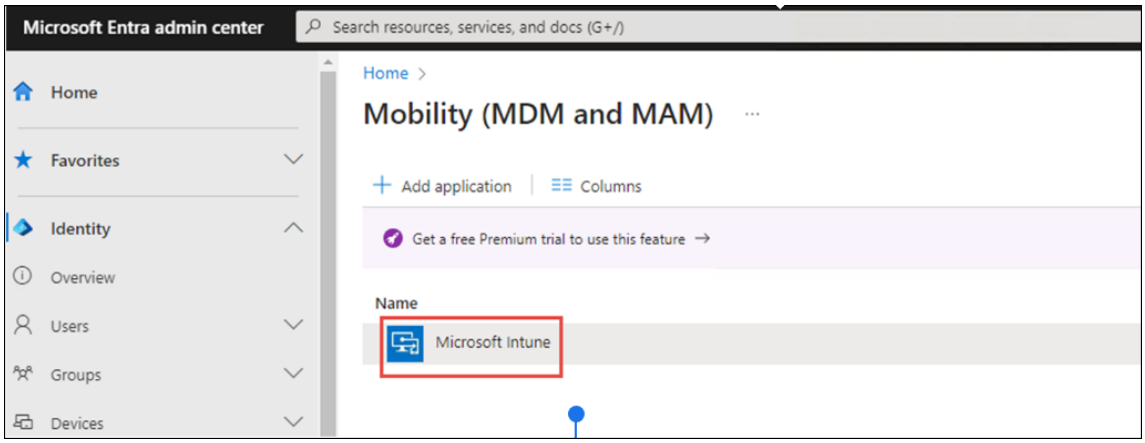


6. Haga clic en la opción para **obtener una prueba Premium gratuita para usar esta función**.

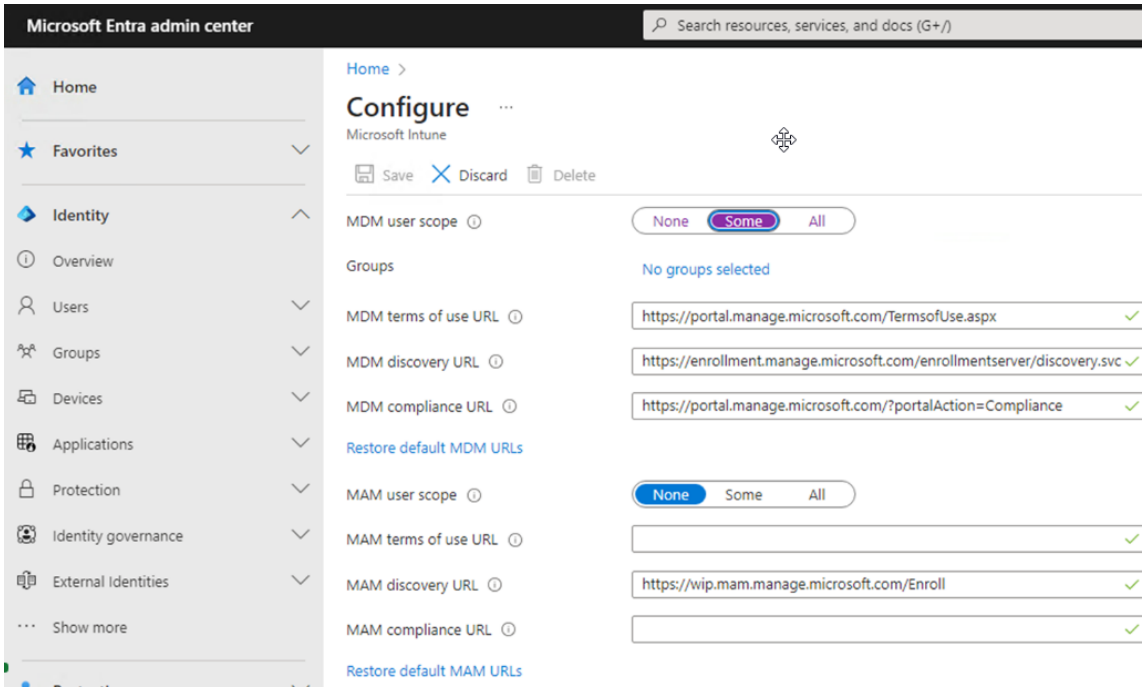
7. Haga clic en **Activar**.



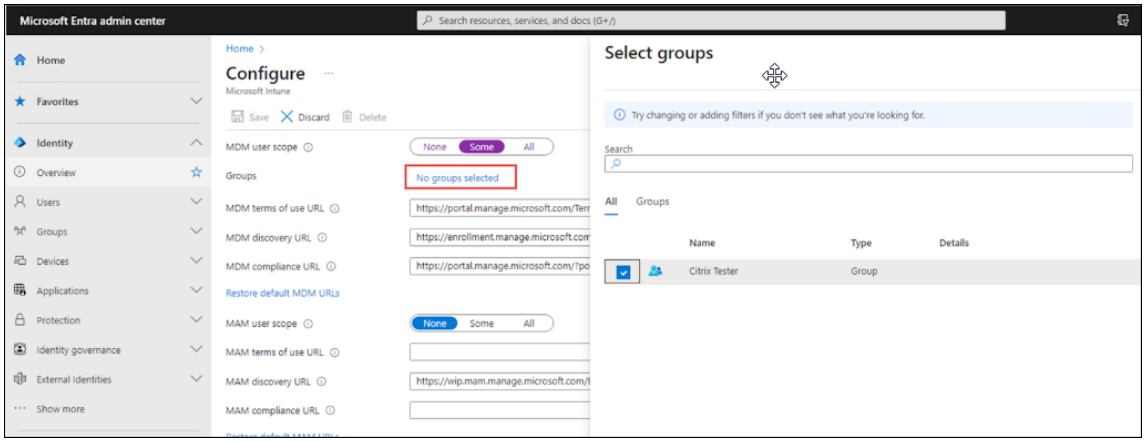
8. Ahora, haga clic en **Microsoft Intune**.



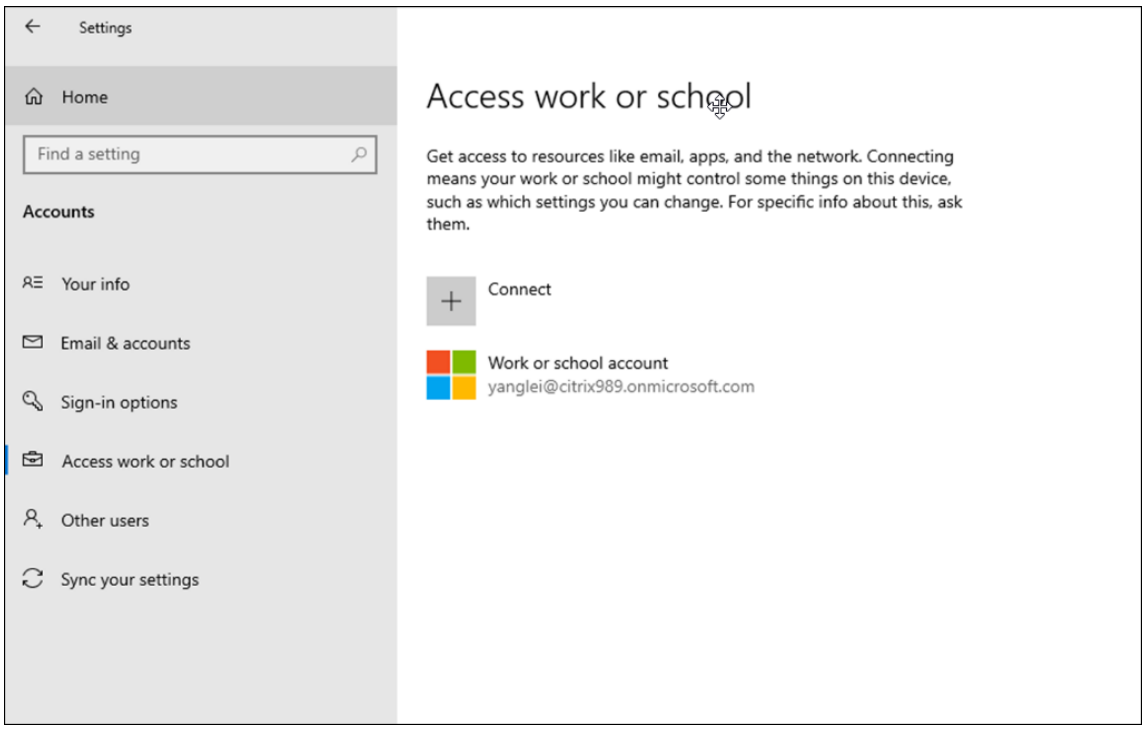
9. En la ficha **Configurar**, introduzca las configuraciones necesarias.



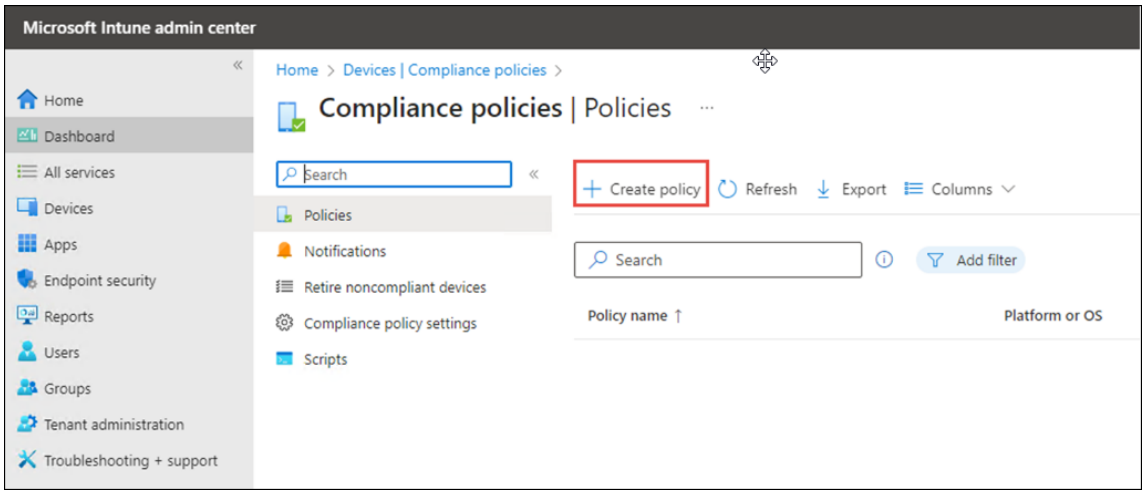
10. Para agregar un grupo, haga clic en **No hay grupos seleccionados**.



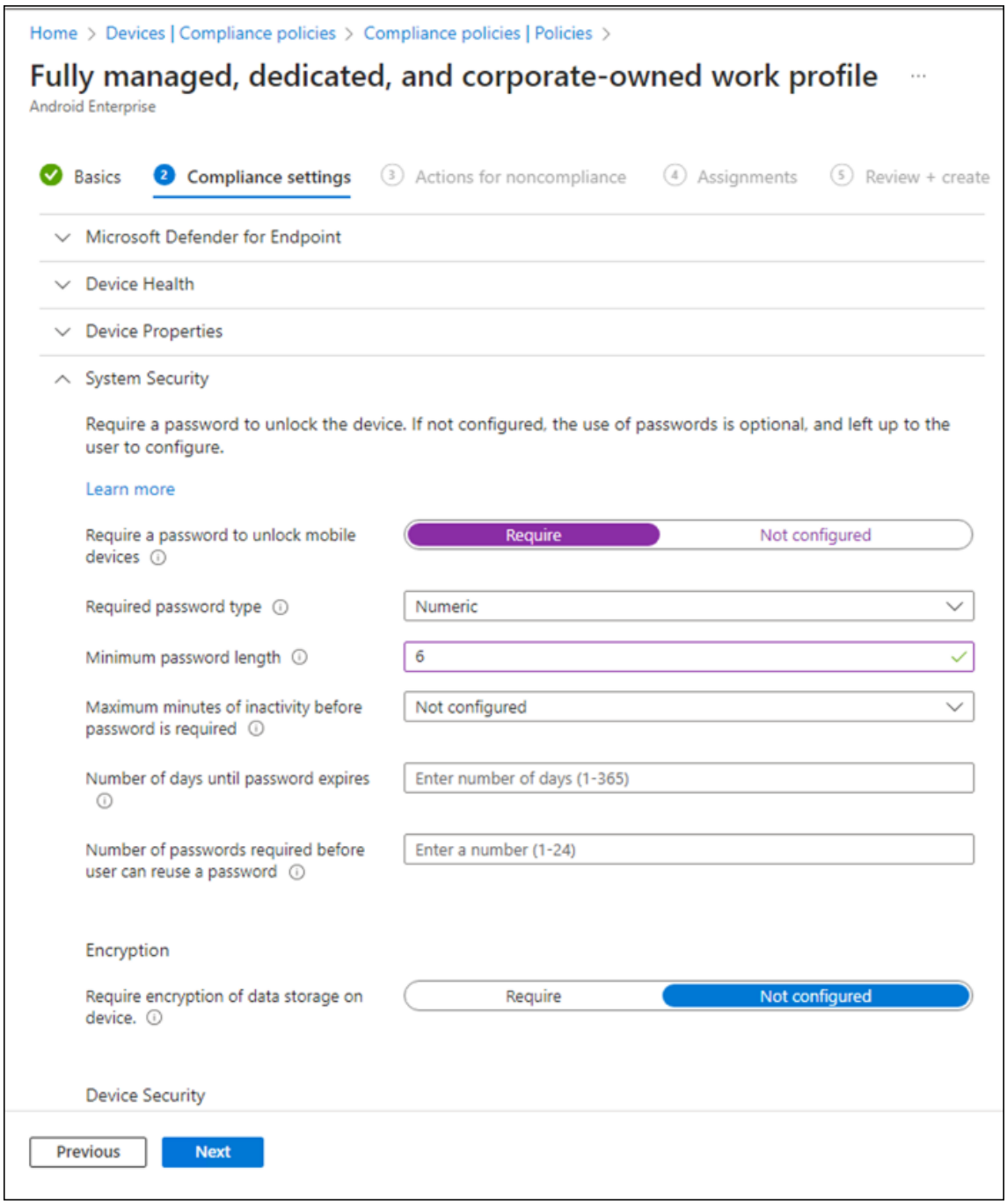
11. Inscriba su dispositivo.



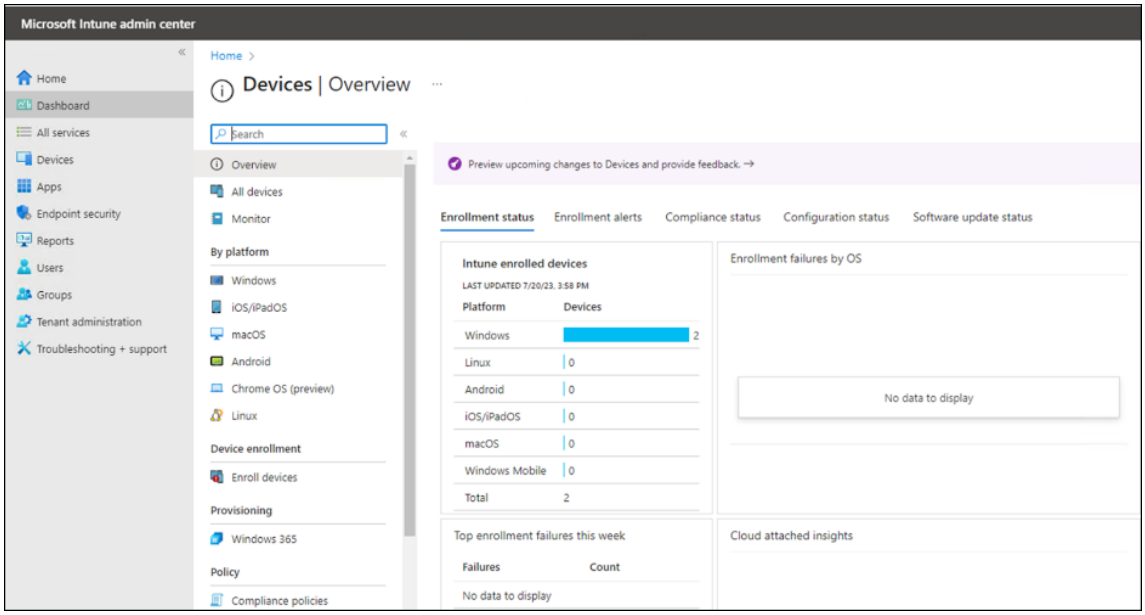
12. Crea una directiva de conformidad de dispositivo para cambiar la conformidad del dispositivo recién creado a `Compliant`.



13. Vaya a la ficha **Tareas** para agregar el grupo recién creado.



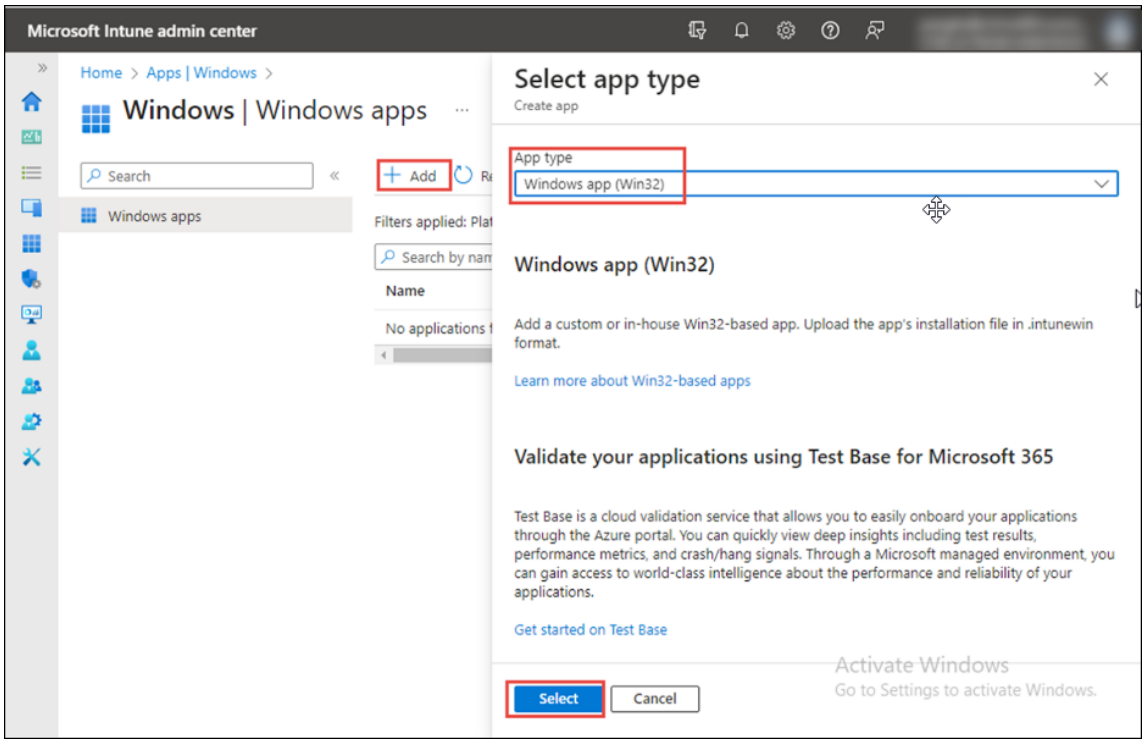
14. Confirme la inscripción del dispositivo.



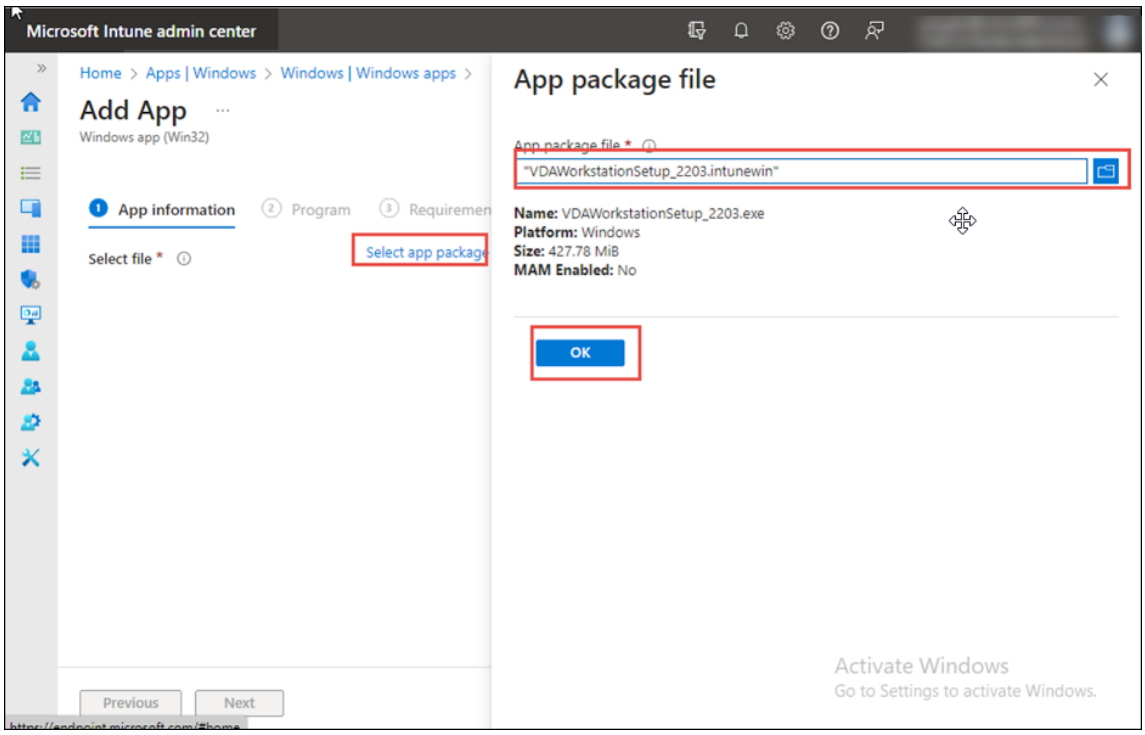
Para obtener información detallada, consulte el programa para desarrolladores de Microsoft 365.

Paso 3: Agregar y asignar una aplicación

1. Inicie sesión en el centro de administración de Microsoft Intune.
2. Seleccione **Aplicaciones > Todas las aplicaciones > Agregar** o vaya a **Aplicaciones > Windows > Aplicaciones de Windows**.

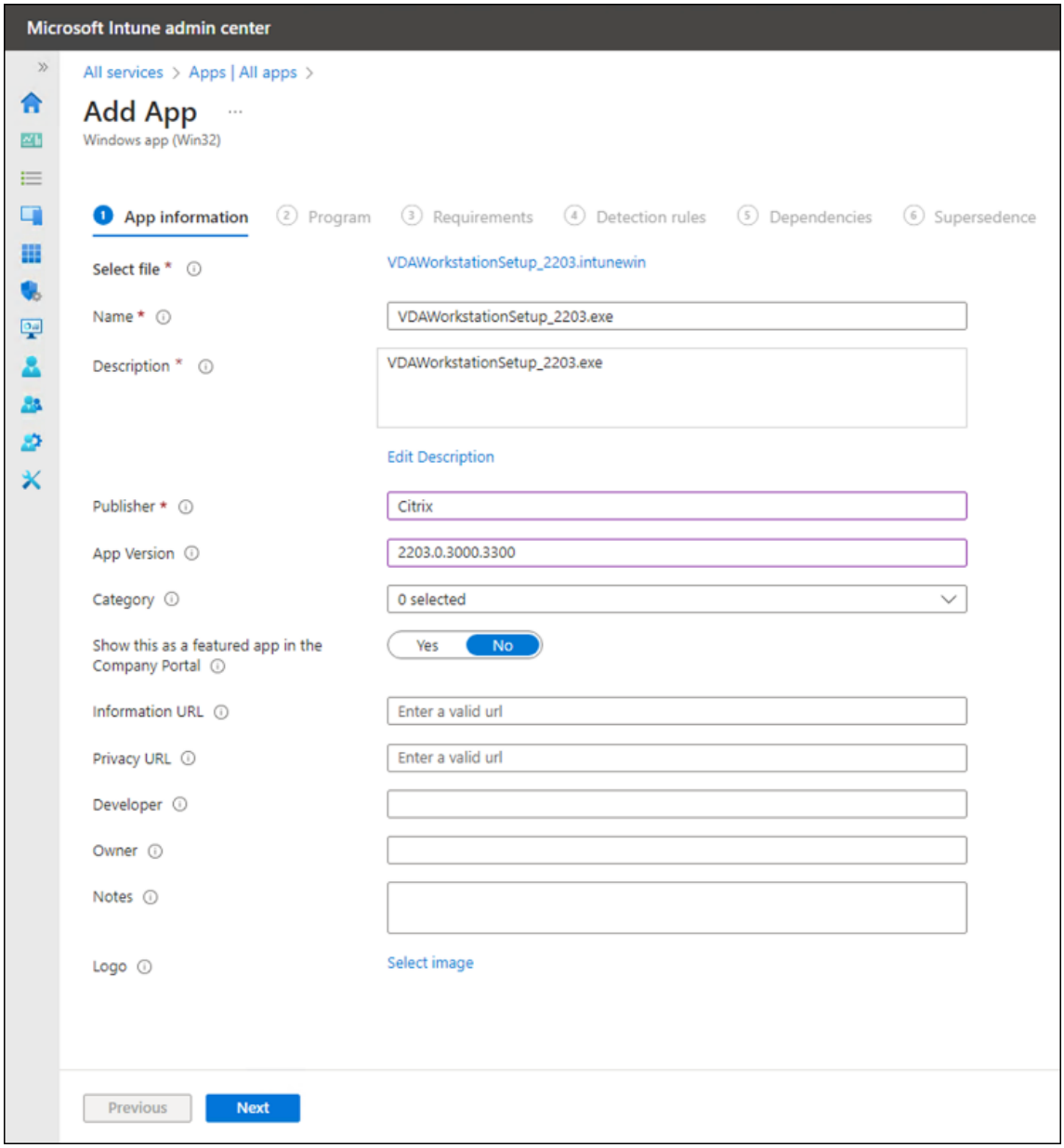


3. En el panel **Seleccionar tipo de aplicación**, seleccione **Otros tipos de aplicaciones > Aplicación de Windows (Win32)** y haga clic en **Seleccionar**.
4. En el panel **Agregar aplicación**, haga clic en **Seleccionar un archivo del paquete de aplicaciones**. Haga clic en **Examinar**.
5. Seleccione el archivo preparado con la extensión `.intunewin`. El archivo preparado se crea durante el paso Preparar la instalación de Citrix VDA. Se muestra una página con información detallada sobre la aplicación.



> **Nota:**
>
> - Si usa una máquina con núcleo de servidor, debe usar el núcleo de estación de trabajo de VDA.
> - Si usa un sistema operativo de escritorio Windows 10, debe usar la estación de trabajo del VDA.
> - Si usa un sistema operativo de servidor (por ejemplo, Windows 2022), debe usar la configuración del servidor VDA.
> - En este ejemplo, usamos la versión 2203, pero es aplicable a todas las versiones.

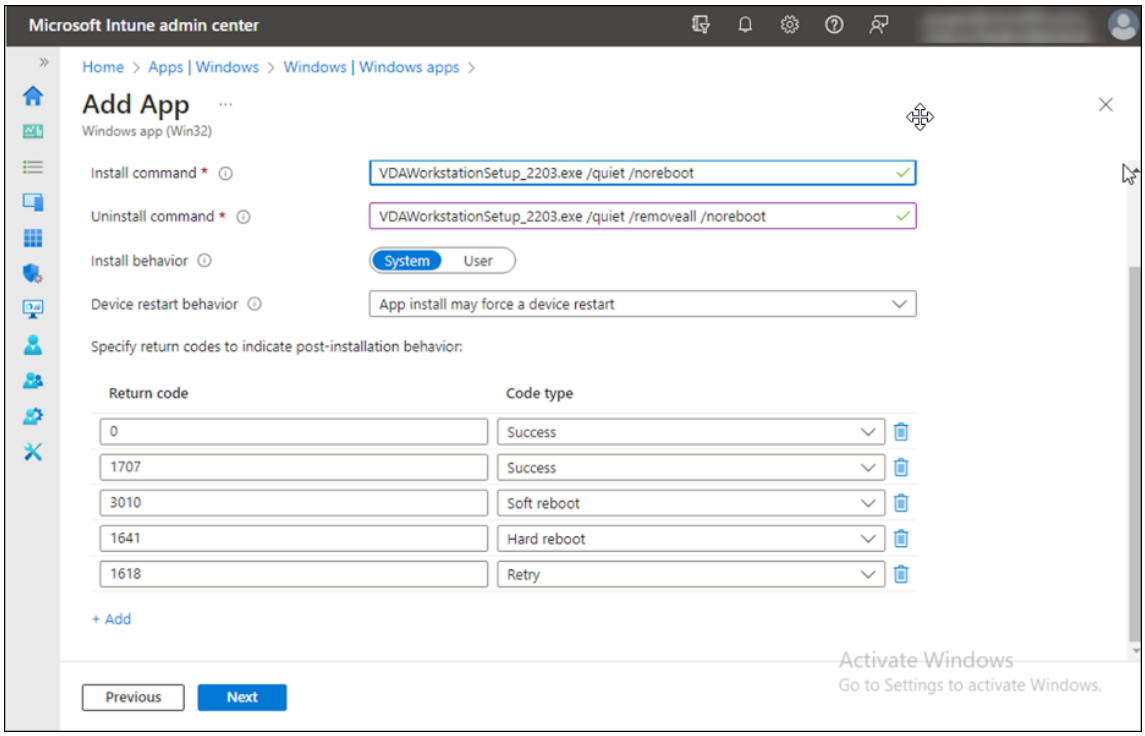
6. Haga clic en **Aceptar** en el panel de **Archivo del paquete de la aplicación**.
7. En la siguiente pantalla, en la ficha **Información de la aplicación**, introduzca el **nombre** y la **descripción** de la aplicación de Windows. Introduzca el nombre del **editor** como `Citrix` y aquí podrá especificar la información adicional de la aplicación. Haga clic en **Siguiente**.



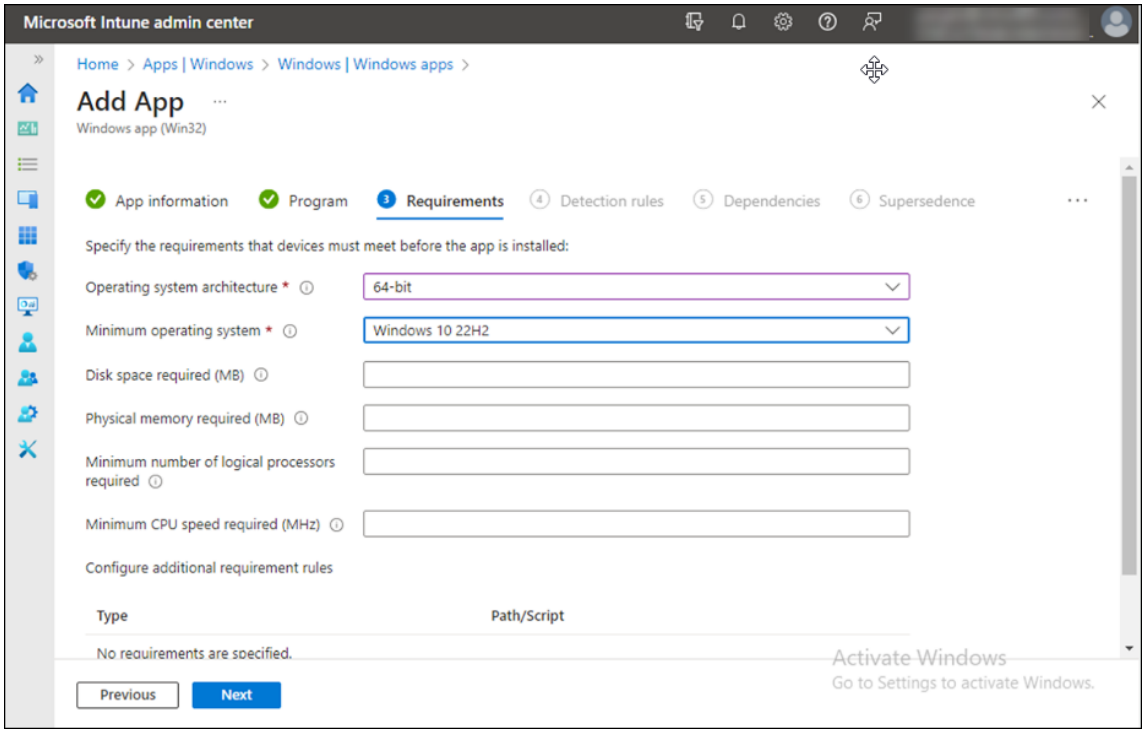
8. En la siguiente pantalla, introduzca los valores siguientes:
   - **Comando Instalar**: `VDAWorkstationSetup_2203.exe /quiet /noreboot`
   - **Comando Desinstalar**: `VDAWorkstationSetup_2203.exe /quiet /removeall /noreboot`
   - **Comportamiento de instalación**:
     - **Sistema**: Seleccione esta opción para instalar la aplicación en todos los dispositivos del grupo.
     - **Usuario**: Seleccione esta opción para instalar la aplicación solo en un dispositivo de usuario específico del grupo.
9. Haga clic en **Siguiente**.

Nota:

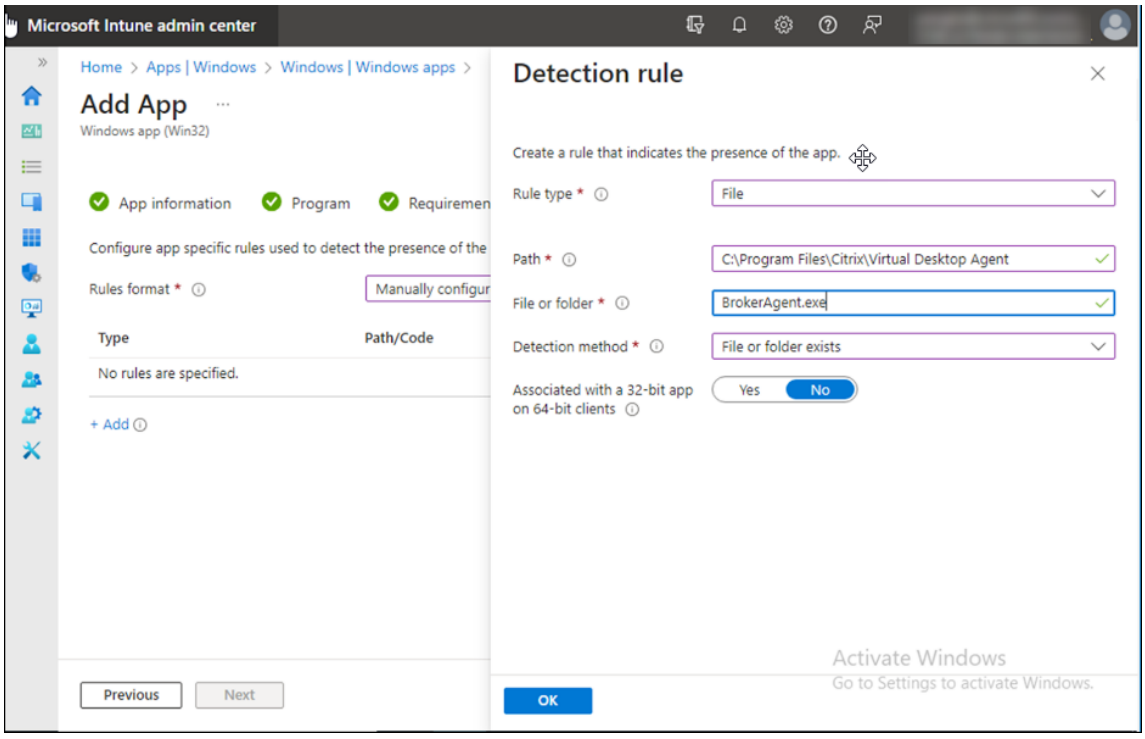
- En este ejemplo se usa la versión 2203, pero se puede usar con cualquier versión.
- Agregar `/noreboot` a un comando no significa que no se reinicie durante la instalación o la implementación, sino que solo impone los reinicios obligatorios.
  Para obtener más información sobre los scripts, consulte Opciones de línea de comandos para instalar un VDA.
- Para **Comportamiento de reinicio del dispositivo**, seleccione **Intune forzará un reinicio obligatorio del dispositivo**.
- En el cuadro de texto **Código de retorno**, escriba `0`, `3` y `8` para que la instalación se complete correctamente.
  Para obtener información sobre otros códigos de retorno, consulte Códigos de retorno en la instalación de Citrix.



10. En la siguiente pantalla, en la ficha **Requisitos**, introduzca los valores necesarios. Haga clic en **Siguiente**.



11. En la siguiente pantalla, en la ficha **Regla de detección**, agregue la **regla de detección** para agregar el agente Broker. Haga clic en **Aceptar**.

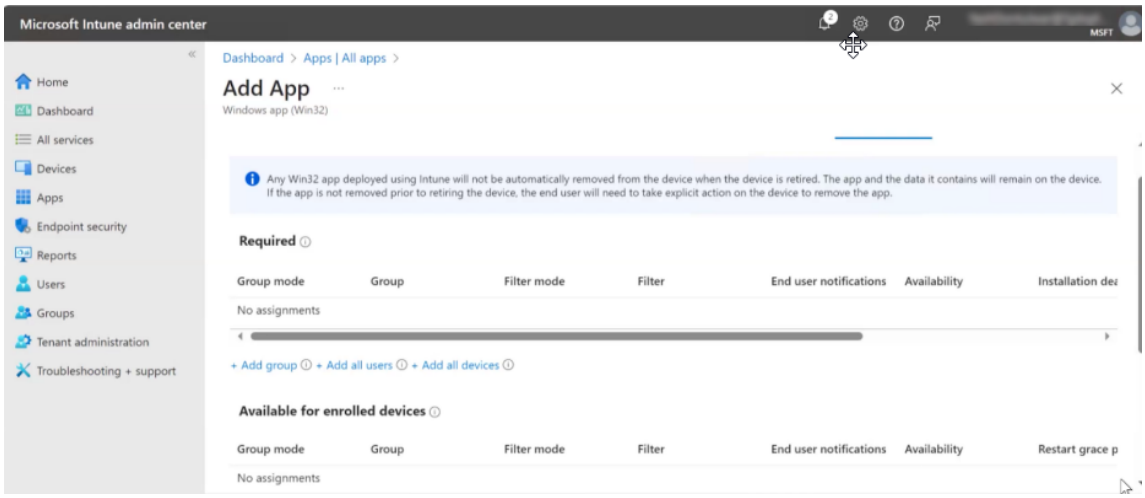


12. En la ficha **Asignaciones**, puede agregar los dispositivos de la siguiente manera:

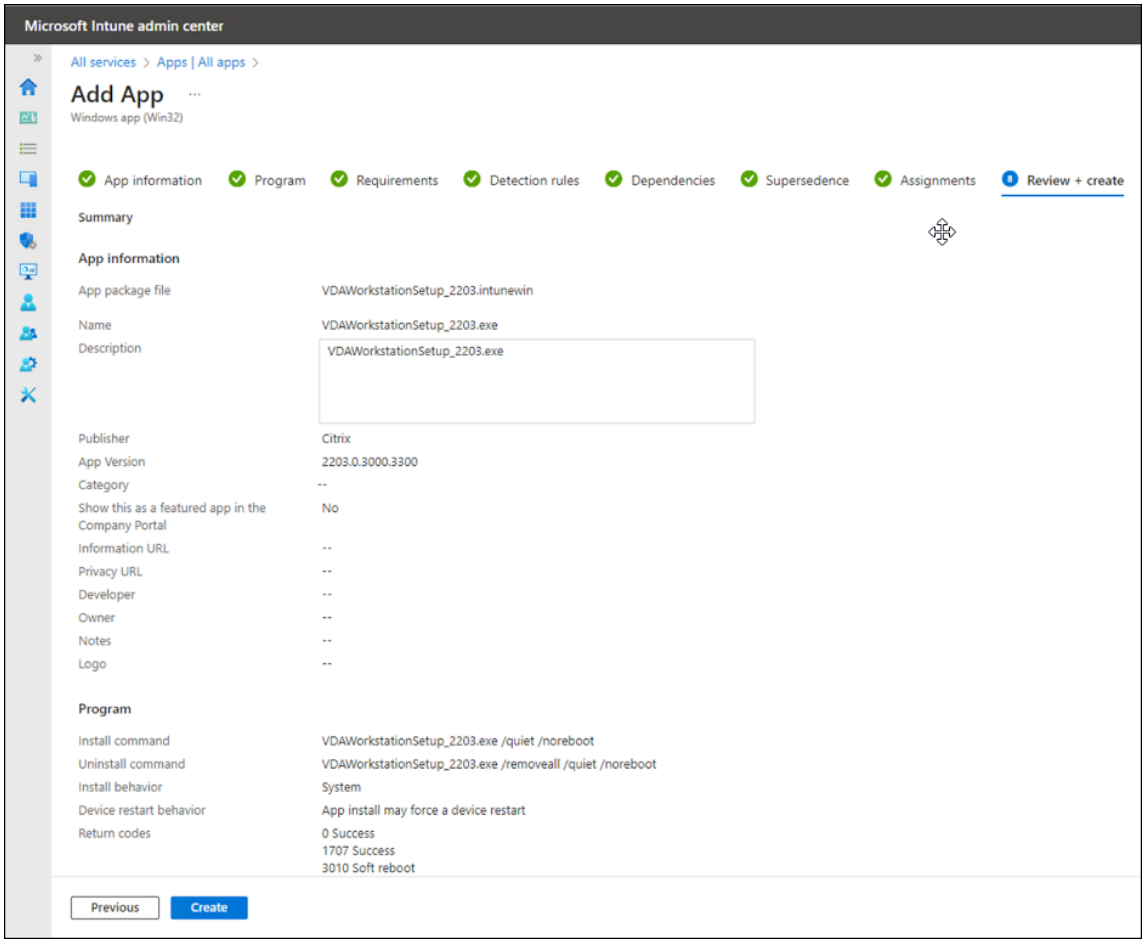
    - **Requerido**: Los dispositivos para los que las actualizaciones se realizan automática-

mente.

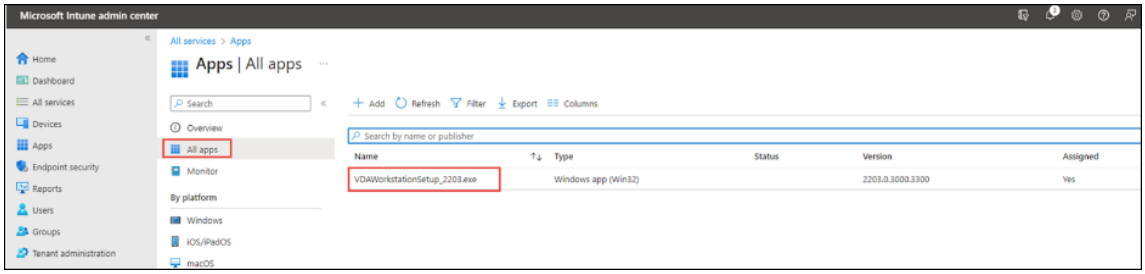
- **Disponible para dispositivos inscritos**: Los dispositivos para los que las actualizaciones se realizan manualmente.



13. Revise los detalles y haga clic en **Crear**.



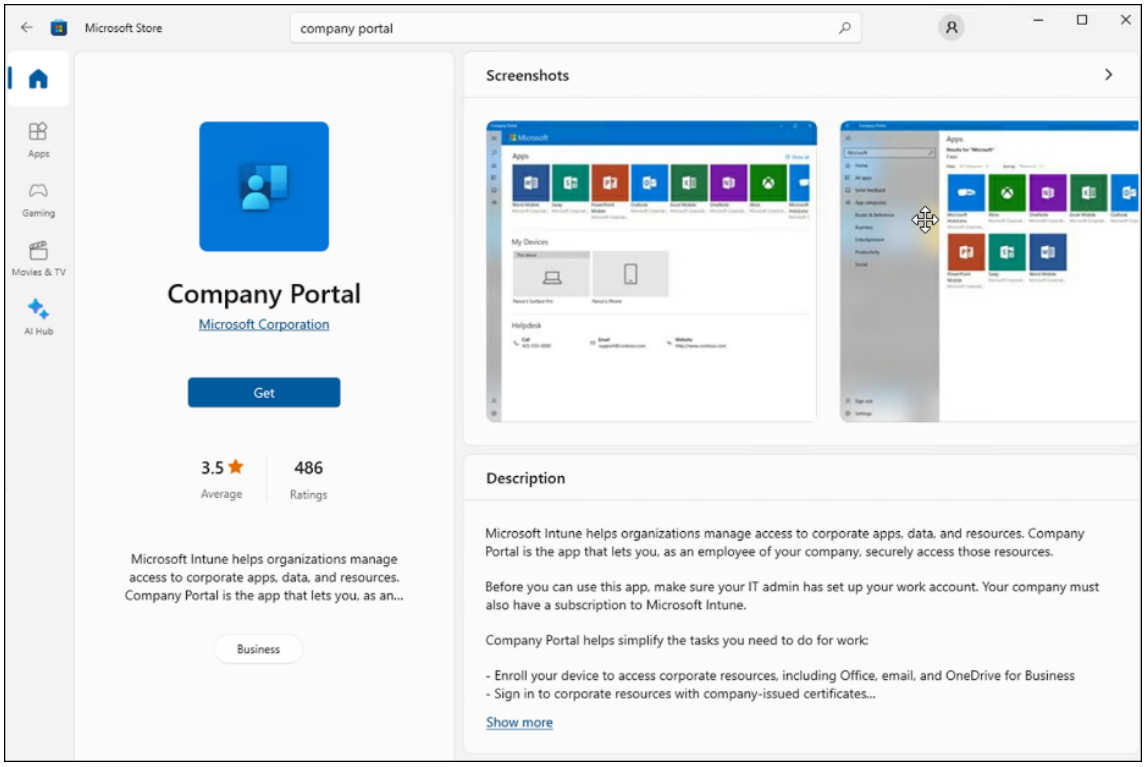
La aplicación se ha asignado correctamente.



Para obtener información detallada, consulte Agregar y asignar una aplicación.

Paso 4: Instalar la aplicación en el dispositivo inscrito

1. Inicie sesión en su dispositivo de escritorio Windows 10 inscrito.
   El dispositivo debe estar inscrito en Microsoft Intune. Además, debe iniciar sesión en el dispositivo con una cuenta incluida en el grupo que asignó a la aplicación. Para obtener más información, consulte la documentación de Microsoft.
2. En el menú **Inicio**, abra **Microsoft Store**.
3. Busque la aplicación **Company Portal** e instálela.



4. Ejecute la aplicación **Company Portal**.
5. Haga clic en la aplicación que agregó con Microsoft Intune.
   Si no ha asignado correctamente ninguna aplicación al usuario de Intune, aparece el siguiente

mensaje:
`Your IT administrator did not make any apps available to you.`

6. Haga clic en **Install**.

Crear un sitio

August 17, 2024

> **Nota:**
>
> Tras agregar una licencia para habilitar la licencia de derechos híbridos, los hosts de nube pública (como Microsoft Azure, Google Cloud Platform y Amazon Web Services) no aparecen en la lista de tipos de conexión hasta que se completa el proceso de creación del sitio.

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 **Parámetros** en el panel de la izquierda de Web Studio y, a continuación, busque el parámetro **Citrix Customer Experience Improvement Program**. Para obtener información detallada, consulte http://more.citrix.com/XD-CEIP.

El usuario que crea un sitio pasa a ser administrador total. Para obtener más información, consulte Administración delegada.

Consulte este artículo antes de crear el sitio para saber a qué atenerse.

Paso 1. Abrir el asistente de creación de sitios, Citrix Site Manager

Utilice la herramienta Citrix Site Manager para configurar la implementación de Citrix Virtual Apps and Desktops (también conocida como sitio). La herramienta se instala automáticamente al instalar un Delivery Controller.

Para ejecutar esta herramienta, abra el menú Inicio del escritorio en un Delivery Controller y seleccione **Citrix > Citrix Site Manager**. Consulte Instalar Web Studio.

Paso 2. Site name

En la página **Introducción**, escriba el 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 las opciones y los requisitos de configuración de las bases de datos, consulte Bases de datos.

> **Nota:**
>
> Si la escucha de Always On de SQL Server se configura para el cifrado TLS, es posible que se le pida introducir credenciales con permisos de creación de bases de datos. Todavía no se puede crear la base de datos aunque se introduzcan credenciales de administrador válidas. Compruebe que el certificado de SQL Server incluye el nombre DNS de la escucha en Nombres alternativos del sujeto (SAN). Para obtener más información, consulte https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/listeners-client-connectivity-application-failover#SSLcertificates.

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 que 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

Connect. 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. Resumen

La página **Resumen** contiene la información especificada. Utilice el botón **Atrás** si quiere cambiar algo. Cuando haya terminado, haga clic en **Finalizar**.

Más información

Conexión de host, red y almacenamiento

Si utiliza máquinas virtuales en un hipervisor o en otro servicio 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 en otros servicios (o si usa Web 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 Virtual Machine Manager** o **Wake on LAN para Remote PC**. Para obtener más información, consulte Wake on LAN.

  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.
- Si tiene una licencia de derechos híbridos y ha agregado conexiones de host de nube pública (por ejemplo, AWS), esas conexiones aparecen aquí. Para ver esas conexiones de host de la nube pública, actualice Web Studio unos minutos después de haberlas agregado.

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.

Crear y administrar conexiones y recursos

August 17, 2024

> **Importante:**
>
> A partir de Citrix Virtual Apps and Desktops 7 2006, si la implementación actual utiliza cualquiera de las siguientes tecnologías, solo podrá actualizar la versión de la implementación a la versión actual (Current Release) después de quitar los elementos con estado "Fin de vida"(EOL) que utilizan dichas tecnologías.
>
> - Discos Personal vDisk (PvD)
> - AppDisks
> - Tipos de host de nube pública: Citrix CloudPlatform, Microsoft Azure Classic
>
> Para obtener información detallada, consulte Quitar discos PvD, AppDisks y hosts no admitidos.
>
> **Nota:**
>
> Puede administrar la implementación de Citrix Virtual Apps and Desktops mediante dos consolas de administración: Web Studio (basada en la web) y Citrix Studio (basada en Windows). Este artículo se refiere únicamente a Web Studio. Para obtener información sobre Citrix Studio, consulte el artículo equivalente en Citrix Virtual Apps and Desktops 7 2212 o versiones anteriores.

Si quiere utilizar conexiones de host de nube pública con la implementación, necesita una licencia de derechos híbridos para completar la nueva instalación o actualizar a la versión actual.

Cuando el instalador detecta una o más de las tecnologías o conexiones de host no compatibles sin licencia de derechos híbridos, la actualización se pone en pausa o se detiene y se muestra un mensaje explicativo. Los registros del instalador contienen información detallada. Para obtener más información, consulte Actualizar una implementación.

Efecto de la licencia de derechos híbridos en la conexión de host

Hay tres casos en los que la conexión de host a los hosts de nube pública se ve afectada por la titularidad de licencia de derechos híbridos:

- Para crear una nueva conexión de host a los hosts de nube pública, debe tener una licencia de derechos híbridos.
- Si tiene una licencia de derechos híbridos pero esta ha caducado, las conexiones existentes a los hosts de nube pública se marcan como no autorizadas y pasan al modo de mantenimiento. Cuando las conexiones de host están en modo de mantenimiento, no puede hacer lo siguiente:

  - Agregar o modificar conexiones de host
  - Crear catálogos y actualizar imágenes
  - Realizar acciones de energía

- Cuando las conexiones de host no autorizadas cambian a autorizadas, vuelven a habilitarse.

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 conexión implica seleccionar el tipo de conexión entre los hipervisores compatibles y el almacenamiento y la red que seleccione de los recursos de esa conexión.

Los administradores de solo lectura pueden ver los detalles de la conexión y los recursos. Para poder realizar tareas de administración de recursos y conexiones, hay que ser un Administrador total. 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.

Para obtener más información, consulte las siguientes fuentes de información:

- **XenServer (anteriormente, Citrix Hypervisor):**
  - Entornos de virtualización de XenServer.
  - Documentación de XenServer.
- **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.

- **Conexiones de host de nube pública (AWS, Google Cloud, Microsoft Azure, soluciones de Nutanix Cloud y de partners y soluciones de VMware Cloud y de partners)**: Para obtener información relativa a los hosts de nube pública, consulte Configurar el tipo de recurso.

  > **Nota:**
  >
  > Las fuentes de información le dirigen a la documentación de Citrix DaaS. Si está familiarizado con los hosts de nube pública en el producto Citrix DaaS, la versión local tiene algunas diferencias. En Virtual Apps and Desktops local, la interfaz de administración se conoce como Web Studio. En el servicio, las actualizaciones se implementan cada cuatro semanas aproximadamente. Por lo tanto, es posible que ciertas funciones disponibles con el servicio no estén disponibles en la versión local.

Almacenamiento de host

Se admite un producto de almacenamiento cuando lo administra un hipervisor compatible. Citrix Support ayuda a los proveedores de los productos de almacenamiento a resolver problemas, y documenta dichos 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. Estos datos 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.

Si se ofrece un almacenamiento por separado para cada tipo de datos se puede reducir la carga y mejorar el rendimiento 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 plug-ins asociados.

El almacenamiento local de los datos temporales evita que haya que atravesar la red para acceder al almacenamiento compartido. También reduce la carga 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 XenServer 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 contiene los discos del sistema operativo.

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, denominado *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. Si usa almacenamiento local para datos temporales, el VDA aprovisionado queda asociado a un host de hipervisor específico. Si ese host falla, la máquina virtual no se puede iniciar.

Excepción: Microsoft System Center Virtual Machine Manager no permite la creación de discos de caché de datos temporales en el almacenamiento local al usar volúmenes de almacenamiento en clúster (CSV).

Cree una conexión para almacenar datos temporales localmente y, a continuación, habilite y configure valores no predeterminados para el tamaño de disco caché y el tamaño de memoria de cada VM. 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: XenServer ofrece IntelliCache, que reduce 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 sistema operativo se transfieren a los hipervisores del sitio. Este proceso se produce para la creación inicial de las máquinas y las futuras actualizaciones de imágenes. Este proceso 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.

Crear una conexión y recursos

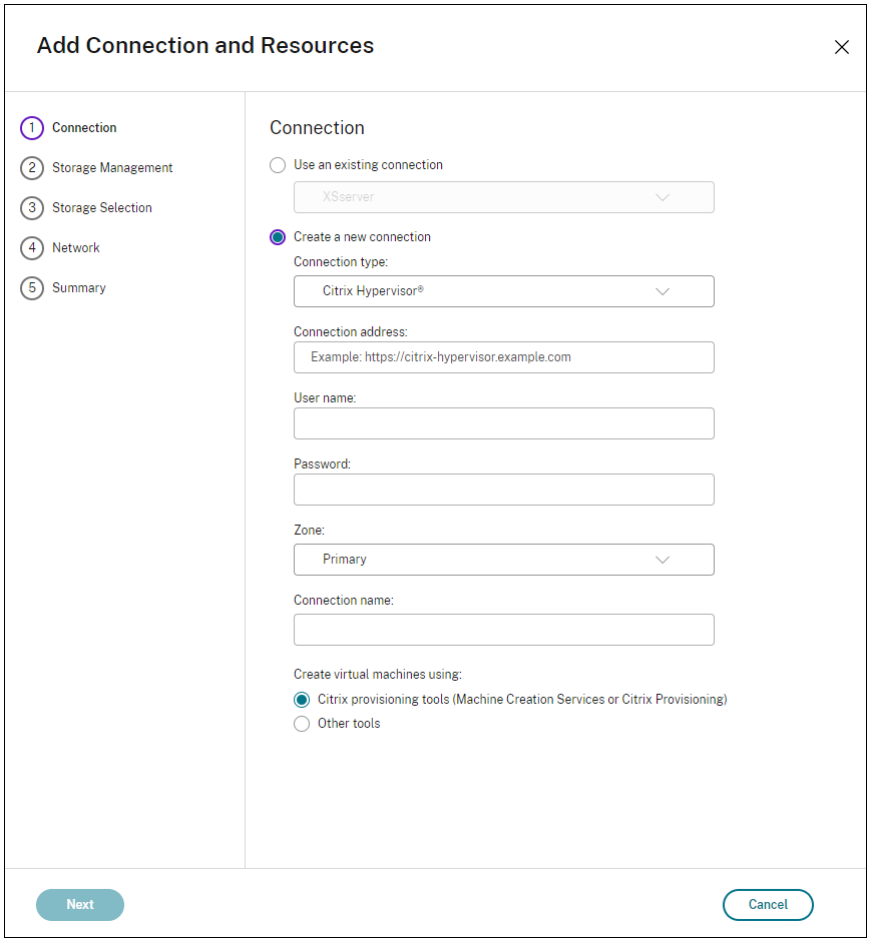
Si quiere, puede crear la primera conexión cuando crea el sitio. El asistente para creación de sitios contiene las páginas relacionadas con la conexión que se describen en las secciones siguientes.

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. Inicie sesión en Web Studio.
2. Seleccione **Alojamiento** en el panel de la izquierda.
3. Seleccione **Agregar conexiones y recursos** en la barra de acciones.
4. 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**.

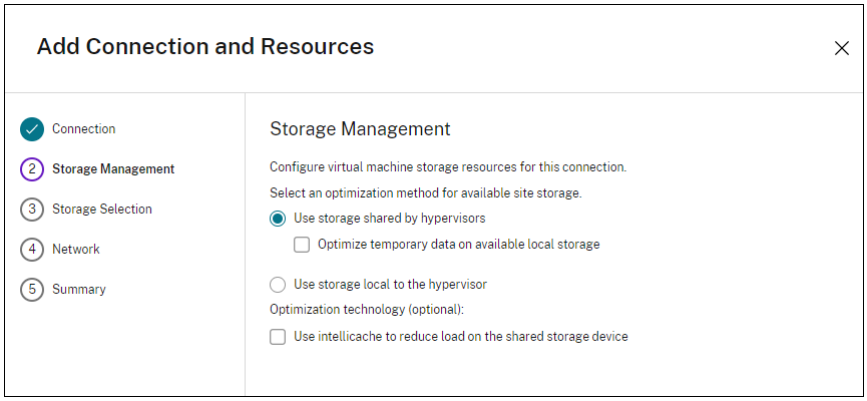
Conexión



En la página **Conexión**:

- Para crear una conexión, seleccione **Crear una 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 que está utilizando en el campo **Tipo de conexión**. Las conexiones de host de nube pública solo se enumeran en la lista desplegable si usa una licencia de derechos híbridos. Como alternativa, puede usar el comando de PowerShell `Get-HypHypervisorPlugin [-ZoneUid] $rluid [-IncludeUnavailable]` false/true para obtener lo siguiente:
  - Lista de todos los plug-ins de hipervisor compatibles con Citrix, incluidos los plug-ins de terceros
  - Disponibilidad del plug-in de hipervisor. Si el estado de disponibilidad es **false**, el motivo podría ser que el plug-in del hipervisor no esté instalado correctamente o que no tenga la licencia de derechos híbridos.
- 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 Web Studio.
- Elija la herramienta que usa para crear máquinas virtuales: herramientas de Web 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.

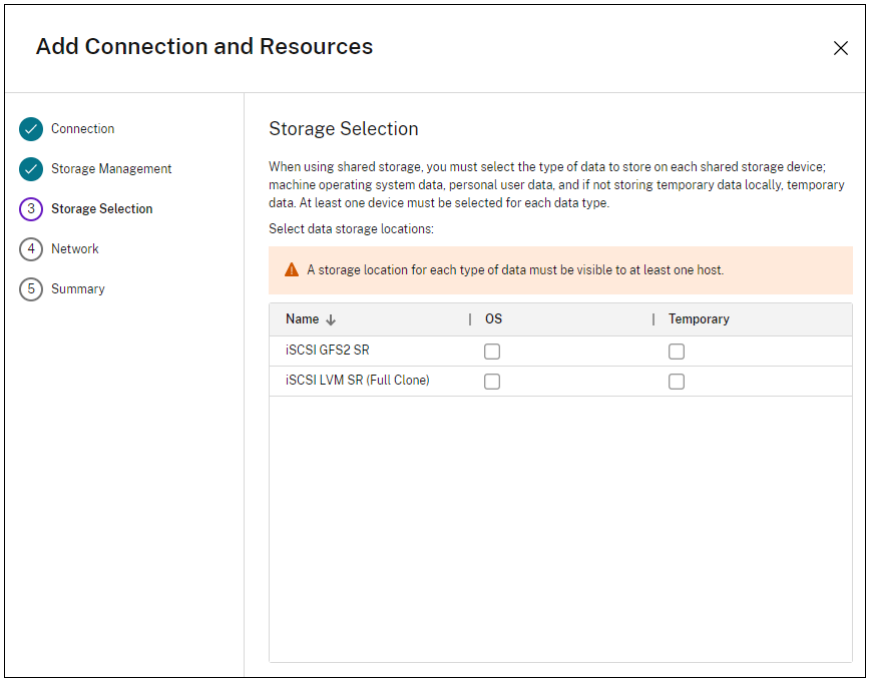
Si está configurando una conexión con un host de Hyper-V o VMware, busque y seleccione el nombre del clúster. Otros tipos de conexión no requieren un nombre de clúster.

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 eso, configurar esa administración de almacenamiento en Web Studio fallará.

Si usa almacenamiento compartido en una agrupación de XenServer, indique si quiere usar IntelliCache para reducir la carga en el dispositivo de almacenamiento compartido. Consulte Uso de IntelliCache para conexiones XenServer.

Selección del almacenamiento



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. Seleccione 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 eligió el almacenamiento compartido por hipervisores y habilitó **Optimizar datos temporales en el almacenamiento local disponible** en la página anterior. Puede seleccionar los dispositivos de

almacenamiento local que quiere usar para los datos temporales.

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 esa entrada, aparecen los nombres de los dispositivos seleccionados.

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 Web 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: Guardar los datos temporales localmente permite 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 conexiones son operaciones diferentes. Cambie la dirección solo si la máquina host actual tiene una nueva dirección. Al introducir una dirección a otra máquina, se desconfiguran 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. Inicie sesión en Web Studio.
2. Seleccione **Alojamiento** en el panel de la izquierda.
3. Seleccione la conexión y, a continuación, seleccione **Modificar conexión** en la barra de acciones.
4. Siga las instrucciones para conocer los parámetros disponibles cuando se modifica una conexión.

5. Cuando haya terminado, haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta, o haga clic en **Guardar** para aplicar los cambios y cerrar la ventana.

Página **Propiedades de la conexión**:

- Para cambiar la dirección de conexión y las credenciales, seleccione **Modificar parámetros…** y, a continuación, escriba la nueva información.
- Si quiere especificar los servidores de alta disponibilidad para una conexión de XenServer, seleccione **Modificar servidores…** y seleccione los servidores. Citrix recomienda seleccionar todos los servidores en la agrupación para permitir la comunicación con XenServer en caso de que falle el servidor principal de la agrupación.

  > **Nota:**
  >
  > Si utiliza HTTPS y quiere configurar servidores de alta disponibilidad, no instale un certificado comodín para todos los servidores de una agrupación. Se requiere un certificado individual para cada servidor.

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 **Acciones simultáneas (de cualquier tipo)**, 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.

Página **Shared Tenants**:

Agregue arrendatarios y suscripciones que compartan Azure Compute Gallery con la suscripción de esta conexión. Como resultado, al crear o actualizar catálogos, puede seleccionar imágenes compartidas de dichos arrendatarios y suscripciones.

- Introduzca el **ID** y el **secreto** de la aplicación asociada a esta conexión. Con esta información, puede autenticarse en Azure. Le recomendamos que cambie las claves con regularidad para garantizar la seguridad.
- Especifique las suscripciones y los arrendatarios compartidos. Puede agregar hasta ocho arrendatarios compartidos. Para cada arrendatario, puede agregar hasta ocho suscripciones.
- Haga clic en **Guardar** y **Aplicar** cuando haya terminado.

Introduzca la información en el campo **Opciones de conexión** únicamente con la ayuda de un representante de asistencia técnica de Citrix Support.

Modificar redes

Es posible cambiar redes con una conexión. Haga lo siguiente:

1. Vaya a **Hosting**.
2. Seleccione los recursos de destino en la conexión y, a continuación, seleccione **Modificar red** en la barra de acciones.
3. Seleccione una o varias redes que usarán las nuevas máquinas virtuales.
4. Haga clic en **Guardar** para guardar los cambios y salir.

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. Inicie sesión en Web Studio.
2. Seleccione **Alojamiento** en el panel de la izquierda.
3. Seleccione la conexión. Para activar el modo de mantenimiento, seleccione **Activar modo de mantenimiento** en la barra de 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 que usan 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. Inicie sesión en Web Studio.
2. Seleccione **Alojamiento** en el panel de la izquierda.
3. Seleccione la conexión y, a continuación, seleccione **Eliminar conexión** en la barra de acciones.
4. 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. Inicie sesión en Web Studio.
2. Seleccione **Alojamiento** en el panel de la izquierda.
3. Seleccione la conexión y, a continuación, seleccione **Cambiar nombre de la conexión** o **Probar conexión** en la barra de acciones.

Ver detalles de máquinas en una conexión

1. Inicie sesión en Web Studio.
2. Seleccione **Alojamiento** en el panel de la izquierda.
3. Seleccione la conexión y, a continuación, seleccione **Ver máquinas** en la barra de 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. Inicie sesión en Web Studio.
2. Seleccione **Alojamiento** en el panel de la izquierda.
3. Seleccione una conexión y, a continuación, seleccione **Ver máquinas** en el panel **Acción**.
4. Seleccione una de estas opciones en la barra de 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.
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).

Acción	Descripción
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 y datos temporales para las VM que usan esa conexión. También puede especificar qué servidores usar para el almacenamiento de cada tipo de datos.

1. Inicie sesión en Web Studio.
2. Seleccione **Alojamiento** en el panel de la izquierda.
3. Seleccione la conexión y, a continuación, seleccione **Modificar almacenamiento** en la barra de acciones.
4. En el panel izquierdo, seleccione el tipo de datos: sistema operativo o datos temporales.
5. Marque o desmarque las casillas de los dispositivos de almacenamiento para el tipo de datos seleccionado.
6. Haga clic en **Aceptar**.

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 usando 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. Inicie sesión en Web Studio.
2. Seleccione **Alojamiento** en el panel de la izquierda.
3. Seleccione el recurso y, a continuación, seleccione la entrada correspondiente en la barra de acciones: **Eliminar recursos**, **Cambiar nombre de recursos** o **Probar recursos**.

Detectar recursos huérfanos de Azure

Los recursos huérfanos son recursos no utilizados presentes en el sistema que pueden generar un gasto innecesario.

Esta función le permite detectar los recursos de Azure huérfanos en los hosts de su sitio en Citrix Virtual Apps and Desktops.

Siga los pasos en Web Studio:

1. En **Administrar**, selecciona **Alojamiento** en el panel izquierdo.
2. Seleccione una conexión y, a continuación, seleccione **Detectar recursos huérfanos** en la barra de acciones. El cuadro de diálogo **Detectar recursos huérfanos** muestra el informe de recursos huérfanos.
3. Para ver el informe de recursos huérfanos, seleccione **Ver informe**.

Como alternativa, puede detectar recursos huérfanos de Azure mediante PowerShell. Para obtener más información, consulte Obtener una lista de recursos huérfanos.

Para entender los motivos de los recursos huérfanos y saber cómo proceder, consulte Efficiently manage Orphaned Azure resources with Citrix.

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**: 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.

Obtener una lista de recursos huérfanos

Puede obtener una lista de los recursos huérfanos que MCS ha creado, pero de los que ya hace seguimiento. Esto se aplica actualmente a los entornos de Azure. Para obtener la lista, puede usar los comandos de PowerShell. Puede filtrar mediante conexiones.

> **Nota:**
>
> - El comando de PowerShell se rechaza si hay algún aprovisionamiento o actualización de imagen en curso.
> - Un recurso administrado por el cliente etiquetado con todas las etiquetas de Citrix se detecta como un recurso huérfano. Sin embargo, si agrega otra etiqueta CitrixDetectIgnore con el valor true para ese recurso, el recurso se omite al detectar los recursos huérfanos.

Limitaciones

- Solo un usuario con el rol de administrador de Cloud o administrador total integrado puede ejecutar el comando de PowerShell y obtener la lista de recursos huérfanos.
- Para evitar el reconocimiento incorrecto de los recursos huérfanos, no encienda las máquinas virtuales mientras filtra los recursos huérfanos.

- Alrededor de 2000 registros se muestran como huérfanos en caso de una posible carga de trabajo grande.

Para mostrar la lista de recursos huérfanos:

1. Abra una ventana de **PowerShell**.
2. Ejecute los comandos siguientes:

   a) Obtenga el identificador de conexión. El uid de conexión es el valor del atributo HypervisorConnectionUID.

   ```
   Get-ChildItem xdhyp:\connections | where {
     $_.PluginId -like 'Azure*'  }
    "
   ```

   b) Obtenga la lista de recursos huérfanos.

   ```
   get-provorphanedresource -HypervisorConnectionUid <connection
       uid>
   ```

Para mostrar la lista de recursos huérfanos de un ID de suscripción:

1. Abra una ventana de **PowerShell**.
2. Ejecute los comandos siguientes:

   a) Busque el identificador de conexión mediante el identificador de suscripción. El uid de conexión es el valor del atributo HypervisorConnectionUID.

   ```
   Get-ChildItem xdhyp:\connections | where {
     $_.CustomProperties -match '<subscriptionId>'  }
   ```

   b) Obtenga la lista de recursos huérfanos:

   ```
   get-provorphanedresource -HypervisorConnectionUid <connection
       uid>
   ```

> **Nota:**
>
> Compruebe los recursos detenidamente antes de eliminarlos.

Qué hacer a continuación

Para obtener información sobre la conexión con tipos de host específicos, consulte:

- Conexión con AWS
- Conexión a XenServer
- Conexión con entornos de Google Cloud

- Conexión con Microsoft Azure
- Conexión con Microsoft System Center Virtual Machine Manager
- Conexión con Nutanix
- Conexión con soluciones de Nutanix Cloud y de partners
- Conexión con VMware
- Conexión con soluciones de VMware Cloud y de partners

Si está en el proceso de implementación inicial, Crear un catálogo de máquinas.

Conexión con AWS

August 17, 2024

Crear y administrar conexiones y recursos describe los asistentes que crean una conexión. La siguiente información incluye detalles específicos de los entornos de nube de AWS.

> **Nota:**
>
> Antes de crear una conexión con AWS, debe terminar de configurar su cuenta de AWS como ubicación de recursos. Consulte Entornos en la nube de AWS.

Crear una conexión

Cuando se crea una conexión desde Web Studio:

- Debe proporcionar la clave de API y los valores de clave secreta. Puede exportar el archivo de claves que contiene esos valores de AWS y, a continuación, importarlos. También debe proporcionar 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.
- 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, la administración de Citrix Virtual Apps and Desktops no puede usar el archivo para rellenar los campos de la clave de API y la clave secreta. Debe utilizar archivos de credenciales de Identity Access Management (IAM) de AWS.

> **Nota:**
>
> Después de crear una conexión, los intentos de actualizar la clave de API y la clave secreta podrían fallar. Para resolver el problema, compruebe las restricciones del servidor proxy o

> del firewall y asegúrese de que se puede contactar con la siguiente dirección: `https://*.amazonaws.com`.

Valores predeterminados de conexión de host

Al crear conexiones de host en entornos de nube de AWS, se muestran los siguientes valores predeterminados:

Opción	Absoluta	Porcentaje
Acciones simultáneas (de cualquier tipo)	125	100
Máximo de acciones nuevas por minuto	125	

MCS admite un máximo de 100 operaciones simultáneas de aprovisionamiento de forma predeterminada.

URL de "punto de enlace"de servicio

URL de "punto de enlace"de servicio de zona estándar

Cuando utiliza MCS, se agrega una nueva conexión de AWS con una clave de API y un secreto de API. Con esta información, junto con la cuenta autenticada, MCS consulta a AWS las zonas admitidas mediante la llamada a la API de EC2 con la acción de AWS DescribeRegions. Para la consulta, se utiliza una URL de dispositivo de punto final de servicio (punto de enlace de servicio, como se conoce en AWS) de EC2 genérica `https://ec2.amazonaws.com/`. Use MCS para seleccionar la zona de la conexión en la lista de zonas admitidas. La URL de punto de enlace del servicio de AWS preferida se selecciona automáticamente para la zona. Sin embargo, después de crear la URL de punto de enlace de servicio, ya no podrá establecerla ni modificarla.

Definir permisos de IAM

Utilice la información de esta sección para definir los permisos de IAM para Citrix Virtual Apps and Desktops en AWS. El servicio IAM de Amazon permite cuentas con varios usuarios que se pueden organizar en grupos. Estos usuarios pueden tener diferentes permisos para controlar su capacidad de realizar operaciones asociadas con la cuenta. Para obtener más información acerca de los permisos de IAM, consulte Referencia de directivas JSON de IAM.

Para aplicar la directiva de permisos de IAM a un nuevo grupo de usuarios:

1. Inicie sesión en la consola de administración de AWS y seleccione el **servicio IAM** en la lista desplegable.

2. Seleccione **Create a New Group of Users**.
3. Escriba un nombre para el nuevo grupo de usuarios y seleccione **Continue**.
4. En la página **Permissions**, elija **Custom Policy**. Seleccione **Select**.
5. Escriba un nombre para la **directiva de permisos** (Permissions policy).
6. En la sección **Policy Document**, introduzca los permisos correspondientes.

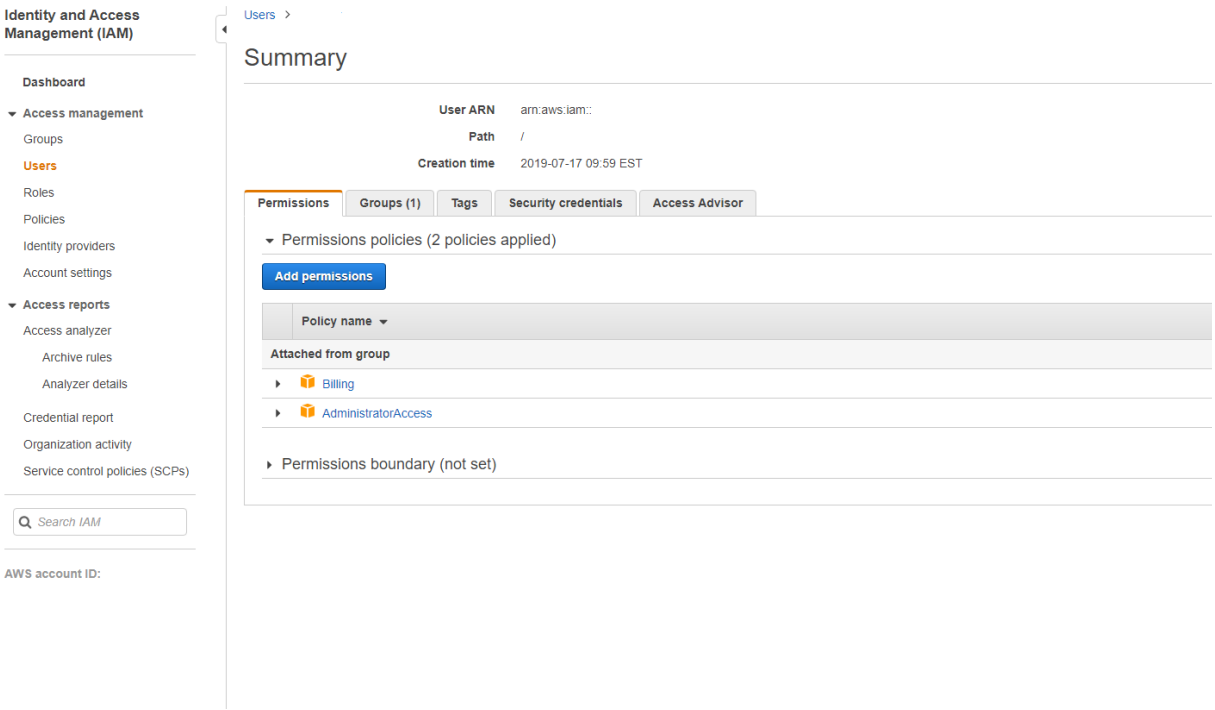
Después de indicar información sobre la directiva, seleccione **Continue** para completar el proceso de creación del grupo de usuarios. Los usuarios del grupo tienen permisos para realizar solo las acciones necesarias para Citrix Virtual Apps and Desktops.

> **Importante:**
>
> Utilice el texto de directiva proporcionado en el ejemplo anterior para indicar las acciones que Citrix Virtual Apps and Desktops utiliza para realizar operaciones en una cuenta de AWS sin restringir esas operaciones a recursos específicos. Citrix recomienda utilizar el ejemplo como prueba. Para entornos de producción, puede optar por agregar más restricciones a los recursos.

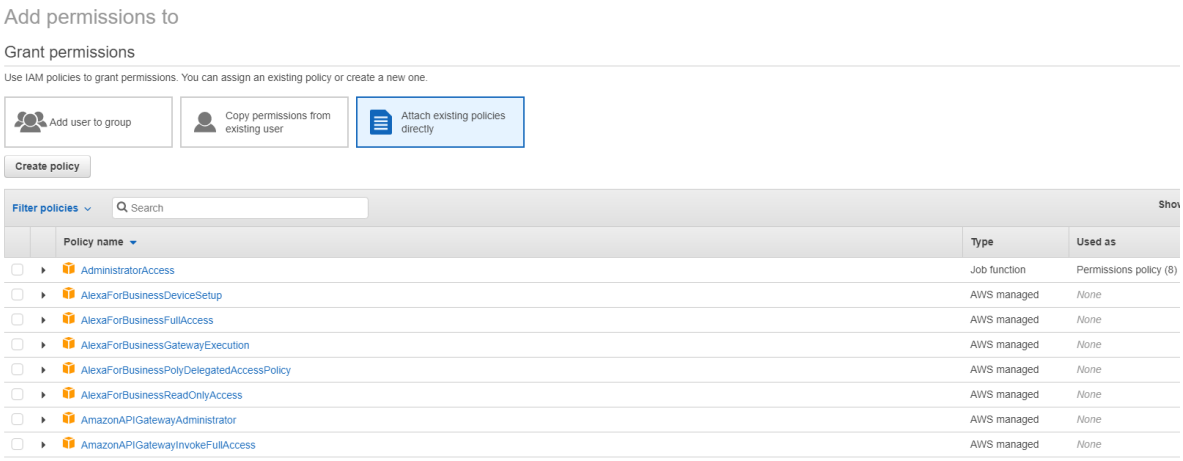
Establecer permisos de IAM

Establezca los permisos en la sección **IAM** de la consola de administración de AWS (AWS Management Console):

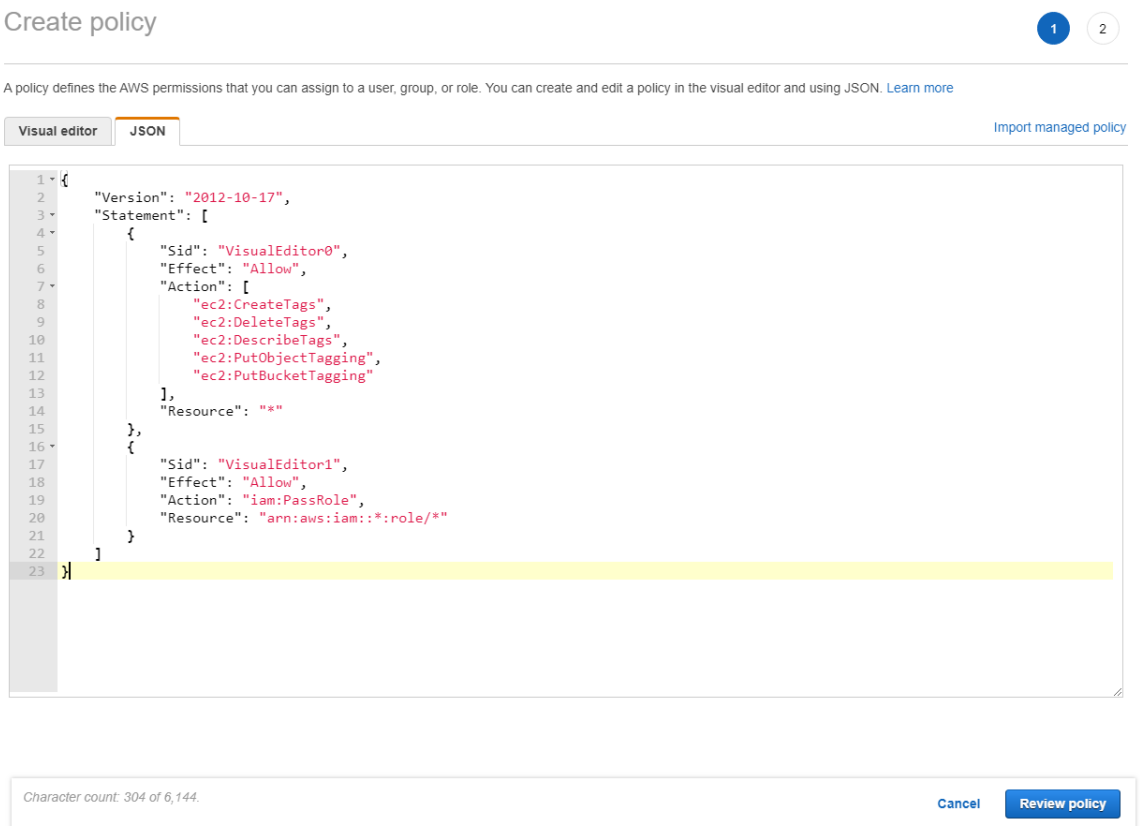
1. En el panel **Summary**, seleccione la ficha **Permissions**.
2. Seleccione **Add permissions**.



En la pantalla **Add Permissions to**, conceda los permisos:



Utilice lo siguiente como ejemplo en la ficha **JSON**:



> **Sugerencia:**
>
> Es posible que el ejemplo sobre JSON indicado no incluya todos los permisos necesarios para su entorno. Para obtener más información, consulte Cómo definir permisos de administración de

> acceso a identidades que ejecutan Citrix Virtual Apps and Desktops en AWS.

Permisos de AWS requeridos

Esta sección contiene la lista completa de permisos de AWS.

> **Nota:**
>
> El permiso *iam:PassRole* solo es necesario para **role_based_auth**.

Crear una conexión de host

Se agrega una nueva conexión de host con la información de AWS.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }

    ]
 }
```

Administración de energía de las máquinas virtuales

Las instancias de máquina están encendidas o apagadas.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:AttachVolume",
```



```
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DetachVolume",
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }

    ]
}
```

Creación, actualización o eliminación de máquinas virtuales

Se crea, actualiza o elimina un catálogo de máquinas con las máquinas virtuales aprovisionadas como instancias de AWS.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
```



```
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }
,
        {

            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }
,
        {

            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:PutBucketAcl",
                "s3:PutBucketTagging",
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
         }
,
        {

            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
```



```
            ],
            "Effect": "Allow",
            "Resource": "*"
        }

    ]
}
```

> **Nota:**
>
> La sección EC2 relacionada con grupos de seguridad solo es necesaria si se debe crear un grupo de seguridad de aislamiento para la máquina virtual de preparación durante la creación del catálogo. Una vez hecho esto, no se requieren estos permisos.

Carga y descarga directa en disco La carga directa en disco elimina el requisito de trabajador de volumen para el aprovisionamiento de catálogos de máquinas y, en su lugar, utiliza las API públicas que proporciona AWS. Esta funcionalidad reduce el coste asociado a las cuentas de almacenamiento adicionales y la complejidad para mantener las operaciones de trabajador de volumen.

> **Nota:**
>
> Se ha retirado la función de trabajador de volumen.

Se deben agregar los siguientes permisos a la directiva:

- `ebs:StartSnapshot`
- `ebs:GetSnapshotBlock`
- `ebs:PutSnapshotBlock`
- `ebs:CompleteSnapshot`
- `ebs:ListSnapshotBlocks`
- `ebs:ListChangedBlocks`
- `ec2:CreateSnapshot`
- `ec2:DeleteSnapshot`
- `ec2:DescribeLaunchTemplates`

> **Importante:**
>
> - Puede agregar una máquina virtual a los catálogos de máquinas existentes sin ninguna operación de trabajador de volumen, como AMI de trabajador de volumen y VM de trabajador de volumen.
> - Si elimina un catálogo que utilizaba trabajador de volumen anteriormente, se eliminan todos los artefactos, incluidos los relacionados con el trabajador de volumen.

Cifrado de EBS de volúmenes creados

EBS puede cifrar automáticamente los volúmenes recién creados si la imagen AMI está cifrada o si EBS está configurado para cifrar todos los volúmenes nuevos. Sin embargo, para implementar la funcionalidad, se deben incluir los siguientes permisos en la directiva de IAM.

```
{

     "Version": "2012-10-17",
     "Statement": [
        {

            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": "*"
         }

    ]
 }
```

> **Nota:**
>
> Los permisos se pueden limitar a claves específicas si se incluye un recurso y bloque de condición, a discreción del usuario. Por ejemplo: **Permisos de KMS con condición**:

```
{

     "Version": "2012-10-17",
     "Statement": [
        {

            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": [
                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-a123
                   -456d-a12b-a123b4cd56ef"
            ],
            "Condition": {
```



```
20
21                  "Bool": {
22
23                      "kms:GrantIsForAWSResource": true
24                   }
25
26              }
27
28          }
29
30      ]
31   }
```

La siguiente instrucción de directiva de claves es la predeterminada para las claves KMS, que es necesaria para permitir que la cuenta utilice las directivas de IAM para delegar el permiso para todas las acciones (kms:*) en la clave KMS.

```
1  {
2
3  "Sid": "Enable IAM policies",
4  "Effect": "Allow",
5  "Principal": {
6
7  "AWS": "arn:aws:iam::111122223333:root"
8   }
9   ,
10 "Action": "kms:",
11 "Resource": ""
12  }
```

Para obtener más información, consulte la documentación oficial de AWS Key Management Service.

Autenticación basada en roles de IAM

Estos permisos se agregan para admitir la autenticación basada en roles.

```
1  {
2
3       "Version": "2012-10-17",
4       "Statement": [
5          {
6
7              "Effect": "Allow",
8              "Action": "iam:PassRole",
9              "Resource": "arn:aws:iam::*:role/*"
10          }
11
12      ]
13   }
```


Directiva de permisos mínimos de IAM

El siguiente código JSON puede utilizarse para todas las funciones compatibles actualmente. Mediante esta directiva, puede crear conexiones de host, crear, actualizar o eliminar máquinas virtuales y administrar la energía.
La directiva se puede aplicar a los usuarios como se explica en las secciones Definir permisos de IAM o también puede usar la autenticación basada en roles mediante la clave de seguridad y la clave secreta de **role_based_auth** .

> **Importante:**
>
> Para usar **role_based_auth**, configure primero el rol de IAM deseado en todos los Delivery Controllers de nuestro sitio. Con Web Studio, agregue la conexión de host y suministre "role_based_auth"para la clave de autenticación y el secreto. Una conexión de host con estos parámetros utiliza la autenticación basada en roles.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateNetworkInterface",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteLaunchTemplate",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DeregisterImage",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
```



```
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
,
        {

            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
,
        {

            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:PutBucketAcl",
                "s3:PutObject",
                "s3:PutBucketTagging",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
        }
,
        {

            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
```



```
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
,
        {

            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:Decrypt",
                "kms:DescribeKey",
                "kms:GenerateDataKeyWithoutPlainText",
                "kms:GenerateDataKey",
                "kms:ReEncryptTo",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*"
        }
,
        {

            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
        }

    ]
}
```

Nota:

- La sección EC2 relacionada con SecurityGroups solo es necesaria si se debe crear un grupo de seguridad de aislamiento para la máquina virtual de preparación durante la creación del catálogo. Una vez hecho esto, no se requieren estos permisos.
- La sección KMS solo es necesaria cuando se utiliza el cifrado de volúmenes de EBS.
- La sección de permisos iam:PassRole solo es necesaria para **role_based_auth**.
- Se pueden agregar permisos específicos a nivel de recursos, en lugar de pleno acceso, en función de los requisitos y el entorno. Para obtener más información, consulte los documentos de AWS Demystifying EC2 Resource-Level Permissions y Access management for AWS resources.

Validar permisos en la conexión de host

Puede validar los permisos en una conexión de host para realizar tareas relacionadas con la creación y la administración de catálogos de máquinas de MCS. Esta implementación le ayuda a conocer con antelación los permisos ausentes necesarios para diferentes situaciones, como la creación, la eliminación y la actualización de máquinas virtuales, la administración de energía de las máquinas virtuales y el cifrado de EBS, para evitar el bloqueo en momentos críticos.

Puede validar los permisos de una conexión de host mediante el comando `Test-HypHypervisorConnectior` de PowerShell. El resultado del comando se captura como una lista en la que cada elemento de la lista se divide en tres secciones.

- Categoría: La acción o tarea que un usuario puede realizar para crear y administrar un catálogo de máquinas de MCS.
- Acción correctiva: El paso que debe seguir un administrador para resolver la discrepancia de permisos ausentes de un usuario.
- Permiso que falta: La lista de permisos ausentes para una categoría.

Para validar los permisos, haga lo siguiente:

1. Cree una conexión de host con AWS.
2. Abra una ventana de PowerShell desde el host del Delivery Controller.
3. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
4. Ejecute el siguiente comando para verificar si tiene los permisos necesarios para buscarlos.

```
Test-HypHypervisorConnection -LiteralPath "XDHyp:\Connections\
    AWSCon"
```

5. Después de agregar los permisos ausentes necesarios para buscar los permisos, ejecuta el siguiente comando para verificar si tiene permisos en las siguientes categorías:

    - Crear, Actualizar, Eliminar
    - Administración de energía
    - Cifrado EBS

```
Test-HypHypervisorConnection -LiteralPath "XDHyp:\Connections\
    AWSCon" [-SecurePassword -Password] "password" -UserName "" -
    CustomProperties ""
```

Para obtener más información sobre cómo agregar permisos, consulte Establecer permisos de IAM.

Qué hacer a continuación

- Si está en el proceso de implementación inicial, consulte Crear catálogos de máquinas

- Para obtener información específica de AWS, consulte Crear un catálogo de AWS

Más información

- Conexiones y recursos
- Crear catálogos de máquinas

Conexión a XenServer

August 17, 2024

Crear y administrar conexiones y recursos describe los asistentes que crean una conexión. La siguiente información incluye detalles específicos de los entornos de virtualización de XenServer.

> **Nota:**
>
> Antes de crear una conexión con XenServer, debe terminar de configurar su cuenta de XenServer como ubicación de recursos. Consulte Entornos de virtualización de XenServer.

Crear una conexión a XenServer

Cuando crea una conexión con XenServer (antes Citrix Hypervisor), 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 XenServer. Para utilizar HTTPS, debe reemplazar el certificado SSL predeterminado que se instaló en XenServer; consulte CTX128656.

Es posible configurar la alta disponibilidad si esta función está habilitada en el servidor XenServer. Citrix recomienda seleccionar todos los servidores de la agrupación (en Edit High Availability) para permitir la comunicación con el servidor XenServer 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 XenServer 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 XenServer 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.)

Puede utilizar Machine Creation Services (MCS) y Citrix Provisioning (antes llamado Provisioning Services) para aprovisionar:

- BIOS antiguos para máquinas virtuales con SO de servidor o escritorio compatibles.
- UEFI para máquinas virtuales con SO de servidor o escritorio compatibles, incluido arranque seguro.

> **Nota:**
>
> Se requieren permisos de operador de grupo, como mínimo, cuando se configura MCS.

Usar IntelliCache para conexiones XenServer

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 XenServer.

- Al instalar XenServer, seleccione **Enable thin provisioning (Optimized storage for Citrix 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 XenServer.
- De forma predeterminada, en Citrix Virtual Apps and Desktops el componente IntelliCache está inhabilitado. Puede cambiar el parámetro únicamente al crear una conexión XenServer; no podrá inhabilitar IntelliCache más tarde. Al agregar una conexión XenServer:
  - Seleccione el tipo de almacenamiento **compartido**.
  - Marque la casilla **Usar IntelliCache**.

Permisos de XenServer necesarios

Los permisos de XenServer se basan en roles (RBAC). La función de control de acceso basado en roles (RBAC) de XenServer le permite asignar usuarios, roles y permisos para controlar quién tiene acceso a su XenServer y qué acciones pueden realizar. El sistema RBAC de XenServer asigna un usuario (o un grupo de usuarios) a roles definidos (un conjunto de permisos con nombre). Los roles tienen permisos de XenServer asociados para realizar determinadas operaciones.

Para obtener más información, consulte Control de acceso por 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
Agregar 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 o quitar máquinas virtuales en las programaciones de instantáneas existentes	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
Agregar o quitar máquinas virtuales (máquinas virtuales habilitadas para GPU)	Operador de agrupaciones

Tarea	Rol mínimo requerido
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.

Qué hacer a continuación

- Si está en el proceso de implementación inicial, consulte Crear catálogos de máquinas
- Para obtener información específica sobre XenServer, consulte Crear un catálogo de XenServer

Más información

- Conexiones y recursos
- Crear catálogos de máquinas

Conexión con entornos de Google Cloud

August 17, 2024

Crear y administrar conexiones y recursos describe los asistentes que crean una conexión. La siguiente información incluye detalles específicos de los entornos de Google Cloud.

> **Nota:**
>
> Antes de crear una conexión con Google Cloud, debe terminar de configurar su cuenta de Google Cloud como ubicación de recursos. Consulte Entornos de Google Cloud.

Agregar una conexión

Siga las instrucciones que se indican en Crear una conexión y recursos. Esta descripción es una guía para configurar una conexión de alojamiento:

1. En **Administrar > Configuración**, seleccione **Alojamiento** en el panel de la izquierda.
2. Seleccione **Agregar conexión y recursos** en la barra de acciones.
3. En la página **Conexión**, seleccione **Crear una conexión** y **Herramientas de aprovisionamiento de Citrix** y, a continuación, seleccione **Siguiente**.
   - **Tipo de conexión**. Seleccione **Google Cloud** en el menú.
   - **Nombre de la conexión**. Escriba un nombre para la conexión.
4. En la página **Región**, seleccione un nombre de proyecto en el menú, seleccione una región que contenga los recursos que quiere utilizar y, a continuación, seleccione **Siguiente**.
5. En la página **Red**, escriba un nombre para los recursos, seleccione una red virtual en el menú, seleccione un subconjunto y, a continuación, seleccione **Siguiente**. El nombre de los recursos ayuda a identificar esta combinación de región y red. Las redes virtuales con el sufijo *(Shared)* (Compartida) anexado a su nombre representan VPC compartidas. Si configura un rol de IAM a nivel de subred para una VPC compartida, solo aparecerán subredes específicas de la VPC compartida en la lista de subredes.

   > **Nota:**
   >
   > - El nombre de conexión puede contener entre 1 y 64 caracteres, y no puede contener solo espacios en blanco o los caracteres `\ / ; : # . * ? = < > | [ ] { } "' ( )' )`.

6. En la página **Resumen**, confirme la información y seleccione **Finalizar** para salir de la ventana **Agregar conexión y recursos**.

Después de crear la conexión y los recursos, podrá verlos. Para configurar la conexión, selecciónela y, a continuación, seleccione la opción correspondiente en la barra de acciones.

Del mismo modo, puede eliminar, cambiar el nombre o probar los recursos creados en la conexión. Para ello, seleccione el recurso de la conexión y, a continuación, seleccione la opción correspondiente de la barra de acciones.

URL de dispositivo de punto final del servicio

Debe tener acceso a las siguientes URL:

- `https://oauth2.googleapis.com`
- `https://cloudresourcemanager.googleapis.com`
- `https://compute.googleapis.com`
- `https://storage.googleapis.com`
- `https://cloudbuild.googleapis.com`

Proyectos de Google Cloud

Existen básicamente dos tipos de proyectos de Google Cloud:

- Proyecto de Provisioning: En este caso, la cuenta de administrador actual es propietaria de las máquinas aprovisionadas del proyecto. Este tipo de proyecto se conoce también como proyecto local.
- Proyecto de nube privada virtual (VPC) compartida: Proyecto en el que las máquinas creadas en el proyecto de aprovisionamiento utilizan la VPC del proyecto de VPC compartida. La cuenta de administrador utilizada para el proyecto de aprovisionamiento tiene permisos limitados en este proyecto, específicamente, solo permisos para usar la nube VPC.

Crear un entorno seguro para el tráfico administrado de GCP

Puede permitir el acceso privado a Google en sus proyectos de Google Cloud. Esta implementación mejora la seguridad a la hora de gestionar datos confidenciales. Para lograrlo, puede optar por una de estas acciones:

- Incluya estas reglas de entrada de controles de servicio de VPC para la cuenta de servicio de Cloud Build. Si hace este paso, no siga los pasos que se indican a continuación con los que crear un entorno seguro para el tráfico administrado por GCP.

```
Ingress Rule 1
From:
Identities:
<ProjectID>@cloudbuild.gserviceaccount.com
Source > All sources allowed
To:
Projects =
All projects
Services =
Service name: All services
```

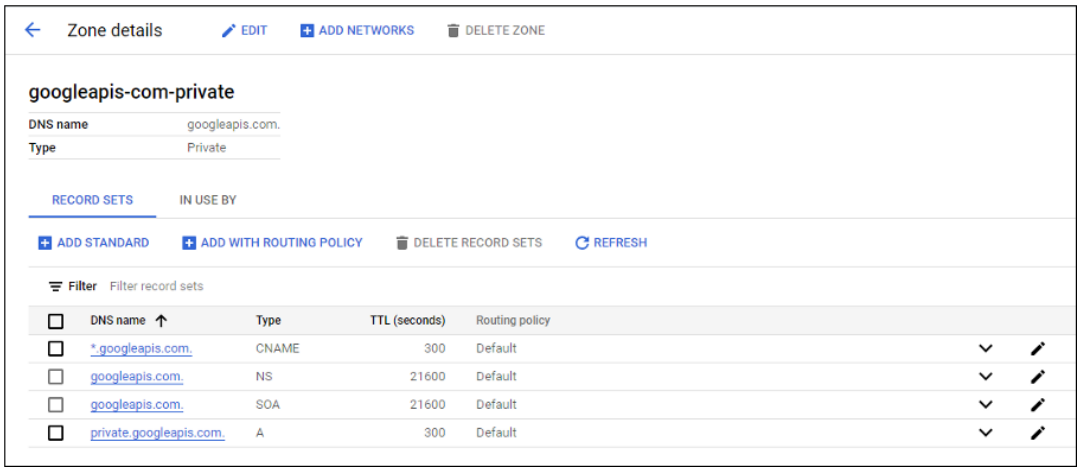
- Si utiliza una agrupación de trabajadores privados, agregue `UsePrivateWorkerPool` a `CustomProperties`. Para obtener información sobre la agrupación de trabajadores privados, consulte Private pools overview.

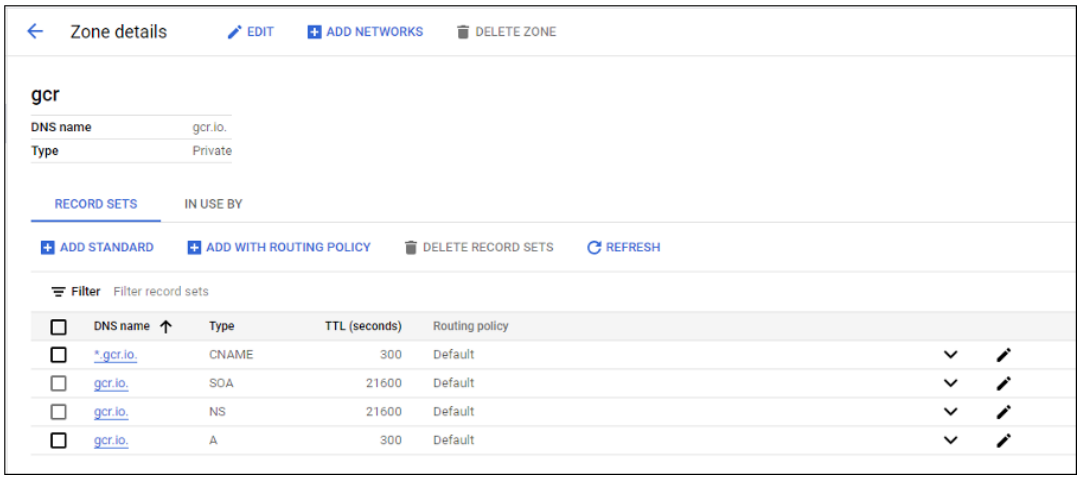
Requisitos para crear un entorno seguro para el tráfico administrado de GCP

Los requisitos para crear un entorno seguro para el tráfico administrado de GCP son los siguientes:

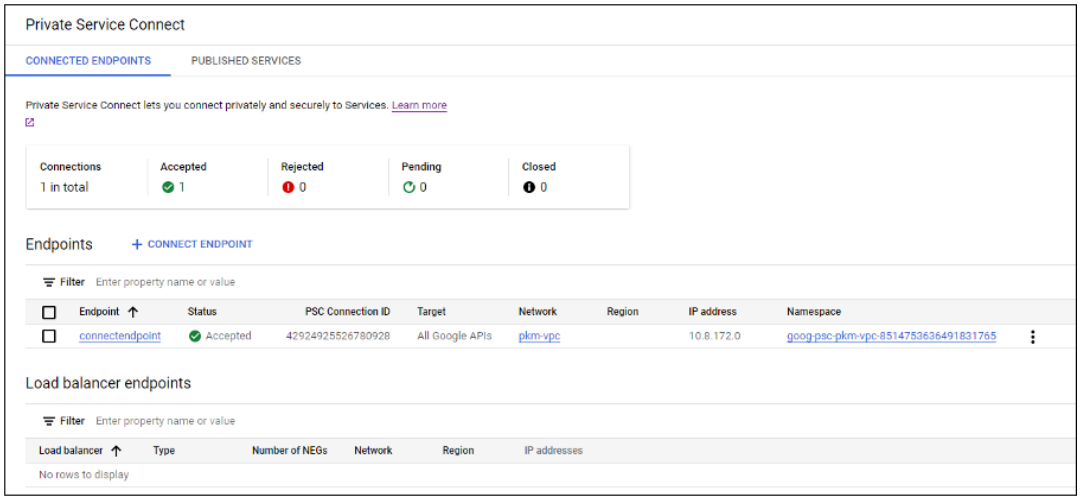
- Asegúrese de que la conexión de alojamiento esté en modo de mantenimiento al actualizar las propiedades personalizadas.
- Para usar agrupaciones de trabajadores privados, se requieren los siguientes cambios:

- Para la cuenta de servicio de Citrix Cloud, agregue los siguientes roles de IAM:
  * Cuenta de servicio de Cloud Build
  * Administrador de instancias de proceso
  * Usuario de cuenta de servicio
  * Creador de tokens de cuentas de servicio
  * Propietario de agrupación de trabajadores de Cloud Build
- Cree la cuenta de servicio de Citrix Cloud en el mismo proyecto que usa para crear una conexión de alojamiento.
- Configure las zonas DNS para `private.googleapis.com` y `gcr.io` como se describe en la Configuración de DNS.

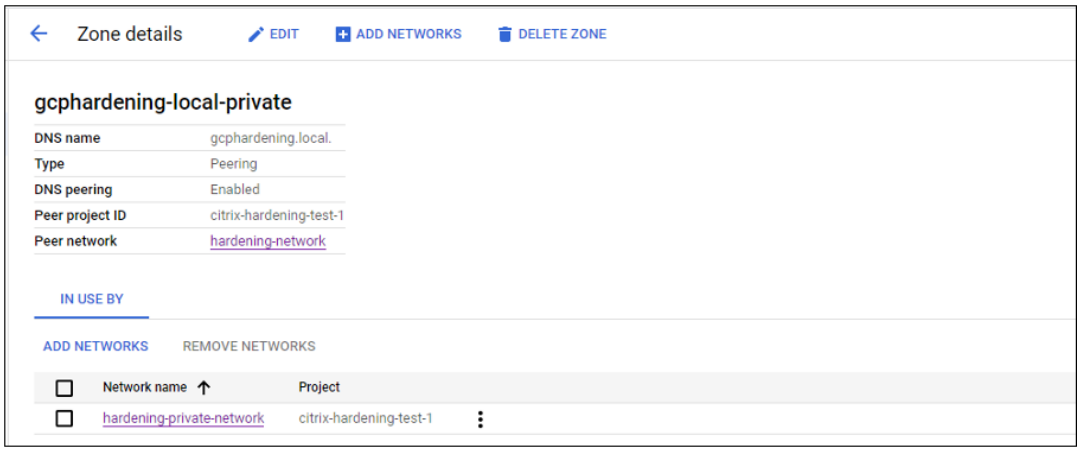




- Configure la traducción de direcciones de red (NAT) privada o utilice una conexión de servicio privada. Para obtener más información, consulte Access Google APIs through endpoints.



- Si usa una VPC emparejada, cree una zona de Cloud DNS que conecte a la VPC emparejada. Para obtener más información, consulte Create a peering zone.



- En los controles de servicio de VPC, configure las reglas de salida para que las API y las máquinas virtuales puedan comunicarse con Internet. Las reglas de entrada son opcionales. Por ejemplo:

```
Egress Rule 1
From:
Identities:ANY_IDENTITY
To:
Projects =
All projects
Service =
Service name: All services
```

Habilitar la agrupación privada de trabajadores

Para habilitar la agrupación privada de trabajadores, defina las propiedades personalizadas de esta manera en la conexión de host:

1. Abra una ventana de PowerShell desde el host del Delivery Controller o utilice el SDK de PowerShell remoto. Para obtener más información sobre el SDK de PowerShell remoto, consulte SDK y API.
2. Ejecute los comandos siguientes:

   a) `Add-PSSnapin citrix*`
   b) `cd XDHyp:\Connections\`
   c) `dir`

3. Copie `CustomProperties` de la conexión a un bloc de notas.
4. Adjunte el parámetro de propiedad `<Property xsi:type="StringProperty"Name="UsePrivateWorkerPool"Value="True"/>`. Por ejemplo:

```
```
<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance" xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation">
<Property xsi:type="StringProperty" Name="UsePrivateWorkerPool"
    Value="True"/>
</CustomProperties>
```
```

5. En la ventana de PowerShell, asigne una variable a las propiedades personalizadas modificadas. Por ejemplo:
   `$customProperty = '<CustomProperties...</CustomProperties>'`.
6. Ejecute `$gcpServiceAccount = "<ENTER YOUR SERVICE ACCOUNT EMAIL HERE>"`.
7. Ejecute `$gcpPrivateKey = "<ENTER YOUR SERVICE ACCOUNT PRIVATE KEY HERE AFTER REMOVING ALL INSTANCES OF \n >"`.
8. Ejecute `$securePassword = ConvertTo-SecureString $gcpPrivateKey -AsPlainText -Force`.
9. Ejecute lo siguiente para actualizar una conexión de host existente:

```
Set-Item -PassThru -Path @('XDHyp:\Connections\<ENTER YOUR
    CONNECTION NAME HERE>') -SecurePassword $securePassword -
    UserName $gcpServiceAccount -CustomProperties $customProperty
```

Permisos de GCP requeridos

En esta sección, se incluye la lista completa de permisos de GCP. Utilice el conjunto completo de permisos que se indica en la sección para que la funcionalidad opere correctamente.

> **Nota:**
>
> GCP presentará cambios en el comportamiento predeterminado de los servicios de Cloud Build y en el uso de las cuentas de servicio a partir del 29 de abril de 2024. Para obtener más información, consulte Cambio de la cuenta de servicio de Cloud Build. Los proyectos de Google existentes con la API de Cloud Build habilitada antes del 29 de abril de 2024 no se ven afectados por este cambio. No obstante, si quiere mantener el comportamiento actual del servicio de Cloud Build a partir del 29 de abril, puede crear o aplicar una directiva de organización para inhabilitar la aplicación de restricciones antes de habilitar la API. Si establece la nueva directiva de organización, puede seguir usando los permisos existentes en esta sección y los elementos marcados en **Antes del cambio de la cuenta de servicio de Cloud Build**. De lo contrario, siga los permisos y elementos existentes que están marcados en **Después del cambio de cuenta de servicio de Cloud Build**.

Crear una conexión de host

- Permisos mínimos requeridos para la cuenta de servicio de Citrix Cloud en el proyecto de Provisioning:

```
compute.instanceTemplates.list
compute.instances.list
compute.networks.list
compute.projects.get
compute.regions.list
compute.subnetworks.list
compute.zones.list
resourcemanager.projects.get
```

  Estos roles definidos por Google tienen los permisos que se indican anteriormente:

  - Administrador de procesos
  - Usuario de almacén de datos en la nube

- Permisos adicionales requeridos para la nube VPC compartida con la cuenta de servicio de Citrix Cloud en el proyecto de nube VPC compartida:

```
compute.networks.list
compute.subnetworks.list
resourcemanager.projects.get
```

  Estos roles definidos por Google tienen los permisos que se indican anteriormente:

  - Compute Network User

Administración de energía de las máquinas virtuales

Permisos mínimos requeridos para la cuenta de servicio de Citrix Cloud en el proyecto de Provisioning en el caso de catálogos solo con administración de energía:

```
compute.instanceTemplates.list
compute.instances.list
compute.instances.get
compute.instances.reset
compute.instances.resume
compute.instances.start
compute.instances.stop
compute.instances.suspend
compute.networks.list
compute.projects.get
compute.regions.list
compute.subnetworks.list
compute.zones.list
resourcemanager.projects.get
compute.zoneOperations.get
```

Estos roles definidos por Google tienen los permisos que se indican anteriormente:

- Administrador de procesos
- Usuario de almacén de datos en la nube

Creación, actualización o eliminación de máquinas virtuales

- Permisos mínimos requeridos para la cuenta de servicio de Citrix Cloud en el proyecto de Provisioning:

```
cloudbuild.builds.create
cloudbuild.builds.get
cloudbuild.builds.list
compute.acceleratorTypes.list
compute.diskTypes.get
compute.diskTypes.list
compute.disks.create
compute.disks.createSnapshot
compute.disks.delete
compute.disks.get
compute.disks.list
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.firewalls.create
compute.firewalls.delete
compute.firewalls.list
compute.globalOperations.get
compute.images.create
```



```
compute.images.delete
compute.images.get
compute.images.list
compute.images.setLabels
compute.images.useReadOnly
compute.instanceTemplates.create
compute.instanceTemplates.delete
compute.instanceTemplates.get
compute.instanceTemplates.list
compute.instanceTemplates.useReadOnly
compute.instances.attachDisk
compute.instances.create
compute.instances.delete
compute.instances.detachDisk
compute.instances.get
compute.instances.list
compute.instances.reset
compute.instances.resume
compute.instances.setDeletionProtection
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.instances.setTags
compute.instances.start
compute.instances.stop
compute.instances.suspend
compute.machineTypes.get
compute.machineTypes.list
compute.networks.list
compute.networks.updatePolicy
compute.nodeGroups.list
compute.nodeTemplates.get
compute.projects.get
compute.regions.list
compute.snapshots.create
compute.snapshots.delete
compute.snapshots.list
compute.snapshots.get
compute.snapshots.setLabels
compute.snapshots.useReadOnly
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.use
compute.zoneOperations.get
compute.zoneOperations.list
compute.zones.get
compute.zones.list
iam.serviceAccounts.actAs
resourcemanager.projects.get
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
```



```
storage.buckets.update
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
compute.networks.get
compute.resourcePolicies.use
```

Estos roles definidos por Google tienen los permisos que se indican anteriormente:

- Administrador de procesos
- Administrador de almacenamiento
- Editor de compilaciones en la nube
- Usuario de cuenta de servicio
- Usuario de almacén de datos en la nube

- Permisos adicionales requeridos para la nube VPC compartida con la cuenta de servicio de Citrix Cloud en el proyecto de nube VPC compartida a fin de crear una unidad de alojamiento mediante la VPC y la subred del proyecto de VPC compartida:

```
compute.firewalls.list
compute.networks.list
compute.projects.get
compute.regions.list
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.use
compute.zones.list
resourcemanager.projects.get
```

Estos roles definidos por Google tienen los permisos que se indican anteriormente:

- Compute Network User
- Usuario de almacén de datos en la nube

- (Antes del cambio de la cuenta de servicio de Cloud Build): Permisos mínimos requeridos por el servicio Google Cloud Build para la cuenta de servicio de Cloud Build en el proyecto de Provisioning al descargar el disco de instrucciones de preparación en MCS:
- (Después del cambio de la cuenta de servicio de Cloud Build): Permisos mínimos requeridos por el servicio Google Cloud Compute para la cuenta de servicio de Cloud Compute en el proyecto de Provisioning al descargar el disco de instrucciones de preparación en MCS:

```
compute.disks.create
compute.disks.delete
compute.disks.get
compute.disks.list
compute.disks.setLabels
compute.disks.use
```



```
compute.disks.useReadOnly
compute.images.get
compute.images.list
compute.images.useReadOnly
compute.instances.create
compute.instances.delete
compute.instances.get
compute.instances.getSerialPortOutput
compute.instances.list
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.machineTypes.list
compute.networks.get
compute.networks.list
compute.projects.get
compute.subnetworks.list
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zones.list
iam.serviceAccounts.actAs
logging.logEntries.create
pubsub.topics.publish
resourcemanager.projects.get
source.repos.get
source.repos.list
storage.buckets.create
storage.buckets.get
storage.buckets.list
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
```

Estos roles definidos por Google tienen los permisos que se indican anteriormente:

- Cuenta de servicio de Cloud Build (después del cambio de la cuenta de servicio de Cloud Build, es una cuenta de servicio de Cloud Compute)
- Administrador de instancias de proceso
- Usuario de cuenta de servicio

- Permisos mínimos requeridos por el servicio Google Cloud Build para la cuenta de servicio de Cloud Compute en el proyecto de Provisioning al descargar el disco de instrucciones de preparación en MCS:

```
resourcemanager.projects.get
storage.objects.create
storage.objects.get
storage.objects.list
```

Estos roles definidos por Google tienen los permisos que se indican anteriormente:

  - Compute Network User
  - Storage Account User
  - Usuario de almacén de datos en la nube

- (Antes del cambio de la cuenta de servicio de Cloud Build): Permisos adicionales requeridos por el servicio Google Cloud Build para la nube VPC compartida con la cuenta de servicio de Cloud Build en el proyecto de Provisioning al descargar el disco de instrucciones de preparación en MCS:

- (Después del cambio de la cuenta de servicio de Cloud Build): Permisos adicionales requeridos por el servicio Google Cloud Compute para la nube VPC compartida con la cuenta de servicio de Cloud Compute en el proyecto de Provisioning al descargar el disco de instrucciones de preparación en MCS:

```
compute.firewalls.list
compute.networks.list
compute.subnetworks.list
compute.subnetworks.use
resourcemanager.projects.get
```

  Estos roles definidos por Google tienen los permisos que se indican anteriormente:

  - Compute Network User
  - Storage Account User
  - Usuario de almacén de datos en la nube

- Permisos adicionales requeridos para Cloud Key Management Service (KMS) con la cuenta de servicio de Citrix Cloud en el proyecto de Provisioning:

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.list
cloudkms.keyRings.get
cloudkms.keyRings.list
```

  Estos roles definidos por Google tienen los permisos que se indican anteriormente:

  - Compute KMS Viewer

Permisos generales

Estos son los permisos de la cuenta de servicio de Citrix Cloud en el proyecto Provisioning para todas las funciones disponibles en MCS. Estos permisos ofrecen la mejor compatibilidad en el futuro:

```
resourcemanager.projects.get
cloudbuild.builds.create
cloudbuild.builds.get
cloudbuild.builds.list
```



```
compute.acceleratorTypes.list
compute.diskTypes.get
compute.diskTypes.list
compute.disks.create
compute.disks.createSnapshot
compute.disks.delete
compute.disks.get
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.firewalls.create
compute.firewalls.delete
compute.firewalls.list
compute.globalOperations.get
compute.images.create
compute.images.delete
compute.images.get
compute.images.list
compute.images.setLabels
compute.images.useReadOnly
compute.instanceTemplates.create
compute.instanceTemplates.delete
compute.instanceTemplates.get
compute.instanceTemplates.list
compute.instanceTemplates.useReadOnly
compute.instances.attachDisk
compute.instances.create
compute.instances.delete
compute.instances.detachDisk
compute.instances.get
compute.instances.list
compute.instances.reset
compute.instances.resume
compute.instances.setDeletionProtection
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setTags
compute.instances.start
compute.instances.stop
compute.instances.suspend
compute.instances.update
compute.instances.updateAccessConfig
compute.instances.updateDisplayDevice
compute.instances.updateSecurity
compute.instances.updateShieldedInstanceConfig
compute.instances.updateShieldedVmConfig
compute.machineTypes.get
compute.machineTypes.list
compute.networks.list
compute.networks.updatePolicy
compute.nodeGroups.list
compute.nodeTemplates.get
compute.projects.get
```



```
compute.regions.list
compute.snapshots.create
compute.snapshots.delete
compute.snapshots.list
compute.snapshots.get
compute.snapshots.setLabels
compute.snapshots.useReadOnly
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zoneOperations.list
compute.zones.get
compute.zones.list
resourcemanager.projects.get
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.list
cloudkms.keyRings.get
cloudkms.keyRings.list
compute.disks.list
compute.instances.setServiceAccount
compute.networks.get
compute.networks.use
compute.networks.useExternalIp
iam.serviceAccounts.actAs
compute.resourcePolicies.use
```

Qué hacer a continuación

- Si está en el proceso de implementación inicial, consulte Crear catálogos de máquinas
- Para obtener información específica de Google Cloud Platform (GCP), consulte Crear un catálogo de Google Cloud Platform

Más información

- Conexiones y recursos
- Crear catálogos de máquinas

Conexión a HPE Moonshot

August 17, 2024

Crear y administrar conexiones y recursos describe los asistentes que crean una conexión. La siguiente información incluye detalles específicos sobre HPE Moonshot.

> **Nota:**
>
> Antes de crear una conexión con HPE Moonshot, debe terminar de configurar su cuenta de HPE. Consulte Entornos de virtualización de HPE Moonshot.

Crear una conexión

Puede crear una conexión a HPE Moonshot mediante:

- Web Studio
- Comandos de PowerShell

Crear una conexión mediante Web Studio

1. En la página **Agregar conexión y recursos**, seleccione **HPE Moonshot** como tipo de conexión.
2. Introduzca la dirección de conexión de su Moonshot iLO Chassis Manager. Puede usar una dirección IP, un nombre de host o un nombre de dominio completo (FQDN) para la dirección.
3. Introduzca las credenciales administrativas del chasis y un nombre de conexión descriptivo.

La configuración de la conexión se detiene cuando se produce una de las siguientes situaciones:

- Citrix Virtual Apps and Desktops recibe un certificado firmado por una entidad de certificación pública con errores: Aparece un mensaje de error. Siga las instrucciones que aparecen en la pantalla para solucionar el problema. De lo contrario, no podrá continuar con la creación de la conexión.
- Citrix Virtual Apps and Desktops recibe un certificado privado firmado por una autoridad certificadora. Aparece una página de advertencia. Compare la huella digital recibida con la del servidor para determinar la validez del certificado. Si es válido, seleccione **Confiar en el certificado** y haga clic en **Aceptar** para continuar con la creación de la conexión. A continuación, Citrix Virtual Apps and Desktops confiará en el certificado y almacenará la huella digital para su futura validación.

Crear una conexión mediante comandos de PowerShell

Al crear una conexión mediante comandos de PowerShell, proporcione la siguiente información:

- IP: Dirección IP del servidor HPE
- Username: Nombre de usuario de HPE
- Password: Contraseña de HPE

Por ejemplo:

```
New-Item -ConnectionType "Custom" -HypervisorAddress $IP -Metadata @{
 "Citrix_Orchestration_Hypervisor_Secret_Allow_Edit"="false" }
  -Path @("XDHyp:\Connections$connectionName") -Persist -PluginId "
     HPMoonshotFactory" -Scope @() -SecurePassword $Password -UserName
     $UserName -sslthumbprint $SslThumbprint New-
     BrokerHypervisorConnection -HypHypervisorConnectionUid
     $HypervisorConnectionID
```

> **Nota:**
>
> El parámetro `sslthumbprint` solo es obligatorio para los certificados firmados por una entidad de certificación privada.

Validación de certificados y huellas digitales

Para crear una conexión con **HPE Moonshot**, el certificado no debe contener errores y la huella digital debe tener un valor correcto. A continuación, se indican los casos de uso relacionados con la validación de certificados y huellas digitales:

- Certificado firmado por una entidad de certificación pública con errores. La conexión no se crea correctamente. Consulte los detalles del error y resuelva el problema.
- Certificado firmado por una entidad de certificación pública sin errores. La conexión se crea correctamente y el valor de `SslThumbprints` es **Null**.
- Certificado firmado por una entidad de certificación privada sin errores y un valor de `sslthumbprint`. La conexión se crea correctamente con un valor de `SslThumbprints` correcto.
- Certificado firmado por una entidad de certificación privada con un valor de huella digital incorrecto. La conexión no se crea correctamente.
- Certificado firmado por una entidad de certificación privada sin errores. La conexión se crea correctamente. El valor de `SSlThumbprints` es **Null** al crear la conexión. El servicio del sitio actualiza el valor de `SSlThumbprints` con un valor.

Administrar conexiones

En esta sección se detalla cómo puede administrar las conexiones:

- Solucionar problemas con los certificados mediante Web Studio
- Actualizar el valor de la huella digital mediante un comando de PowerShell

Corregir problemas de certificados

Citrix Virtual Apps and Desktops bloquea una conexión a HPE Moonshot cuando surgen problemas con los certificados, lo que le impide entregar y administrar cargas de trabajo en los nodos de HPE Moonshot asociados. Aparecerá un icono de error junto a la conexión en la lista de **conexiones de host**. Consulte la siguiente tabla para ver problemas específicos y soluciones.

Problema	Solución
Hay un error en el certificado firmado por una entidad de certificación pública	Haga clic en la conexión y seleccione la ficha **Solucionar problemas**. Consulte los detalles del error y resuelva el problema.
El certificado recibido está firmado por una entidad de certificación privada o ha caducado.	Modifique la conexión del host para actualizar la huella digital del certificado. Pasos detallados 1. Seleccione la conexión y haga clic en **Modificar conexión**. 1. En la página **Propiedades de la conexión**, haga clic en **Modificar parámetros**. 1. Introduzca la contraseña para conectarse al chasis HPE Moonshot y, a continuación, haga clic en **Guardar**. 1. En la página de **advertencia** que aparece, compare la huella digital recibida con la del servidor para comprobar la validez del certificado. 1. Si son iguales, seleccione **Confiar en el certificado** y, a continuación, haga clic en **Aceptar**.

Actualizar el valor de la huella digital

Después de crear la conexión, puede actualizar el valor de su huella digital mediante el comando `Set-Item` de PowerShell. Por ejemplo, ejecute estos comandos:

1. Obtenga los detalles de una conexión. Por ejemplo:

```
1 Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```


2. Actualice el valor de la huella digital. Por ejemplo:

```
Set-Item -LiteralPath xdhyp:\connections\SinMoonshot-101 -Username
    Administrator -SslThumbprint
   xxxxxxxxxxx12AD048480631BB7AB10D69xxxxx
```

3. Compruebe el valor actualizado de la huella digital. Por ejemplo:

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
```

> **Nota:**
>
> La actualización falla si se proporciona un valor de huella digital incorrecto en el comando `Set-Item`.

Qué hacer a continuación

- Si está en el proceso de implementación inicial, consulte Crear catálogos de máquinas
- Para obtener información específica sobre AWS, consulte Crear un catálogo de máquinas de HPE Moonshot

Más información

- Conexiones y recursos
- Crear catálogos de máquinas

Conexión con Microsoft Azure

August 17, 2024

> **Nota:**
>
> Desde julio de 2023, Microsoft cambió el nombre de Azure Active Directory (Azure AD) a Microsoft Entra ID. En este documento, cualquier referencia a Azure Active Directory, Azure AD o AAD ahora se refiere a Microsoft Entra ID.

Crear y administrar conexiones y recursos describe los asistentes que crean una conexión. La siguiente información incluye detalles específicos de los entornos de nube de Azure Resource Manager.

> **Nota:**
>
> Antes de crear una conexión con Microsoft Azure, debe terminar de configurar su cuenta de Azure

> como ubicación de recursos. Consulte Entornos en la nube de Microsoft Azure Resource Manager

Crear conexiones y entidades principales de servicio

Antes de crear conexiones, debe configurar entidades principales de servicio que las conexiones utilizan para acceder a recursos de Azure. Puede crear una conexión de dos maneras:

- Crear una entidad principal de servicio y una conexión juntos mediante Web Studio
- Crear una conexión mediante una entidad principal de servicio creada previamente

En esta sección se muestra cómo completar estas tareas:

- Crear una entidad principal de servicio y una conexión con Web Studio
- Crear una entidad principal de servicio con PowerShell
- Obtener el secreto de la aplicación en Azure
- Crear una conexión mediante una entidad principal de servicio existente

Consideraciones

- Citrix recomienda usar la entidad de servicio con rol de colaborador. Sin embargo, consulte la sección Permisos mínimos para obtener la lista de permisos mínimos correspondientes.
- 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 que tener en cuenta: "cuenta profesional o educativa"y "cuenta personal de Microsoft"Para más información, consulte CTX219211.
- Puede usar una cuenta existente de Microsoft si la agrega como miembro del directorio de suscripción. Sin embargo, puede haber complicaciones si el usuario antes tenía acceso como invitado a uno de los recursos del directorio. En ese caso, puede tener una entrada de marcador de posición en el directorio que no le concederá los permisos necesarios, y se producirá un error.

  Rectifíquelo eliminando los recursos del directorio y agregándolos 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. Por regla general, configuraciones como esta

se producen con las cuentas de directorio antiguas establecidas. Solución temporal: Agregue una cuenta al directorio, con el valor correcto de membresía.

- Los grupos de recursos son simplemente contenedores de recursos, y pueden contener recursos de regiones distintas a su propia región. Eso puede ser confuso si cree que los recursos que se muestran en la región de un grupo de recursos están disponibles.
- Su red y subred deben ser lo suficientemente grandes como para alojar la cantidad de máquinas que necesita. Eso requiere previsión, pero Microsoft le ayuda a especificar los valores correctos, con orientación sobre la capacidad del espacio de direcciones.

Crear una entidad principal de servicio y una conexión con Web Studio

> **Importante:**
>
> Esta función aún no está disponible para las suscripciones de Azure China.

Con Web Studio, puede crear una entidad principal de servicio y una conexión en un único flujo de trabajo. Las entidades principales de servicio permiten a las conexiones acceder a recursos de Azure. Al autenticarse en Azure para crear una entidad principal de servicio, se registra una aplicación en Azure. Se crea una clave secreta (denominada secreto de cliente o secreto de aplicación) para la aplicación registrada. La aplicación registrada (una conexión en este caso) usa el secreto de cliente para autenticarse en Azure AD.

Antes de empezar, asegúrese de cumplir estos requisitos previos:

- 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.
- Tiene permisos de administrador global, administrador de aplicaciones o desarrollador de aplicaciones para la autenticación. Estos permisos se pueden revocar después de crear una conexión de host. Para obtener más información sobre los roles, consulte Roles integrados de Azure AD.

Utilice el asistente **Agregar conexiones y recursos** para crear una entidad principal de servicio y una conexión juntos:

1. En la página **Conexión**, seleccione **Crear una conexión**, el tipo de conexión **Microsoft Azure** y su entorno de Azure.
2. Seleccione las herramientas a utilizar para crear las máquinas virtuales y, a continuación, seleccione **Siguiente**.
3. En la página **Detalles de conexión**, escriba su ID de suscripción de Azure y un nombre para la conexión. Después de introducir el ID de suscripción, se habilita el botón **Crear**.

> **Nota:**
>
> El nombre de la conexión puede contener de 1 a 64 caracteres, y no puede contener solo espacios en blanco ni los caracteres `\/;:#.*?=<>|[]{ } "'()'`.

4. Seleccione **Crear** e introduzca el nombre de usuario y la contraseña de la cuenta de Azure Active Directory.
5. Seleccione **Iniciar sesión**.
6. Seleccione **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 en nombre del usuario especificado.
7. Después de seleccionar **Aceptar**, volverá a la página **Conexión** del asistente.

   > **Nota:**
   >
   > Después de autenticarse correctamente en Azure, desaparecen los botones **Crear** y **Usar existente**. Aparece el texto **Conexión correcta**, con una marca de verificación verde que indica la conexión correcta a su suscripción de Azure.

8. En la página **Detalles de conexión**, seleccione **Siguiente**.

   > **Nota:**
   >
   > No puede pasar a la página siguiente hasta que se haya autenticado correctamente en Azure y haya dado su consentimiento para otorgar los permisos necesarios.

9. Configure recursos para la conexión. Los recursos constituyen la región y la red.

   - En la página **Región**, seleccione una región.
   - En la página **Red**, haga lo siguiente:
     - Escriba un nombre de recurso de 1 a 64 caracteres para identificar más fácilmente la combinación de región y red. El nombre de un recurso no puede contener solo espacios en blanco ni los caracteres `\/;:#.*?=<>|[]{ } "'()'`.
     - Seleccione un par de red virtual y grupo de recursos (si tiene más de una red virtual con el mismo nombre, emparejar un nombre de red con un grupo de recursos ofrece combinaciones únicas). Si en la página anterior seleccionó una región que no tiene redes virtuales, vuelva a esa página y seleccione una región que las tenga.

10. En la página **Resumen**, verá un resumen de los parámetros. Seleccione **Finalizar** para completar la configuración.

Ver el ID de la aplicación Después de crear una conexión, puede ver el ID de aplicación que la conexión usa para acceder a los recursos de Azure.

En la lista **Agregar conexión y recursos**, seleccione la conexión para ver los detalles. La ficha **Detalles** muestra el ID de la aplicación.

Crear una entidad principal de servicio con PowerShell

Para crear una entidad principal de servicio con PowerShell, conéctese a su suscripción de Azure Resource Manager y use los siguientes cmdlets de PowerShell que se proporcionan en las siguientes secciones.

Asegúrese de tener preparados estos elementos:

- **SubscriptionId:** `SubscriptionID` de Azure Resource Manager perteneciente a la suscripción donde quiere aprovisionar los agentes VDA.
- **ActiveDirectoryID**: ID de arrendatario de la aplicación que registró en Azure AD.
- **ApplicationName:** Nombre de la aplicación que se va a crear en Azure AD.

Estos son los pasos detallados:

Conéctese a su suscripción de Azure Resource Manager.

```
1 `Connect-AzAccount`
```

1. Seleccione la suscripción de Azure Resource Manager donde crear la entidad principal de servicio.

   ```
   Get-AzSubscription -SubscriptionId $subscriptionId | Select-
   AzSubscription
   ```

2. Cree la aplicación en su arrendatario de AD.

   ```
   $AzureADApplication = New-AzADApplication -DisplayName $ApplicationName
   ```

3. Cree una entidad principal de servicio.

   ```
   New-AzADServicePrincipal -ApplicationId $AzureADApplication.AppId
   ```

4. Asigne un rol a la entidad principal de servicio.

   ```
   New-AzRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName
    $AzureADApplication.AppId –scope /subscriptions/$SubscriptionId
   ```

5. 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.

Obtener el secreto de la aplicación en Azure

Para crear una conexión mediante una entidad principal de servicio existente, primero debe obtener el ID de la aplicación y el secreto de la entidad principal del servicio en Azure Portal.

Estos son los pasos detallados:

1. Obtenga el **ID de aplicación** en Web Studio o mediante PowerShell.
2. Inicie sesión en Azure Portal.
3. En Azure, seleccione **Azure Active Directory**.
4. En **Registros de aplicaciones**, en Azure AD, seleccione su aplicación.
5. Vaya a **Certificados y secretos**.
6. Haga clic en **Secretos del cliente**.

Crear una conexión mediante una entidad principal de servicio existente

Si ya tiene una entidad principal de servicio, puede usarla para crear una conexión mediante Web Studio.

Asegúrese de tener estos elementos listos:

- SubscriptionId
- ActiveDirectoryID (ID de arrendatario).
- ID de aplicación
- Secreto de la aplicación

  Para obtener más información, consulte Obtener el secreto de la aplicación.
- Fecha de caducidad del secreto

Estos son los pasos detallados:

En el asistente **Agregar conexión y recursos**:

1. En la página **Conexión**, seleccione **Crear una conexión**, el tipo de conexión **Microsoft Azure** y su entorno de Azure.
2. Seleccione las herramientas a utilizar para crear las máquinas virtuales y, a continuación, seleccione **Siguiente**.
3. En la página **Detalles de conexión**, escriba su ID de suscripción de Azure y un nombre para la conexión.

> **Nota:**
>
> El nombre de la conexión puede contener de 1 a 64 caracteres, y no puede contener solo espacios en blanco ni los caracteres `\/;:#.*?=<>|[]{ } "'()'`.

4. Seleccione **Usar existente**. En la ventana **Detalles de entidad principal de servicio existente**, introduzca estos parámetros para la entidad principal de servicio existente. Después de introducir la información, se habilitará el botón **Guardar**. Seleccione **Guardar**. No puede avanzar más allá de esta página hasta que haya proporcionado detalles válidos.

   - **ID de suscripción**. Introduzca el ID de su suscripción de Azure. Para obtener su ID de suscripción, inicie sesión en Azure Portal y vaya a **Suscripciones > Vista general**.
   - **ID de Active Directory** (ID de arrendatario). Escriba el ID del directorio (arrendatario) de la aplicación con la que se registró en Azure AD.
   - **ID de la aplicación**. Escriba el ID de la aplicación (cliente) con la que se registró en Azure AD.
   - **Secreto de la aplicación**. Cree una clave secreta (secreto de cliente). La aplicación registrada utiliza la clave para autenticarse en Azure AD. Le recomendamos cambiar las claves con frecuencia por motivos de seguridad. Asegúrese de guardar la clave porque no podrá recuperarla más tarde.
   - **Fecha de caducidad del secreto**. Introduzca la fecha en la cual caduca el secreto de la aplicación. Recibirá una alerta en la consola antes de que caduque la clave secreta. Sin embargo, si la clave secreta caduca, recibirá errores.

     > **Nota:**
     >
     > Por motivos de seguridad, el período de caducidad no puede ser superior a dos años a partir de ahora.

   - **URL de autenticación**. Este campo se rellena automáticamente y no se puede modificar.
   - **URL de administración**. Este campo se rellena automáticamente y no se puede modificar.
   - **Sufijo de almacenamiento**. Este campo se rellena automáticamente y no se puede modificar.

     Se requiere acceso a los siguientes dispositivos de punto final para crear un catálogo de MCS en Azure. El acceso a estos dispositivos de punto final optimiza la conectividad entre la red local y Azure Portal y sus servicios.

     - URL de autenticación: https://login.microsoftonline.com/
     - URL de administración: https://management.azure.com/ Esta es una URL de solicitud para las API del proveedor de Azure Resource Manager. El dispositivo de punto final

para la administración depende del entorno. Por ejemplo: para Azure Global es https://management.azure.com/ y, para Azure US Government, https://management.usgovcloudapi.net/.
- Sufijo de almacenamiento: https://*.core.windows.net./ Este (*) es un carácter comodín para el sufijo de almacenamiento. Por ejemplo, `https://demo.table.core.windows.net/`.

5. Tras seleccionar **Guardar**, volverá a la página **Detalles de conexión**. Seleccione **Siguiente** para pasar a la siguiente página.
6. Configure recursos para la conexión. Los recursos constituyen la región y la red.
   - En la página **Región**, seleccione una región.
   - En la página **Red**, haga lo siguiente:
     - Escriba un nombre de recurso de 1 a 64 caracteres para identificar más fácilmente la combinación de región y red. El nombre de un recurso no puede contener solo espacios en blanco ni los caracteres `\/;:#.*?=<>|[]{ } "'()'`.
     - Seleccione un par de red virtual y grupo de recursos (si tiene más de una red virtual con el mismo nombre, emparejar un nombre de red con un grupo de recursos ofrece combinaciones únicas). Si en la página anterior seleccionó una región que no tiene redes virtuales, vuelva a esa página y seleccione una región que las tenga.
7. En la página **Resumen**, verá un resumen de los parámetros. Seleccione **Finalizar** para completar la configuración.

Administrar entidades principales de servicio y conexiones

En esta sección se detalla cómo puede administrar entidades principales de servicio y conexiones:

- Configurar parámetros de limitación de Azure
- Habilitar el uso compartido de imágenes en Azure
- Agregar arrendatarios compartidos a una conexión mediante la Configuración completa
- Implementar el uso compartido de imágenes con PowerShell
- Administrar el secreto de aplicación y la fecha de caducidad del secreto

Configurar parámetros de limitación de Azure

Azure Resource Manager limita las solicitudes de suscripciones y arrendatarios mediante la redirección del tráfico en función de límites definidos y adaptada a las necesidades específicas del proveedor. Consulte Limitación de solicitudes de Resource Manager en el sitio de Microsoft para obtener más información. Existen límites para las suscripciones y los arrendatarios, donde administrar muchas

máquinas podría resultar problemático. Por ejemplo: es posible que una suscripción que contenga muchas máquinas sufra problemas de rendimiento relacionados con las operaciones de energía.

> **Sugerencia:**
>
> Para obtener más información, consulte Mejora del rendimiento de Azure con Machine Creation Services.

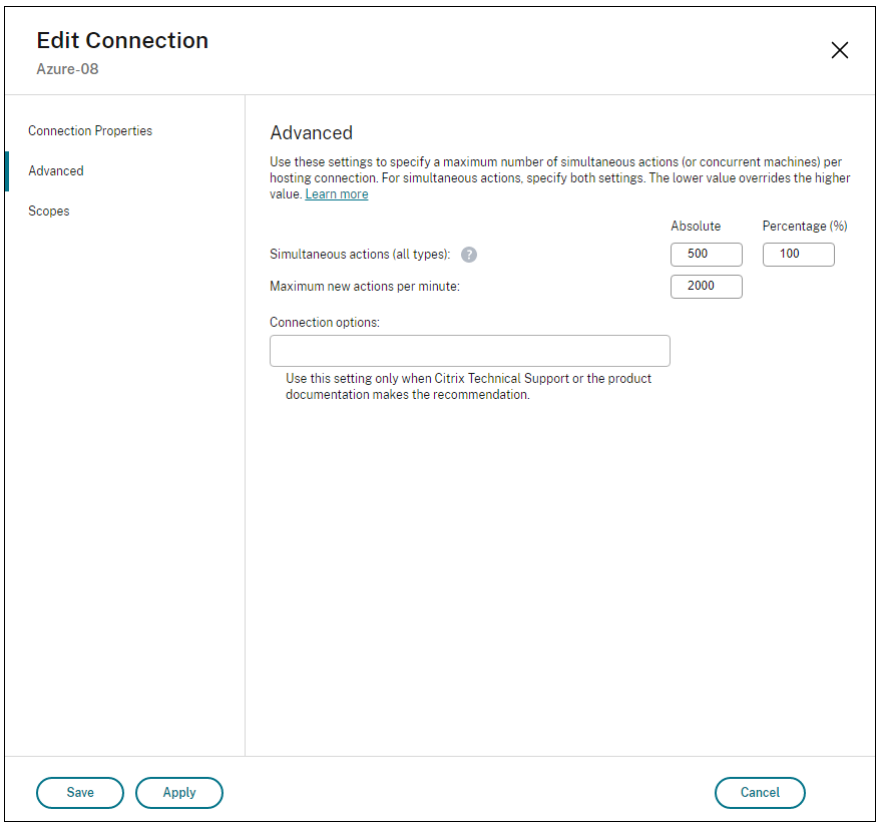
Para ayudar a mitigar estos problemas, puede quitar la limitación interna de MCS para usar más cuota de solicitudes disponible de Azure.

Le recomendamos la siguiente configuración óptima al encender o apagar máquinas virtuales en suscripciones grandes, como, por ejemplo, aquellas que contengan 1000 máquinas virtuales:

- Operaciones simultáneas absolutas: 500
- Máximo de nuevas operaciones por minuto: 2000
- Máximo de operaciones simultáneas: 500

Use Web Studio en la configuración de operaciones de Azure para una conexión de Azure determinada:

1. En Web Studio, seleccione **Alojamiento** en el panel de la izquierda.
2. Seleccione la conexión.
3. En el asistente **Modificar conexión**, seleccione **Avanzado**.
4. En la página **Avanzado**, utilice las opciones de configuración para especificar la cantidad de acciones simultáneas y el máximo de acciones nuevas por minuto y las opciones de conexión adicionales.



MCS admite un máximo de 500 operaciones simultáneas de forma predeterminada. De forma alternativa, puede utilizar el SDK de PowerShell remoto para establecer el máximo de operaciones simultáneas.

Utilice la propiedad de **PowerShell** `MaximumConcurrentProvisioningOperations` para especificar el máximo de operaciones simultáneas de aprovisionamiento de Azure. Al usar esta propiedad, tenga en cuenta lo siguiente:

- El valor predeterminado de `MaximumConcurrentProvisioningOperations` es 500.
- Configure el parámetro `MaximumConcurrentProvisioningOperations` mediante el comando `Set-item` de PowerShell.

Habilitar el uso compartido de imágenes en Azure

Al crear o actualizar catálogos de máquinas, puede seleccionar imágenes compartidas de diferentes suscripciones y arrendatarios de Azure (compartidas a través de Azure Compute Gallery). Para habilitar el uso compartido de imágenes con o entre arrendatarios, debe hacer los ajustes necesarios en Azure:

- Compartir imágenes con un arrendatario (entre suscripciones)
- Compartir imágenes entre arrendatarios

Compartir imágenes con un arrendatario (entre suscripciones) Para seleccionar una imagen de Azure Compute Gallery que pertenezca a una suscripción diferente, la imagen debe compartirse con la entidad principal de servicio (SPN) de esa suscripción.

Por ejemplo: si hay una entidad principal de servicio (SPN 1) que está configurada en Studio como:

Entidad principal de servicio: SPN 1

Suscripción: suscripción 1

Arrendatario: arrendatario 1

La imagen está en una suscripción diferente, que está configurada en Studio como:

Suscripción: suscripción 2

Arrendatario: arrendatario 1

Si quiere compartir la imagen de la suscripción 2 con la suscripción 1 (SPN 1), vaya a la suscripción 2 y comparta el grupo de recursos con SPN 1.

La imagen debe compartirse con otro SPN mediante control de acceso por roles (RBAC) de Azure. Azure RBAC es el sistema de autorización que se utiliza para administrar el acceso a los recursos de Azure. Para obtener más información sobre Azure RBAC, consulte el documento de Microsoft What is Azure role-based access control (Azure RBAC). Para conceder acceso, asigne roles a las entidades principales de servicio en el ámbito del grupo de recursos con el rol Colaborador. Para asignar roles de Azure, debe tener el permiso `Microsoft.Authorization/roleAssignments/write`, como administrador de acceso de usuario o propietario. Para obtener más información sobre cómo compartir imágenes con otro SPN, consulte el documento de Microsoft Assign Azure roles using the Azure portal.

Para obtener información sobre los comandos de PowerShell al seleccionar una imagen de una suscripción diferente, consulte Seleccionar una imagen de una suscripción diferente.

Compartir imágenes entre arrendatarios Para compartir imágenes entre arrendatarios con Azure Compute Gallery, cree un registro de aplicaciones.

Por ejemplo, si hay dos arrendatarios (arrendatario 1 y arrendatario 2) y quiere compartir su galería de imágenes con el arrendatario 1, entonces:

1. Cree un registro de aplicaciones para el arrendatario 1. Para obtener más información, consulte Create the app registration.
2. Permita que el arrendatario 2 acceda a la aplicación mediante una solicitud de inicio de sesión con explorador web. Sustituya `Tenant2 ID` por el ID del arrendatario 1. Sustituya `Application (client)ID` por el ID de la aplicación del registro de aplicaciones que creó. Cuando haya terminado con las sustituciones, pegue la URL en un explorador web y siga las instrucciones de inicio de sesión para iniciar sesión en el arrendatario 2. Por ejemplo:


```
https://login.microsoftonline.com/<Tenant 2 ID>/oauth2/authorize?
    client_id=<Application (client) ID>&response_type=code&
    redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F
```

Para obtener más información, consulte Give Tenant 2 access.

3. Permita a la aplicación acceder al grupo de recursos del arrendatario 2. Inicie sesión como el arrendatario 2 y otorgue acceso al registro de aplicaciones para el grupo de recursos que contiene la imagen de la galería. Para obtener más información, consulte Authenticate requests across tenants.

Para crear un catálogo con una imagen de un arrendatario diferente con comandos de PowerShell:

1. Actualice las propiedades personalizadas de la conexión de host con identificadores de arrendatarios compartidos.
2. Seleccione una imagen de otro arrendatario.

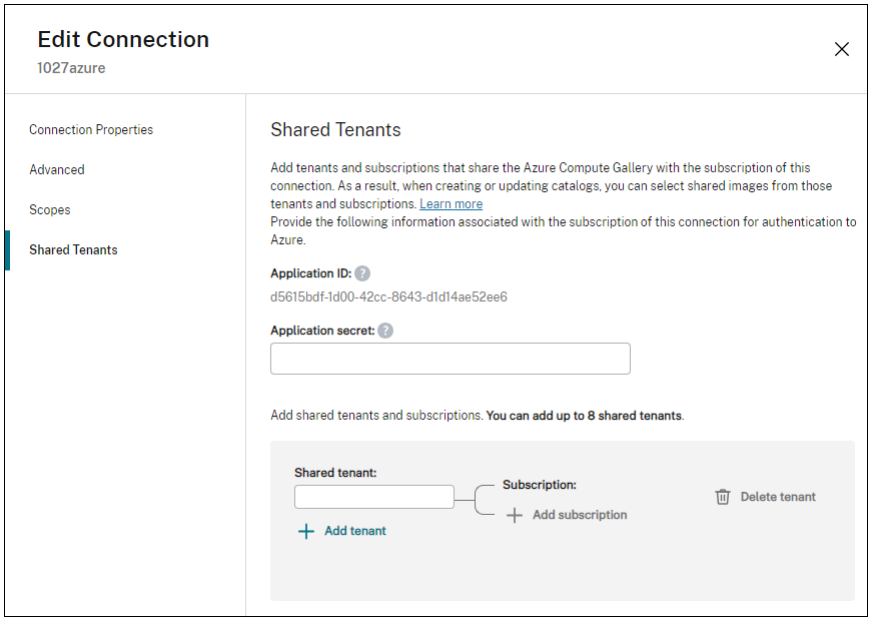
Agregar arrendatarios compartidos a una conexión mediante la Configuración completa

Al crear o actualizar catálogos de máquinas en Web Studio, puede seleccionar imágenes compartidas de diferentes suscripciones y arrendatarios de Azure (compartidas a través de Azure Compute Gallery). La función requiere que proporcione información compartida sobre la suscripción y los arrendatarios compartidos para las conexiones de host asociadas.

> **Nota:**
>
> Asegúrese de haber configurado los ajustes necesarios en Azure para permitir el uso compartido de imágenes entre arrendatarios. Para obtener más información, consulte Compartir imágenes entre arrendatarios.

Complete estos pasos para establecer una conexión:

1. En Web Studio, seleccione **Alojamiento** en el panel de la izquierda.
2. Seleccione la conexión y, a continuación, seleccione **Modificar conexión** en la barra de acciones.



3. En **Shared Tenants**, haga lo siguiente:
    - Proporcione el ID de la aplicación y el secreto de la aplicación asociados a la suscripción de la conexión. Citrix Virtual Apps and Desktops usa esta información para autenticarse en Azure AD.
    - Agregue arrendatarios y suscripciones que compartan Azure Compute Gallery con la suscripción de la conexión. Puede agregar hasta 8 arrendatarios compartidos y 8 suscripciones por cada arrendatario.
4. Cuando haya terminado, seleccione **Aplicar** para aplicar los cambios que haya hecho y deje la ventana abierta, o bien seleccione **Aceptar** para aplicar los cambios y cierre la ventana.

Implementar el uso compartido de imágenes con PowerShell

Esta sección le guiará a través de los procesos para compartir imágenes con PowerShell:

- Seleccionar una imagen de una suscripción diferente
- Actualizar las propiedades personalizadas de la conexión de host con identificadores de arrendatarios compartidos
- Seleccionar una imagen de otro arrendatario

Seleccionar una imagen de una suscripción diferente Puede seleccionar una imagen en Azure Compute Gallery que pertenezca a una suscripción compartida diferente del mismo arrendatario de Azure para crear y actualizar catálogos de MCS mediante los comandos de PowerShell.

1. En la carpeta raíz de la unidad de alojamiento, Citrix crea una nueva carpeta de suscripción compartida llamada `sharedsubscription`.

2. Enumere todas las suscripciones compartidas de un arrendatario.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\sharedsubscription.
    folder"
```

3. Seleccione una suscripción compartida y, a continuación, enumere todos los grupos de recursos compartidos de esa suscripción compartida.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription"
```

4. Seleccione un grupo de recursos y, a continuación, enumere todas las galerías de ese grupo de recursos.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription\ xyz.resourcegroup"
```

5. Seleccione una galería y, a continuación, enumere todas las definiciones de imágenes de esa galería.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription\xyz.resourcegroup\testgallery.gallery"
```

6. Seleccione una definición de imagen y, a continuación, enumere todas las versiones de imagen de esa definición de imagen.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription\xyz.resourcegroup\sigtestdef.
    imagedefinition"
```

7. Cree y actualice un catálogo de MCS con los siguientes elementos:

   - Resource group
   - Galería
   - Definición de imagen de la galería
   - Versión de la imagen de la galería

   Para obtener información sobre cómo crear un catálogo con el SDK de PowerShell remoto, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Actualizar las propiedades personalizadas de la conexión de host con identificadores de arrendatarios compartidos Use `Set-Item` para actualizar las propiedades personalizadas de la conexión de host con un ID de arrendatario y un ID de suscripción compartidos. Agregue una propiedad `SharedTenants` en `CustomProperties`. El formato de `Shared Tenants` es:

```
[{
```



```
 "Tenant":"94367291-119e-457c-bc10-25337231f7bd","Subscriptions":["7
    bb42f40-8d7f-4230-a920-be2781f6d5d9"] }
,{
"Tenant":"50e83564-c4e5-4209-b43d-815c45659564","Subscriptions":["06
    ab8944-6a88-47ee-a975-43dd491a37d0"] }
]
```

Por ejemplo:

```
Set-Item -CustomProperties "<CustomProperties xmlns=`"http://schemas.
    citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org
    /2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`" Value=`"
    123`" />
<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`" Value
    =`"https://management.azure.com/`" />
<Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
    Value=`"https://login.microsoftonline.com/`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`" Value=`"
    core.windows.net`" />
<Property xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"123abc`
    " />
<Property xsi:type=`"StringProperty`" Name=`"SharedTenants`" Value=`"`[
     {
  'Tenant':'123abc', 'Subscriptions':['345', '567']  }
  ]`"` />
</CustomProperties>"
-LiteralPath @("XDHyp:\Connections\aazure") -PassThru -UserName "
    advc345" -SecurePassword
$psd
```

> **Nota:**
>
> Puede agregar más de un arrendatario. Cada arrendatario puede tener más de una suscripción.

Seleccionar una imagen de otro arrendatario Puede seleccionar una imagen en Azure Compute Gallery que pertenezca a otro arrendatario de Azure para crear y actualizar catálogos de MCS mediante comandos de PowerShell.

1. En la carpeta raíz de la unidad de alojamiento, Citrix crea una nueva carpeta de suscripción compartida llamada `sharedsubscription`.
2. Enumere todas las suscripciones compartidas.

   ```
   Get-ChildItem XDHyp:\HostingUnits\azres\sharedsubscription.folder
   ```

3. Seleccione una suscripción compartida y, a continuación, enumere todos los grupos de recursos compartidos de esa suscripción compartida.

   ```
   Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
       sharedsubscription
   ```


4. Seleccione un grupo de recursos y, a continuación, enumere todas las galerías de ese grupo de recursos.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\ xyz.resourcegroup
```

5. Seleccione una galería y, a continuación, enumere todas las definiciones de imágenes de esa galería.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\xyz.resourcegroup\efg.gallery
```

6. Seleccione una definición de imagen y, a continuación, enumere todas las versiones de imagen de esa definición de imagen.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
    sharedsubscription\xyz.resourcegroup\efg.gallery\hij.
    imagedefinition
```

7. Cree y actualice un catálogo de MCS con los siguientes elementos:

   - Resource group
   - Galería
   - Definición de imagen de la galería
   - Versión de la imagen de la galería

   Para obtener información sobre cómo crear un catálogo con el SDK de PowerShell remoto, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Administrar el secreto de aplicación y la fecha de caducidad del secreto

Asegúrese de cambiar el secreto de aplicación para una conexión antes de que caduque. Recibirá una alerta en Web Studio antes de que caduque la clave secreta.

Crear un secreto de aplicación en Azure Puede crear un secreto de aplicación para una conexión a través de Azure Portal.

1. Seleccione **Azure Active Directory**.
2. En **Registros de aplicaciones**, en Azure AD, seleccione su aplicación.
3. Vaya a **Certificados y secretos**.
4. Haga clic en **Secretos de cliente > Nuevo secreto de cliente**.

5. Proporcione una descripción del secreto y especifique una duración. Cuando haya terminado, seleccione **Agregar**.

   > **Nota:**
   >
   > Guarde el secreto de cliente porque no podrá recuperarlo más tarde.

6. Copie el valor del secreto del cliente y la fecha de caducidad.
7. En la interfaz de Web Studio, modifique la conexión correspondiente y sustituya el contenido de los campos **Secreto de la aplicación** y **Fecha de caducidad del secreto** por los valores copiados.

Cambiar la fecha de caducidad del secreto Puede usar Web Studio para agregar o modificar la fecha de caducidad del secreto de la aplicación en uso.

1. En el asistente **Agregar conexión y recursos**, haga clic con el botón secundario en una conexión y haga clic en **Modificar conexión**.
2. En la página **Propiedades de conexión**, haga clic en **Fecha de caducidad del secreto** para agregar o modificar la fecha de caducidad del secreto de la aplicación en uso.

Permisos de Azure requeridos

Esta sección contiene los permisos mínimos y generales requeridos para Azure.

Permisos mínimos

Los permisos mínimos ofrecen un mejor control de la seguridad. Sin embargo, es posible que las nuevas funciones que requieren permisos adicionales fallen porque solo se usan permisos mínimos.

Crear una conexión de host Agregue una nueva conexión de host con la información obtenida de Azure.

```
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/disks/read",
"Microsoft.Resources/providers/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Resources/tenants/read"
```


Administración de energía de las máquinas virtuales Encienda o apague las instancias de máquina.

```
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/restart/action",
"Microsoft.Insights/diagnosticsettings/delete",
"Microsoft.Insights/diagnosticsettings/read",
"Microsoft.Insights/diagnosticsettings/write",
```

Creación, actualización o eliminación de máquinas virtuales Cree un catálogo de máquinas y, a continuación, agregue, elimine y actualice máquinas, y elimine el catálogo de máquinas.

A continuación, se muestra la lista de permisos mínimos requeridos cuando la imagen maestra es un disco administrado o las instantáneas se encuentran en la misma región que la conexión de host.

```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/tags/read",
"Microsoft.Resources/tags/write",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/snapshots/read",
"Microsoft.Compute/snapshots/write",
"Microsoft.Compute/snapshots/delete",
"Microsoft.Compute/snapshots/beginGetAccess/action",
"Microsoft.Compute/snapshots/endGetAccess/action",
"Microsoft.Compute/disks/read",
"Microsoft.Compute/disks/write",
"Microsoft.Compute/disks/delete",
"Microsoft.Compute/disks/beginGetAccess/action",
"Microsoft.Compute/disks/endGetAccess/action",
"Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
   read",
"Microsoft.Compute/skus/read",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Features/providers/features/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
```



```
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/locations/usages/read",
```

Necesita los siguientes permisos adicionales, en función de los permisos mínimos, para las siguientes funciones:

- Si la imagen maestra es un disco duro virtual de una cuenta de almacenamiento ubicada en la misma región que la conexión de host:

```
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/listKeys/action",
```

- Si la imagen maestra es una versión de imagen de Shared Image Gallery:

```
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/read",
```

- Si la imagen maestra es un disco administrado, las instantáneas o los VHD que se encuentran en una región diferente de la región de la conexión de host:

```
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/locations/usages/read",
"Microsoft.Storage/skus/read",
```

- Si usa un grupo de recursos administrado por Citrix:

```
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
```

- Si coloca la imagen maestra en Azure Compute Gallery (anteriormente, Shared Image Gallery) en un arrendatario o en una suscripción compartidos:

```
"Microsoft.Compute/galleries/write",
"Microsoft.Compute/galleries/images/write",
"Microsoft.Compute/galleries/images/versions/write",
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/read",
"Microsoft.Compute/galleries/delete",
"Microsoft.Compute/galleries/images/delete",
"Microsoft.Compute/galleries/images/versions/delete",
"Microsoft.Resources/subscriptions/read",
```

- Si usa compatibilidad con hosts dedicados de Azure:


```
"Microsoft.Compute/hostGroups/read",
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/hostGroups/hosts/read",
```

- Si utiliza cifrado del lado del servidor (SSE) con claves administradas por el cliente (CMK):

```
"Microsoft.Compute/diskEncryptionSets/read",
```

- Si implementa máquinas virtuales mediante plantillas ARM (perfil de máquina):

```
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/deployments/operationstatuses/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/delete",
"Microsoft.Insights/DataCollectionRuleAssociations/Read",
"Microsoft.Insights/dataCollectionRules/read",
```

- Si usa la especificación de plantilla de Azure como perfil de máquina:

```
"Microsoft.Resources/templateSpecs/read",
"Microsoft.Resources/templateSpecs/versions/read",
```

Crear, actualizar y eliminar máquinas con discos no administrados A continuación, se muestra la lista de permisos mínimos requeridos cuando la imagen maestra es un disco duro virtual (VHD) y se utiliza el grupo de recursos proporcionado por el administrador:

```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/tags/read",
"Microsoft.Resources/tags/write",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/locations/usages/read",
"Microsoft.Storage/skus/read",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
```



```
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/locations/usages/read",
```

Permiso general

El rol de colaborador tiene pleno acceso para administrar todos los recursos. Este conjunto de permisos no le impide obtener nuevas funcionalidades.

El siguiente conjunto de permisos proporciona la mejor compatibilidad de cara al futuro, aunque incluye más permisos de los necesarios con el conjunto de funciones actual:

```
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/disks/beginGetAccess/action",
"Microsoft.Compute/disks/delete",
"Microsoft.Compute/disks/endGetAccess/action",
"Microsoft.Compute/disks/read",
"Microsoft.Compute/disks/write",
"Microsoft.Compute/galleries/delete",
"Microsoft.Compute/galleries/images/delete",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/delete",
"Microsoft.Compute/galleries/images/versions/read",
"Microsoft.Compute/galleries/images/versions/write",
"Microsoft.Compute/galleries/images/write",
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/write",
"Microsoft.Compute/hostGroups/hosts/read",
"Microsoft.Compute/hostGroups/read",
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/snapshots/beginGetAccess/action",
"Microsoft.Compute/snapshots/delete",
"Microsoft.Compute/snapshots/endGetAccess/action",
"Microsoft.Compute/snapshots/read",
"Microsoft.Compute/snapshots/write",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/restart/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
   read",
"Microsoft.Compute/skus/read",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
```



```
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/locations/usages/read",
"Microsoft.Resources/deployments/operationstatuses/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/deployments/delete",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
"Microsoft.Resources/providers/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Resources/subscriptions/read",
"Microsoft.Resources/tags/read",
"Microsoft.Resources/tags/write",
"Microsoft.Resources/tenants/read",
"Microsoft.Resources/templateSpecs/read",
"Microsoft.Resources/templateSpecs/versions/read",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/locations/usages/read",
"Microsoft.Storage/skus/read",
"Microsoft.Features/providers/features/read",
"Microsoft.Insights/DataCollectionRuleAssociations/Read",
"Microsoft.Insights/dataCollectionRules/read",
"Microsoft.Insights/diagnosticsettings/delete",
"Microsoft.Insights/diagnosticsettings/read",
"Microsoft.Insights/diagnosticsettings/write",
```

Validar permisos en la conexión de host

Puede validar los permisos en una conexión de host para realizar tareas relacionadas con la creación y la administración de catálogos de máquinas de MCS. Esta implementación le ayuda a conocer con antelación los permisos ausentes necesarios para diferentes situaciones, como la creación, la eliminación y la actualización de máquinas virtuales, y la administración de energía de las máquinas virtuales, para evitar el bloqueo en momentos críticos.

Puede validar los permisos de una conexión de host mediante el comando `Test-HypHypervisorConnectior` de PowerShell. El resultado del comando se captura como una lista en la que cada elemento de la lista se divide en tres secciones.

- Categoría: La acción o tarea que un usuario puede realizar para crear y administrar un catálogo

de máquinas de MCS.
- Acción correctiva: El paso que debe seguir un administrador para resolver la discrepancia de permisos ausentes de un usuario.
- Permiso que falta: La lista de permisos ausentes para una categoría.

Para validar los permisos, haga lo siguiente:

1. Cree una conexión de host con Azure.
2. Abra una ventana de PowerShell desde el host del Delivery Controller.
3. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
4. Ejecute el siguiente comando para verificar si tiene los permisos necesarios para probar una conexión.

```
Test-HypHypervisorConnection -LiteralPath "XDHyp:\Connections\
    AzureCon"
```

Se requiere permiso de nivel de rol para el SPN:

- Microsoft.Authorization/roleDefinitions/read (a nivel de suscripción o a nivel de grupo de recursos si se proporciona un grupo de recursos)
- Microsoft.Authorization/roleAssignments/read (a nivel de suscripción o a nivel de grupo de recursos si se proporciona un grupo de recursos)

Permisos de nivel de API necesarios para el SPN:

Microsoft.Graph:

- Application.Read.All
- Directory.Read.All
- ServicePrincipalEndpoint.Read.All

5. Después de agregar los permisos ausentes necesarios para buscar los permisos, ejecute el siguiente comando para verificar si tiene permisos en las distintas categorías.

   Ejemplo:

   Para probar una conexión a nivel de suscripción con un nivel de autorización más alto:

```
Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\
    AzureCon -SecurePassword $password -UserName 922e65d5-38ae-4cf5
    -xxxx-xxxxxxxxx
```

   Ejemplo:

   Para probar una conexión a nivel de grupo de recursos sin un nivel alto de autorización:

```
Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\
    testles -CustomProperties $customProperties | Format-List
```


> **Nota:**
>
> El parámetro CustomProperties se usa para proporcionar el nivel de grupo de recursos, puesto que el grupo de recursos es una información específica de la conexión.

Ejemplo:

Para probar una conexión con el nivel más alto de autorización a nivel de grupo de recursos:

```
Test-HypHypervisorConnection -LiteralPath XDHyp:\Connections\
    testles -SecurePassword $password -UserName 922e65d5-38ae-4cf5
    -832b-54122196b7dd -CustomProperties $customProperties
```

Para obtener información sobre los permisos, consulte Permisos de Azure requeridos.

Qué hacer a continuación

- Si está en el proceso de implementación inicial, consulte Crear catálogos de máquinas
- Para obtener información específica de Azure, consulte Crear un catálogo de Microsoft Azure

Más información

- Conexiones y recursos
- Crear catálogos de máquinas

Conexión con Microsoft System Center Virtual Machine Manager

August 17, 2024

Crear y administrar conexiones y recursos describe los asistentes que crean una conexión. La siguiente información incluye detalles específicos de Microsoft System Center Virtual Machine Manager (VMM).

> **Nota:**
>
> Antes de crear una conexión con VMM, debe terminar de configurar su cuenta de VMM como ubicación de recursos. Consulte Entornos de virtualización de Microsoft System Center Virtual Machine Manager.

Crear una conexión

Si utiliza MCS para aprovisionar las VM, haga esto en el asistente de creación de conexiones:

- Escriba la dirección como el nombre de dominio completo del servidor host.
- Introduzca las credenciales de la cuenta del administrador que configuró. Esa cuenta debe tener permisos para crear nuevas máquinas virtuales.
- En el cuadro de diálogo Detalles del host, seleccione el clúster o el host independiente a utilizar para crear las VM.

  > **Importante**
  >
  > Busque un clúster o un host independiente aunque utilice una implementación de host de Hyper-V único.

Qué hacer a continuación

- Si está en el proceso de implementación inicial, consulte Crear catálogos de máquinas
- Para crear catálogos de máquinas con MCS en un recurso compartido de archivos de SMB 3, consulte Crear un catálogo de Microsoft System Center Virtual Machine Manager

Más información

- Conexiones y recursos
- Crear catálogos de máquinas

Conexión con Nutanix

August 17, 2024

Crear y administrar conexiones y recursos describe los asistentes que crean una conexión. La siguiente información incluye detalles específicos sobre Nutanix.

> **Nota:**
>
> Antes de crear una conexión con Nutanix, debe terminar de configurar su cuenta de Nutanix como ubicación de recursos. Consulte Entornos de virtualización de Nutanix.

Crear una conexión con Nutanix

La información siguiente es un complemento de las instrucciones que aparecen en Conexiones y recursos. Para crear una conexión Nutanix, siga las instrucciones generales de ese artículo, teniendo en cuenta los detalles específicos de Nutanix.

En el asistente **Agregar conexión y recursos**, seleccione el tipo de conexión Nutanix en la página **Conexión** y luego especifique la dirección y las credenciales, además de un nombre para la conexión. En la página **Red**, seleccione una red para la unidad de alojamiento.

Es posible seleccionar los siguientes tipos de conexión: **Nutanix AHV**, **Nutanix AHV Xi** y **Nutanix AHV PC**.

- Para **Nutanix AHV**, especifique la dirección y las credenciales del clúster de Prism Element (PE).
- Para **Nutanix AHV PC**, especifique la dirección y las credenciales de Prism Central (PC).

  > **Nota:**
  >
  > Actualmente, el tipo de conexión Nutanix AHV PC solo se usa para crear una conexión a Nutanix Cloud Cluster (NC2) en Azure. Además, un catálogo de máquinas solo se puede hospedar en un solo clúster en una conexión de NC2 en Azure.

- Para **Nutanix AHV DRaaS**, especifique la dirección y el nombre de usuario del arrendatario de DRaaS. Importe sus archivos de credenciales de Nutanix DRaaS públicos y privados (`.pem`).

> **Sugerencia:**
>
> Si implementa máquinas que utilizan Nutanix AHV (Prism Element) como recurso, seleccione el contenedor en el que reside el disco de la VM.

Qué hacer a continuación

- Si está en el proceso de implementación inicial, consulte Crear catálogos de máquinas
- Para obtener información específica de Nutanix, consulte Crear un catálogo de Nutanix

Más información

- Conexiones y recursos
- Crear catálogos de máquinas

Conexión con soluciones de Nutanix Cloud y de partners

August 17, 2024

Crear y administrar conexiones y recursos describe los asistentes que crean una conexión. La siguiente información incluye detalles específicos de las soluciones de Nutanix Cloud y de partners.

Citrix Virtual Apps and Desktops admite estas soluciones de Nutanix Cloud y de partners:

- Nutanix Cloud Clusters en AWS

> **Nota:**
>
> Antes de crear una conexión con una solución de Nutanix Cloud y de partners, debe terminar de configurar su cuenta correspondiente como ubicación de recursos. Consulte Soluciones de Nutanix Cloud y de partners.

Conectarse a Nutanix Prism

Después de crear un clúster de Nutanix, conéctese a Nutanix Prism.

Para conectarse a Nutanix Prism:

1. Cree una máquina virtual bastión en la subred 10.0.129.0/24.
2. Conéctese por RDP a la VM bastión, vaya a la URL de **Prism Element** que copió en la sección anterior.
3. Inicie sesión con las credenciales predeterminadas: `admin`:`nutanix`/`4u`. Recuerde cambiar la contraseña.

Crear una VM en el clúster de Nutanix

Después de conectarse a **Nutanix Prism**, cree máquinas virtuales en el clúster de Nutanix.

Si la VM necesita acceder a Internet

1. Vaya a la consola de AWS.
2. Cree otra subred 10.0.130.0/24 en la misma VPC que la creada por Nutanix CFS.
3. Agregue una ruta a la tabla de rutas de esta subred para dirigir todo el tráfico que no sea local a la puerta de enlace NAT mencionada.
4. Conéctese por RDP a la VM bastión, vaya a la URL de **Prism Element** que copió en la sección anterior e inicie sesión.

5. Agregue una nueva red. Vaya a **Parámetros > Configuración de red > Crear subred**. Use la misma subred 10.0.130.0/24 que se usa en AWS.
6. Cree todas las máquinas virtuales (AD, CC, VDA, etc.) en esa nueva subred.

Si la VM no necesita acceder a Internet

1. Conéctese por RDP a la VM bastión, vaya a la URL de **Prism Element** que copió en la sección anterior e inicie sesión.
2. Agregue una nueva red. Vaya a **Parámetros > Configuración de red > Crear subred**. Use la subred 10.0.129.0/24.
3. Cree todas las máquinas virtuales (AD, CC, VDA, etc.) en esa subred.

> **Sugerencia:**
>
> Asegúrese de que la información sobre la hora y la zona horaria de las VM esté configurada correctamente. Sobre todo para AD.

Crear una conexión de host

1. Inicie Web Studio.
2. Seleccione el nodo de alojamiento y haga clic en **Agregar conexión y recursos**.
3. En la pantalla **Conexión**, seleccione **Crear una conexión** y, en la **Dirección de la conexión**, introduzca `https://xxx.xxx.xxx.xxx:9440`.
4. Siga las instrucciones de la interfaz de usuario para completar el asistente.

> **Nota:**
>
> Para ver la opción de Nutanix en Web Studio, todas las VM de conectores deben tener instalado el plug-in de Nutanix, aunque no se usen en la zona de Nutanix.

Qué hacer a continuación

- Si está en el proceso de implementación inicial, consulte Crear catálogos de máquinas
- Para obtener información específica de Nutanix, consulte Crear un catálogo de Nutanix

Más información

- Conexiones y recursos
- Crear catálogos de máquinas

Conexión con VMware

August 17, 2024

Crear y administrar conexiones y recursos describe los asistentes que crean una conexión. La siguiente información incluye detalles específicos de los entornos de virtualización de VMware.

> **Nota:**
>
> Antes de crear una conexión con VMware, debe terminar de configurar su cuenta de VMware como ubicación de recursos. Consulte Entornos de virtualización de VMware.

Crear una conexión

En el asistente para la creación de conexiones:

1. Seleccione el tipo de conexión VMware.
2. Especifique la dirección del punto de acceso para el SDK de vCenter.
3. Especifique las credenciales de la cuenta de usuario VMware que ha configurado y que incluye permisos para crear máquinas virtuales. Especifique el nombre de usuario en el formato dominio/nombre_de_usuario.

Huella digital SSL de VMware

La funcionalidad de la huella digital SSL de VMware elimina la necesidad de crear manualmente una conexión de host a un hipervisor de VMware vSphere. Ahora ya no es necesario crear manualmente una relación de confianza entre los Delivery Controllers del sitio y el certificado del hipervisor antes de crear una conexión.

La funcionalidad de huella digital SSL de VMware almacena la huella digital del certificado que no es de confianza en la base de datos del sitio. Esta configuración garantiza que Citrix Virtual Apps and Desktops pueda identificar continuamente el hipervisor como de confianza, incluso aunque los Controllers no lo hagan.

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.

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, asócielos 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
Sistema. 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
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
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

SDK	Interfaz de usuario
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:

> **Nota:**
>
> Estos permisos son necesarios para crear catálogos de máquinas de MCS con una máquina virtual equipada con vTPM.

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

SDK	Interfaz de usuario
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.

Obtener e importar un certificado

Para proteger las comunicaciones de vSphere, Citrix recomienda utilizar HTTPS en lugar de HTTP.

HTTPS requiere certificados digitales. Utilice un certificado digital emitido por una entidad de certificación que cumpla con la directiva de seguridad de su organización.

Si no puede utilizar un certificado digital emitido por una entidad de certificación, puede utilizar el certificado autofirmado instalado por VMware. Utilice este método solo si la directiva de seguridad de su organización lo permite. 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 utiliza Internet Explorer, haga clic con el botón secundario en Internet Explorer y elija **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 la opción **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.

Qué hacer a continuación

- Si está en el proceso de implementación inicial, consulte Crear catálogos de máquinas
- Para obtener información específica de VMware, consulte Crear un catálogo de VMware

Más información

- Conexiones y recursos
- Crear catálogos de máquinas

Conexión con soluciones de VMware Cloud y de partners

August 17, 2024

Tras configurar el clúster de Azure VMware Solution (AVS), Google Cloud VMware Engine y VMware Cloud en AWS, cree las conexiones. Para crear conexiones, consulte Conexión con VMware.

Qué hacer a continuación

- Si está en el proceso de implementación inicial, consulte Crear catálogos de máquinas
- Para obtener información específica de VMware, consulte Crear un catálogo de VMware

Más información

- Conexiones y recursos
- Crear catálogos de máquinas

Administración de imágenes (Technical Preview)

August 17, 2024

Introducción

El proceso de creación o actualización de catálogos de MCS tiene dos fases:

- Masterización: Una imagen fuente se convierte en una imagen publicada
- Clonación: Se crean nuevas máquinas virtuales a partir de la imagen publicada

Con la funcionalidad de administración de imágenes, MCS separa la fase de masterización del flujo de trabajo general de aprovisionamiento.

Puede preparar varias versiones de imágenes de MCS (imagen preparada) a partir de una única imagen de origen y usarla en varios catálogos de máquinas de MCS diferentes. Esta implementación reduce significativamente los costes de almacenamiento y tiempo, y simplifica el proceso de implementación de máquinas virtuales y actualización de imágenes.

Las ventajas de usar esta funcionalidad de administración de imágenes son:

- Genere imágenes preparadas por adelantado sin crear un catálogo.
- Reutilice las imágenes preparadas en diferentes escenarios, como crear y actualizar un catálogo.
- Reduzca considerablemente el tiempo de creación o actualización de catálogos.

> **Nota:**
>
> - Esta función se aplica actualmente a los entornos de virtualización de Azure y VMware.
> - Puede crear un catálogo de máquinas MCS sin usar imágenes preparadas. En ese caso, no podrá aprovechar las ventajas de la función.

Casos de uso

Algunos de los casos de uso de la funcionalidad de administración de imágenes son:

- *Administración de versiones*: Las versiones de imágenes le permiten:
  - administrar diferentes iteraciones o actualizaciones de una imagen en particular.
  - mantener varias versiones de una imagen para diferentes fines.
- *Agrupación lógica*: Puede crear varias definiciones de imágenes para:
  - agrupar lógicamente las versiones de las imágenes en función de diversos criterios, como el proyecto, el departamento o el tipo de aplicación y escritorio.
  - administrar las imágenes de manera más eficiente dentro de una organización.

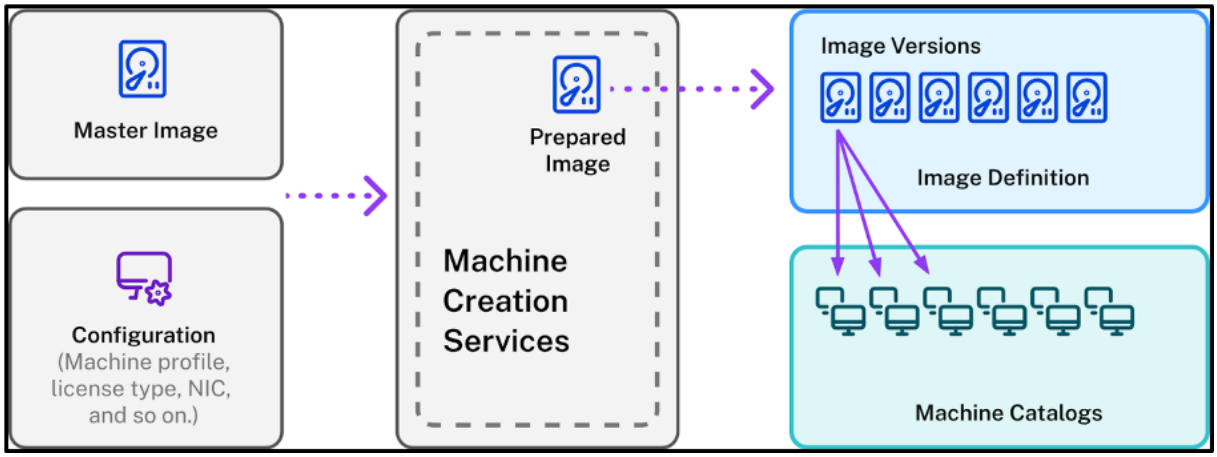
¿Qué es una imagen preparada?

Con la funcionalidad de administración de imágenes, MCS desvincula la fase de masterización del flujo de trabajo general de creación o actualización del catálogo y divide el proceso en dos etapas:

1. Crear imágenes preparadas a partir de una única imagen fuente.
2. Usar la imagen preparada para crear o actualizar un catálogo de máquinas de MCS.

Puede crear las imágenes preparadas por adelantado. Puede usar una sola imagen preparada para crear o actualizar varios catálogos de máquinas aprovisionadas por MCS.

Explicación de cómo se usa una imagen preparada en varios catálogos de máquinas de MCS cuando usa Web Studio desde la imagen:



Definición de imagen: Las definiciones de imagen son una agrupación lógica de versiones de una imagen. La definición de la imagen contiene información sobre:

- por qué se creó la imagen
- para qué sistema operativo es
- otra información sobre el uso de la imagen.

Un catálogo no se crea a partir de una definición de imagen, sino a partir de las versiones de imagen que se crean en función de la definición de imagen.

Versión de imagen: Las versiones de una imagen administran el control de versiones de la definición de imagen. Una definición de imagen puede tener varias versiones de imagen. Use las versiones de las imágenes como imágenes preparadas para crear o actualizar un catálogo.

Como alternativa, si quiere usar los comandos de PowerShell para crear un esquema de aprovisionamiento para crear o actualizar un catálogo, debe crear una especificación de versión de imagen preparada basada en la especificación de versión de la imagen maestra, según sea necesario para su entorno.

Participar en Tech Preview

Si está interesado en participar en Tech Preview, proporcione su información de contacto aquí.

Le ayudaremos a configurar el entorno de prueba y le proporcionaremos asistencia técnica si es necesario.

Requisito

- Para la imagen maestra de Windows, solo se admiten imágenes de VDA con la versión 2311 y posteriores y con E/S de MCS habilitada.

Limitaciones

Actualmente, la función no admite lo siguiente:

- Varias NIC en Azure
- Funcionalidad de disco de datos persistente
- Hibernación para multisesión
- Cambio del tipo de imagen

Administración del ciclo de vida de las imágenes mediante Web Studio

El ciclo de vida de la imagen cuando usa Web Studio es:

1. Crear una imagen preparada: Crear una definición de imagen y su versión de imagen inicial.
2. Crear versiones de la imagen a partir de la versión de imagen inicial.
3. Usar una versión de imagen como imagen preparada para crear catálogos.
4. Actualizar un catálogo de máquinas con una imagen preparada diferente.

5. Administrar las definiciones y versiones de las imágenes: Modificar el nombre y la descripción de las versiones de las imágenes y la descripción de una definición de imagen.
6. Eliminar una versión de imagen.
7. Eliminar una definición de imagen.

Como alternativa, también puede administrar imágenes mediante PowerShell. Consulte Administración del ciclo de vida de las imágenes mediante PowerShell.

Crear o actualizar un catálogo mediante una imagen preparada

Cree imágenes preparadas y úselas para crear o actualizar un catálogo de máquinas de MCS mediante:

- Web Studio
- Los comandos de PowerShell

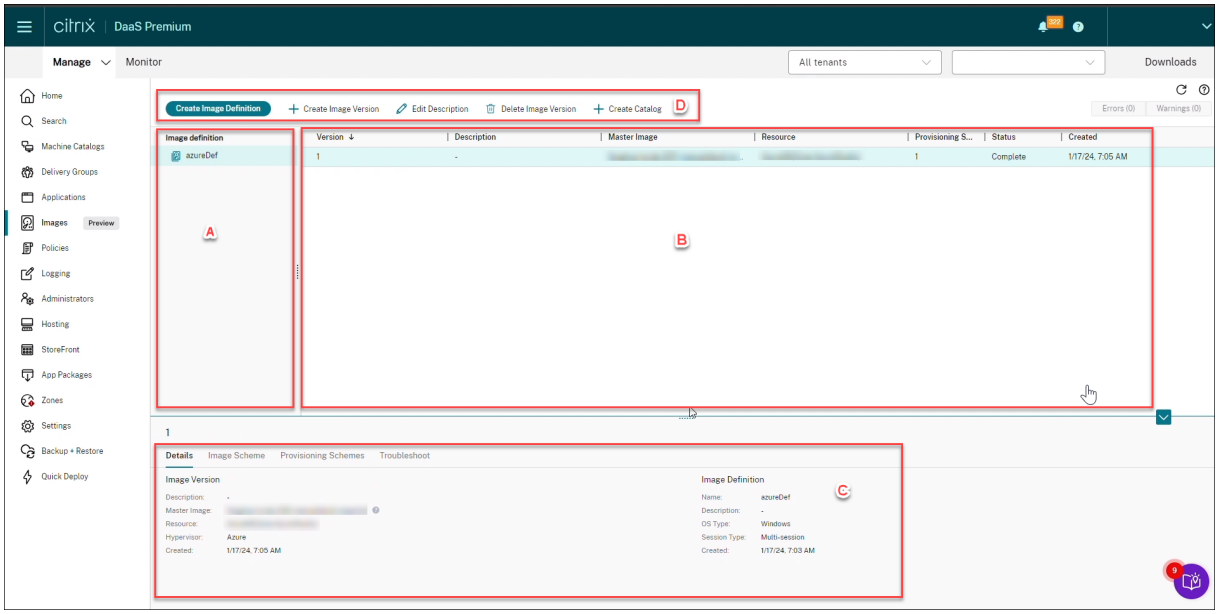
Usar Web Studio

Consulte los siguientes temas:

- Explicación del nodo Imágenes
- Crear una definición de imagen y una versión de imagen inicial
- Crear versiones de imágenes
- Crear un catálogo de máquinas desde el nodo Imágenes
- Crear un catálogo de máquinas desde el nodo Catálogos de máquinas
- Actualizar un catálogo de máquinas con una imagen preparada diferente
- Administrar las definiciones y versiones de las imágenes

Explicación del nodo Imágenes

Use el nodo **Imágenes** para crear y administrar imágenes preparadas de MCS. Su vista principal se divide en cuatro partes:



Etiqueta	Parte	Descripción
A	Definiciones de imágenes	Muestra las definiciones de imagen creadas anteriormente.
B	Versiones de imágenes	Muestra las versiones de imagen de la definición de imagen seleccionada.
C	Detalles	• La ficha **Detalles** muestra información detallada sobre la definición o versión de la imagen seleccionada, como la imagen maestra, el recurso, el hipervisor, el nombre de la definición de imagen, el tipo de sistema operativo y el tipo de sesión. • La ficha **Esquema de imagen** muestra información sobre la plantilla usada para preparar las imágenes, como el disco duro, el tamaño de la máquina, el tipo de licencia, el conjunto de cifrado del disco, el perfil de máquina, etc. • La ficha **Esquemas de aprovisionamiento** muestra el nombre del
D	Barra de acciones	Enumera las acciones que puede realizar en las definiciones y versiones de imágenes, como **Crear versión de imagen**, **Modificar descripción**, **Eliminar versión de imagen** y **Crear catálogo**.

Crear un catálogo de máquinas con la imagen preparada

Los pasos clave para crear un catálogo de máquinas MCS con la imagen preparada son:

1. Crear la definición de la imagen y las versiones iniciales de la imagen.

2. Usar la versión de imagen como una imagen preparada para crear un catálogo.

Crear una definición de imagen y una versión de imagen inicial

Para crear una definición de imagen y la versión inicial de la imagen, haga lo siguiente:

1. Inicie sesión en Web Studio y seleccione el nodo **Imágenes**. En la página **Introducción**, haga clic en **Siguiente**.
2. En la página **Definición de imagen**, especifique el **tipo de sistema operativo** y el **tipo de sesión** para la definición de la imagen.
3. En la página **Imagen**, seleccione **Recursos** y una imagen maestra para usarla como plantilla para crear la versión de imagen. Puede seleccionar la casilla **Usar un perfil de máquina** para seleccionar uno.

   > **Nota:**
   >
   > Antes de seleccionar una imagen, verifique que la imagen maestra tenga instalado el VDA 2311 o una versión posterior y que el controlador de E/S de MCS esté instalado en el VDA.

4. (Solo para Azure) En la página **Tipos de licencia y almacenamiento**, seleccione el tipo de almacenamiento y licencia que se usará como parte del proceso de preparación de la imagen.

   > **Nota:**
   >
   > Si selecciona un perfil de máquina en la página **Imagen**, el tipo de licencia del perfil de máquina se preselecciona en función de la configuración del perfil.

5. En la página **Especificación de máquina**:

   - Para Azure, seleccione un tamaño de máquina. Si selecciona un perfil de máquina en la página **Imagen**, se selecciona de forma predeterminada el tamaño de máquina del perfil de máquina.
   - En el caso de VMware, si selecciona un perfil de máquina, puede ver el recuento de CPU virtual derivado del perfil de máquina y no se puede cambiar. Si no selecciona un perfil de máquina, solo podrá ver el tamaño de memoria que se deriva de la imagen maestra.

6. En la página **Tarjetas NIC**, seleccione o agregue tarjetas NIC para la imagen de preparación. Para cada tarjeta NIC, seleccione una red virtual asociada.

   Para VMware, si no selecciona un perfil de máquina, se selecciona de forma predeterminada la tarjeta NIC asociada a la imagen maestra. Si selecciona un perfil de máquina, las tarjetas NIC se derivan del perfil de máquina y el recuento no se puede cambiar.

> **Nota:**
>
> Azure no admite varias tarjetas NIC.

7. (Solo para Azure) En la página **Parámetros del disco**, seleccione la clave de cifrado administrada por el cliente (CMEK). Si el perfil de la máquina no tiene una CMEK, pero la imagen maestra sí, preselecciona la CMEK de la imagen maestra.
8. En la página **Descripción de la versión**, introduzca una descripción para la versión de imagen inicial creada.
9. En la página **Resumen**, compruebe los detalles de la definición de imagen y la versión inicial de la imagen creada. Introduzca un nombre y una descripción para la definición de imagen. Haga clic en **Finalizar**.

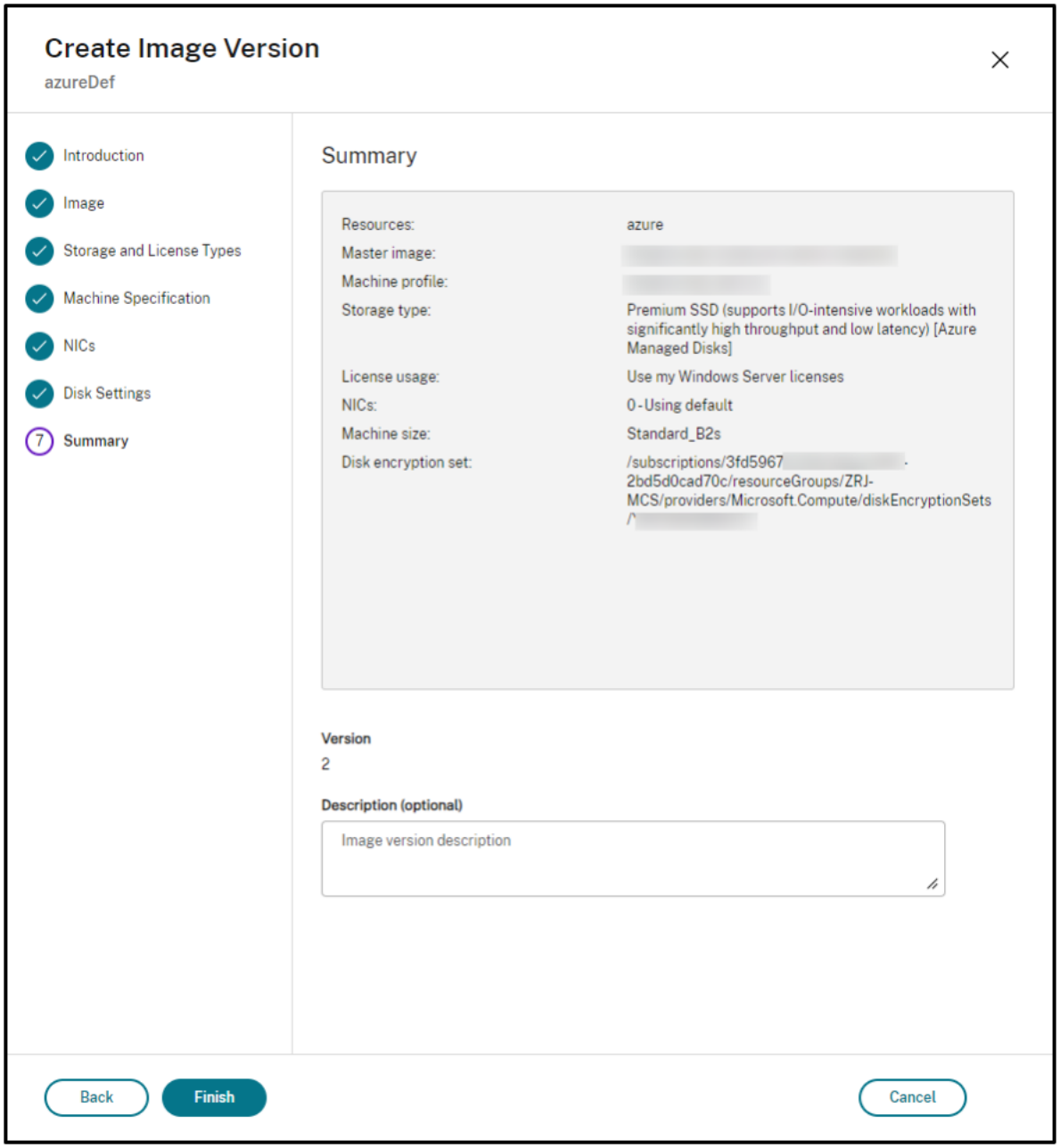
Crear versiones de imágenes

Las versiones de imagen permiten administrar diferentes iteraciones o actualizaciones de una imagen en particular. Esta funcionalidad le permite mantener varias versiones de una imagen para diferentes fines.

Para crear versiones de imagen a partir de la versión de imagen inicial, haga lo siguiente:

> **Nota:**
>
> La unidad de alojamiento de todas las versiones de la imagen debe ser la misma.

1. Vaya al nodo **Imágenes**, seleccione una versión de imagen y seleccione **Crear versión de imagen**.
2. Si quiere que la configuración de la versión de imagen sea diferente de la versión de imagen configurada inicialmente, configure los parámetros de las páginas **Imagen**, **Tipos de licencia y almacenamiento**, **Especificaciones de la máquina**, **Tarjetas NIC** y **Parámetros del disco** del cuadro de diálogo **Crear versión de imagen**.
3. Agregue una descripción para la versión de la imagen. Haga clic en **Finalizar**.



Crear un catálogo de máquinas desde el nodo Imágenes

Use la opción **Crear catálogo** del nodo **Imágenes** para crear un catálogo con la versión de la imagen.

Como alternativa, puede seleccionar la versión al crear un catálogo en el nodo **Catálogos de máquinas** y vincularla a la opción de imagen preparada en el flujo de trabajo de creación del catálogo. Consulte Crear un catálogo de máquinas desde el nodo Catálogos de máquinas

Para crear un catálogo de máquinas de MCS desde el nodo **Imágenes**, haga lo siguiente:

1. Seleccione una versión de imagen y haga clic en **Crear catálogo**. En la página **Introducción**, haga clic en **Siguiente**.
2. En la página **Experiencia de escritorio**, seleccione la experiencia de escritorio requerida.
3. Desde la página **Imagen** hasta la página **Parámetros del disco**, los parámetros se preseleccionan en función de la versión de imagen seleccionada.
4. (Para Azure) En la página **Grupo de recursos**, puede optar por crear un nuevo grupo de recursos o usar un grupo de recursos existente para colocar los recursos de este catálogo.
5. Complete los parámetros de las páginas siguientes.
6. En la página **Resumen**, compruebe los detalles del catálogo de máquinas. Introduzca un nombre y una descripción para el catálogo de máquinas. Haga clic en **Finalizar**.
7. Vaya al nodo **Catálogos de máquinas** para ver el catálogo de máquinas creado.

Crear un catálogo de máquinas desde el nodo Catálogos de máquinas

Para crear un catálogo de máquinas de MCS desde el nodo **Catálogos de máquinas**, haga lo siguiente:

1. Haga clic en **Catálogos de máquinas** en el panel de navegación izquierdo.
2. Haga clic en **Crear catálogo de máquinas**. Aparecerá la página **Configuración de catálogo de máquinas**. Haga clic en **Siguiente** en las páginas **Introducción**, **Tipo de máquina** y **Administración de máquinas**.
3. En la página **Imagen**:
    a) Seleccione **Imagen preparada**.
    b) En la **imagen preparada**, seleccione una versión de imagen de una definición de imagen.
    c) Haga clic en el nombre de la versión de la imagen. Para ver más detalles sobre la versión de la imagen seleccionada, haga clic en el número de versión, que aparece subrayado.
    d) Si la versión de imagen seleccionada está configurada con un perfil de máquina, seleccione un perfil de máquina. Si la versión de imagen seleccionada no está configurada con un perfil de máquina, no puede elegir usar un perfil de máquina.
4. Configure los parámetros en las páginas siguientes.
5. En la página **Parámetros del disco**, si la imagen preparada seleccionada usa un conjunto de cifrado de disco, no puede quitar el conjunto de cifrado, pero puede cambiar la clave por otra clave de cifrado.
6. (Para Azure) En la página **Grupo de recursos**, puede optar por crear un nuevo grupo de recursos o usar un grupo de recursos existente para colocar los recursos de este catálogo.
7. Complete los parámetros de las páginas siguientes.
8. En la página **Resumen**, compruebe los detalles del catálogo de máquinas. Introduzca un nombre y una descripción para el catálogo de máquinas. Haga clic en **Finalizar**.

Actualizar un catálogo de máquinas con una imagen preparada diferente

Para actualizar un catálogo de máquinas de MCS con una imagen preparada diferente, haga lo siguiente:

1. Haga clic en **Catálogos de máquinas** en el panel de navegación izquierdo y seleccione el catálogo de máquinas que quiere actualizar. Haga clic con el botón secundario y seleccione **Cambiar imagen preparada**.
2. En la página **Imagen**, seleccione una imagen preparada.
3. En la página **Estrategia de implantación**, seleccione cuándo quiere actualizar este catálogo con la imagen preparada seleccionada.
4. En la página **Resumen**, compruebe los detalles. Haga clic en **Finalizar**.

Puede ver el historial de los cambios de imagen realizados en un catálogo. Para ver el historial, haga lo siguiente:

1. Seleccione un catálogo de máquinas.
2. En la ficha **Propiedades de plantilla** del campo **Imagen preparada**, haga clic en **Ver historial de imágenes**.

Administrar las definiciones y versiones de las imágenes

Puede modificar y eliminar las definiciones y versiones de las distintas imágenes creadas.

Modificar una definición de imagen Puede modificar el nombre y la descripción de una definición de imagen.

Para modificar una definición de imagen, haga lo siguiente:

1. Vaya al nodo **Imágenes**, seleccione una definición de imagen y seleccione **Modificar definición de la imagen**.

Modificar una versión de imagen Puede modificar la descripción de una versión de imagen para especificar su propósito.

Para modificar una versión de imagen, haga lo siguiente:

1. Vaya al nodo **Imágenes**, seleccione una versión de imagen y seleccione **Modificar descripción**.

Eliminar una versión de imagen Para eliminar una versión de imagen, haga lo siguiente:

1. Vaya al nodo **Imágenes**, seleccione una versión de imagen y seleccione **Eliminar versión de imagen**.

> **Nota:**
>
> No se puede eliminar una versión de imagen si se usa en un catálogo de máquinas.

Eliminar una definición de imagen Para eliminar una definición de imagen, haga lo siguiente:

1. Vaya al nodo **Imágenes**, seleccione una definición de imagen y seleccione **Eliminar definición de imagen**.

> **Nota:**
>
> No puede eliminar una definición de imagen si contiene una versión de imagen.

Administración del ciclo de vida de las imágenes mediante PowerShell Si quiere usar los comandos de PowerShell para crear un esquema de aprovisionamiento, debe crear una especificación de versión de imagen preparada basada en la especificación de versión de imagen maestra, según sea necesario para su entorno.

Especificación de versión de imagen maestra: Una especificación de versión de imagen maestra es una imagen específica que se agrega o crea bajo una versión de imagen. Puede agregar una imagen existente en el hipervisor como especificación de versión de imagen maestra o crear una especificación de versión de imagen preparada basada en la especificación de versión de imagen maestra, según sea necesario para su entorno. La especificación de versión de imagen preparada se puede usar para varios esquemas de aprovisionamiento.

El ciclo de vida de una imagen cuando se usan los comandos de PowerShell es:

1. Crear una imagen:
    a) Crear una definición de imagen.
    b) Crear una versión de imagen.
    c) Agregar una especificación de versión de imagen maestra.
    d) Crear una especificación de versión de imagen preparada.
2. Crear un catálogo de máquinas de MCS con una especificación de versión de imagen preparada:
    a) Crear un catálogo de brokers.
    b) Crear un grupo de identidades.
    c) Crear un esquema de aprovisionamiento con el parámetro UID de especificación de versión de imagen preparada mediante el comando `New-ProvScheme`.
    d) Vincular el catálogo de brokers al esquema de aprovisionamiento.
3. Crear máquinas virtuales en el catálogo de máquinas de MCS.

4. Cambiar la especificación de versión de imagen preparada de un esquema de aprovisionamiento mediante el comando `Set-ProvScheme`.
5. Administrar las definiciones y versiones de las imágenes: Modificar las versiones y definiciones de las imágenes.
6. Eliminar un catálogo de máquinas de MCS. El orden de eliminación es: especificación de versión de imagen preparada > especificación de versión de imagen maestra > versión de imagen > definición de imagen. Antes de eliminar la especificación de versión de la imagen, asegúrese de que la especificación de versión de la imagen preparada no esté asociada a ningún catálogo de máquinas de MCS.

Usar PowerShell

Puede hacer lo siguiente con los comandos de PowerShell:

- Crear una imagen preparada
- Crear un catálogo mediante la especificación de versión de imagen preparada
- Actualizar un catálogo mediante una especificación de versión de imagen preparada
- Eliminar la definición de imagen, versión de imagen y especificación de versión de imagen preparada
- Administrar la definición y la versión de imagen
- Obtener la definición de imagen, versión de imagen, especificación de versión de imagen preparada y detalles del esquema de aprovisionamiento

Crear una imagen preparada

Los comandos detallados de PowerShell para crear una especificación de versión de imagen preparada son los siguientes:

1. Compruebe los nombres de definición de imagen disponibles mediante `Test-ProvImageDefinitionN` `command`. Por ejemplo,

```
Test-ProvImageDefinitionNameAvailable -ImageDefinitionName <string
    []>
```

2. Cree una definición de imagen con el comando `New-ProvImageDefinition`. Por ejemplo,

```
New-ProvImageDefinition -ImageDefinitionName image1 -OsType
    Windows -VdaSessionSupport MultiSession
```

3. Cree una versión de imagen con el comando `New-ProvImageVersion`. Por ejemplo,


```
New-ProvImageVersion -ImageDefinitionName image1 -Description "
    version 1"
```

4. Agregue una especificación de versión de imagen maestra a la versión de la imagen mediante el comando `Add-ProvImageVersionSpec`. Por ejemplo,

```
Add-ProvImageVersionSpec -ImageDefinitionName  image1  -
    ImageVersionNumber  1 -HostingUnitName azure -MasterImagePath "
    XDHyp:\HostingUnits\azure\image.folder\azureresourcegroup.
    resourcegroup\win2022-snapshot.snapshot"
```

> **Nota:**
>
> Solo puede agregar una especificación de versión de imagen maestra a una versión de imagen para una unidad de alojamiento.

5. Cree una especificación de versión de imagen preparada a partir de la especificación de versión de imagen maestra mediante el comando `New-ProvImageVersionSpec`. Por ejemplo,

```
New-ProvImageVersionSpec
-SourceImageVersionSpecUid  c6e7384c-b2f8-46d6-9519-29a2c57ed3cb
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure\virtualprivatecloud.folder\
     azureresourcegroup.resourcegroup\azure-vnet-eastus.
     virtualprivatecloud\dev.network"
-ServiceOffering "XDHyp:\HostingUnits\azure\serviceoffering.folder
    \Standard_B2ms.serviceoffering" -CustomProperties "<
    CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
    machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
    instance`"></CustomProperties>" -RunAsynchronously
```

> **Nota:**
>
> Una unidad de alojamiento y un tipo de preparación solo pueden tener una instancia preparada.

Ejemplo del conjunto completo de comandos de PowerShell para crear la definición de imagen, versión de imagen y especificación de versión de imagen preparada en Azure:

```
$ImageDefintion = New-ProvImageDefinition
-ImageDefinitionName image1 -OsType Windows -VdaSessionSupport
    MultiSession
 $ImageVersion = New-ProvImageVersion -ImageDefinitionName
     $ImageDefintion.ImageDefinitionName -Description "version 1"
$MasterImagePath = "XDHyp:\HostingUnits\azure\image.folder\
    azureresourcegroup.resourcegroup\win2022-snapshot.snapshot"
$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
     $ImageVersion.ImageDefinitionName -ImageVersionNumber $ImageVersion
    .ImageVersionNumber -HostingUnitName azure -MasterImagePath
    $MasterImagePath
```



```
$Task = New-ProvImageVersionSpec -SourceImageVersionSpecUid
    $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure\virtualprivatecloud.folder\
    azureresourcegroup.resourcegroup\azure-vnet-eastus.
    virtualprivatecloud\dev.network" }
  -ServiceOffering "XDHyp:\HostingUnits\azure\serviceoffering.folder\
    Standard_B2ms.serviceoffering" -CustomProperties "<
    CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
    machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
    instance`"></CustomProperties>" -RunAsynchronously
Get-ProvTask -TaskId $Task.TaskId
```

Ejemplo del conjunto completo de comandos de PowerShell para crear la definición de imagen, versión de imagen y especificación de versión de imagen preparada en VMware:

```
$ImageDefintion = New-ProvImageDefinition -ImageDefinitionName image2 -
    OsType Windows -VdaSessionSupport SingleSession
$ImageVersion = New-ProvImageVersion -ImageDefinitionName
    $ImageDefintion.ImageDefinitionName -Description "version 1"
$MasterImagePath = "XDHyp:\HostingUnits\vmware\win10-master.vm\win10-
    master-snap.snapshot"
$SourceImageVersionSpec = Add-ProvImageVersionSpec -ImageDefinitionName
    $ImageVersion.ImageDefinitionName -ImageVersionNumber $ImageVersion
    .ImageVersionNumber -HostingUnitName vmware -MasterImagePath
    $MasterImagePath
$Task = New-ProvImageVersionSpec -SourceImageVersionSpecUid
    $SourceImageVersionSpec.ImageVersionSpecUid -NetworkMapping @{
 "0"="XDHyp:\HostingUnits\vmware\DSwitch-VM Network.network" }
  -VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
Get-ProvTask -TaskId $Task.TaskId
```

Nota:

- Todas las especificaciones de versión de imagen de una definición de imagen deben pertenecer a la misma unidad de alojamiento.
- Una versión de imagen solo puede tener una especificación de versión de imagen maestra y una especificación de versión de imagen preparada.
- Todas las especificaciones de versión de imagen deben tener un perfil de máquina o ninguna de las especificaciones de versión de imagen debe tener un perfil de máquina.
- No puede especificar un grupo de recursos al crear una especificación de versión de imagen.

Crear un catálogo mediante una especificación de versión de imagen preparada

Para crear un catálogo de máquinas de MCS a partir de la especificación de versión de imagen preparada, use el comando `New-ProvScheme`. Por ejemplo,


```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid <
    Guid> -HostingUnitUid <Guid> -IdentityPoolUid <Guid> [-VMCpuCount <
    int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-NetworkMapping <
    Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-Metadata <Hashtable
    >] [-ServiceOffering <string>] [-SecurityGroup <string[]>] [-
    TenancyType <string>] [-MachineProfile <string>] [-CustomProperties
    <string>] [-ResetAdministratorPasswords] [-
    UseFullDiskCloneProvisioning] [-RunAsynchronously] [-
    PurgeJobOnSuccess] [-ProvisioningSchemeType <ProvisioningSchemeType
    >]
```

O bien,

```
New-ProvScheme -ProvisioningSchemeName <string> -ImageVersionSpecUid <
    Guid> -HostingUnitName <string> -IdentityPoolName <string> [-
    VMCpuCount <int>] [-VMMemoryMB <int>] [-UseWriteBackCache] [-
    NetworkMapping <Hashtable>] [-CleanOnBoot] [-Scope <string[]>] [-
    Metadata <Hashtable>] [-ServiceOffering <string>] [-SecurityGroup <
    string[]>] [-TenancyType <string>] [-MachineProfile <string>] [-
    CustomProperties <string>] [-ResetAdministratorPasswords] [-
    UseFullDiskCloneProvisioning] [-RunAsynchronously] [-
    PurgeJobOnSuccess] [-ProvisioningSchemeType <ProvisioningSchemeType
    >]
```

Ejemplo del conjunto completo de comandos de PowerShell para crear un catálogo en Azure:

```
$Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC
    $False  -MinimumFunctionalLevel "L7_20" -Name "azurecatalog" -
    PersistUserChanges "Discard" -ProvisioningType "MCS" -Scope @() -
    SessionSupport "MultiSession"
$IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "azure.
    local" -IdentityPoolName "azurecatalog" -IdentityType "
    ActiveDirectory"  -NamingScheme "azure##" -NamingSchemeType "Numeric
    " -Scope @()
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -
    ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "
    PreparationType -eq 'Mcs'"
$Task = New-ProvScheme -ProvisioningSchemeName azurecatalog -
    ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid -
    HostingUnitName azure -IdentityPoolName azurecatalog -CleanOnBoot -
    Scope @() -SecurityGroup @() -ServiceOffering "XDHyp:\HostingUnits\
    azure\serviceoffering.folder\Standard_B2s.serviceoffering" -
    NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure\virtualprivatecloud.folder\
     azureresourcegroup.resourcegroup\azure-vnet-eastus.
     virtualprivatecloud\dev.network" }
  -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.
     com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
     XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
     StorageAccountType`" Value=`"StandardSSD_LRS`" /></
     CustomProperties>" -RunAsynchronously
Get-ProvTask -TaskId $Task.TaskId
$ProvScheme = Get-ProvScheme -ProvisioningSchemeName azurecatalog
```



```
9 Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId $ProvScheme
      .ProvisioningSchemeUid
```

Ejemplo del conjunto completo de comandos de PowerShell para crear un catálogo en VMware:

```
1 $Catalog = New-BrokerCatalog  -AllocationType "Random"  -IsRemotePC
      $False  -MinimumFunctionalLevel "L7_20" -Name "vmwarecatalog" -
      PersistUserChanges "Discard" -ProvisioningType "MCS" -Scope @() -
      SessionSupport "MultiSession"
2 $IdentityPool = New-AcctIdentityPool  -AllowUnicode  -Domain "vmware.
      local" -IdentityPoolName "vmwarecatalog" -IdentityType "
      ActiveDirectory"  -NamingScheme "vmware##" -NamingSchemeType "
      Numeric" -Scope @()
3 $PreparedImageVersionSpec = Get-ProvImageVersionSpec -
      ImageDefinitionName image2 -ImageVersionNumber 1 -Filter "
      PreparationType -eq 'Mcs'"
4 $Task = New-ProvScheme -ProvisioningSchemeName vmwarecatalog -
      ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid -
      HostingUnitName vmware -IdentityPoolName vmwarecatalog -CleanOnBoot
      -Scope @() -SecurityGroup @() -NetworkMapping @{
5  "0"="XDHyp:\HostingUnits\vmware\DSwitch-VM Network.network" }
6   -VMCpuCount 2 -VMMemoryMB 4096 -RunAsynchronously
7 Get-ProvTask -TaskId $Task.TaskId
8 $ProvScheme = Get-ProvScheme -ProvisioningSchemeName vmwarecatalog
9 Set-BrokerCatalog -Name $Catalog.Name -ProvisioningSchemeId $ProvScheme
      .ProvisioningSchemeUid
```

Actualizar un catálogo mediante una especificación de versión de imagen preparada

Puede actualizar un catálogo mediante el comando `Set-ProvSchemeImage`. Por ejemplo,

```
1 Set-ProvSchemeImage -ProvisioningSchemeUid <Guid> -ImageVersionSpecUid
      <Guid> [-DoNotStoreOldImage] [-RunAsynchronously] [-
      PurgeJobOnSuccess]
```

O bien,

```
1 Set-ProvSchemeImage -ProvisioningSchemeName <string> -
      ImageVersionSpecUid <Guid> [-DoNotStoreOldImage] [-RunAsynchronously
      ] [-PurgeJobOnSuccess]
```

Ejemplo del conjunto completo de comandos de PowerShell para actualizar un catálogo:

```
1 $PreparedImageVersionSpec = Get-ProvImageVersionSpec -
      ImageDefinitionName image1 -ImageVersionNumber 2 -Filter "
      PreparationType -eq 'Mcs'"
2 Set-ProvSchemeImage -ProvisioningSchemeName azurecatalog -
      ImageVersionSpecUid $PreparedImageVersionSpec.ImageVersionSpecUid -
      RunAsynchronously
```


Eliminar la definición de imagen, versión de imagen y especificación de versión de imagen preparada

Tenga en cuenta lo siguiente antes de eliminar una definición de imagen, versión de imagen y especificación de versión de imagen preparada:

- No se puede eliminar una definición de imagen si contiene alguna versión de imagen.
- No se puede eliminar una versión de imagen si contiene alguna especificación de versión de imagen.
- No se puede eliminar una especificación de versión de imagen maestra si la usa cualquier otra especificación de versión de imagen preparada.
- No se puede eliminar una especificación de versión de imagen preparada si la usa algún esquema de aprovisionamiento.

Estos son los pasos detallados:

1. Quite una especificación de versión de imagen preparada. Por ejemplo,

```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -
    ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "
    PreparationType -eq 'Mcs'"
Remove-ProvImageVersionSpec -ImageVersionSpecUid
    $PreparedImageVersionSpec.ImageVersionSpecUid -
    RunAsynchronously
```

> **Nota:**
>
> La especificación de versión de imagen maestra solo se puede eliminar cuando no tiene ninguna especificación de versión de imagen preparada asociada.

2. Quite la especificación de versión de imagen maestra. Por ejemplo,

```
$MasterImageVersionSpec = Get-ProvImageVersionSpec -
    ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "
    PreparationType -eq 'None'"
Remove-ProvImageVersionSpec -ImageVersionSpecUid
    $PreparedImageVersionSpec.ImageVersionSpecUid -
    RunAsynchronously
```

3. Quite una versión de imagen. Por ejemplo,

```
Remove-ProvImageVersion -ImageDefinitionName image1 -
    ImageVersionNumber 1
```

4. Quite una definición de imagen. Por ejemplo,

```
Remove-ProvImageDefinition -ImageDefinitionName image1
```

Ejemplo del conjunto completo de comandos de PowerShell:


```
$PreparedImageVersionSpec = Get-ProvImageVersionSpec -
    ImageDefinitionName image1 -ImageVersionNumber 1 -Filter "
    PreparationType -eq 'Mcs'"
$Task = Remove-ProvImageVersionSpec -ImageVersionSpecUid
    $PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously
$MasterImageVersionSpec = Get-ProvImageVersionSpec -ImageDefinitionName
     image1 -ImageVersionNumber 1 -Filter "PreparationType -eq 'None'"
$Task = Remove-ProvImageVersionSpec -ImageVersionSpecUid
    $PreparedImageVersionSpec.ImageVersionSpecUid -RunAsynchronously
Remove-ProvImageVersion -ImageDefinitionName image1 -ImageVersionNumber
     1
Remove-ProvImageDefinition -ImageDefinitionName image1
```

Administrar la definición y la versión de imagen

Puede cambiar el nombre de una definición de imagen y modificarla. También puede modificar una versión de imagen.

- Para cambiar el nombre de una definición de imagen, use el comando `Rename-ProvImageDefinition`. Por ejemplo:

  ```
  Rename-ProvImageDefinition -ImageDefinitionUid <Guid> -
      NewImageDefinitionName <string>
  ```

  O bien,

  ```
  Rename-ProvImageDefinition -ImageDefinitionName <string> -
      NewImageDefinitionName <string>
  ```

- Para modificar una definición de imagen, use el comando `Set-ProvImageDefinition`. Por ejemplo:

  ```
  Set-ProvImageDefinition -ImageDefinitionUid <Guid> [-Description
      <string>]
  ```

  O bien,

  ```
  Set-ProvImageDefinition -ImageDefinitionName <string> [-
      Description <string>]
  ```

- Para modificar una versión de imagen, use el comando `Set-ProvImageVersion`. Por ejemplo:

  ```
  Set-ProvImageVersion -ImageVersionUid <Guid> [-Description <
      string>]
  ```

  O bien,


```
Set-ProvImageVersion -ImageDefinitionName <string> -
    ImageVersionNumber <int> [-Description <string>]
```

Obtener la definición de imagen, versión de imagen, especificación de versión de imagen preparada y detalles del esquema de aprovisionamiento

- Para obtener los detalles de una definición de imagen, use el comando `Get-ProvImageDefinition`. Por ejemplo:

```
Get-ProvImageDefinition [-ImageDefinitionName <string>] [-
    ImageDefinitionUid <Guid>] [-ReturnTotalRecordCount] [-
    MaxRecordCount <int>] [-Skip <int>] [-SortBy <string>] [-
    Filter <string>]
```

- Para obtener los detalles de una versión de imagen, use el comando `Get-ProvImageVersion`. Por ejemplo:
  - Para enumerar las versiones de imagen de una definición de imagen,

    ```
    Get-ProvImageVersion -ImageDefinitionUid <Guid>
    ```

    O bien,

    ```
    Get-ProvImageVersion -ImageDefinitionName <string>
    ```

  - Para obtener los detalles de una versión de imagen,

    ```
    Get-ProvImageVersion -ImageVersionUid <Guid>
    ```

    O bien,

    ```
    Get-ProvImageVersion -ImageDefinitionName <string> -
        ImageVersionNumber <int>
    ```

- Para obtener la especificación de versión de imagen preparada, use el comando `Get-ProvImageVersionSpec`. Por ejemplo:
  - Para enumerar todas las especificaciones de versión de imagen preparada de una versión de imagen,

    ```
    Get-ProvImageVersionSpec -ImageVersionUid <Guid>
    ```

  - Para enumerar las especificaciones de versión de imagen maestra de una especificación de versión de imagen preparada,

    ```
    Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter '
        PreparationType -eq "None"'
    ```


- Para enumerar las especificaciones de versión de imagen preparada de una versión de imagen que esté asociada a una imagen maestra,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter '
    PreparationType -eq "MCS" -and SourceImageVersionSpecUid -
    eq "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"'
```

- Para obtener correctamente las especificaciones de versión de imagen preparada de una versión de imagen,

```
Get-ProvImageVersionSpec -ImageVersionUid <Guid> -Filter '
    PreparationType -eq "MCS" -and SourceImageVersionSpecUid -
    eq "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" -and
    ImageVersionSpecStatus -eq "Complete"'
```

- Para obtener los detalles de la especificación de versión de imagen preparada,

```
Get-ProvImageVersionSpec -ImageVersionSpecUid <Guid>
```

- Para obtener los detalles del esquema de aprovisionamiento, use el comando `Get-ProvScheme`. Por ejemplo:

```
Get-ProvScheme [[-ProvisioningSchemeName] <String>] [-
    ProvisioningSchemeUid <Guid>] [-ScopeId <Guid>] [-ScopeName <
    String>] [-ReturnTotalRecordCount] [-MaxRecordCount <Int32>]
    [-Skip <Int32>] [-SortBy <String>] [-Filter <String>] [-
    FilterScope <Guid>]
```

- Para obtener un historial de especificaciones de versión de imagen preparada de un esquema de aprovisionamiento, use el comando `Get-ProvSchemeImageVersionSpecHistory`. Por ejemplo:

```
Get-ProvSchemeImageVersionSpecHistory [-ProvisioningSchemeName <
    String>] [-ProvisioningSchemeUid <Guid>] [-ImageVersionSpecUid
     <Guid>] [-ImageVersionSpecHistoryUid <Guid>] [-
    ReturnTotalRecordCount] [-MaxRecordCount <Int32>] [-Skip <
    Int32>] [-SortBy <String>] [-Filter <String>] [-FilterScope <
    Guid>]
```

Crear catálogos de máquinas

August 20, 2024

> **Importante:**
>
> A partir de Citrix Virtual Apps and Desktops 7 2006, si la implementación actual utiliza cualquiera

> de las siguientes tecnologías, solo podrá actualizar la versión de la implementación a la versión actual (Current Release) después de quitar los elementos con estado "Fin de vida"(EOL) que utilizan dichas tecnologías.
>
> - Discos Personal vDisk (PvD)
> - AppDisks
> - Tipos de host de nube pública: Citrix CloudPlatform, Microsoft Azure Classic
>
> Para obtener información detallada, consulte Quitar discos PvD, AppDisks y hosts no admitidos.
>
> **Nota:**
>
> Puede administrar la implementación de Citrix Virtual Apps and Desktops mediante dos consolas de administración: Web Studio (basada en la web) y Citrix Studio (basada en Windows). Este artículo se refiere únicamente a Web Studio. Para obtener información sobre Citrix Studio, consulte el artículo equivalente en Citrix Virtual Apps and Desktops 7 2212 o versiones anteriores.

Si quiere usar conexiones de host de nube pública con la implementación, necesita una licencia de derechos híbridos para completar la nueva instalación o actualizar a la versión actual.

Cuando el instalador detecta una o más de las tecnologías o conexiones de host no compatibles sin licencia de derechos híbridos, la actualización se pone en pausa o se detiene. Aparecerá un mensaje explicativo. Los registros del instalador contienen información detallada. Para obtener más información, consulte Actualizar una implementación.

Introducción

Las colecciones de máquinas físicas o virtuales se administran como una entidad única, llamada catálogo de máquinas. Todas las máquinas de un catálogo tienen el mismo tipo de sistema operativo: SO multisesión o SO de sesión única y son máquinas Windows o Linux.

Web Studio le guiará para crear el primer catálogo de máquinas después de crear el sitio. Después de crear el primer catálogo de máquinas, Web 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 Virtual Delivery Agent (VDA) y la actualización del Delivery Controller gestionan la actualización de E/S de MCS.

Información general

Cuando crea un catálogo de máquinas virtuales, debe indicar cómo aprovisionarlas. Puede utilizar Machine Creation Services (MCS). 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 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 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 Web 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.
- El uso de plantillas para aprovisionar 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.

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 completadas las pruebas, generan un informe que podrá ver. Ejecute las pruebas en cualquier momento desde Web 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, Web 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 RDS de Microsoft en el panel **Detalles de la máquina**. Este panel se encuentra en 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 cuando se inicien sesiones con intermediario. Los VDA no registrados pueden derivar en una infrautilización 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, Web Studio proporciona información en el Asistente para la creación de catálogos, y después de agregar máquinas de un catálogo a un grupo de entrega.

Después de agregar las máquinas existentes desde el asistente, 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 identifica una máquina problemática, quite esa máquina o agréguela. Por ejemplo: si un mensaje indica que es posible que no se obtenga información acerca de una máquina, 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:

  - Optimización de almacenamiento de MCS crea un disco de estilo de caché de escritura para cada máquina virtual.

  - MCS agregó la capacidad de usar clones completos, en lugar del caso de uso del disco Delta descrito en la sección anterior.

  Las funciones del hipervisor también pueden entrar en la ecuación. Por ejemplo:

  - XenServer IntelliCache crea un disco de lectura en el almacenamiento local para cada XenServer. Esta opción ahorra en IOPS en la imagen maestra que podría mantenerse en la ubicación de almacenamiento compartido.

- Sobrecarga del hipervisor

  Cada hipervisor usa archivos específicos que crean sobrecarga para las máquinas virtuales. Los hipervisores también usan el almacenamiento para operaciones de administración y registro general. Calcular el 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 y 100 MB para los archivos de registros; 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.
  - Actualizar el catálogo para 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:\vdiskdif.vhdx`, y el nombre de archivo en la memoria caché de escritura de E/S de MCS es `D:\mcsdif.vhdx`.
- Para obtener mejoras en los diagnósticos, incluya 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:

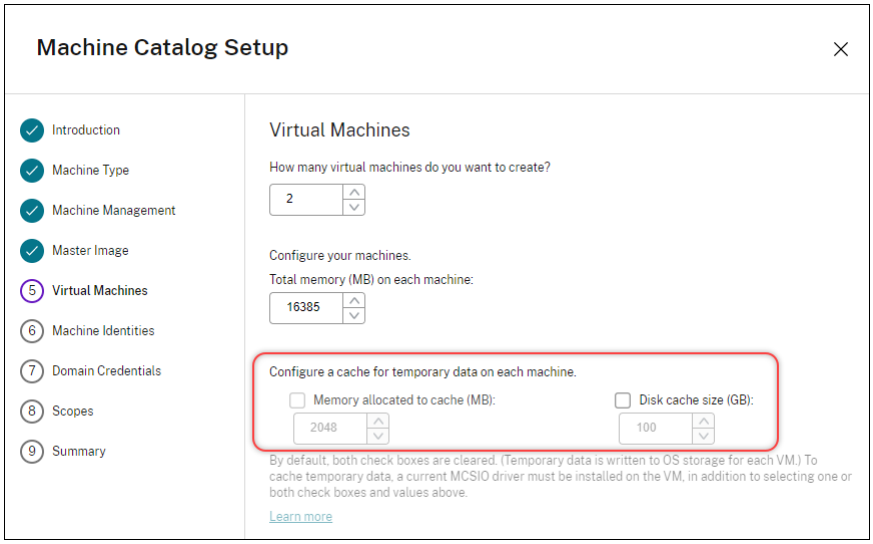
1. E/S de MCS ya no admite la memoria caché solo en RAM. Especifique un tamaño de disco en Web Studio durante la creación del catálogo de máquinas.
2. El disco de la memoria caché de escritura de una VM se crea y se formatea automáticamente al arrancar la VM por primera vez. Cuando la VM ya está activa, el archivo de la memoria caché de escritura `mcsdif.vhdx` se escribe en el volumen formateado `MCSWCDisk`.
3. El archivo de paginación se redirige a este volumen con formato, `MCSWCDisk`. Como resultado, este tamaño de disco tiene en cuenta la cantidad total de espacio en disco. Incluye el delta entre el tamaño del disco y la carga de trabajo generada, más el tamaño del archivo de paginación. Normalmente, esto se asocia al tamaño de la RAM de la VM.

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.



- Al actualizar un catálogo de máquinas existente en función de la nueva instantánea de una VM que contiene un VDA configurado para la versión 1903, la instantánea nueva sigue utilizando la configuración de E/S de MCS del catálogo existente para 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 1903. 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 más 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 tamaño adicional del 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.

Asignar una letra de unidad específica al disco de la memoria caché de reescritura de E/S de MCS

Puede asignar una letra de unidad específica al disco de la memoria caché de reescritura de E/S de MCS. Esta implementación le ayuda a evitar conflictos entre la letra de la unidad de cualquier aplicación que utilice y la letra de la unidad del disco de la memoria caché de reescritura de E/S de MCS.

Para asignar la letra de unidad al disco de caché de reescritura de E/S de MCS, puede usar los comandos de PowerShell. Los hipervisores compatibles son Azure, GCP, VMware, SCVMM y XenServer.

> **Nota:**
>
> Esta función requiere la versión 2305 de VDA o una posterior.

Limitaciones

- Aplicable solo al sistema operativo Windows
- Letra de unidad aplicable al disco de la memoria caché de reescritura: De E a Z
- No se aplica cuando el disco temporal de Azure se utiliza como disco de la memoria caché de reescritura
- Aplicable solo cuando al crear otros catálogos de máquinas

Asignar una letra de unidad al disco de la memoria caché de reescritura

Para asignar una letra de unidad al disco de la memoria caché de reescritura:

1. Abra la ventana de **PowerShell**.
2. Ejecute `asnp citrix*`.
3. Cree un grupo de identidades si aún no se ha creado.
4. Cree un esquema de aprovisionamiento mediante el comando `New-ProvScheme` con la propiedad `WriteBackCacheDriveLetter`. Por ejemplo:

```
New-ProvScheme -CleanOnBoot `
-HostingUnitName "<name>" `
-IdentityPoolName $schemeName `
-ProvisioningSchemeName $schemeName `
-InitialBatchSizeHint 1 `
-UseWriteBackCache -WriteBackCacheDiskSize 127 -
   WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `
-MasterImageVM "XDHyp:\HostingUnits<name>\image.folder\abcd-
   resources.resourcegroup\
   MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxx2130aa145ec77.
   manageddisk" `
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\name\virtualprivatecloud.folder\East US.
    region\virtualprivatecloud.folder\abcd-resources.resourcegroup
    \abcd-resources-vnet.virtualprivatecloud\default.network" }
  `
-ServiceOffering "XDHyp:\HostingUnits\<name>\serviceoffering.
   folder\Standard_D2s_v5.serviceoffering" `
-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="OsType" Value="Windows"
    />
<Property xsi:type="StringProperty" Name="StorageType" Value="
    Premium_LRS"/>
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false
    " />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="
    false" />
<Property xsi:type="StringProperty" Name="PersistVm" Value="false"
     />
<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
    Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value
    ="false" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
    abcd-group1" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2"
     />
</CustomProperties>'
```

5. Termine de crear el catálogo. Para obtener información, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Preparar una imagen maestra

Para obtener información sobre la creación de hosts de conexión, 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 hosts emplean términos distintos.
- Compruebe que el host tiene 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.

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 Machine Creation Services, no ejecute Sysprep en imágenes maestras.

Para preparar una imagen maestra:

1. Con 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 Web 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 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.
5. Citrix recomienda crear y asignar un nombre a una instantánea de la imagen maestra. Si especifica una imagen maestra en lugar de una instantánea al crear un catálogo de máquinas, Web

Studio crea una instantánea. No se puede darle el nombre.

Activación de licencias por volumen

MCS admite la activación de licencias por volumen para automatizar y administrar la activación de los sistemas operativos Windows y Microsoft Office. Los tres modelos que admite MCS para la activación de licencias por volumen son:

- Servicio de administración de claves KMS (Key Management Service)
- Activación basada en Active Directory (ADBA)
- Multiple Activation Key (MAK)

Puede cambiar la configuración de activación después de crear el catálogo de máquinas.

Servicio de administración de claves KMS (Key Management Service)

KMS es un servicio ligero que no requiere un sistema dedicado y se puede alojar fácilmente y de manera conjunta en un sistema que proporcione otros servicios. Esta funcionalidad se admite en todas las versiones de Windows compatibles con Citrix. Durante la preparación de la imagen, MCS realiza el rearmado de Microsoft Windows y Microsoft Office KMS. Puede omitir el rearmado ejecutando el comando `Set-Provserviceconfigurationdata`. Para obtener más información sobre el rearmado de Microsoft Windows KMS y Microsoft Office KMS durante la preparación de imágenes, consulte Machine Creation Services: Image Preparation Overview and Fault-Finding. Para obtener más información sobre la activación de KMS, consulte Activate using Key Management Service.

> **Nota:**
>
> Todos los catálogos de máquinas creados después de ejecutar el comando `Set-Provserviceconfigurat` tienen la misma configuración que se proporciona en el comando.

Activación basada en Active Directory (ADBA)

ADBA le permite activar máquinas a través de sus conexiones de dominio. Las máquinas se activan inmediatamente cuando se unen al dominio. Estas máquinas permanecen activadas mientras sigan unidas al dominio y en contacto con él. Esta funcionalidad se admite en todas las versiones de Windows compatibles con Citrix, excepto en Windows Server 2022. Para obtener más información sobre la activación basada en Active Directory, consulte Activate using Active Directory-based activation.

Multiple Activation Key (MAK)

MAK es una modalidad de activación por volumen y de autenticación del sistema Windows con la ayuda del servidor de Microsoft. Es necesario comprar la clave MAK de Microsoft, a la que se le asigna una cantidad fija de recuentos de activación. Cada vez que se activa un sistema Windows, el recuento de activaciones se reduce. Hay dos maneras de activar el sistema:

- Activación con conexión: Si el sistema Windows que quiere activar tiene acceso a Internet, el sistema activa Windows automáticamente al instalar la clave de producto. Este proceso reduce el recuento de activaciones en 1 para la instancia MAK correspondiente.
- Activación sin conexión: Si el sistema Windows no puede conectarse a Internet para la activación en línea, MCS obtiene un ID de confirmación y un ID de instalación del servidor de Microsoft para activar el sistema Windows. Esta forma de activación es útil para catálogos de máquinas no persistentes.

> **Nota:**
>
> - MCS no admite la activación de Microsoft Office mediante MAK.
> - La versión mínima de VDA requerida es 2303.

Requisitos clave

- El Delivery Controller debe tener acceso a Internet.
- Crear un nuevo catálogo si la nueva imagen que va a actualizarse tiene una clave MAK distinta de la original.
- Instalar la clave MAK en la imagen maestra. Consulte Deploy MAK Activation para conocer los pasos para instalar la clave MAK en un sistema Windows.
- Si no está utilizando la preparación de imágenes:

  1. Agregue el valor de registro de DWORD `Manual` en `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatfo\Activation`.
  2. Defina el valor en 1.

Recuentos de activación Para ver el número de activaciones restantes para la clave MAK o para comprobar si una máquina virtual consume dos o más activaciones, utilice la herramienta de gestión de activación por volumen (Volume Activation Management Tool, VAMT). Consulte Install VAMT.

Activar el sistema Windows mediante MAK Para activar el sistema Windows mediante MAK:

1. Instale la clave de producto en la imagen maestra. Este paso consume un recuento de activación.
2. Cree un catálogo de máquinas de MCS.
3. Si no utiliza la preparación de imágenes:

   a) Agregue el valor de registro de DWORD `Manual` en `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatfo\Activation`.
   b) Defina el valor en 1.

   Este método inhabilita la opción de activación con conexión.
4. Agregue máquinas virtuales al catálogo de máquinas.
5. Encienda las máquinas virtuales.
6. Dependiendo de si se trata de una activación con o sin conexión, se activa el sistema Windows.

   - Si se trata de una activación con conexión, el sistema Windows se activa después de instalar la clave del producto.
   - Si se trata de una activación si conexión, MCS se comunica con las máquinas virtuales aprovisionadas para obtener el estado de activación del sistema Windows. A continuación, MCS obtiene un ID de confirmación y un ID de instalación del servidor de Microsoft. Estos identificadores se utilizan para activar el sistema Windows.

Solución de problemas Si la máquina virtual aprovisionada no está activada con la clave MAK instalada, ejecute el comando `Get-ProvVM` o `Get-ProvScheme` en una ventana de PowerShell.

- El comando `Get-ProvScheme`: Consulte el parámetro `WindowsActivationType` asociado al catálogo de máquinas de MCS en la imagen maestra más reciente.
- El comando `Get-ProvVM`. Consulte los parámetros `WindowsActivationType`, `WindowsActivationStatus`, `WindowsActivationStatusErrorCode` y `WindowsActivation` .

Puede comprobar el error y comprobar los pasos para resolver el problema.

Crear un catálogo de máquinas mediante Web Studio

Antes de crear un catálogo:

- Consulte esta sección para obtener más información acerca de las decisiones que deberá tomar y la información que deberá facilitar.

- Compruebe que ha creado una conexión con el hipervisor, servicio de nube u otros recursos que alojan las máquinas.
- Si ha creado una imagen maestra para aprovisionar máquinas, compruebe que ha instalado un VDA en esa imagen.

Para iniciar al asistente de creación de catálogos:

1. Si este es el primer catálogo que se crea, se le guiará para la selección correcta (como "Configure las máquinas y cree catálogos de máquinas para ejecutar aplicaciones y escritorios"). Se abrirá el asistente para la creación de catálogos.
2. Si ya creó un catálogo y quiere crear otro, siga estos pasos:

    a) Inicie sesión en Web Studio, seleccione **Catálogos de máquinas** en el panel de la izquierda y, a continuación, seleccione **Crear catálogo de máquinas** en la barra de acciones.

    b) Para organizar los catálogos por medio de carpetas, cree carpetas en la carpeta **Catálogos de máquinas** predeterminada. Para obtener más información, consulte Crear una carpeta de catálogo.

    c) Seleccione la carpeta en la que quiere crear el catálogo y, a continuación, haga clic en **Crear catálogo de máquinas**. Se abrirá el asistente para la creación de catálogos.

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 herramientas se implementan.

Elija si la administración de energía de las máquinas del catálogo se llevará a cabo a través de Web Studio.

- Las opciones de energía de las máquinas se administran a través de Web Studio (por ejemplo, máquinas virtuales o equipos PC blade). Esta opción solo está disponible si ya ha configurado una conexión a un host.
- Las opciones de energía de las máquinas no se administran a través de Web Studio (por ejemplo, máquinas físicas).

Si ha indicado que las opciones de energía de las máquinas se administran a través de Web Studio, elija la herramienta que se va a utilizar para crear las máquinas virtuales.

- Tecnología de Citrix Provisioning
  - **Citrix Machine Creation Services (MCS)** Crea un catálogo de máquinas virtuales aprovisionadas y de las que se han creado imágenes mediante MCS. MCS copia las imágenes clonadas de una imagen maestra a esas máquinas virtuales.
  - **Citrix Provisioning Services (PVS)** Crea un catálogo de máquinas virtuales aprovisionadas mediante MCS y de las que se han creado imágenes mediante PVS. Esas máquinas virtuales funcionan como dispositivos de destino de PVS y el servidor PVS puede transmitirles una única imagen de disco compartida.

    > **Nota:**
    >
    > * Esta opción solo está disponible para los sitios de PVS registrados en Citrix Cloud y actualmente está limitada a los recursos de Azure.
    > * Al crear un catálogo de Citrix Provisioning, en la página **Dispositivo de destino**, es posible que vea que, en el menú desplegable para seleccionar la comunidad y el sitio para las máquinas que se van a aprovisionar, aparecen comunidades y sitios que ya no existen. Como solución temporal, puede ejecutar el comando PowerShell `Unregister-HypPvsSite` para eliminar las comunidades y los sitios de la base de datos. Para obtener información sobre el comando de PowerShell, consulte Unregister-HypPvsSite.

- **Otro servicio o tecnología** Una herramienta que administra las 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)

> **Nota:**
>
> Las opciones de la página **Experiencia de escritorio** varían según el tipo de máquina que seleccione en la página **Tipo de máquina**.

- En las máquinas con **sistema operativo multisesión**, a los usuarios se les asigna un escritorio aleatorio cada vez que inician sesión. Seleccione una de estas opciones:
  - **Sí, guardar los cambios en el disco local de la máquina que aloja los escritorios virtuales.** (Persistente)
  - **No; descartar todos los cambios y eliminar el escritorio virtual cuando el usuario cierre la sesión.** (No persistente)

  > **Nota:**
  >
  > En el caso de las máquinas multisesión persistentes, los cambios que hagan los usuarios en los escritorios se guardarán y podrán acceder a ellos todos los usuarios autorizados.

- En el caso de las máquinas con **sistema operativo de sesión única**, tiene disponibles las siguientes opciones en la página **Experiencia de escritorio**:
  - **Quiero que los usuarios se conecten a un escritorio nuevo (aleatorio) cada vez que inicien sesión.**
  - **Quiero que los usuarios se conecten al mismo escritorio (estático) cada vez que inicien sesión.**

    Además, para los escritorios estáticos, puede decidir si los cambios realizados por los usuarios se guardarán o se descartarán después de cerrar sesión.

Imagen

Esta página solo aparece cuando se utiliza Machine Creation Services para crear máquinas virtuales.

1. Seleccione un tipo de imagen para el catálogo de máquinas y, a continuación, seleccione una imagen. Hay dos tipos de imágenes disponibles:
   - **Imagen maestra.** Una imagen que no ha pasado por el proceso de preparación de imágenes. El proceso de preparación de imágenes se inicia automáticamente cuando se inicia la creación del catálogo.

     > **Nota:**
     >
     > - Si utiliza Machine Creation Services, no debe ejecutar Sysprep en las imágenes maestras.
     > - Si especifica una imagen maestra en lugar de una instantánea, Web Studio creará

> una instantánea, pero usted no le podrá asignar ningún nombre.

- **Imagen preparada.** Una imagen que ha pasado por el proceso de preparación de imágenes y que se puede usar directamente para la creación de máquinas virtuales. Al optar por imágenes preparadas en lugar de imágenes maestras, el proceso de creación de catálogos es más rápido y fiable, a la vez que se optimiza la administración de las imágenes durante todo el ciclo de vida.

  > **Nota:**
  >
  > – Las máquinas virtuales creadas mediante imágenes preparadas no admiten la hibernación.
  > – Actualmente, la creación de catálogos con imágenes preparadas solo está disponible en entornos de Azure y VMware.

Para obtener más información sobre cómo crear imágenes preparadas, consulte Administración de imágenes (Technical Preview).

Al seleccionar una imagen, puede agregar una nota relativa a la imagen seleccionada si es necesario.

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.

2. Para usar una máquina virtual existente como perfil de máquina, seleccione **Usar un perfil de máquina** y después seleccione la máquina virtual.

   > **Nota:**
   >
   > Actualmente, el uso de perfiles de máquina está restringido a máquinas virtuales de Azure, AWS, GCP y VMware.

   En el caso de las implementaciones de VMware, al crear un catálogo de máquinas mediante un perfil de máquina, debe especificar la carpeta en la que quiere guardar las máquinas virtuales.

   Para proporcionar la ubicación de la carpeta de las máquinas virtuales, en el asistente de creación de catálogos, vaya a la página **Máquinas virtuales**, a continuación, a **Seleccione una carpeta para colocar las máquinas** y seleccione la ubicación para la carpeta de las máquinas virtuales. Si no se especifica, el sistema considera la carpeta del perfil de máquina seleccionado como la ubicación predeterminada.

3. Seleccione el nivel funcional mínimo para el catálogo. Para que pueda utilizar las funciones más recientes del producto, compruebe que la imagen maestra tiene instalada la versión más reciente de VDA.

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. Introduzca **0** (cero) si no quiere crear ninguna. Más adelante, puede crear máquinas virtuales para un catálogo vacío mediante **Agregar máquinas**.
- Seleccione la cantidad de memoria (en MB) que tendrá cada máquina virtual.
- Cada máquina virtual creada tendrá un disco duro. El tamaño se este se configura en la imagen maestra. No se puede cambiar el tamaño del disco duro en el catálogo.
- 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 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.

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 otras herramientas (pero no MCS):

Un icono y un cuadro de información emergente acerca de cada máquina agregada (o importada) pueden ayudarle a identificar aquellas máquinas que no sean aptas para ser agregadas al catálogo o no puedan registrarse en un Delivery Controller. Para obtener más información, consulte Niveles funcionales y versiones de VDA.

Agregar SID al crear máquinas virtuales

Ahora puede agregar el parámetro `ADAccountSid` para identificar unívocamente las máquinas al crear nuevas máquinas virtuales.

Para hacerlo:

1. Cree un catálogo con el tipo de identidad admitido.
2. Agregue máquinas al catálogo mediante `NewProvVM`. Por ejemplo:

```
New-ProvVM  -ProvisioningSchemeName "name"  -ADAccountSid @("SID "
    )  -RunAsynchronously
```

Sin embargo, no puede aprovisionar una máquina con:

- Una cuenta de AD que no esté en el grupo de identidades del catálogo
- Una cuenta de AD que no esté disponible

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. El artículo Novedades de cada versión indica cualquier cambio en el nivel funcional predeterminado.

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:**
>
> En la versión 1811, se agregó 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. Sin embargo, si el catálogo solo contiene VDA 1811 o versiones posteriores admitidas, todos podrán registrarse. Esto incluye catálogos que contienen agentes VDA configurados para versiones posteriores de Citrix Virtual Apps and Desktops, incluidas la versión 1903 y otras versiones 19XX anteriores a la versión actual.

Configurar la caché de datos temporales

Al usar MCS para administrar máquinas aleatorias no persistentes en un catálogo, puede habilitar la memoria caché de reescritura para las máquinas a fin de mejorar el rendimiento de E/S.

La memoria caché de reescritura se denomina E/S de MCS. Para obtener más información, consulte este artículo del blog.

Requisitos previos Para habilitar la memoria caché de reescritura, el catálogo debe cumplir estos requisitos:

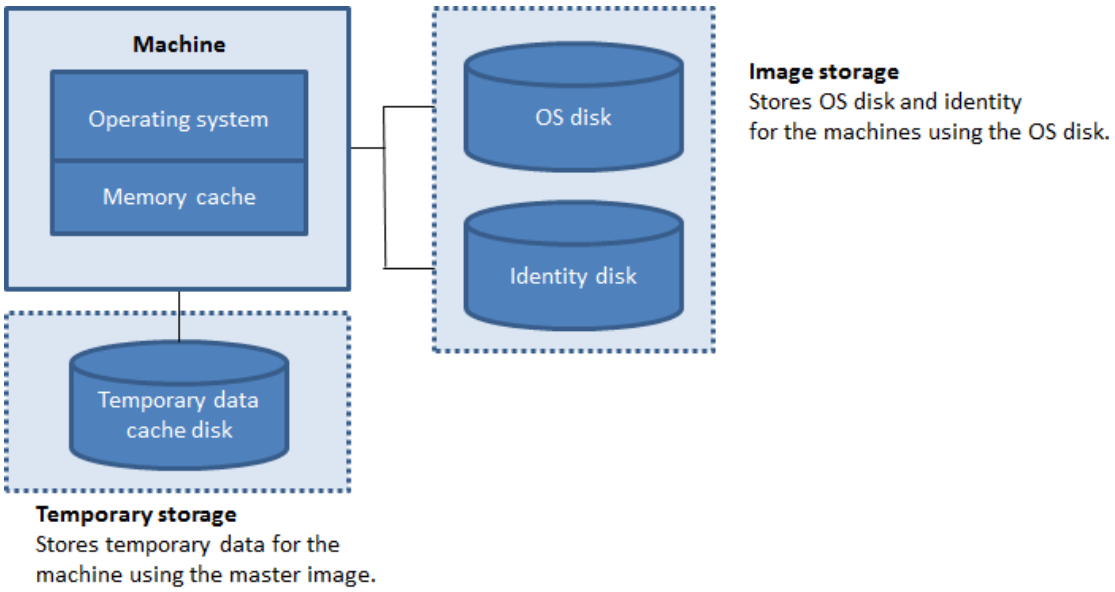
- Debe usar una conexión que especifique el almacenamiento de datos temporales. Para obtener más información, consulte Conexiones y recursos.
- Los VDA deben tener al menos la versión 7.9 e instalarse con un controlador de E/S de MCS actual.

  > **Nota:**
  >
  > La instalación de este controlador es una opción cuando instala o actualiza la versión de un VDA. De forma predeterminada, ese controlador no se instala.

- Para habilitar la asignación de letras de unidad para las cachés de disco, las máquinas virtuales deben cumplir estos requisitos adicionales:
  - Sistema operativo: Windows
  - Versión de VDA: 2305 o una posterior

Consideraciones

- Las memorias cachés de reescritura vienen en caché de *memoria* y en caché de *disco*. De forma predeterminada, sus valores predeterminados varían según el tipo de conexión. Por lo general, los valores predeterminados son suficientes para la mayoría de los casos, sin embargo, considere 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.



- La configuración de la caché de reescritura con solo una memoria caché de disco y sin memoria caché ha quedado obsoleta. Para habilitar una caché para datos temporales, recomendamos seleccionar **Tamaño de caché de disco (GB)** y **Memoria asignada para caché (MB)** y especificar un tamaño superior a 0 para la memoria caché. Los datos temporales se escriben inicialmente en la memoria caché. Cuando la memoria caché alcanza su límite configurado, los datos más antiguos se trasfieren al disco de caché de datos temporales.
- La memoria caché es parte de la memoria total de cada máquina. Por lo tanto, si habilita la casilla **Tamaño de memoria caché (MB) (recomendado)**, considere aumentar la cantidad total de memoria en cada máquina.
- Si mantiene la casilla **Tamaño de memoria caché (MB) (recomendado)** sin marcar, los datos temporales se escriben directamente en la memoria caché del disco, lo que emplea una cantidad mínima de memoria.
- Cambiar el valor predeterminado del **tamaño de la caché del disco (GB)** puede afectar al rendimiento. El tamaño debe coincidir con los requisitos de los usuarios y la carga que se coloca en la máquina.

  > **Importante:**
  >
  > Si la memoria caché de disco se queda sin espacio, la sesión del usuario se vuelve inutilizable.

- Si desmarca la casilla **Tamaño de caché de disco**, no se creará ninguna caché de disco. En este caso, especifique un valor de **Memoria asignada para caché** que sea suficiente para contener todos los datos temporales. Esto es factible solo si hay grandes cantidades de RAM disponibles para asignarse a cada VM.

- Si deja sin marcar ambas casillas, los datos temporales no se almacenan en caché. Se escriben en el disco de diferenciación (ubicado en el almacenamiento de SO) para cada VM. (esta es la acción de aprovisionamiento en las versiones anteriores a la 7.9).
- No habilite el almacenamiento en caché si va a usar este catálogo para crear AppDisks.
- No puede cambiar los valores de caché en un catálogo de máquinas después de haberlo creado.

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.

Al agregar unidades organizativas, puede hacer lo siguiente si el dominio no aparece en la lista:

- Buscarlo mediante una coincidencia exacta.
- Buscar en todos los dominios para encontrarlo.

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.

Identidades de las máquinas

Esta página solo aparece cuando se utiliza Machine Creation Services para crear máquinas virtuales.

Cada máquina del catálogo debe tener una identidad única. Esta página le permite configurar las identidades de las máquinas del catálogo. Las máquinas se unen a la identidad después de aprovisionarse. No se puede cambiar el tipo de identidad después de crear el catálogo.

Un flujo de trabajo general para configurar los parámetros de esta página es el siguiente:

1. Seleccione una identidad de la lista.
2. Indique si se van a crear cuentas o si se van a utilizar cuentas existentes, además de la ubicación (dominio) de estas.

Se pueden seleccionar una de las siguientes opciones:

- **Active Directory local**. Máquinas propiedad de una organización en las que se ha iniciado sesión con una cuenta de Active Directory perteneciente a esa organización. Están presentes en instancias locales.
- **Unido a Azure Active Directory híbrido**. Máquinas propiedad de una organización en las que se ha iniciado sesión con una cuenta de Active Directory Domain Services perteneciente a esa organización. Existen en la nube y en instancias locales. Para obtener información sobre los requisitos, las limitaciones y los aspectos a tener en cuenta, consulte Unido a Azure Active Directory híbrido.

  > **Nota:**
  >
  > - Antes de poder usar la opción de unido a Azure Active Directory híbrido, asegúrese de que su entorno de Azure cumpla con los requisitos previos. Consulte https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-managed-domains.
  > - Esta opción requiere que la imagen maestra cumpla los requisitos del sistema operativo. Para obtener más información, consulte la documentación de Microsoft: https://learn.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join-hybrid.

> **Importante:**
>
> - Si selecciona **Active Directory local** o **Unido a Azure Active Directory híbrido** como el tipo de identidad, cada máquina del catálogo debe tener una cuenta de equipo de Active Directory correspondiente.

Si crea cuentas, debe tener permiso para crear cuentas de equipo en la unidad organizativa donde residen las máquinas. Cada máquina del catálogo debe tener un nombre exclusivo. Especifique el esquema de denominación de cuentas para las máquinas que quiere crear. Para obtener más información, consulte Esquema de nomenclatura de cuentas de máquina.

> **Nota:**
>
> Asegúrese de que en los nombres de las unidades organizativas no se utilizan barras inclinadas hacia delante (`/`).

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:

- [ADComputerAccount] ADcomputeraccountname.domain

Compruebe que hay cuentas suficientes para las máquinas que está agregando. La interfaz de Web Studio administra esas cuentas. Por eso, permita que dicha interfaz 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.

Esquema de nomenclatura de cuentas de máquina

Cada máquina de un catálogo debe tener un nombre único. Debe especificar un esquema de nomenclatura de cuentas de máquina al crear un catálogo. Use comodines (marcas hash) como marcadores de posición para los números o letras secuenciales que aparecen en el nombre.

Al especificar un esquema de nomenclatura, tenga en cuenta las siguientes reglas:

- El esquema de nomenclatura debe contener, al menos, un comodín. Debe poner todos los comodines juntos.
- El nombre completo, incluidos los comodines, debe contener al menos 2 caracteres, pero no más de 15. Debe incluir al menos un carácter no numérico y un carácter # (comodín).
- El nombre no debe incluir espacios ni ninguno de estos caracteres: `,~!@'$%^&.()} {\/*?"<>|=+[];:_".`.
- El nombre no puede terminar con un guion (-).

Además, deje suficiente espacio para que crezca cuando especifique el esquema de nomenclatura. Considere este ejemplo: Si crea 1000 cuentas de máquina con el esquema "granlongitud#", el último nombre de cuenta creado (granlongitud1000) contiene 16 caracteres. Por tanto, el esquema de nomenclatura genera al menos un nombre de máquina que supera el máximo de 15 caracteres.

Puede indicar si los valores secuenciales son números (0-9) o letras (A-Z):

- **0-9**. Si se selecciona, los comodines especificados se traducen a números secuenciales.

  > **Nota:**
  >
  > Si solo hay un comodín (#), los nombres de las cuentas comienzan por 1. Si hay dos, los nombres de las cuentas comienzan por 01. Si hay tres, los nombres de las cuentas comienzan por 001, y así sucesivamente.

- **A-Z**. Si se selecciona, los comodines especificados se traducen a letras secuenciales.

Por ejemplo, un esquema de denominación PC-Ventas-## (con números del **0 al 9** seleccionados) da como resultado cuentas llamadas PC-Ventas-01, PC-Ventas-02, PC-Ventas-03, etc.

Si lo quiere, puede especificar con qué empiezan los nombres de las cuentas.

- Si selecciona **0-9**, las cuentas se designan secuencialmente, empezando por los números especificados. Introduzca uno o más dígitos, según el número de comodines que utilice en el campo anterior. Por ejemplo, si usa dos comodines, introduzca dos dígitos o más.
- Si selecciona **A-Z**, las cuentas se designan secuencialmente, empezando por las letras especificadas. Introduzca una o más letras, según el número de comodines que utilice en el campo anterior. Por ejemplo, si usa dos comodines, introduzca dos letras o más.

Credenciales de dominio

Seleccione **Introducir credenciales** e introduzca las credenciales de un administrador con permiso para realizar operaciones de cuentas en el dominio de Active Directory de destino.

Utilice la opción **Comprobar nombre** para comprobar si el nombre de usuario es válido o único. La opción es útil, por ejemplo, cuando:

- El mismo nombre de usuario existe en varios dominios. Se le solicita que seleccione el usuario correspondiente.
- No se acuerda del nombre del dominio. Puede introducir el nombre del usuario sin especificar el nombre del dominio. Si la comprobación se realiza correctamente, el nombre del dominio se rellena automáticamente.

> **Nota:**
>
> Si el tipo de identidad que seleccionó en **Identidades de máquina** es **Unido a Azure Active Directory híbrido**, las credenciales que introduzca deben tener el permiso `Write userCertificate`.

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 Web Studio.

Cuando termine, haga clic en **Finalizar** para iniciar la creación del catálogo.
Cuando haya terminado, seleccione **Finalizar** para iniciar la creación del catálogo.

En **Catálogos de máquinas**, el nuevo catálogo aparece con una barra de progreso integrado.

Para ver los detalles del progreso de la creación:

1. Pase el mouse por encima del catálogo de máquinas.

2. En el texto de ayuda que aparece, haga clic en **Ver detalles**.

   Aparece un gráfico de progreso detallado en el que puede ver lo siguiente:

   - Historial de los pasos
   - Progreso y tiempo de ejecución del paso actual
   - Pasos restantes

Sincronización horaria de MCS

La sincronización horaria viene determinada por la imagen maestra y el tipo de identidad de la máquina unida al catálogo. Obtendrá este método de sincronización horaria según la imagen maestra y el catálogo:

Imagen maestra	Catálogo	Método de sincronización horaria resultante
NDJ	AD o Azure AD híbrido	De forma predeterminada, NT5DS. Puede inhabilitar MCS para que no cambie el parámetro de sincronización horaria mediante los parámetros del Registro de la imagen maestra.
NDJ	No unido a ningún dominio (NDJ) o Azure AD	Igual que el parámetro de sincronización horaria original
AD o Azure AD híbrido	AD o Azure AD híbrido	Igual que el parámetro de sincronización horaria original
Azure AD	Azure AD	Igual que el parámetro de sincronización horaria original

> **Nota:**
>
> La sincronización horaria original se controla mediante este parámetro del Registro y no se puede cambiar:
>
> - Equipo\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config
>
> Valor: MaxAllowedPhaseOffset, MaxNegPhaseCorrection, and MaxPosPhaseCorrection
>
> - Equipo\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters

> Valor: Tipo

Para impedir que MCS cambie el parámetro de sincronización horaria, establezca el valor de este parámetro del Registro en la imagen maestra:

- `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix`
- Nombre: TimeSyncMethodKeep
- Tipo: DWORD
- 0 (o el valor TimeSyncMethodKeep no está configurado): No conserva el parámetro original de sincronización horaria.
- 1: Conserva el parámetro original de sincronización horaria y los valores de los parámetros predeterminados.

Consideraciones importantes sobre la configuración de propiedades personalizadas

Las propiedades personalizadas se deben establecer correctamente en `New-ProvScheme` y `Set-ProvScheme` en entornos de GCP y Azure. Si especifica propiedades personalizadas que no existen, aparece este mensaje de error y los comandos no se ejecutan.

- En Azure: `Invalid property found: <invalid property>. Ensure that the CustomProperties parameter supports the property.`
- En GCP: `Invalid property found: <invalid property>. Ensure that the value supplied for the property is supported in the Hypervisor.`

Solucionar problemas

> **Importante:**
>
> Después de crear el catálogo de máquinas con Web 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 a que Web 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-ProvServiceConfigurati -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 Imageprep.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`.

Problemas de preparación de imagen

Debido a que MCS crea muchas máquinas a partir de una sola imagen, se deben realizar algunos pasos para asegurarse de que todas las máquinas tienen identificadores únicos y licencias correctas. La preparación de imágenes forma parte del proceso de creación de catálogos. Esta preparación garantiza que todas las máquinas aprovisionadas tengan direcciones IP únicas y se anuncien correctamente al servidor KMS como instancias únicas. En MCS, la preparación de la imagen se produce después de seleccionar la instantánea de la imagen maestra. Se realiza una copia para que el catálogo se aísle de la máquina seleccionada. Se crea una máquina virtual de *preparación*, basada en la máquina virtual original, pero con la conexión de red desconectada. Al desconectar la conexión de red, se evitan conflictos con otras máquinas, y se garantiza que la máquina virtual preparada solo esté conectada al disco recién copiado.

Se adjunta a la máquina virtual preparada un pequeño disco de *instrucciones* que contiene los pasos necesarios para ejecutar la preparación de la imagen. Cuando arranca esa máquina virtual preparada, comienza el proceso de preparación de imagen. La preparación de imagen consta de los siguientes procesos:

- Activación del protocolo de configuración dinámica de host (DHCP). Habilitar DHCP garantiza que las máquinas aprovisionadas no causen conflictos de direcciones IP. DHCP está habilitado en todas las tarjetas de red.
- Rearmado de Key Management Server (KMS) de Microsoft Windows. El rearmado de KMS garantiza que Microsoft Windows tenga una licencia correcta. Se invoca el sistema operativo rearmado para que informe correctamente como una instancia nueva al servidor de licencias de KMS.
- Rearmado de KMS de Microsoft Office (si Microsoft Office está instalado). Rearmar Microsoft Office garantiza que cualquier versión de Microsoft Office (a partir de 2010) se registre correctamente en el servidor KMS. Una vez invocado el rearmado de Microsoft Office, informa como una instancia nueva al servidor de licencias de KMS.

> **Sugerencia:**
>
> Cuando finaliza el proceso de preparación de imagen, el disco de instrucciones se obtiene del hipervisor. El hipervisor contiene la información obtenida del proceso de preparación de imagen.

El proceso de preparación de imagen puede fallar por varios motivos. Aparece un mensaje de error similar al siguiente: Falló el rearmado de Office para preparación de imagen.

Estos fallos se analizan en las siguientes secciones.

Habilitar DHCP Estos errores se deben a tarjetas de red que no admiten direcciones IP estáticas. Por ejemplo: versiones anteriores de tarjetas de red Dell SonicWALL. La operación falla porque la tarjeta SonicWALL es una tarjeta de red de firewall, por lo que establecer la tarjeta en DHCP no tiene sentido, ya que solo admite DHCP. Este problema se solucionó en versiones posteriores de Citrix Virtual Apps and Desktops. Sin embargo, si el problema aparece en otros tipos de tarjetas de red, debe informarse a Citrix a través de los foros o de la persona de contacto de asistencia técnica.

> **Nota:**
>
> La configuración de PowerShell de los ejemplos siguientes se aplica al sitio de Citrix Virtual Apps and Desktops, por lo que afecta a todos los catálogos nuevos y actualizaciones de imagen realizadas en catálogos existentes.

Si este problema se produce con otras tarjetas de red, puede resolverlo ejecutando un comando de PowerShell en el Delivery Controller:

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps
 -Value EnableDHCP
```

Rearmar Microsoft Office Existen varios errores de rearmado de KMS que pueden producirse durante la etapa de rearmado de Microsoft Office. Los principales fallos son:

- Algunos runtimes de Microsoft Office (por ejemplo, **Access Runtime**) pueden invocar el rearmado de Office, lo que provoca el fallo de la operación.
- No se ha instalado una versión KMS de Microsoft Office.
- Se ha superado el recuento de rearmados.

Si el error es un falso positivo, puede resolverlo ejecutando el siguiente comando de PowerShell en el Delivery Controller:

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps
 -Value OfficeRearm
```


Rearmar Microsoft Windows Se pueden producir varios fallos de KMS durante la etapa de rearmado de Microsoft Windows. Los principales fallos son:

- La versión de Windows instalada no se activó mediante KMS. Por ejemplo: se utilizó una clave de activación múltiple (MAK).
- Se ha superado el recuento de rearmados.

Si la versión de Microsoft Windows tiene una licencia correcta, puede borrar el rearmado del sistema operativo ejecutando el siguiente comando de PowerShell en el Delivery Controller:

```
Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps
 -Value OsRearm
```

Instancias de fallo de toda la operación La máquina de preparación de imagen no está conectada a la red por diseño, esto significa que a veces la etapa de preparación de imagen solo puede informar de un fallo del proceso completo. Un ejemplo de este tipo de error es similar al siguiente: Error al preparar la imagen de la VM maestra. Asegúrese de que la imagen seleccionada tiene un SO compatible (por ejemplo, Windows 7) y de que tiene instalada la versión correcta de VDA (7.0 o posterior).

A continuación, dispone de los motivos principales de fallo de toda la operación:

Virtual Delivery Agent (VDA) no está instalado o está instalado VDA 5.x Si VDA 7.x no está instalado en la imagen maestra, se agota el tiempo de preparación de imagen después de 20 minutos y se informa del error anterior. Esto se debe a que no hay ningún software instalado en la imagen maestra para ejecutar la etapa de preparación de imagen e informar de fallo u operación correcta. Para resolver este problema, compruebe que el VDA (versión mínima 7) está instalado en la instantánea seleccionada como imagen maestra.

Directiva `DISKPART SAN` La etapa completa de preparación de imagen puede fallar debido a la directiva `DISKPART SAN` establecida en la imagen maestra. Si esta directiva no está configurada para poner en línea el disco de instrucciones de preparación de imagen, la máquina se apaga e Image preparation (preparación de imagen) informa de un error después de 20 minutos. Para comprobarlo en la imagen maestra, ejecute los siguientes comandos:

```
1 C:>; Diskpart.exe
2 DISKPART>; San
```

Este comando devuelve la directiva actual. Si no es *Online All*, cambie este valor ejecutando el siguiente comando:

```
DISKPART>; San policy=OnlineAll
```

Apague la imagen maestra, cree una instantánea de esa máquina y, a continuación, úsela como imagen base de MCS.

Si la preparación de imagen falla por otro motivo Si la preparación de imagen falla y no hay una razón clara para el fallo, puede omitir el proceso de preparación de imagen al crear un catálogo de MCS. Sin embargo, omitir este proceso puede causar problemas con las licencias y redes de KMS (DHCP) en el sitio. Utilice el siguiente comando de PowerShell:

```
Set-ProvServiceConfigurationData -Name
    ImageManagementPrep_DoImagePreparation -Value $false
```

Siempre que sea posible, recopile registros para el equipo de asistencia de Citrix Support, o bien, informe del problema a Citrix a través de foros o a través de la persona de contacto de asistencia técnica. Para recopilar 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. En el Delivery Controller, inicie PowerShell con los complementos de Citrix PowerShell cargados y ejecute `Set-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown -Value $True`.
3. Cree un catálogo basado en esa instantánea.
4. Cuando se cree la VM de preparación en el hipervisor, inicie sesión y extraiga los siguientes archivos desde la raíz C:

```
Image-prep.log
PvsVmAgentLog.txt
```

Apague la máquina. En este punto, la máquina informa del fallo.

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
```

Asignar una letra de unidad específica a un disco de la memoria caché de reescritura de E/S de MCS

Puede asignar una letra de unidad específica a un disco de la memoria caché de reescritura de E/S de MCS. Esta implementación le ayuda a evitar conflictos entre la letra de la unidad de cualquier aplicación que utilice y la letra de la unidad del disco de la memoria caché de reescritura de E/S de MCS. Para hacer esto, puede ser comandos de PowerShell. Los hipervisores compatibles son Azure, GCP, VMware, SCVMM y XenServer.

> **Nota:**
>
> Esta función requiere la versión 2305 de VDA o una posterior.

Limitaciones

- Aplicable solo al sistema operativo Windows
- Letra de unidad aplicable al disco de la memoria caché de reescritura: De E a Z
- No se aplica cuando el disco temporal de Azure se utiliza como disco de la memoria caché de reescritura
- Aplicable solo cuando al crear otros catálogos de máquinas

Asignar una letra de unidad a un disco de la memoria caché de reescritura

Para asignar una letra de unidad al disco de la memoria caché de reescritura:

1. Abra la ventana de **PowerShell**.
2. Ejecute `asnp citrix*`.
3. Cree un grupo de identidades si aún no se ha creado. Para obtener más información, consulte Creación de un catálogo.
4. Cree un esquema de aprovisionamiento mediante el comando `New-ProvScheme` con la propiedad `WriteBackCacheDriveLetter`. Por ejemplo:

```
New-ProvScheme -CleanOnBoot `
-HostingUnitName "<name>" `
-IdentityPoolName $schemeName `
-ProvisioningSchemeName $schemeName `
-InitialBatchSizeHint 1 `
-UseWriteBackCache -WriteBackCacheDiskSize 127 -
   WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `
-MasterImageVM "XDHyp:\HostingUnits<name>\image.folder\abcd-
   resources.resourcegroup\
   MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxx2130aa145ec77.
   manageddisk" `
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\name\virtualprivatecloud.folder\East US.
    region\virtualprivatecloud.folder\abcd-resources.resourcegroup
    \abcd-resources-vnet.virtualprivatecloud\default.network" }
  `
-ServiceOffering "XDHyp:\HostingUnits\<name>\serviceoffering.
   folder\Standard_D2s_v5.serviceoffering" `
-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="OsType" Value="Windows"
   />
<Property xsi:type="StringProperty" Name="StorageType" Value="
   Premium_LRS"/>
```



```
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false
    " />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="
    false" />
<Property xsi:type="StringProperty" Name="PersistVm" Value="false"
     />
<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
    Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value
    ="false" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
    abcd-group1" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2"
     />
</CustomProperties>'
```

5. Termine de crear el catálogo.

Validar la configuración antes de crear un catálogo de máquinas MCS

Puede validar los parámetros de configuración antes de crear un catálogo de máquinas MCS mediante el parámetro `-validate` del comando `New-ProvScheme`. Después de ejecutar este comando de PowerShell con ese parámetro, se muestra el mensaje de error correspondiente si se usa un parámetro incorrecto o si un parámetro está en conflicto con otro parámetro. A continuación puede usar el mensaje de error para resolver el problema y crear sin problemas un catálogo de máquinas MCS con PowerShell. Actualmente, esta función se aplica a los entornos de virtualización de Azure, GCP y VMware.

> **Nota:**
>
> Durante la validación, no debe crear un catálogo de máquinas MCS real. Debe usar el resultado del comando para corregir los errores y después crear un catálogo correcto. Por lo tanto, mientras ejecuta el comando `New-ProvScheme`, use un nombre de grupo de identidades falso.

Para validar la configuración, lleve a cabo los siguientes pasos:

1. Abra una ventana de PowerShell desde el host del Delivery Controller.
2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
3. Ejecute el comando `New-ProvScheme` y use el parámetro `-validate`. Proporcione un nombre de grupo de identidades falso para que el comando funcione. Por ejemplo,

```
$result =New-ProvScheme  -CleanOnBoot -HostingUnitName "vSanRg" -
    IdentityPoolName "mptmpcatalogdemo" -InitialBatchSizeHint 1  -
    MasterImageVM "XDHyp:\HostingUnits\vSanRg\Windows19MasterImage.
    vm\Citrix_XD_NonMachineProfileWin19Machines.snapshot" -
    NetworkMapping @{
```



```
 "0"="XDHyp:\HostingUnits\vSanRg\VM Network.network" }
  -ProvisioningSchemeName "MachineProfileW10Machines"  -Scope @()
-VMCpuCount 2  -VM
MemoryMB 6143 -MachineProfile "XDHyp:\HostingUnits\vSanRg\TRW-
   Win11-tpm-BL-TEMPLATE.template" -TenancyType Shared  -
   FunctionalLevel "L7_20" -Validate
$result.TerminatingError | Format-List -Property *
```

Mensaje de error:

```
ErrorData    : {
 [[ValidationFailureCount, xxx], [InvalidMemoryValue, The memory
    size provided 6143 must be a multiple of 4 MB and must be
    greater than or equal to 4 MB.], [InconsistentGuestOsSetting,
    The GuestOs setting - windows9_64Guest of the selected machine
     profile does not match with the setting -
    windows2019srv_64Guest of master image. Please select a
    machine profile that matches the GuestOs setting of the master
     image.], [InconsistentVtpmSetting, The vTPM setting of the
    selected machine profile does not match with the selected
    master image. Please select a machine profile that matches the
     vTPM setting of the master image.], [
    InconsistentFirmwareSetting, The firmware setting - efi of the
     selected machine profile does not match with the setting -
    bios of master image. Please select a machine profile that
    matches the firmware setting of the master image ErrorId
    : ValidationFailure
ErrorMessage : ValidationFailure
Operation    : ValidatingInputs
```

4. Tras validar los parámetros de configuración, puede crear un catálogo de máquinas MCS con un nombre real del grupo de identidades y los parámetros correctos.

Qué hacer a continuación

Para obtener información sobre la creación de catálogos de servicios en la nube específicos, consulte:

- Crear un catálogo de AWS
- Crear un catálogo de XenServer
- Crear un catálogo de Google Cloud Platform
- Crear un catálogo de Microsoft Azure
- Crear un catálogo de Microsoft System Center Virtual Machine Manager
- Crear un catálogo de Nutanix
- Crear un catálogo de VMware

Si este es el primer catálogo creado, Web Studio le guiará para crear un grupo de entrega.

Para revisar todo el proceso de configuración, consulte Instalar y configurar.

Ahora puede crear un catálogo de Citrix Provisioning mediante la interfaz de usuario de Configuración completa y PowerShell.
Esta implementación le ofrece las siguientes ventajas:

- Una única consola unificada para administrar los catálogos de MCS y de Citrix Provisioning.
- Hay nuevas funciones para los catálogos de Citrix Provisioning, como la solución de administración de identidades, el aprovisionamiento bajo demanda, etc.

Actualmente, esta función solo está disponible para las cargas de trabajo de Azure y VMware. Sin embargo, en los entornos VMware, actualmente puede crear los catálogos utilizando únicamente comandos de PowerShell. Para obtener más información, consulte Crear catálogos de Citrix Provisioning en Citrix Studio.

Más información

- Crear y administrar conexiones y recursos
- Crear catálogos de diferentes tipos de unión
- Administrar catálogos de máquinas

Crear un catálogo de AWS

August 17, 2024

Crear catálogos de máquinas describe los asistentes con los que se crea un catálogo de máquinas. La siguiente información incluye detalles específicos de los entornos de virtualización de AWS.

> **Nota:**
>
> Antes de crear un catálogo de AWS, debe terminar de crear una conexión con AWS. Consulte Conexión con AWS.

Configuración de la red durante la preparación de imágenes

Durante la preparación de la imagen, se crea una máquina virtual (VM) de preparación basada en la máquina virtual original. Esta máquina virtual de preparación está desconectada de la red. Para desconectar la red de la máquina virtual de preparación, se crea un grupo de seguridad de red para denegar todo el tráfico entrante y saliente. Este grupo de seguridad de red persiste y se reutiliza. El nombre del grupo de seguridad de red es `Citrix.XenDesktop.IsolationGroup-GUID`, donde el GUID se genera aleatoriamente.

Configurar el arrendamiento de AWS

AWS ofrece las siguientes opciones de arrendamiento:

- Arrendamiento compartido (el tipo predeterminado): Varias instancias de Amazon EC2 de diferentes clientes pueden residir en el mismo hardware físico.
- Arrendamiento dedicado: Sus instancias de EC2 se ejecutan únicamente en hardware con otras instancias que haya implementado. Los demás clientes no utilizan el mismo hardware.

Puede usar MCS para aprovisionar hosts dedicados de AWS a través de PowerShell.

Configurar el arrendamiento de host dedicado de AWS mediante PowerShell

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.

Capture las propiedades de la máquina desde las AMI

Cuando crea un catálogo para aprovisionar máquinas con Machine Creation Services (MCS) en AWS, selecciona una imagen AMI que represente la imagen maestra de ese catálogo. A partir de esa imagen AMI, MCS utiliza una instantánea del disco. En versiones anteriores, si quería incluir roles o etiquetas en sus máquinas, tenía que usar la consola de AWS para definirlos individualmente. Esta funcionalidad está habilitada de forma predeterminada.

> **Sugerencia:**
>
> Para utilizar la captura de propiedades de instancias de AWS, debe tener una máquina virtual asociada a la imagen AMI.

Para mejorar este proceso, **MCS lee** las propiedades de la instancia de la que se obtuvo la imagen AMI y aplica el rol y etiquetas de IAM (Administración de acceso e identidad) de la máquina a las máquinas aprovisionadas de un catálogo determinado. Cuando se utiliza esta función opcional, el proceso de creación de catálogos busca la instancia AMI de origen seleccionada, leyendo un conjunto limitado de propiedades. Estas propiedades se almacenan en una plantilla de inicio de AWS, que sirve para aprovisionar las máquinas de ese catálogo. Cualquier máquina del catálogo heredará las propiedades de instancia capturadas.

Las propiedades capturadas incluyen:

- Roles de IAM: Aplicados a las instancias aprovisionadas.
- Etiquetas: Aplicadas a las instancias aprovisionadas, su disco y NIC. Estas etiquetas se aplican a los recursos transitorios de Citrix, incluidos: el depósito y objetos de S3, imágenes AMI, instantáneas y plantillas de inicio.

> **Sugerencia:**
>
> El etiquetado de los recursos transitorios de Citrix es optativo y se puede configurar mediante la propiedad personalizada `AwsOperationalResourcesTagging`.

Capturar la propiedad de instancia de AWS

Puede utilizar esta funcionalidad especificando una propiedad personalizada, `AwsCaptureInstancePropert`, al crear un esquema de aprovisionamiento para una conexión de host de AWS:

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true"
...<standard provscheme parameters
```

Consulte la documentación para desarrolladores de Citrix para obtener más información.

> **Nota:**
>
> `AwsCaptureInstanceProperties` se ha retirado. En su lugar, recomendamos usar perfiles de máquina para especificar las propiedades de las máquinas virtuales.

Capture las propiedades de la máquina desde los perfiles de la máquina

Al crear un catálogo para aprovisionar máquinas de AWS mediante MCS, puede usar un perfil de máquina para preestablecer ciertos parámetros de propiedades de la máquina.

Para ello, siga estos pasos:

1. Almacene los perfiles de las máquinas en la misma zona de disponibilidad que los recursos en los que va a crear este catálogo.
2. En la página **Plantilla de máquina** del asistente de creación de catálogos, seleccione **Usar un perfil de máquina**. Se muestran los perfiles de máquina que se encuentran en la misma zona disponible que los recursos que seleccionó.
3. Seleccione un perfil de máquina según sea necesario.

> **Nota:**
>
> Puede usar un perfil de máquina o una AMI para capturar las propiedades de la máquina. En Web Studio, al seleccionar **Usar un perfil de máquina**, la opción **Aplicar propiedades de plantilla de máquina a máquinas virtuales** se oculta automáticamente.

Etiquetar un recurso operativo de AWS

Al crear un catálogo para aprovisionar máquinas mediante MCS en AWS, puede decidir si aplicar las propiedades de etiqueta y el rol de IAM a esas máquinas. También puede decidir si aplicar etiquetas de máquina a los recursos operativos.

Una imagen AMI (Amazon Machine Image) representa un tipo de dispositivo virtual utilizado para crear una máquina virtual dentro del entorno de Amazon Cloud, conocido comúnmente como EC2. Puede utilizar una imagen AMI para implementar servicios que utilicen el entorno EC2. Cuando crea un catálogo para aprovisionar máquinas con MCS en AWS, selecciona una imagen **AMI** que sirve de imagen maestra para ese catálogo.

> **Importante:**
>
> La creación de catálogos mediante la captura de una propiedad de instancia y una plantilla de inicio es necesaria para utilizar el etiquetado de recursos operativos.

Para crear un catálogo de AWS, primero debe crear una imagen AMI de la instancia que quiere que sirva de imagen maestra. MCS lee las etiquetas de esa instancia y las incorpora a la plantilla de inicio. A continuación, las etiquetas de la plantilla de inicio se aplican a todos los recursos de Citrix creados en su entorno de AWS, incluidos:

- Máquinas virtuales
- Discos de VM
- Interfaces de red de VM
- Depósitos de S3
- Objetos de S3
- Plantillas de lanzamiento
- Imágenes AMI

Etiquetar un recurso operativo

Para usar PowerShell para etiquetar recursos:

1. Abra una ventana de PowerShell desde el host de DDC (Desktop Delivery Controller).
2. Ejecute el comando `asnp citrix` para cargar módulos de PowerShell específicos de Citrix.

Para etiquetar un recurso para una máquina virtual aprovisionada, utilice la nueva propiedad personalizada `AwsOperationalResourcesTagging`. La sintaxis de esta propiedad es:

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true;
AwsOperationalResourcesTagging,true"...<standard provscheme parameters
>
```

Copiar etiquetas en máquinas virtuales

Puede copiar las etiquetas de las NIC y los discos (disco de identidad, disco de caché de reescritura y disco de sistema operativo) que se especifican en el perfil de la máquina a las máquinas virtuales recién creadas en un catálogo de máquinas de MCS. Puede especificar estas etiquetas en cualquiera de las fuentes de perfiles de máquinas (instancia de máquina virtual de AWS o versión de plantilla de lanzamiento de AWS). Esta función se aplica a máquinas virtuales y catálogos de máquinas persistentes y no persistentes.

> **Nota:**
>
> - En la consola AWS EC2, no puede ver los valores de **Etiquetar interfaces de red** en las **etiquetas de recursos de la versión de la plantilla de lanzamiento**. No obstante, puede ejecutar el comando de PowerShell `aws ec2 describe-launch-template-versions --launch-template-id lt-0bb652503d45dcbcd --versions 12` para ver las especificaciones de las etiquetas.
> - Si un origen de perfil de máquina (máquina virtual o versión de plantilla de inicio) tiene dos interfaces de red (eni-1 y eni-2), y eni-1 tiene la etiqueta t1 y eni-2 tiene la etiqueta t2, la VM obtiene las etiquetas de las dos interfaces de red.

Crear un catálogo mediante un perfil de máquina

Puede usar un perfil de máquina para capturar las propiedades de hardware de una instancia de EC2 (VM) o versión de plantilla de inicio y aplicarlas a las máquinas aprovisionadas. Las propiedades que se capturan pueden incluir, por ejemplo, las propiedades del volumen de EBS, el tipo de instancia, la optimización de EBS, opciones de CPU, tipo de arrendamiento, capacidad de hibernación y otras configuraciones de AWS compatibles.

Puede usar una instancia (VM) de AWS EC2 o una versión de plantilla de inicio de AWS como entrada del perfil de máquina.

> **Nota:**
>
> - Las propiedades del volumen de EBS se derivan únicamente de un perfil de máquina.
> - MCS aprovisiona las máquinas virtuales con discos de identidad del tipo de volumen GP3. Como el tipo de volumen GP3 es la opción más económica que ofrece AWS, esta función minimiza los costes. La implementación solo se aplica a las máquinas virtuales agregadas a un nuevo catálogo y a las máquinas virtuales nuevas agregadas a un catálogo existente. Las máquinas virtuales existentes creadas antes de esta función seguirán teniendo discos de ID con el tipo de volumen GP2, a menos que se restablezca el disco de ID.

Consideraciones importantes

Consideraciones importantes a la hora de crear un catálogo de máquinas de MCS:

- Si agrega parámetros de propiedades de hardware de máquina en los comandos `New-ProvScheme` y `Set-ProvScheme`, los valores proporcionados en los parámetros sobrescriben los valores del perfil de máquina.
- Si asigna a `AwsCaptureInstanceProperties` el valor **`true`** y no establece la propiedad `MachineProfile`, solo se capturarán los roles y etiquetas de IAM.
- No puede establecer `AwsCaptureInstanceProperties` y `MachineProfile` al mismo tiempo.

  > **Nota:
  >
  > `AwsCaptureInstanceProperties` se ha retirado.

- Si no se proporciona un perfil de máquina, debe proporcionar explícitamente los valores de las siguientes propiedades:
  - Grupo de seguridad
  - ENI o red virtual
- Solo puede habilitar `AwsOperationalResourcesTagging` si habilita `AwsCaptureInstanceProper` o especifica un perfil de máquina.

Consideraciones importantes después de crear un catálogo de máquinas de MCS:

- No puede cambiar un catálogo de un catálogo basado en perfiles de máquinas a uno que no esté basado en perfiles de máquinas.

Crear un catálogo de máquinas mediante un perfil de máquina

Para crear un catálogo de máquinas mediante un perfil de máquina

1. Abra una ventana de **PowerShell**.
2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
3. Cree un grupo de identidades si aún no se ha creado. Por ejemplo,

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms## -
    Domain abcdf -NamingSchemeType Numeric
```

4. Ejecute el comando New-ProvScheme. Por ejemplo:

```
New-ProvScheme -ProvisioningSchemeName demet-test-1
-HostingUnitUid aa633238-9xxd-4cf6-80e8-232a758a1xx1
-IdentityPoolUid 34d5b088-e312-416f-907d-16573xxxxxc4
-CleanOnBoot
-MasterImageVM 'XDHyp:\HostingUnits\cvad-test-scalestress\citrix-
    demet-ami.0 (ami-0ca813xxxxxx061ef).template'
-MachineProfile 'XdHyp:\HostingUnits\cvad-test-scalestress\us-east
    -1a.availabilityzone\machine-profile-instance i (i-0xxxxxxxx).
    vm'
```

5. Complete la creación del catálogo. Para obtener más información, consulte SDK de PowerShell de Citrix.

Actualizar el perfil de las máquinas

Para actualizar el perfil de máquina en un catálogo al que inicialmente se aprovisionó un perfil de máquina, haga lo siguiente. También puede cambiar el tipo de arrendamiento y la capacidad de hibernación del origen del perfil de máquina mientras modifica un catálogo de máquinas de MCS.

1. Ejecute el comando `Set-ProvScheme`. Por ejemplo,

```
Set-ProvScheme `
-ProvisioningSchemeUid "<ID" `
-MachineProfile "XDHyp:\HostingUnits\abc\us-east-1a.
    availabilityzone\citrix-cvad-machineprofile-instance (i-0
    xxxxxxxx).vm"
```

Crear un catálogo con una versión de plantilla de inicio

Puede crear un catálogo de máquinas de MCS con una versión de plantilla de inicio como entrada del perfil de máquina. También puede actualizar la entrada de un catálogo de perfiles de máquina de

una máquina virtual a una versión de plantilla de inicio y de una versión de plantilla de inicio a una máquina virtual.

En la consola EC2 de AWS, puede proporcionar la información de configuración de instancia de una plantilla de inicio junto con el número de versión. Cuando se especifica la versión de la plantilla de inicio como entrada del perfil de máquina al crear o actualizar un catálogo de máquinas, las propiedades de esa versión de la plantilla de inicio se copian en las máquinas virtuales con VDA aprovisionadas.

Las siguientes propiedades se pueden proporcionar mediante la entrada del perfil de máquina o de forma explícita como parámetros en los comandos `New-ProvScheme` y `Set-ProvScheme`. Si se proporcionan en los comandos `New-ProvScheme` o `Set-ProvScheme`, tienen prioridad sobre los valores de estas propiedades del perfil de máquina.

- Oferta de servicios
- Redes
- Grupos de seguridad
- Tipo de arrendamiento

> **Nota:**
>
> Si la oferta de servicios no se proporciona en la plantilla de inicio del perfil de la máquina o como parámetro del comando `New-ProvScheme`, aparecerá el error correspondiente.

Para crear un catálogo con la versión de la plantilla de inicio como entrada del perfil de máquina:

1. Abra una ventana de **PowerShell**.
2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
3. Obtenga la lista de versiones de una plantilla de inicio. Por ejemplo:

```
XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate>
    ls | Select FullPath
```

4. Cree un grupo de identidades si no se ha creado. Por ejemplo:

```
New-AcctIdentityPool `
-IdentityPoolName "abc11" `
-NamingScheme "abc1-##" `
-NamingSchemeType Numeric `
-Domain "citrix-xxxxxx.local" `
-ZoneUid "xxxxxxxx" `
```

5. Cree un esquema de aprovisionamiento con una versión de plantilla de inicio como entrada del perfil de máquina. Por ejemplo:

```
New-ProvScheme `
-ProvisioningSchemeName "MPLT1" `
-HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `
```



```
-IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `
-MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-
   persistent-vda-win2022 (ami-0axxxxxxxxxxx).template" `
-CleanOnBoot `
-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
   (lt-01xxxxx).launchtemplate\lt-01xxxxx (1).
   launchtemplateversion"
```

6. Registre el esquema de aprovisionamiento como un catálogo de broker. Por ejemplo:

```
New-BrokerCatalog -Name "MPLT1" `
-AllocationType Random `
-Description "Machine profile catalog" `
-ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `
-ProvisioningType Mcs `
-SessionSupport MultiSession `
-PersistUserChanges Discard
```

7. Complete la creación del catálogo. Para obtener más información, consulte SDK de PowerShell de Citrix

También puede actualizar la entrada de un catálogo de perfiles de máquina de una máquina virtual a una versión de plantilla de inicio y de una versión de plantilla de inicio a una máquina virtual. Por ejemplo:

- Para actualizar la entrada de un catálogo de perfiles de máquina de una VM a una versión de plantilla de inicio:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest"
    `
-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
    (lt-0bxxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxx (1).
   launchtemplateversion"
```

- Para actualizar la entrada de un catálogo de perfiles de máquina de una versión de plantilla de inicio a una VM:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest"
    `
-MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-east-1a.
   availabilityzone\apollo-non-persistent-vda-win2022-2 (i-08
   xxxxxxxxx).vm"
```

Cifrar los discos de ID y sistema operativo

Puede crear un catálogo persistente y no persistente de máquinas virtuales con claves de AWS KMS (clave administrada por el cliente y clave administrada por AWS) que se puede usar para cifrar el disco del sistema operativo y el disco de identidad.

- Las claves administradas por AWS se rotan automáticamente cada año.
- La rotación automática de las claves administradas por el cliente es opcional y se puede administrar manualmente.

Puede consultar los siguientes documentos de AWS para obtener más información sobre las claves de KMS:

- Conceptos de AWS KMS
- Cómo funciona la rotación automática de claves.

Para el cifrado del sistema operativo y los discos de ID, configure una de las siguientes opciones:

- Use una imagen maestra cifrada (por ejemplo, una AMI creada a partir de una instancia o instantánea que contenga un volumen raíz de EBS cifrado con una clave de KMS)
- Use un origen de perfil de máquina (máquina virtual o plantilla de inicio) que contenga un volumen raíz de EBS cifrado.

Limitaciones

Tenga en cuenta las siguientes limitaciones:

- Actualmente, MCS solo admite un disco en la AMI de imagen maestra.
- No puede cifrar directamente los volúmenes o las instantáneas de EBS sin cifrar existentes, ni modificar la clave de KMS de un volumen cifrado existente. Para ello, debe:

  1. Crear una nueva instantánea de ese volumen.
  2. Crear un nuevo volumen a partir de esa instantánea.
  3. Cifrar el nuevo volumen.

Consulte los siguientes documentos de AWS:

- Cifrar recursos no cifrados
- Limitaciones del cifrado automático o predeterminado de los volúmenes de EBS: Cifrar automáticamente volúmenes de Amazon EBS nuevos y existentes.

Crear un catálogo con cifrado de disco

Puede crear un catálogo de máquinas de MCS con cifrado de disco mediante:

- Imagen maestra
- Perfil de máquina

Consideraciones al usar la entrada de perfil de máquina para el cifrado de discos:

- La clave de KMS de la entrada del perfil de máquina tiene prioridad sobre la clave de KMS de la imagen maestra.
- Si no se proporciona ninguna entrada de perfil de máquina, se usa la clave de KMS de la AMI de la imagen maestra para cifrar los discos de las máquinas virtuales del catálogo.
- Si el perfil de máquina contiene asignaciones de dispositivos de bloques, los dispositivos de bloques presentes en la plantilla de imagen maestra (AMI) y el perfil de máquina deben coincidir. Por ejemplo, si la AMI tiene un dispositivo definido en `/dev/sda1`, el perfil de la máquina también debe tener un dispositivo definido en `/dev/sda1`.
- Si no hay ninguna clave en el origen del perfil de máquina y la imagen maestra no está cifrada, los discos de las máquinas virtuales del catálogo no se cifran.
- Cuando la imagen maestra está cifrada, una plantilla de inicio o VM de origen de perfil de máquina debe tener un volumen raíz cifrado para que se considere una entrada válida.

Modificar un catálogo existente

Puede modificar un catálogo existente mediante `Set-ProvScheme` para tener:

- Una entrada de perfil de máquina con un volumen que contiene una nueva clave de KMS.
- Una AMI de plantilla de imagen maestra cifrada con una nueva clave de KMS.

Consideraciones importantes

- Los volúmenes de nuevas máquinas virtuales que se agregan al catálogo se cifran con la nueva clave de KMS.
- Para actualizar los parámetros de cifrado cuando hay un perfil de máquina existente, ejecute `Set-ProvScheme` con un nuevo perfil de máquina.
- No puede modificar un catálogo existente para que pase de tener volúmenes cifrados a volúmenes no cifrados.
  No puede actualizar la imagen de una AMI maestra cifrada a una AMI maestra no cifrada.

Filtrar instancias de VM

Una instancia de máquina virtual de AWS EC2 que utilice como máquina virtual de perfil de máquina debe ser compatible para que el catálogo de máquinas se cree y funcione correctamente. Para enumerar las instancias de máquinas virtuales de AWS EC2 que se pueden usar como máquinas virtuales de entrada de perfil de máquina, puede usar el comando `Get-HypInventoryItem`. El comando puede buscar en páginas y filtrar el inventario de máquinas virtuales disponibles en una unidad de alojamiento.

Paginación:

Get-HypInventoryItem admite dos modos de paginación:

- El modo de paginación utiliza los parámetros `-MaxRecords` y `-Skip` para devolver conjuntos de elementos:
  - `-MaxRecords`: El valor predeterminado es **1**. Esto controla la cantidad de elementos que devolverán.
  - `-Skip`: El valor predeterminado es **0**. Esto controla la cantidad de elementos que se deben omitir desde el principio absoluto (o el final absoluto) de la lista en el hipervisor.
- El modo de desplazamiento utiliza los parámetros `-MaxRecords`, `-ForwardDirection` y `-ContinuationToken` para permitir el desplazamiento por los registros:
  - `-ForwardDirection`: El valor predeterminado es **True**. Esto se usa junto con `-MaxRecords` para devolver el siguiente conjunto de registros coincidentes o el conjunto anterior de registros coincidentes.
  - `-ContinuationToken`: Devuelve los elementos inmediatamente después (o antes si `ForwardDirection` es **false**), pero sin incluir el elemento indicado en `ContinuationToken`.

Ejemplos de paginación:

- Para devolver un solo registro de la plantilla de máquina con el nombre más bajo. El campo `AdditionalData` tiene `TotalItemsCount` y `TotalFilteredItemsCount`:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template
```

- Para devolver diez registros de la plantilla de máquina con el nombre más bajo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -MaxRecords 10 | select Name
```

- Para devolver una matriz de registros que termine con el nombre más alto:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -ForwardDirection $False -MaxRecords 10
     | select Name
```

- Para devolver una matriz de registros que comience en la plantilla de máquina asociada al `ContinuationToken` correspondiente:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -ContinuationToken "ami-07xxxxxxxxx" -
    MaxRecords 10
```

Filtros:

Se admiten estos parámetros opcionales adicionales para el filtrado. Puede combinar estos parámetros con las opciones de paginación.

- `-ContainsName "my_name"`: Si la cadena dada coincide con parte del nombre de una AMI, la AMI se incluye en el resultado de `Get`. Por ejemplo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -MaxRecords 100 -ContainName ‘apollo’
     | select Name
```

- `-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" }'`: Si una AMI tiene al menos una de estas etiquetas, se incluye en el resultado de `Get`. Por ejemplo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -MaxRecords 100 -Tags '{
"opex owner": "Not tagged" }
' | select Name
```

> **Nota:**
>
> Se admiten dos valores de etiqueta. El valor de la etiqueta **Not Tagged** coincide con elementos que no tienen la etiqueta especificada en su lista de etiquetas. El valor de la etiqueta **All values** coincide con elementos que tienen la etiqueta, independientemente del valor de la etiqueta. De lo contrario, la coincidencia solo se produce si el elemento tiene la etiqueta y el valor es igual al indicado en el filtro.

- `-Id "ami-0a2d913927e0352f3"`: Si la AMI coincide con el ID proporcionado, se incluye en el resultado de `Get`. Por ejemplo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -Id ami-xxxxxxxxxxxxx
```

Filtrado en el parámetro AdditionalData:

El parámetro de filtrado `AdditionalData` muestra plantillas o máquinas virtuales en función de su capacidad, oferta de servicio o cualquier propiedad que se encuentre en AdditionalData. Por ejemplo:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -
   LiteralPath "XDHyp:\HostingUnits\aws" -MaxRecords 200).
   AdditionalData
```

También puede agregar un parámetro `-Warn` para indicar las máquinas virtuales incompatibles. Las máquinas virtuales se incluyen en un campo de `AdditionalData` denominado **Warning**. Por ejemplo:


```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -
    LiteralPath "XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami
    -015xxxxxxxx" -Warn $true).AdditionalData
```

Qué hacer a continuación

- Si este es el primer catálogo creado, Web Studio le guiará para crear un grupo de entrega
- Para revisar todo el proceso de configuración, consulte Instalar y configurar
- Para administrar catálogos, consulte Administrar catálogos de máquinas y Administrar un catálogo de AWS

Más información

- Crear y administrar conexiones y recursos
- Conexión con AWS
- Crear catálogos de máquinas

Crear un catálogo de XenServer

August 17, 2024

Crear catálogos de máquinas describe los asistentes con los que se crea un catálogo de máquinas. La siguiente información incluye detalles específicos de los entornos de virtualización de XenServer.

> **Nota:**
>
> Antes de crear un catálogo de XenServer, debe terminar de crear una conexión a XenServer. Consulte Conexión a XenServer.

Crear un catálogo de máquinas a través una conexión XenServer

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. Despeje 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.

Limitaciones

- Si una implementación de Citrix Virtual Apps and Desktops con sus máquinas virtuales alojadas en Citrix Hypervisor 8.2 Cumulative Update 1 utiliza varios repositorios de almacenamiento (RA) GFS2 en un único catálogo de MCS, las máquinas virtuales del catálogo no pueden acceder a las imágenes VDI durante la implementación. Se notifica un error que indica que "la VDI está actualmente en uso".
- Citrix Hypervisor 8.2 Cumulative Update 1 no admite máquinas virtuales totalmente clonadas de MCS con RA GFS2.

Para obtener más información, consulte Restricciones.

Estas restricciones no se aplican a XenServer 8 y versiones posteriores.

Crear un catálogo de máquinas mediante un perfil de máquina

Al crear un catálogo para aprovisionar máquinas mediante MCS, puede usar un perfil de máquina para capturar las propiedades del hardware de una máquina virtual y aplicarlas a las máquinas virtuales recién aprovisionadas del catálogo. Si no se utiliza el parámetro `MachineProfile`, las propiedades del hardware se obtienen de la instantánea o la VM de la imagen maestra.

> **Nota:**
>
> Actualmente, solo puede usar una máquina virtual como entrada de perfil de máquina.

Puede configurar explícitamente estos parámetros para sobrescribir los valores de los parámetros en la entrada del perfil de máquina:

- `VMCpuCount`
- `VMMemory`
- `NetworkMapping`

Para crear un catálogo con un perfil de máquina:

1. Abra la ventana de PowerShell.
2. Ejecute `asnp citrix*`.
3. Crear un grupo de identidades. El grupo de identidades es un contenedor para las cuentas de Active Directory (AD) de las máquinas virtuales que se crearán. Por ejemplo:

```
New-AcctIdentityPool -Domain "citrix-xxxxxx.local" -
    IdentityPoolName "ExampleIdentityPool" -NamingScheme "abc1-##"
    -NamingSchemeType "Numeric" -Scope @() -ZoneUid "xxxxxxxx"
```

4. Cree las cuentas de equipo de AD necesarias en Active Directory.

```
$password = "password123" | ConvertTo-SecureString -AsPlainText -
    Force
New-AcctADAccount -IdentityPoolName "ExampleIdentityPool" -Count
    10 -ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
Set-AcctAdAccountUserCert -IdentityPoolName "ExampleIdentityPool"
    -ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
```

5. Ejecute el comando `New-ProvScheme` para crear un catálogo. Por ejemplo:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "ExampleHostingUnit"
    -IdentityPoolName "ExampleIdentityPool" -InitialBatchSizeHint 2
     -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" />
</CustomProperties>'
-MasterImageVM "XDHyp:\HostingUnits\ExampleHostingUnit\ExampleVDA.
    vm\ExampleVDA.snapshot" -ProvisioningSchemeName "ExampleCatalog
    " -Scope @() -SecurityGroup @()
-MachineProfile "XDHyp:\HostingUnits\ExampleHostingUnit\
    ExampleMachineProfile.vm"
```

6. Registre el esquema de aprovisionamiento como un catálogo de broker. Por ejemplo:

```
$ConfigZone = Get-ConfigZone | Where-Object {
  $_.Name -eq "xxxxxx"  }

New-BrokerCatalog -Name "MPLT1" -AllocationType Random -
    Description "Machine profile catalog" -ProvisioningSchemeId
    fe7df345-244e-4xxxx-xxxxxxxxx -ProvisioningType Mcs -
    SessionSupport MultiSession -PersistUserChanges Discard -
    ZoneUid ($ConfigZone.Uid)
```

7. Agregue las VM al catálogo.

Para actualizar el catálogo con un nuevo perfil de máquina:

1. Ejecute el comando `Set-ProvScheme`. Por ejemplo:


```
Set-ProvScheme -ProvisioningSchemeName "ExampleCatalog" -
    MachineProfile "XDHyp:\HostingUnits\ExampleHostingUnit\
    ExampleMachineProfileVm.vm\ExampleMachineProfileSnapshot.
    snapshot"
```

Para obtener más información sobre el comando Set-ProvScheme, consulte Set-ProvScheme.

> **Nota:**
>
> - En este caso, el comando `Set-ProvScheme` no cambia el perfil de máquina de las máquinas virtuales existentes del catálogo. Solo las nuevas máquinas virtuales que se agregan al catálogo tienen el nuevo perfil de máquina.
> - No puede convertir catálogos de máquinas basado en perfiles de máquina en catálogos de máquinas no basados en perfiles de máquina.

Qué hacer a continuación

- Si este es el primer catálogo creado, Web Studio le guiará para crear un grupo de entrega
- Para revisar todo el proceso de configuración, consulte Instalar y configurar
- Para administrar catálogos, consulte Administrar catálogos de máquinas y Administrar un catálogo de XenServer

Más información

- Crear y administrar conexiones y recursos
- Conexión a XenServer
- Crear catálogos de máquinas

Crear un catálogo de Google Cloud Platform

August 20, 2024

Crear catálogos de máquinas describe los asistentes con los que se crea un catálogo de máquinas. La siguiente información incluye detalles específicos de los entornos de Google Cloud.

> **Nota:**
>
> Antes de crear un catálogo de Google Cloud Platform (GCP), debe terminar de crear una conexión con GCP. Consulte Conexión con entornos de Google Cloud.

Preparar la instancia de una VM maestra y un disco persistente

> **Sugerencia:**
>
> "Disco persistente"es el término de Google Cloud para "disco virtual".

Para preparar la instancia de una VM maestra, cree y configure una instancia de VM con propiedades que coincidan con la configuración que quiera para las instancias de VDA clonadas en el catálogo de máquinas planificado. La configuración no se aplica solamente al tamaño y al tipo de instancia. También incluye atributos de instancia como metadatos, etiquetas, asignaciones de GPU, etiquetas de red y propiedades de cuenta de servicio.

Como parte del proceso, MCS utiliza la instancia de VM maestra para crear la *plantilla de instancias* de Google Cloud. A continuación, la plantilla de instancias se utiliza para crear las instancias de VDA clonadas que componen el catálogo de máquinas. Las instancias clonadas heredan las propiedades (excepto las propiedades de VPC, subred y disco persistente) de la instancia de VM maestra a partir de la cual se creó la plantilla de instancias.

Después de configurar las propiedades de la instancia de VM maestra según sus especificaciones, inicie la instancia y, a continuación, prepare el disco persistente para la instancia.

Le recomendamos crear manualmente una instantánea del disco. Esto le permite utilizar una convención de nomenclatura útil para realizar un seguimiento de las versiones, le ofrece más opciones para administrar versiones anteriores de la imagen maestra y le ahorra tiempo en la creación de catálogos de máquinas. Si no crea su propia instantánea, MCS crea una instantánea temporal (que se elimina al final del proceso de aprovisionamiento).

Creación de un catálogo de máquinas

Puede crear un catálogo de máquinas de dos maneras:

- Crear un catálogo de máquinas mediante Web Studio
- Crear un catálogo de máquinas con PowerShell

Crear un catálogo de máquinas mediante Web Studio

> **Nota:**
>
> Cree los recursos antes de crear los catálogos de máquinas. Al configurar catálogos de máquinas, utilice las convenciones de nomenclatura establecidas por Google Cloud. Consulte Lineamientos para asignar nombres a buckets para obtener más información.

Siga las instrucciones que se indican en Crear catálogos de máquinas. La siguiente descripción se aplica exclusivamente a los catálogos de Google Cloud.

1. Inicie sesión en Web Studio y seleccione **Catálogos de máquinas** en el panel de la izquierda.
2. Seleccione **Crear catálogo de máquinas** en la barra de acciones.
3. En la página **Sistema operativo**, seleccione **SO multisesión** y, a continuación, seleccione **Siguiente**.
    - Citrix Virtual Apps and Desktops Service también admite SO de sesión única.
4. En la página **Administración de máquinas**, seleccione las opciones **Máquinas con administración de energía** y **Citrix Machine Creation Services** y, a continuación, seleccione **Siguiente**. Si hay varios recursos, seleccione uno en el menú.
5. En la página **Imagen**, complete estos pasos según sea necesario y, a continuación, haga clic en **Siguiente**.
    a) Seleccione una instantánea o una máquina virtual como imagen maestra. Si quiere utilizar la funcionalidad de arrendamiento único, debe seleccionar una imagen cuya propiedad de grupo de nodos esté configurada correctamente. Consulte Habilitar selección de zona.
    b) Para usar una máquina virtual existente como perfil de máquina, seleccione Usar un perfil de máquina y después seleccione la máquina virtual.

    > **Nota:**
    >
    > Actualmente, las máquinas virtuales de este catálogo heredan el ID del conjunto de cifrado del disco, el tamaño de la máquina, el tipo de almacenamiento y los parámetros de zona del perfil de máquina.

    c) Seleccione el nivel funcional mínimo para el catálogo. Para usar la funcionalidad de arrendamiento único, debe seleccionar una imagen cuya propiedad de grupo de nodos esté configurada correctamente.
6. En la página **Tipos de almacenamiento**, seleccione el tipo de almacenamiento utilizado para contener el sistema operativo con este catálogo de máquinas. Cada una de las siguientes opciones de almacenamiento tiene características de precio y rendimiento únicas. (Se crea siempre un disco de identidad con el disco persistente estándar zonal).
    - Disco persistente estándar
    - Disco persistente equilibrado
    - Disco persistente SSD

    Para obtener más información sobre las opciones de almacenamiento de Google Cloud, consulte https://cloud.google.com/compute/docs/disks/.
7. En la página **Máquinas virtuales**, especifique cuántas máquinas virtuales quiere crear, revise la especificación detallada de dichas máquinas y, a continuación, seleccione **Siguiente**. Si utiliza

grupos de nodos de arrendatario único para catálogos de máquinas, deberá seleccionar **solo** las zonas en las que están disponibles los nodos de arrendatario único reservados. Consulte Habilitar selección de zona.

8. En la página **Cuentas de equipo**, seleccione una cuenta de Active Directory y, a continuación, seleccione **Siguiente**.
    - Si selecciona **Crear nuevas cuentas de Active Directory**, seleccione un dominio y, a continuación, introduzca la secuencia de caracteres que representa el esquema de nomenclatura para las cuentas de equipo de VM aprovisionadas creadas en Active Directory. El esquema de nomenclatura de cuentas puede contener de 1 a 64 caracteres y no puede contener espacios en blanco, ni caracteres no ASCII o especiales.
    - Si selecciona **Usar cuentas de Active Directory existentes**, seleccione **Examinar** para desplazarse a las cuentas de equipo de Active Directory existentes de las máquinas seleccionadas.
9. En la página **Credenciales de dominio**, seleccione **Introducir credenciales**, escriba el nombre de usuario y la contraseña, seleccione **Guardar** y, a continuación, seleccione **Siguiente**.
    - Las credenciales que escriba deben tener permisos para realizar operaciones en cuentas de Active Directory.
10. En la página **Resumen**, confirme la información, especifique un nombre para el catálogo y seleccione **Finalizar**.

    > **Nota:**
    >
    > A partir de la versión 2402, los nombres de los catálogos de GCP deben cumplir estas reglas:
    >
    > - Empezar con una letra minúscula.
    > - Incluir solo letras minúsculas (a-z), números y guiones.
    > - Terminar con una letra minúscula o un número.
    >
    > Cuando intenta cambiar el nombre de los catálogos de GCP existentes que no cumplen con estas reglas, aparecen mensajes de error que le indican que debe cambiarles el nombre conforme a las reglas actualizadas.

La creación del catálogo de máquinas puede tardar mucho tiempo en completarse. Para comprobar que las máquinas se hayan creado en los grupos de nodos de destino, vaya a la consola de Google Cloud.

Importar máquinas de Google Cloud creadas manualmente

Puede *crear una conexión a Google Cloud* y, a continuación, *crear un catálogo que contenga las máquinas de Google Cloud*. Luego, puede apagar y encender manualmente las máquinas de Google

Cloud a través de Citrix Virtual Apps and Desktops. Con esta función, puede:

- Importar las máquinas con SO multisesión de Google Cloud creadas manualmente al catálogo de máquinas de Citrix Virtual Apps and Desktops.
- Quitar las máquinas con SO multisesión de Google Cloud creadas manualmente de un catálogo de Citrix Virtual Apps and Desktops.
- Utilizar las prestaciones de administración de energía existentes en Citrix Virtual Apps and Desktops para administrar la energía de las máquinas con SO multisesión Windows en Google Cloud. Por ejemplo, establecer una programación de reinicio para dichas máquinas.

Esta funcionalidad no requiere cambios en el flujo de aprovisionamiento de Citrix Virtual Apps and Desktops; tampoco se necesita eliminar ninguna función existente. Se recomienda utilizar MCS para aprovisionar máquinas en Web Studio en lugar de importar máquinas de Google Cloud creadas manualmente.

Nube privada virtual compartida

Las nubes VPC compartidas constan de un proyecto host (desde el que están disponibles las subredes compartidas) y uno o varios proyectos de servicios que utilizan el recurso. Las nubes VPC compartidas son las opciones idóneas para instalaciones grandes, ya que ofrecen control, uso y administración centralizados de los recursos de empresa compartidos de Google Cloud. Para obtener más información, consulte el sitio de documentación de Google.

Con esta función, Machine Creation Services (MCS) admite el aprovisionamiento y la administración de catálogos de máquinas implementados en las nubes VPC compartidas. Esta compatibilidad, equivalente en funcionalidad a la compatibilidad que se ofrece en nubes VPC locales, difiere en dos áreas:

1. Debe conceder permisos adicionales a la cuenta de servicio utilizada para crear la conexión de host. Este proceso permite a MCS acceder a los recursos de VPC compartida y utilizarlos.
2. Debe crear dos reglas de firewall, una para la entrada y otra para la salida. Estas reglas de firewall se utilizan durante el proceso de creación de imágenes maestras.

Se necesitan nuevos permisos

Se requiere una cuenta de servicio de Google Cloud con permisos específicos cuando se crea la conexión de host. Estos permisos adicionales se deben conceder a todas las cuentas de servicio utilizadas para crear conexiones de host basadas en VPC compartidas.

> **Sugerencia:**
>
> Esos permisos adicionales no son nuevos para Citrix Virtual Apps and Desktops. Se utilizan para facilitar la implementación de VPC locales. Con las VPC compartidas, estos permisos adicionales

> permiten el acceso a otros recursos de VPC compartidas.

Se debe conceder un máximo de cuatro permisos adicionales a la cuenta de servicio asociada a la conexión de host para admitir una nube VPC compartida:

1. **compute.firewalls.list**: Este permiso es obligatorio. Permite a MCS recuperar la lista de reglas de firewall presentes en la nube VPC compartida.
2. **compute.networks.list**: Este permiso es obligatorio. Permite a MCS identificar las redes de nubes VPC compartidas disponibles para la cuenta de servicio.
3. **compute.subnetworks.list**: Este permiso es opcional, en función de cómo utilice las nubes VPC. Permite a MCS identificar las subredes dentro de las nubles VPC compartidas que sean visibles. Este permiso ya es necesario para utilizar nubes VPC locales, pero también debe asignarse en el proyecto host de nubes VPC compartidas.
4. **compute.subnetworks.use**: Este permiso es opcional, en función de cómo utilice las nubes VPC. Es necesario utilizar recursos de subred en los catálogos de máquinas aprovisionadas. Este permiso ya es necesario para utilizar nubes VPC locales, pero también debe asignarse en el proyecto host de nubes VPC compartidas.

Al utilizar estos permisos, tenga en cuenta que existen diferentes enfoques basados en el tipo de permiso utilizado para crear el catálogo de máquinas:

- Permiso a nivel de proyecto:
  - Permite el acceso a todas las nubes VPC compartidas dentro del proyecto host.
  - Requiere que los permisos #3 y #4 estén asignados a la cuenta de servicio.
- Permiso a nivel de subred:
  - Permite el acceso a subredes específicas dentro de la nube VPC compartida.
  - Los permisos #3 y #4 son intrínsecos a la asignación a nivel de subred y, por lo tanto, no es necesario asignarlos directamente a la cuenta de servicio.

Seleccione el enfoque que se adapte a las necesidades y los estándares de seguridad de su organización.

> **Sugerencia:**
>
> Para obtener más información sobre las diferencias entre los permisos a nivel de proyecto y a nivel de subred, consulte la documentación de Google Cloud.

Reglas de firewall

Durante la preparación de un catálogo de máquinas, se prepara una imagen de máquina para que sirva como disco del sistema de la imagen maestra del catálogo. Cuando se produce este proceso, el

disco se conecta temporalmente a una máquina virtual. Esta máquina virtual debe ejecutarse en un entorno aislado que impida todo el tráfico de red entrante y saliente. Este aislamiento se logra gracias a un par de reglas de firewall "deny-all"(denegar todo): una para el tráfico de entrada y otra para el tráfico de salida. Al utilizar nubes VPC locales de Google Cloud, MCS crea este firewall en la red local y lo aplica a la máquina para la creación de imagen maestra. Una vez finalizada la creación de la imagen maestra, la regla de firewall se elimina de la imagen.

Se recomienda mantener al mínimo la cantidad de nuevos permisos necesarios para usar nubes VPC compartidas. Las nubes VPC compartidas son recursos de empresa de alto nivel y suelen tener protocolos de seguridad más rígidos. Por este motivo, cree un par de reglas de firewall en el proyecto host en los recursos de VPC compartida, una para la entrada y otra para la salida. Asígneles la máxima prioridad. Aplique una nueva etiqueta de destino a cada una de estas reglas, con el siguiente valor:

```
citrix-provisioning-quarantine-firewall
```

Cuando MCS crea o actualiza un catálogo de máquinas, busca reglas de firewall que contengan esta etiqueta de destino. A continuación, comprueba que las reglas sean correctas y las aplica a la máquina utilizada para preparar la imagen maestra del catálogo. Si no se encuentran reglas de firewall o se encuentran, pero son incorrectas o ellas o sus prioridades, aparecerá un mensaje similar al siguiente:

```
"Unable to find valid INGRESS and EGRESS quarantine firewall rules
for VPC <name> in project <project>. "Please ensure you have created
 'deny all'firewall rules with the network tag 'citrix-provisioning-
quarantine-firewall'and proper priority.""Refer to Citrix Documentation
 for details."
```

Configurar la nube VPC compartida

Antes de agregar la VPC compartida como conexión de host en Web Studio, lleve a cabo estos pasos para agregar cuentas de servicio desde el proyecto que aprovisionará:

1. Crear un rol de IAM.
2. Agregue la cuenta de servicio utilizada para crear una conexión de host de CVAD al rol de IAM del proyecto host de VPC compartida.
3. Agregue la cuenta del servicio de Cloud Build desde el proyecto que quiere aprovisionar al rol de IAM del proyecto host de VPC compartida.
4. Crear reglas de firewall.

Crear un rol de IAM Determine el nivel de acceso del rol: *Acceso a nivel de proyecto* o un modelo más restringido con *acceso a nivel de subred*.

Acceso a nivel de proyecto para el rol de IAM. Para el rol de IAM a nivel de proyecto, incluya los siguientes permisos:

- compute.firewalls.list
- compute.networks.list
- compute.subnetworks.list
- compute.subnetworks.use

Para crear un rol de IAM a nivel de proyecto:

1. En la consola de Google Cloud, vaya a **IAM & Admin > Roles**.
2. En la página **Roles**, seleccione **CREATE ROLE**.
3. En la página **Create Role**, especifique el nombre del rol. Seleccione **ADD PERMISSIONS**.
    a) En la página **Add permissions**, agregue permisos al rol de forma individual. Para agregar un permiso, escriba el nombre del permiso en el campo **Filter table**. Seleccione el permiso y, a continuación, seleccione **ADD**.
    b) Seleccione **CREATE**.

Subnet-level IAM role. Este rol omite la adición de los permisos `compute.subnetworks.list` y `compute.subnetworks.use` después de seleccionar **CREATE ROLE**. Para este nivel de acceso de IAM, los permisos `compute.firewalls.list` y `compute.networks.list` deben aplicarse al nuevo rol.

Para crear un rol de IAM a nivel de subred:

1. En la consola de Google Cloud, vaya a **VPC network** > **Shared VPC**. Aparecerá la página **Shared VPC**, que muestra las subredes de las redes de VPC compartidas que contiene el proyecto host.
2. En la página **Shared VPC**, seleccione la subred a la que quiere acceder.
3. En la esquina superior derecha, seleccione **ADD MEMBER** para agregar una cuenta de servicio.
4. En la página **Add members**, siga estos pasos:
    a) En el campo **New members**, escriba el nombre de su cuenta de servicio y, a continuación, selecciónela en el menú.
    b) Seleccione el campo **Select a role** y, a continuación, **Compute Network User**.
    c) Seleccione **SAVE**.
5. En la consola de Google Cloud, vaya a **IAM & Admin** > **Roles**.
6. En la página **Roles**, seleccione **CREATE ROLE**.
7. En la página **Create Role**, especifique el nombre del rol. Seleccione **ADD PERMISSIONS**.
    a) En la página **Add permissions**, agregue permisos al rol de forma individual. Para agregar un permiso, escriba el nombre del permiso en el campo **Filter table**. Seleccione el permiso y, a continuación, seleccione **ADD**.
    b) Seleccione **CREATE**.

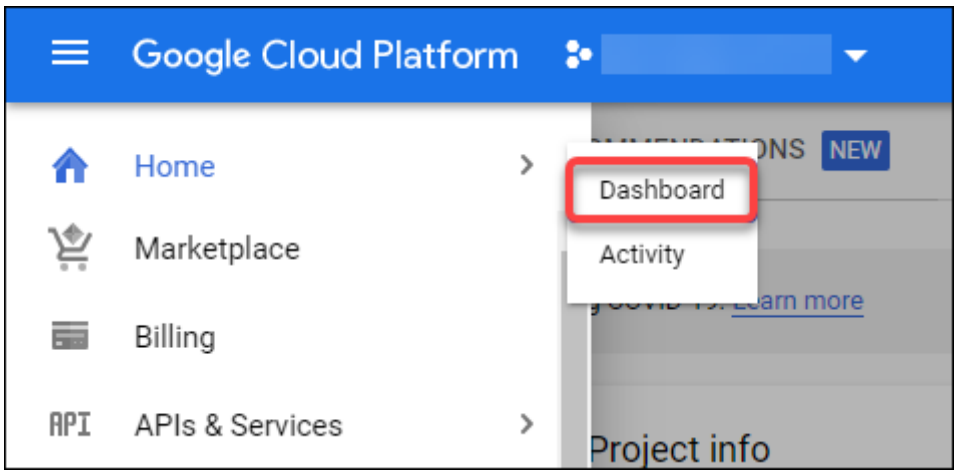
Agregar una cuenta de servicio al rol de IAM del proyecto host Después de crear un rol de IAM, siga estos pasos para agregar una cuenta de servicio para el proyecto host:

1. En la consola de Google Cloud, vaya al proyecto host y, a continuación, a **IAM & Admin > IAM**.
2. En la página **IAM**, seleccione **ADD** para agregar una cuenta de servicio.
3. En la página **Add members**:
    a) En el campo **New members**, escriba el nombre de su cuenta de servicio y, a continuación, selecciónela en el menú.
    b) En el campo Select a role, introduzca el rol de IAM que creó y, a continuación, seleccione el rol en el menú.
    c) Seleccione **SAVE**.

Ahora la cuenta de servicio está configurada para el proyecto host.

Agregar la cuenta de servicio de Cloud Build a la VPC compartida Cada suscripción a Google Cloud tiene una cuenta de servicio que tiene, como nombre, el número de identificación del proyecto, seguido de `cloudbuild.gserviceaccount`. Por ejemplo: `705794712345@cloudbuild.gserviceaccount`.

Para determinar el número de ID del proyecto, seleccione **Home** y **Dashboard** en la consola de Google Cloud:



Busque el **número del proyecto** en el área **Project Info** de la pantalla.

Siga estos pasos para agregar la cuenta de servicio de Cloud Build a la VPC compartida:

1. En la consola de Google Cloud, vaya al proyecto host y, a continuación, a **IAM & Admin** > **IAM**.
2. En la página **Permissions**, seleccione **ADD** para agregar una cuenta.
3. En la página **Add members**, siga estos pasos:
    a) En el campo **New members**, escriba el nombre de la cuenta de servicio de Cloud Build y, a continuación, selecciónela en el menú.
    b) Seleccione el campo **Select a role**, escriba `Computer Network User` y, a continuación, seleccione el rol en el menú.
    c) Seleccione **SAVE**.

Crear reglas de firewall Como parte del proceso de masterización, MCS copia la imagen de máquina seleccionada y la utiliza para preparar el disco del sistema de la imagen maestra para el catálogo. Durante la masterización, MCS conecta el disco a una máquina virtual temporal, que luego ejecuta scripts de preparación. Esta máquina virtual debe ejecutarse en un entorno aislado que prohíba todo el tráfico de red entrante y saliente. Para crear un entorno aislado, MCS requiere dos reglas "*deny all*"en el firewall (una regla de entrada y una regla de salida). Por lo tanto, cree dos reglas de firewall en el *proyecto host* de la siguiente manera:

1. En la consola de Google Cloud, vaya al proyecto host y, a continuación, a **VPC Network > Firewall**.
2. En la página **Firewall**, seleccione **CREATE FIREWALL RULE**.
3. En la página **Create a firewall rule**, complete lo siguiente:
    - **Nombre**. Escriba el nombre de la regla.
    - **Network**. Seleccione la red de VPC compartida a la que se aplica la regla de firewall de entrada.
    - **Priority**. Cuanto menor sea el valor, mayor será la prioridad de la regla. Recomendamos un valor pequeño (por ejemplo, 10).
    - **Direction of traffic**. Seleccione **Ingress**.
    - **Action on match**. Seleccione **Deny**.
    - **Targets**. Utilice el valor predeterminado, **Specified target tags**.
    - **Target tags**. Escriba `citrix-provisioning-quarantine-firewall`.
    - **Source filter**. Utilice el valor predeterminado, **IP ranges**.
    - **Source IP ranges**. Escriba un intervalo que tenga en cuenta todo el tráfico. Escriba `0.0.0.0/0`.
    - **Protocols and ports**. Seleccione **Deny all**.
4. Seleccione **CREATE** para crear la regla.
5. Repita los pasos del 1 al 4 para crear otra regla. En **Direction of traffic**, seleccione **Egress**.

Agregar una conexión Agregue una conexión a los entornos de Google Cloud. Consulte Agregar una conexión.

Habilitar selección de zona

Citrix Virtual Apps and Desktops admite la selección de zonas. Con la selección de zonas, puede especificar las zonas en las que quiere crear máquinas virtuales. Con la selección de zonas, los administradores pueden colocar nodos de arrendatario único en las zonas de su elección. Para configurar el arrendamiento único, debe completar lo siguiente en Google Cloud:

- Reservar un nodo de arrendatario único de Google Cloud

- Crear la imagen maestra del VDA

Reservar un nodo de arrendatario único de Google Cloud

Para reservar un nodo de arrendatario único de Google Cloud, consulte la documentación de Google Cloud.

> **Importante:**
>
> Una plantilla de nodos se utiliza para indicar las características de rendimiento del sistema que se reserva al grupo de nodos. Estas características incluyen la cantidad de vGPU, la cantidad de memoria asignada al nodo y el tipo de máquina utilizado para las máquinas creadas en el nodo. Para obtener más información, consulte la documentación de Google Cloud.

Crear la imagen maestra del VDA

Para implementar máquinas en el nodo de arrendatario único, debe realizar pasos adicionales al crear una imagen de máquina virtual maestra. Las instancias de máquina en Google Cloud tienen una propiedad llamada *node affinity labels* (etiquetas de afinidad de nodos). Las instancias utilizadas como imágenes maestras para catálogos implementados en el nodo de arrendatario único requieren una *etiqueta de afinidad de nodos* que coincida con el nombre del **grupo de nodos de destino**. Para lograr esto, tenga en cuenta lo siguiente:

- Establezca la etiqueta en la consola de Google Cloud cuando cree la instancia. Para obtener información detallada, consulte Establecer una etiqueta de afinidad de nodos al crear una instancia.
- En el caso de una instancia existente, establezca la etiqueta desde la línea de comandos de **gcloud**. Para obtener información detallada, consulte Configurar una etiqueta de afinidad de nodos para una instancia existente.

> **Nota:**
>
> Si quiere utilizar el arrendamiento único con una VPC compartida, consulte Nube privada virtual compartida.

Establecer una etiqueta de afinidad de nodos al crear una instancia Para configurar la etiqueta de afinidad de nodos:

1. En la consola de Google Cloud, vaya a **Compute Engine > VM instances**.
2. En la página **VM instances**, seleccione **Create instance**.

3. En la página **Instance creation**, escriba o configure la información necesaria y, a continuación, seleccione **management, security, disks, networking, sole tenancy** para abrir el panel de parámetros.
4. En la ficha **Sole Tenancy**, seleccione **Browse** para ver los grupos de nodos disponibles en el proyecto actual. Aparecerá la página **Sole-tenant node**, que muestra una lista de los grupos de nodos disponibles.
5. En la página **Sole-tenant node**, seleccione el grupo de nodos correspondiente de la lista y, a continuación, seleccione **Select** para volver a la ficha **Sole tenancy**. El campo de las etiquetas de afinidad de nodos se rellena con la información seleccionada. Esta configuración garantiza que los catálogos de máquinas creados a partir de la instancia se implementarán en el grupo de nodos seleccionado.
6. Seleccione **Create** para crear la instancia.

Configurar una etiqueta de afinidad de nodos para una instancia existente Para configurar la etiqueta de afinidad de nodos:

1. En la ventana del terminal de Google Cloud Shell, utilice el comando *gcloud compute instances* para establecer una etiqueta de afinidad de nodos. Incluya la siguiente información en el comando **gcloud**:

   - **Nombre de la VM**. Por ejemplo, utilice una máquina virtual existente denominada `s*2019-vda-base`.*
   - **Nombre del grupo de nodos**. Utilice el nombre de grupo de nodos creado anteriormente. Por ejemplo, `mh-sole-tenant-node-group-1`.
   - **La zona en la que reside la instancia**. Por ejemplo, la máquina virtual reside en `*us-east-1b* zone`.

   Por ejemplo, escriba el siguiente comando en la ventana de terminal:

   - `gcloud compute instances set-scheduling "s2019-vda-base"--node-group="mh-sole-tenant-node-group-1"--zone="us-east1-b"`

   Para obtener más información sobre el comando *gcloud compute instances*, consulte la documentación de Google Developer Tools en https://cloud.google.com/sdk/gcloud/reference/beta/compute/instances/set-scheduling.
2. Vaya a la página **VM instance details** de la instancia y verifique que el campo **Node Affinities** se rellenó con la etiqueta.

Creación de un catálogo de máquinas Después de establecer la etiqueta de afinidad de nodos, configure el catálogo de máquinas.

Claves de cifrado administradas por el cliente (CMEK)

Puede utilizar claves de cifrado administradas por el cliente (CMEK) para catálogos de MCS. Al utilizar esta funcionalidad, asigna el rol `CryptoKey Encrypter/Decrypter` del servicio Key Management Service (KMS) de Google Cloud al agente de servicio de Compute Engine. La cuenta de Citrix Virtual Apps and Desktops debe tener los permisos correctos en el proyecto en el que se almacena la clave. Consulte Ayuda a proteger los recursos con claves de Cloud KMS para obtener más información.

El agente de servicio de Compute Engine tiene el siguiente formato: `service-<Project_Number>@compute-system.iam.gserviceaccount.com`. Este formato es distinto de la cuenta de servicio predeterminada de Compute Engine.

> **Nota:**
>
> Puede que esta cuenta de servicio de Compute Engine no aparezca en la pantalla **IAM Permissions** de Google Console. En tales casos, use el comando `gcloud` como se describe en Ayuda a proteger los recursos con claves de Cloud KMS.

Asignar permisos a la cuenta de Citrix Virtual Apps and Desktops

Los permisos de Google Cloud KMS se pueden configurar de varias formas. Puede proporcionar permisos de KMS a *nivel de proyecto* o a *nivel de recursos*. Consulte Permisos y funciones para obtener más información.

Permisos a nivel de proyecto Una opción es proporcionar a la cuenta de Citrix Virtual Apps and Desktops permisos a nivel de proyecto para examinar los recursos de Cloud KMS. Para ello, cree un rol personalizado y agregue los siguientes permisos:

- `cloudkms.keyRings.list`
- `cloudkms.keyRings.get`
- `cloudkms.cryptokeys.list`
- `cloudkms.cryptokeys.get`

Asigne este rol personalizado a su cuenta de Citrix Virtual Apps and Desktops. Esto le permite examinar las claves regionales del proyecto correspondiente del inventario.

Permisos a nivel de recursos Para la otra opción, los permisos a nivel de recursos, en la consola de Google Cloud, vaya a la `cryptoKey` que utiliza para aprovisionamiento de MCS. Agregue la cuenta de Citrix Virtual Apps and Desktops a un llavero o a una clave que utilice para aprovisionamiento de catálogos.

> **Sugerencia:**
>
> Con esta opción, no puede examinar las claves regionales de su proyecto en el inventario, puesto que la cuenta de Citrix Virtual Apps and Desktops no tiene permisos de lista a nivel de proyecto sobre los recursos de Cloud KMS. Sin embargo, aún podrá aprovisionar un catálogo con CMEK especificando el `cryptoKeyId` correcto en las propiedades personalizadas de `ProvScheme`, que se describen a continuación.

Aprovisionamiento con CMEK mediante propiedades personalizadas

Al crear el esquema de aprovisionamiento a través de PowerShell, especifique una propiedad `CryptoKeyId` en `ProvScheme CustomProperties`. Por ejemplo:

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
    <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="<
       yourCryptoKeyId>" />
</CustomProperties>'
```

`cryptoKeyId` debe especificarse en el siguiente formato:

`projectId:location:keyRingName:cryptoKeyName`

Por ejemplo, si quiere usar la clave `my-example-key` en el llavero `my-example-key-ring` de la región `us-east1` y el proyecto con ID `my-example-project-1`, su configuración personalizada de `ProvScheme` se asemejaría a:

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
    <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-
       example-project-1:us-east1:my-example-key-ring:my-example-key"
       />
</CustomProperties>'
```

Todas las imágenes y discos aprovisionados de MCS relacionados con este esquema de aprovisionamiento utilizan esta clave de cifrado administrada por el cliente.

> **Sugerencia:**
>
> Si utiliza claves globales, la ubicación de las propiedades del cliente debe indicar `global`, y no el nombre de la **región**, que en el ejemplo anterior es **us-east1**. Por ejemplo: `<Property xsi:type="StringProperty"Name="CryptoKeyId"Value="my-example-project-1:global:my-example-key-ring:my-example-key"/>`.

Rotar claves administradas por el cliente

Google Cloud no admite claves de rotación en discos o imágenes persistentes existentes. Una vez que se aprovisiona una máquina, se asocia a la versión de clave en uso en el momento de su creación. Sin embargo, se puede crear una nueva versión de la clave y esa nueva clave se utilizará con las máquinas o recursos recién aprovisionados creados al actualizar un catálogo con una nueva imagen maestra.

Consideraciones importantes acerca de los llaveros Los llaveros no se pueden cambiar de nombre ni eliminar. Además, podría incurrir en cargos imprevistos al configurarlos. Al eliminar o quitar un llavero, Google Cloud muestra un mensaje de error:

```
1 Sorry, you can't delete or rename keys or key rings. We were concerned
    about the security implications of allowing multiple keys or key
    versions over time to have the same resource name, so we decided to
    make names immutable. (And you can't delete them, because we wouldn'
    t be able to do a true deletion--there would still have to be a
    tombstone tracking that this name had been used and couldn't be
    reused).
2 We're aware that this can make things untidy, but we have no immediate
    plans to change this.
3 If you want to avoid getting billed for a key or otherwise make it
    unavailable, you can do so by deleting all the key versions; neither
     keys nor key rings are billed for, just the active key versions
    within the keys.
```

> **Sugerencia:**
>
> Para obtener más información, consulte Editing or deleting a key ring from the console.

Compatibilidad con “Acceso uniforme a nivel de bucket”

Citrix Virtual Apps and Desktops es compatible con la directiva de acceso uniforme a nivel de depósito de Google Cloud. Esta funcionalidad amplía el uso de la directiva de IAM que concede permisos a una cuenta de servicio para permitir la manipulación de recursos, incluidos los depósitos de almacenamiento. Con control de acceso uniforme a nivel de depósito, Citrix Virtual Apps and Desktops le permite utilizar una lista de control de acceso (ACL) para controlar el acceso a los depósitos de almacenamiento o a los objetos almacenados en ellos. Para obtener información general acerca del acceso uniforme a nivel de depósito de Google Cloud, consulte Acceso uniforme a nivel de bucket. Para obtener información sobre la configuración, consulte Requerir acceso uniforme a nivel de bucket.

Crear un catálogo de máquinas con PowerShell

En esta sección se detalla cómo puede crear catálogos con PowerShell:

- Crear un catálogo con un disco persistente de caché de reescritura
- Mejorar el rendimiento del arranque con E/S de MCS
- Crear un catálogo de máquinas mediante un perfil de máquina
- Crear un catálogo de máquinas con el perfil de máquina como plantilla de instancias
- Usar PowerShell para crear un catálogo con máquinas virtuales blindadas
- Crear máquinas virtuales de Windows 11 en el nodo de arrendatario único

Crear un catálogo con un disco persistente de caché de reescritura

Para configurar un catálogo con disco persistente de caché de reescritura, use el parámetro `New-ProvScheme CustomProperties` de PowerShell.

> **Sugerencia:**
>
> Use el parámetro de PowerShell solo para conexiones de alojamiento basadas en la nube. Si quiere aprovisionar máquinas con un disco persistente de caché de reescritura para una solución local (por ejemplo, XenServer), PowerShell no es necesario porque el disco conserva automáticamente los datos.

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. 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.

> **Nota:**
>
> Este comportamiento se aplica tanto a Azure como a GCP, donde los datos del disco de caché de reescritura predeterminado de E/S de MCS se eliminan y se vuelven a crear cuando se apaga o se enciende la máquina. Puede optar por conservar los datos del disco para evitar la eliminación y la recreación de los datos del disco caché de reescritura de E/S de MCS.

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 desde la interfaz de administración.

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 desde la interfaz de administración.

> **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 desde la interfaz de administración.

Por ejemplo, usar el parámetro CustomProperties para establecerlo `PersistWBC` en **`true`**:

```
<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="
   benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
</CustomProperties>
```

> **Nota:**
>
> 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 de reescritura cuando se apaga una máquina.

Por ejemplo, configure `New-ProvScheme` para utilizar la memoria caché de reescritura mientras configura la propiedad `PersistWBC` en **`true`**:

```
New-ProvScheme
-CleanOnBoot
-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=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
   =`"PersistWBC`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
   GoldImages.resourcegroup\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
   folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
```


Mejorar el rendimiento del arranque con E/S de MCS

Puede mejorar el rendimiento de arranque de los discos administrados de Azure y GCP cuando E/S de MCS está habilitada. Utilice la propiedad personalizada `PersistOSDisk` de PowerShell en el comando `New-ProvScheme` para configurar esta función. Las opciones asociadas a `New-ProvScheme` son:

```
<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="Resource ``````<!--NeedCopy-->
```````Groups" Value="benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />
</CustomProperties>
```

Para habilitar esta función, establezca la propiedad personalizada `PersistOSDisk` en **`true`**. Por ejemplo:

```
New-ProvScheme
-CleanOnBoot
-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=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSIO-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualprivatecloud\adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
```


```

### Crear un catálogo de máquinas mediante un perfil de máquina

Al crear un catálogo para aprovisionar máquinas mediante Machine Creation Services (MCS), puede usar un perfil de máquina para capturar las propiedades del hardware de una máquina virtual y aplicarlas a las máquinas virtuales recién aprovisionadas del catálogo. Cuando no se utiliza el parámetro `MachineProfile`, las propiedades del hardware se obtienen de la instantánea o la VM de la imagen maestra.
Algunas propiedades se definen de forma explícita; por ejemplo `StorageType`, `CatalogZones` y `CryptoKeyIs` se omiten en el perfil de la máquina.

- Para crear un catálogo con un perfil de máquina, utilice el comando `New-ProvScheme`. Por ejemplo, `New-ProvScheme –MachineProfile "path to VM"`. Si no especifica el parámetro `MachineProfile`, las propiedades del hardware se capturan de la máquina virtual de la imagen maestra.
- Para actualizar un catálogo con un nuevo perfil de máquina, utilice el comando `Set-ProvScheme`. Por ejemplo, `Set-ProvScheme –MachineProfile "path to new VM"`. Este comando no cambia el perfil de máquina de las máquinas virtuales existentes del catálogo. Solo las nuevas máquinas virtuales que se agregan al catálogo tienen el nuevo perfil de máquina.
- También puede actualizar la imagen maestra; sin embargo, al actualizar la imagen maestra, las propiedades del hardware no se actualizan. Si quiere actualizar las propiedades del hardware, debe actualizar el perfil de la máquina con el comando `Set-ProvScheme`. Estos cambios solo se aplicarán a las nuevas máquinas del catálogo. Para actualizar las propiedades de hardware de una máquina existente, puede utilizar el comando `Set-ProvVMUpdateTimeWindow` mediante los parámetros `-StartsNow` y `-DurationInMinutes -1`.

  > **Nota:**
  >
  > - `StartsNow` indica que la hora de inicio programada es la hora actual.
  > - `DurationInMinutes` con un número negativo (por ejemplo, -1) indica que no hay ningún límite superior en la ventana de tiempo de la programación.

### Crear un catálogo de máquinas con el perfil de máquina como plantilla de instancias

Puede seleccionar una plantilla de instancias de GCP como entrada para el perfil de la máquina. Las plantillas de instancias son recursos ligeros de GCP y, por lo tanto, muy rentables.

#### Crear un nuevo catálogo de máquinas con el perfil de máquina como plantilla de instancias

1. Abra una ventana de PowerShell.

2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
3. Utilice el siguiente comando para encontrar una plantilla de instancias en su proyecto de GCP:

```
cd XDHyp:\HostingUnits<HostingUnitName>\instanceTemplates.folder
```

4. Cree un nuevo catálogo de máquinas con el perfil de máquina como plantilla de instancias mediante el comando NewProvScheme:

```
New-ProvScheme -ProvisioningSchemeName <CatalogName>  -
    HostingUnitName <HostingUnitName> -IdentityPoolName <identity
    pool name> -MasterImageVM
XDHyp:\HostingUnits<HostingUnitName> \Base.vm\Base.snapshot -
    MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
    instanceTemplates.folder\mytemplate.template
```

   Para obtener más información sobre el comando New-ProvScheme, consulte https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/New-ProvScheme/.

5. Utilice los comandos de PowerShell para terminar de crear el catálogo de máquinas. Para obtener información sobre cómo crear un catálogo con el SDK de PowerShell remoto, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Cambiar el perfil de máquina de un catálogo de máquinas existente y convertirlo en plantilla de instancias

Estos son los pasos detallados para cambiar el perfil de máquina de un catálogo de máquinas existente y convertirlo en plantilla de instancias:

1. Abra una ventana de PowerShell.
2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
3. Ejecute este comando:

```
Set-ProvScheme -ProvisioningSchemeName  <CatalogName> -
    MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
    instanceTemplates.folder<TemplateName>.template
```

   Para obtener información sobre el comando Set-ProvScheme, consulte https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/Set-ProvScheme/.

Usar PowerShell para crear un catálogo con máquinas virtuales blindadas

Puede crear un catálogo de máquinas de MCS con propiedades de VM blindada. Una máquina virtual blindada se ve reforzada por un conjunto de controles de seguridad que proporcionan integri-

dad verificable de sus instancias de Compute Engine, con prestaciones avanzadas de seguridad de plataforma como el arranque seguro, un módulo de plataforma virtual de confianza, firmware UEFI y la supervisión de la integridad.

MCS admite la creación del catálogo mediante el flujo de trabajo del perfil de máquina. Si utiliza un flujo de trabajo de perfil de máquina, debe habilitar las propiedades de máquina virtual blindad de una instancia de máquina virtual. A continuación, puede utilizar esta instancia de máquina virtual como entrada del perfil de máquina.

Para crear un catálogo de máquinas de MCS con máquinas virtuales blindadas mediante el flujo de trabajo del perfil de máquina.

1. Habilite las opciones de máquina virtual blindada de una instancia de máquina virtual en la consola de Google Cloud. Consulte Quickstart: Enable Shielded VM options.
2. Cree un catálogo de máquinas de MCS con un flujo de trabajo de perfil de máquina mediante la instancia de máquina virtual.
    a) Abra una ventana de PowerShell.
    b) Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
    c) Cree un grupo de identidades si aún no se ha creado.
    d) Ejecute el comando `New-ProvScheme`. Por ejemplo:

```
New-ProvScheme -ProvisioningSchemeName <catalog-name>
-HostingUnitName gcp-hostint-unit
-MasterImageVM XDHyp:\HostingUnits\gcp-hostint-unit\catalog-
    vda.vm
-MachineProfile XDHyp:\HostingUnits\gcp-hostint-unit\catalog-
    machine.vm
```

3. Termine de crear el catálogo de máquinas.

Para actualizar el catálogo de máquinas con un nuevo perfil de máquina:

1. Ejecute el comando `Set-ProvScheme`. Por ejemplo:

```
Set-ProvScheme -ProvisioningSchemeName <catalog-name>
-MasterImageVM XDHyp:\HostingUnits<hostin-unit>\catalog-vda.vm
-MachineProfile "DHyp:\HostingUnits<hostin-unit>\catalog-machine.
    vm
```

Para aplicar el cambio realizado en `Set-ProvScheme` a las máquinas virtuales existentes, ejecute el comando `Set-ProvVMUpdateTimeWindow`.

1. Ejecute el comando `Set-ProvVMUpdateTimeWindow`. Por ejemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
    VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```


2. Reinicie las máquinas virtuales.

Crear máquinas virtuales de Windows 11 en el nodo de arrendatario único

Puede crear máquinas virtuales de Windows 11 en GCP. Sin embargo, si instala Windows 11 en la imagen maestra, debe habilitar vTPM durante el proceso de creación de la imagen maestra. Además, debe habilitar vTPM en el origen del perfil de máquina (plantilla de instancia o máquina virtual).

Los pasos clave para crear máquinas virtuales de Windows 11 en el nodo de arrendatario único son:

1. Configurar los entornos de virtualización de Google Cloud. Para obtener información, consulte Entornos de Google Cloud.
2. Instalar un VDA. Consulte Instalar VDA.
3. Crear una conexión con entornos de Google Cloud. Para obtener más información, consulte Conexión con entornos de nube de Google.
4. Crear una imagen maestra de Bring Your Own License (BYOL) de Windows 11 e importarla en Google Cloud. Consulte Crear una imagen maestra de BYOL para Windows 11.
5. Crear el origen del perfil de la máquina: aprovisione la máquina virtual en el nodo de arrendatario único y habilite el vTPM del perfil de máquina de origen. Consulte Aprovisionar una máquina virtual en un nodo de arrendatario único.
6. Crear un catálogo de máquinas de MCS con el origen del perfil de máquina de Windows 11 habilitado con vTPM. El origen del perfil de máquina debe tener el mismo tipo de instancia que se describe en el nodo de arrendatario único. Consulte Crear un catálogo de máquinas de MCS con el origen del perfil de máquina de Windows 11.

Crear una imagen maestra de BYOL para Windows 11

Hay dos opciones para crear una imagen maestra de BYOL para Windows 11 e importar la imagen maestra en Google Cloud:

- Usar las herramientas de Cloud Build de Google Cloud
- Crear la imagen maestra en cualquier otro hipervisor

Usar las herramientas de Cloud Build de Google Cloud

1. Cargue los archivos de instalación ISO de Windows 11, SDK de GCP, .NET Framework y PowerShell en el depósito de almacenamiento de GCP.
2. Proporcione la ubicación del archivo en el archivo `.yaml` de Cloud Build como parámetro.
3. Ejecute el siguiente Cloud Build desde la línea de comandos para compilar la imagen final de Windows 11. GCP arranca y crea la imagen maestra en el proyecto seleccionado mediante un flujo de trabajo de Daisy en GCP, y la imagen maestra se importa a GCP.


```
gcloud compute instances import INSTANCE-NAME--source-uri=gs://
    BUCKET/IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE
    --byol --machine-type=MACHINE-TYPE --zone=ZONE
```

> **Nota:**
>
> Sustituya todo el texto en mayúscula por los detalles reales del recurso.

Para obtener la información completa, consulte Crear imágenes de BYOL de Windows personalizadas.

Crear la imagen maestra en cualquier otro hipervisor

1. Cree la imagen maestra de Windows 11 con cualquier otro hipervisor.
2. Exporte la imagen maestra en formato OVF a la máquina local.
3. Cargue los archivos OVF en el depósito de almacenamiento de GCP mediante la CLI de gcloud local.

```
gsutil cp LOCAL_IMAGE_PATH_OVF_FILES gs://BUCKET_NAME/
```

4. Ejecute el siguiente Cloud Build desde la línea de comandos para compilar la imagen final de Windows 11. GCP arranca y crea la imagen maestra en el proyecto seleccionado mediante un flujo de trabajo de Daisy en GCP, y la imagen maestra se importa a GCP.

```
gcloud compute instances import INSTANCE-NAME --source-uri=gs://
    BUCKET/IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE
    --byol --machine-type=MACHINE-TYPE --zone=ZONE
```

> **Nota:**
>
> Sustituya todo el texto en mayúscula por los detalles reales del recurso.

Aprovisionar una máquina virtual en un nodo de arrendatario único

Use los nodos de arrendatario único para mantener sus máquinas virtuales separadas físicamente de las máquinas virtuales de otros proyectos, o para agruparlas en el mismo hardware de host. Para obtener información sobre el nodo de arrendatario único, consulte el documento de GCP Descripción general de los usuarios únicos.

Para aprovisionar una máquina virtual (origen del perfil de máquina) en el nodo de arrendatario único, consulte el documento de GCP Aprovisionar VM en nodos de usuario único.

> **Nota:**
>
> - Seleccione el mismo tipo de instancia y región que el grupo de nodos.
> - Habilite vTPM en la sección de VM protegida. Para obtener más información, consulte Guía de inicio rápido: Habilita las opciones de VM protegida.
> - Inhabilite Bitlocker en la máquina virtual de origen.

Crear un catálogo de máquinas de MCS con el origen del perfil de máquina de Windows 11

Puede crear un catálogo de máquinas de MCS para crear máquinas virtuales de Windows 11 mediante los comandos de Web Studio o PowerShell.

> **Nota:**
>
> - Para la imagen maestra, seleccione instantánea o VM de Windows 11.
> - Para el origen del perfil de la máquina, seleccione VM de Windows 11 como perfil de máquina. El origen del perfil de máquina debe tener el mismo tipo de instancia que se describe en el nodo de arrendatario único.

Para obtener información sobre el uso de Web Studio, consulte Crear un catálogo de máquinas mediante Web Studio.

Para obtener información sobre los comandos de PowerShell, consulte Crear un catálogo de máquinas mediante un perfil de máquina

Después de crear el catálogo y encender las máquinas virtuales, puede ver las máquinas virtuales de Windows 11 que se ejecutan en el nodo de arrendatario único en la consola de Google Cloud.

Máquinas virtuales y discos con etiquetas heredadas

Las máquinas virtuales y los discos del catálogo de máquinas de MCS (disco de identidad, disco con caché de escritura y disco del sistema operativo) pueden heredar las etiquetas de un origen de perfil de máquina (plantilla de instancia o instancia de máquina virtual de GCP). Puede usar las etiquetas para distinguir las instancias pertenecientes a diferentes equipos (por ejemplo, team:research y team:analytics) y usarlas para la contabilidad de costes o la elaboración de presupuestos. Para obtener más información sobre las etiquetas, consulte el documento de GCP Organize resources using labels.

Puede crear o actualizar un catálogo y actualizar las máquinas virtuales existentes para que hereden las etiquetas a través del origen de perfil de máquina.

Esta función se aplica a catálogos de máquinas de MCS persistentes y no persistentes.

Puede realizar lo siguiente:

- Crear un catálogo con etiquetas heredadas
- Actualizar un catálogo existente con etiquetas heredadas
- Actualizar las máquinas virtuales existentes con etiquetas heredadas
- Obtener información para las etiquetas de VM y discos de arranque
- Quitar una máquina virtual

Crear un catálogo con etiquetas heredadas

Para crear un catálogo de máquinas de MCS en el que las máquinas virtuales y el disco hereden las etiquetas del origen del perfil de máquina, haga lo siguiente:

1. Cree un origen de perfil de máquina (instancia de VM o plantilla de instancia) con etiquetas. Para obtener información sobre la creación de máquinas virtuales con etiquetas, consulte el documento de GCP Create resources with labels. Se crea una plantilla de instancia a partir de la VM y toma las etiquetas definidas en la VM.
2. Cree un catálogo de MCS mediante la Configuración completa o los comandos de PowerShell.
3. Si usa la interfaz de Configuración completa, en la página **Imagen**, seleccione **Usar un perfil de máquina** y, a continuación, seleccione la VM o plantilla.
4. Si usa comandos de PowerShell, haga lo siguiente:

   a) Abra la ventana de PowerShell.

   b) Ejecute asnp citrix*.

   c) Crear un grupo de identidades. El grupo de identidades es un contenedor para las cuentas de Active Directory (AD) de las máquinas virtuales que se crearán.

   d) Cree las cuentas de equipo de AD necesarias en Active Directory.

   e) Ejecute el comando `New-ProvScheme` para crear un catálogo. Por ejemplo:

   New-ProvScheme con plantilla como entrada de perfil de máquina (catálogo persistente):

```
New-ProvScheme `
-ProvisioningSchemeName "catalog-name" `
-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `
-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `
-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.
   vm" `
-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\
   instanceTemplates.folder\instance-template-name.template" `
```

   New-ProvScheme con plantilla de instancia como entrada de perfil de máquina (catálogo no persistente):


```
New-ProvScheme `
-ProvisioningSchemeName "catalog-name" `
-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `
-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `
-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.
    vm" `
-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\
    instanceTemplates.folder\instance-template-name.template" `
-CleanOnBoot
```

New-ProvScheme con instancia de VM como entrada de perfil de máquina (catálogo persistente):

```
New-ProvScheme `
-ProvisioningSchemeName "catalog-name" `
-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `
-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `
-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.
    vm" `
-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name
    .vm" `
```

New-ProvScheme con instancia de VM como entrada de perfil de máquina (catálogo no persistente):

```
New-ProvScheme `
-ProvisioningSchemeName "catalog-name" `
-HostingUnitUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `
-IdentityPoolUid "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" `
-MasterImageVM "XDHyp:\HostingUnits\hosting-unit-name\vm-name.
    vm" `
-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name
    .vm" `
-CleanOnBoot
```

f) Registre el esquema de aprovisionamiento como un catálogo de broker.

g) Agregue las VM al catálogo.

Actualizar un catálogo existente con etiquetas heredadas

Para actualizar un catálogo para que tenga un nuevo perfil de máquina, ejecute el comando Set-ProvScheme. Después de ejecutar el comando, las nuevas máquinas virtuales que se agreguen al catálogo tendrán las etiquetas del nuevo origen de perfil de máquina. El catálogo no persistente se actualiza en el siguiente encendido.

Por ejemplo:

Set-ProvScheme con plantilla de instancia como entrada de perfil de máquina:


```
Set-ProvScheme `
-ProvisioningSchemeName "catalog-name" `
-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\
   instanceTemplates.folder\instance-template-name.template" `
```

Set-ProvScheme con instancia de VM como entrada de perfil de máquina:

```
Set-ProvScheme `
-ProvisioningSchemeName "catalog-name" `
-MachineProfile "XDHyp:\HostingUnits\hosting-unit-name\vm-name.vm" `
```

Actualizar las máquinas virtuales existentes con etiquetas heredadas

Para actualizar las máquinas virtuales existentes con el origen de perfil de máquina actualizado, ejecute los siguientes comandos:

1. `Set-ProvScheme`
2. `Set-ProvVMUpdateTimeWindow`. Por ejemplo:

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
      VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
   ```

3. Reinicie las máquinas virtuales.

Obtener información para las etiquetas de VM y discos de arranque

Después de crear las máquinas virtuales, puede obtener la información de las etiquetas de VM y del disco de arranque mediante el comando `Get-Item` con el parámetro `AdditionalData`.

Para obtener la información de etiqueta de VM, ejecute el siguiente comando:

```
(Get-Item XDHyp:\HostingUnits\hosting-unit-name\vm_name.vm).
   AdditionalData.Tags
```

Para obtener la información de etiqueta del disco de arranque, ejecute el siguiente comando:

```
(Get-Item XDHyp:\HostingUnits\hosting-unit-name\vm_name.vm\bootdisk-
   name.attacheddisk).AdditionalData.Tags
```

> **Nota:**
>
> Para mantener la coherencia entre los distintos hipervisores, hemos usado el término Etiquetas para mostrar las etiquetas de GCP.

Quitar una máquina virtual

Puede optar por quitar una máquina virtual de un catálogo, pero no puede eliminarla de GCP. En este caso, las etiquetas de Citrix solo se quitan de la VM. Todas las demás etiquetas agregadas no se eliminan de la VM. Puede quitar una máquina virtual desde la interfaz de Configuración completa o usar los comandos de PowerShell.

Mediante la interfaz de Configuración completa

1. Seleccione y haga clic con el botón secundario en la máquina virtual.
2. Haga clic en **Eliminar**.
3. Seleccione **Quitar las máquinas virtuales del catálogo pero no eliminarlas**.

Mediante los comandos de PowerShell Ejecute `Remove-ProvVM` con el parámetro `ForgetVM`. Para obtener más información, consulte el documento del SDK Remove-ProvVM.

Google Cloud Marketplace

Puede buscar y seleccionar imágenes que ofrece Citrix en **Google Cloud Marketplace** para crear catálogos de máquinas. Actualmente, MCS solo admite el flujo de trabajo de perfiles de máquina para esta función.

Para buscar el producto de VM Citrix VDA en Google Cloud Marketplace, vaya a https://console.cloud.google.com/marketplace.

Puede usar una imagen personalizada o una imagen preparada por Citrix en **Google Cloud Marketplace** para actualizar una imagen de un catálogo de máquinas.

> **Nota:**
>
> Si el perfil de la máquina no contiene información sobre el tipo de almacenamiento, el valor se deriva de las propiedades personalizadas.

Las imágenes compatibles de Google Cloud Marketplace son:

- Windows 2019 de sesión única
- Windows 2019 multisesión
- Ubuntu

Ejemplo de uso de una imagen preparada por Citrix como origen para crear un catálogo de máquinas:


```
New-ProvScheme -ProvisioningSchemeName GCPCatalog \
-HostingUnitName GcpHu -IdentityPoolName gcpPool -CleanOnBoot \
-MasterImageVM XDHyp:\HostingUnits\GcpHu\images.folder\citrix-daas-
   win2019-single-vda-v20220819.publicimage \
-MachineProfile XDHyp:\HostingUnits\GcpHu\Base.vm
```

Qué hacer a continuación

- Si este es el primer catálogo creado, Web Studio le guiará para crear un grupo de entrega
- Para revisar todo el proceso de configuración, consulte Instalar y configurar
- Para administrar catálogos, consulte Administrar catálogos de máquinas y Administrar un catálogo de Google Cloud Platform

Más información

- Crear y administrar conexiones y recursos
- Conexión con entornos de Google Cloud
- Crear catálogos de máquinas

Crear un catálogo de máquinas de HPE Moonshot

August 17, 2024

Crear catálogos de máquinas describe los asistentes con los que se crea un catálogo de máquinas. La siguiente información incluye detalles específicos de los entornos de HPE Moonshot.

> **Nota:**
>
> - Crear una conexión con HPE Moonshot
> - Compruebe que tiene uno o más nodos de HPE Moonshot disponibles e instale los VDA en esos nodos.
> - Para obtener información sobre cómo crear la imagen de cartucho inicial de HPE Moonshot, consulte el documento OS Deployment on Moonshot User Guide.

Puede crear un catálogo de máquinas de HPE Moonshot con:

- Web Studio
- Comandos de PowerShell

Crear un catálogo de máquinas mediante Web Studio

En el asistente de **Configuración de catálogo de máquinas**:

1. En la página **Sistema operativo**, seleccione **SO multisesión** o **SO de sesión única**.
2. En la página **Administración de máquinas**, seleccione **Máquinas con administración de energía** y **Otro servicio o tecnología**.
3. En la página **Máquinas virtuales**, agregue máquinas y sus cuentas de máquinas de Active Directory. Puede realizar una de las siguientes acciones:
    - Haga clic en **Agregar máquinas** para agregar máquinas manualmente. Aparecerá la ventana **Seleccionar VM**. Expanda la conexión de chasis HPE Moonshot que creó anteriormente y seleccione los nodos (VM) que quiere agregar. A continuación, agregue los nombres de las cuentas de máquina asociadas.
    - Haga clic en **Agregar archivo CSV** para agregar máquinas en bloque. Para obtener información sobre el uso de archivos CSV para agregar máquinas, consulte Usar archivos CSV para agregar máquinas en bloque a un catálogo.

Las páginas **Ámbitos** y **Resumen** no contienen información específica de HPE Moonshot.

Crear un catálogo de máquinas mediante comandos de PowerShell

Ejecute los comandos `New-BrokerCatalog` y `New-BrokerMachine` de PowerShell para crear un catálogo de brokers e importar máquinas a dicho catálogo.

Por ejemplo:

```
1 New-BrokerCatalog  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
     "103.14.252.249" -AllocationType "Random" -IsRemotePC $False -
     MachinesArePhysical $False -MinimumFunctionalLevel "L7_20" -Name "
     BurMC" -PersistUserChanges "OnLocal" -ProvisioningType "Manual" -
     Scope @() -SessionSupport "MultiSession" -ZoneUid "e166e2cb-25dc
     -4578-bc07-bcf2a82d1463"
2 New-BrokerMachine  -AdminAddress "MyDDC.MyDomain.local" -AdminClientIP
     "103.14.252.249" -CatalogUid 3 -HostedMachineId "c10n1" -
     HypervisorConnectionUid 4 -IsReserved $False -MachineName "S
     -1-5-21-2589939477-3963209805-1860259709-1121"
```

Qué hacer a continuación

- Si este es el primer catálogo creado, Web Studio le guiará para crear un grupo de entrega
- Para revisar todo el proceso de configuración, consulte Instalar y configurar
- Para administrar catálogos, consulte Administrar catálogos de máquinas y Administrar un catálogo de HPE Moonshot

Más información

- Crear y administrar conexiones y recursos
- Conexión a HPE Moonshot
- Crear catálogos de máquinas

Crear un catálogo de Microsoft Azure

August 20, 2024

> **Nota:**
>
> Desde julio de 2023, Microsoft cambió el nombre de Azure Active Directory (Azure AD) a Microsoft Entra ID. En este documento, cualquier referencia a Azure Active Directory, Azure AD o AAD ahora se refiere a Microsoft Entra ID.

Crear catálogos de máquinas describe los asistentes con los que se crea un catálogo de máquinas. La siguiente información incluye detalles específicos de los entornos de nube de Microsoft Azure Resource Manager.

> **Nota:**
>
> Antes de crear un catálogo de Microsoft Azure, debe terminar de crear una conexión con Microsoft Azure. Consulte Conexión con Microsoft Azure.

Creación de un catálogo de máquinas

Puede crear un catálogo de máquinas de dos maneras:

- Crear un catálogo de máquinas con una imagen de Azure Resource Manager en Web Studio
- Crear un catálogo de máquinas con PowerShell

Crear un catálogo de máquinas con una imagen de Azure Resource Manager en Web Studio

Una imagen puede ser un disco, una instantánea o la versión de una imagen de una definición de imagen en Azure Compute Gallery que se usa para crear las máquinas virtuales en un catálogo de máquinas. Antes de crear el catálogo de máquinas, cree una imagen en Azure Resource Manager. Para obtener información general acerca de las imágenes, consulte Crear catálogos de máquinas.

> **Nota:**
>
> Se retiró la compatibilidad con el uso de una imagen maestra de una región diferente a la configurada en la conexión del host. Use Azure Compute Gallery para replicar la imagen maestra en la región deseada.

Durante la preparación de la imagen, se crea una VM de preparación basada en la máquina virtual original. Esta máquina virtual de preparación está desconectada de la red. Para desconectar la red de la máquina virtual de preparación, se crea un grupo de seguridad de red para denegar todo el tráfico entrante y saliente. El grupo de seguridad de red se crea automáticamente una vez por catálogo. El nombre del grupo de seguridad de red es `Citrix-Deny-All-a3pgu-GUID`, donde el GUID se genera aleatoriamente. Por ejemplo, `Citrix-Deny-All-a3pgu-3f161981-28e2-4223-b797-88b04d336dd1`.

En el asistente para la creación de catálogos de máquinas:

- Las páginas **Tipo de máquina** y **Administración de máquinas** no contienen información específica de Azure. Siga las instrucciones indicadas en el artículo Crear catálogos de máquinas.
- En la página **Imagen**, elija una imagen que quiera usar como plantilla para crear máquinas en este catálogo.

  Si selecciona **Imagen maestra** como el tipo de imagen que va a usar, haga clic en **Seleccionar una imagen** y siga estos pasos para seleccionar una imagen maestra según sea necesario:

  1. (Aplicable solo a las conexiones configuradas con imágenes compartidas en o entre arrendatarios). Seleccione una suscripción en la que resida la imagen.
  2. Seleccione un grupo de recursos.
  3. Vaya a Azure VHD, Azure Compute Gallery o la versión de imagen de Azure. Si es necesario, agregue una nota a la imagen seleccionada.

  Al seleccionar una imagen, tenga en cuenta lo siguiente:

  - Compruebe que hay un VDA de Citrix instalado en la imagen.
  - Si selecciona un disco duro virtual (VHD) conectado a una máquina virtual, debe apagar esta antes de continuar con el siguiente paso.

  > **Nota:**
  >
  > - La suscripción correspondiente a la conexión (host) que creó las máquinas del catálogo se indica con un punto verde. Las demás suscripciones son aquellas en las que se comparte Azure Compute Gallery con esa suscripción. En esas suscripciones, solo se muestran las galerías compartidas. Para obtener información sobre cómo configurar las suscripciones compartidas, consulte Compartir imágenes con un arrendatario (entre suscripciones) y Compartir imágenes entre arrendatarios.

- Es obligatorio usar un perfil de máquina con Inicio seguro como **Tipo de seguridad** al seleccionar una imagen o una instantánea que tenga habilitado el inicio seguro. A continuación, para habilitar o inhabilitar SecureBoot y vTPM, especifique sus valores en el perfil de la máquina. El inicio de confianza no se admite en Shared Image Gallery. Para obtener información sobre el inicio de confianza de Azure, consulte https://docs.microsoft.com/en-us/azure/virtual-machines/trusted-launch.
- Puede crear un esquema de aprovisionamiento mediante un disco de SO efímero en Windows con inicio seguro. Al seleccionar una imagen con inicio seguro, debe seleccionar un perfil de máquina con inicio seguro que esté habilitado con vTPM. Para crear catálogos de máquinas con un disco de SO efímero, consulte Cómo crear máquinas con discos de SO efímeros.
- Durante la replicación de imágenes, puede continuar y seleccionar la imagen como imagen maestra y completar la configuración. Sin embargo, es posible que la creación de catálogos tarde más tiempo en completarse mientras se replica la imagen. MCS necesita que la replicación se complete en una hora a partir de la creación de catálogos. Si la replicación tarda más, no se crean los catálogos. Puede verificar el estado de la replicación en Azure. Inténtelo de nuevo si la replicación sigue pendiente o después de que se haya completado.
- Al seleccionar una imagen maestra para catálogos de máquinas en Azure, MCS identifica el tipo de SO en función de la imagen maestra y el perfil de máquina que seleccione. Si MCS no puede identificarlo, seleccione el tipo de SO que coincida con el de la imagen maestra.
- Puede aprovisionar un catálogo de máquinas virtuales de 2.ª generación mediante una imagen de 2.ª generación para mejorar el rendimiento del tiempo de arranque. Sin embargo, no se admite la creación de catálogos de máquinas de 2.ª generación con una imagen de 1.ª generación. Del mismo modo, tampoco se admite la creación de catálogos de máquinas de 1.ª generación con una imagen de 2.ª generación. Además, cualquier imagen antigua que no tenga información de generación es una imagen de 1.ª generación.

Si selecciona **Imagen preparada** como el tipo de imagen que va a usar, haga clic en **Seleccionar una imagen** y seleccione una imagen preparada según sea necesario.

Para garantizar la creación correcta de la máquina virtual, verifique que la imagen tenga instalado Citrix VDA 2311 o una versión posterior y que E/S de MCS esté presente en el VDA.

Tras seleccionar una imagen, la casilla **Usar un perfil de máquina (obligatoria para Azure Active Directory)** se selecciona automáticamente. Haga clic en **Seleccione un perfil de máquina** para buscar una VM o una especificación de plantilla de ARM en una lista de grupos de recursos. Las máquinas virtuales del catálogo pueden heredar configuraciones del perfil de máquina seleccionado.

Valide la especificación de plantilla ARM para asegurarse de que se puede utilizar como perfil de máquina para crear un catálogo de máquinas. Hay dos formas de validar la especificación de la plantilla ARM:

- Después de seleccionar la especificación de plantilla ARM en la lista de grupos de recursos, haga clic en **Siguiente**. Aparecen mensajes de error si la especificación de plantilla ARM contiene errores.
- Ejecute uno de estos comandos de PowerShell:
  * `Test-ProvInventoryItem -HostingUnitName <string> -InventoryPath <string>`
  * `Test-ProvInventoryItem -HostingUnitUid <Guid> -InventoryPath <string>`

Algunos ejemplos de configuraciones que las máquinas virtuales pueden heredar de un perfil de máquina incluyen:

- Redes aceleradas
- Diagnóstico de arranque
- Almacenamiento en caché de discos de host (relacionado con discos de SO y de E/S de MCS)
- Tamaño de máquina (a menos que se especifique lo contrario)
- Etiquetas colocadas en la máquina virtual

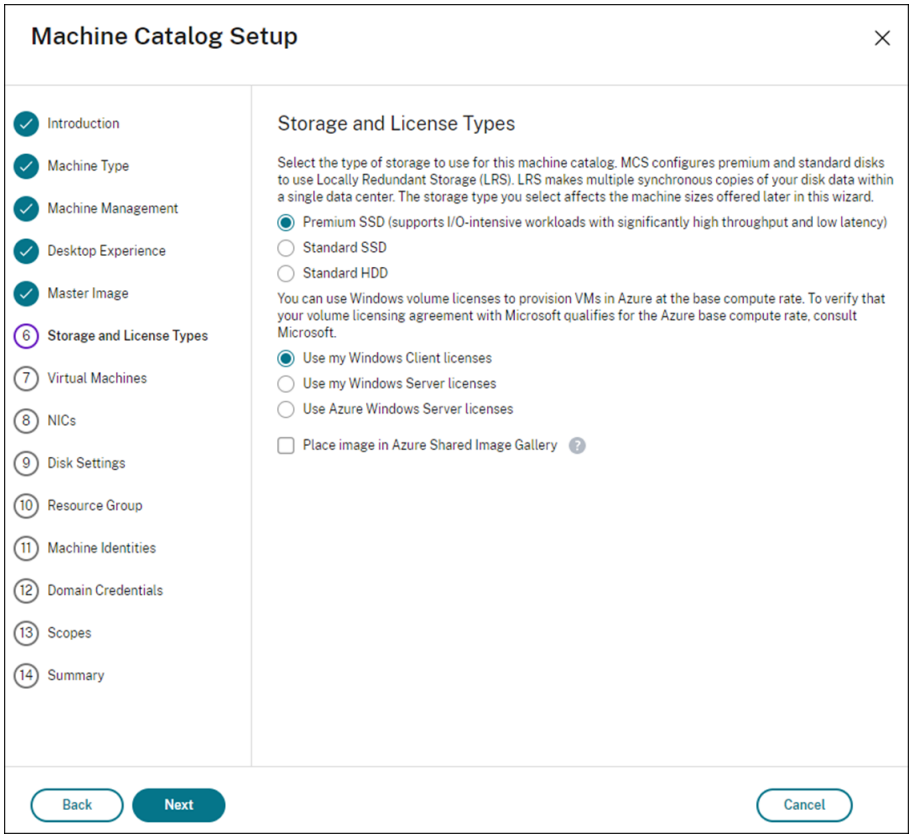
Tras crear el catálogo, podrá ver las configuraciones que la imagen hereda del perfil de máquina. En el nodo **Catálogos de máquinas**, seleccione el catálogo para ver sus detalles en el panel inferior. A continuación, haga clic en la ficha **Propiedades de plantilla** para ver las propiedades del perfil de máquina. La sección **Etiquetas** muestra hasta tres etiquetas. Para ver todas las etiquetas colocadas en la máquina virtual, haga clic en **Ver todo**.

Si quiere que MCS aprovisione máquinas virtuales en un host dedicado de Azure, active la casilla de verificación **Usar un grupo de hosts dedicado** y, a continuación, seleccione un grupo de hosts de la lista. Un grupo de hosts es un recurso que representa un conjunto de hosts dedicados. Un host dedicado es un servicio que proporciona servidores físicos que alojan una o más VM. Su servidor está dedicado a su suscripción de Azure, no se comparte con otros suscriptores. Cuando utiliza un host dedicado, Azure garantiza que sus máquinas virtuales sean las únicas máquinas activas en ese host. Esta función es adecuada para situaciones en las que debe cumplir con requisitos normativos o de seguridad interna. Para obtener más información sobre los grupos de hosts y las consideraciones para usarlos, consulte Hosts dedicados de Azure.

> **Importante:**
>
> - Solo se muestran los grupos de hosts que tienen habilitada la ubicación automática de Azure.

> – El uso de un grupo de hosts cambia la página **Máquinas virtuales** que se ofrece más adelante en el asistente. En esa página, solo se muestran los tamaños de máquina que contiene el grupo de hosts seleccionado. Además, las zonas de disponibilidad se seleccionan automáticamente y no están disponibles para selección manual.

- La página **Tipos de licencia y almacenamiento** solo aparece cuando se usa una imagen de Azure Resource Manager.



Puede utilizar los siguientes tipos de almacenamiento para el catálogo de máquinas:

- **SSD Premium**. Ofrece una opción de almacenamiento en disco de alto rendimiento y baja latencia, adecuada para máquinas virtuales con cargas de trabajo intensivas de E/S.
- **SSD estándar**. Ofrece una opción de almacenamiento rentable, adecuada para cargas de trabajo que necesitan un rendimiento uniforme a niveles de IOPS más bajos.
- **HDD estándar**. Ofrece una opción de almacenamiento en disco fiable y de bajo coste, adecuada para máquinas virtuales que ejecutan cargas de trabajo donde no importa la latencia.
- **Disco de SO efímero de Azure**. Ofrece una opción de almacenamiento rentable que reutiliza el disco local de las VM para alojar el disco del sistema operativo. Como alternativa, puede usar PowerShell para crear máquinas que usen discos de SO efímeros. Para obtener más información, consulte Discos efímeros de Azure. Tenga en cuenta las siguientes consideraciones cuando utilice un disco de SO efímero:

* El disco de SO efímero de Azure y la E/S de MCS no se pueden habilitar al mismo tiempo.
* Para actualizar máquinas que usan discos de SO efímeros, debe seleccionar una imagen cuyo tamaño no exceda el tamaño del disco de caché o el disco temporal de la VM.
* No puede usar la opción **Conservar VM y disco del sistema durante los ciclos de energía** que se ofrece más adelante en el asistente.

> **Nota:**
>
> El disco de identidad siempre se crea con un SSD estándar, independientemente del tipo de almacenamiento que elija.

El tipo de almacenamiento determina el tamaño de las máquinas que se ofrecen en la página **Máquinas virtuales** del asistente. MCS configura discos premium y estándar para uso de almacenamiento con redundancia local (LRS). LRS hace varias copias sincrónicas de los datos en un único centro de datos. Los discos de SO efímeros de Azure usan el disco local de las VM para almacenar el sistema operativo. 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 licencias de Windows o de Linux existentes.

- Licencias de Windows: El uso de licencias de Windows junto con imágenes de Windows (imágenes que admita la plataforma Azure o imágenes personalizadas) permite ejecutar máquinas virtuales de Windows en Azure a un coste reducido. Existen dos tipos de licencias:
  * **Licencia de Windows Server**. Le permite utilizar sus licencias de Windows Server o Azure Windows Server, con lo que puede usar las ventajas híbridas de Azure. Para obtener información detallada, consulte https://azure.microsoft.com/en-us/pricing/hybrid-benefit/. Las ventajas híbridas de Azure reducen los costes de ejecución de máquinas virtuales en Azure a la tarifa básica de procesamiento, lo que elimina el gasto en licencias de Windows Server adicionales desde la galería de Azure.
  * **Licencia de cliente de Windows**. Le permite llevar sus licencias de Windows 10 y Windows 11 a Azure, con lo que puede usar máquinas virtuales con Windows 10 y Windows 11 en Azure sin necesidad de licencias adicionales. Para obtener más información, consulte Licencias de acceso de cliente y licencias de administración.

Para comprobar que la máquina virtual aprovisionada aprovecha los beneficios de las licencias, ejecute este comando de PowerShell: `Get-AzVM -ResourceGroup MyResourceGroup -Name MyVM`.

- Para el tipo de licencia de Windows Server, 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/.
- Para el tipo de licencia de cliente de Windows, compruebe que el tipo de licencia es **Windows_Client**. Encontrará instrucciones adicionales en https://docs.microsoft.com/en-us/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/.

También puede usar el SDK de PowerShell `Get-Provscheme` para hacer la verificación. Por ejemplo: `Get-Provscheme -ProvisioningSchemeName "My Azure Catalog"`. Para obtener más información sobre este cmdlet, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/.

- Licencias de Linux: Con las licencias de Linux de su propia suscripción (BYOS), no tiene que pagar por el software. El cargo de las licencias BYOS solo incluye la tarifa de hardware del procesamiento. Existen dos tipos de licencias:
  - **RHEL_BYOS**: Para usar correctamente el tipo RHEL_BYOS, habilite Red Hat Cloud Access en su suscripción de Azure.
  - **SLES_BYOS**: Las versiones de BYOS de SLES permiten el uso de SUSE.

  Puede establecer el valor de LicenseType en opciones de Linux con `New-ProvScheme` y `Set-ProvScheme`.

  Ejemplo de configuración de LicenseType en RHEL_BYOS con `New-ProvScheme`:

```
New-ProvScheme -CleanOnBoot -ProvisioningSchemeName "
    azureCatalog" -RunAsynchronously -Scope @() -SecurityGroup
    @() -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="StandardSSD_LRS" /><Property xsi:type="
    StringProperty" Name="ResourceGroups" Value="hu-dev-mcs"
    /><Property xsi:type="StringProperty" Name="OsType" Value="
    Linux" /><Property xsi:type="StringProperty" Name="
    LicenseType" Value="RHEL_BYOS" /></CustomProperties>'
```

  Ejemplo de configuración de LicenseType en SLES_BYOS con `Set-ProvScheme`:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -
    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="StandardSSD_LRS" /><Property xsi:type="
        StringProperty" Name="ResourceGroups" Value="hu-dev-mcs"
        /><Property xsi:type="StringProperty" Name="OsType" Value="
        Linux" /><Property xsi:type="StringProperty" Name="
        LicenseType" Value="SLES_BYOS" /></CustomProperties>'
```

> **Nota:**
>
> Si el valor `LicenseType` está vacío, los valores predeterminados son Azure Windows Server License o Azure Linux License, según el valor de OsType.

Ejemplo de configuración de LicenseType vacío:

```
1 Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -
      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="StandardSSD_LRS" /><Property xsi:type="
      StringProperty" Name="ResourceGroups" Value="hu-dev-mcs"
      /><Property xsi:type="StringProperty" Name="OsType" Value="
      Linux" /></CustomProperties>'
```

Consulte estos documentos para comprender los tipos de licencias y sus beneficios:

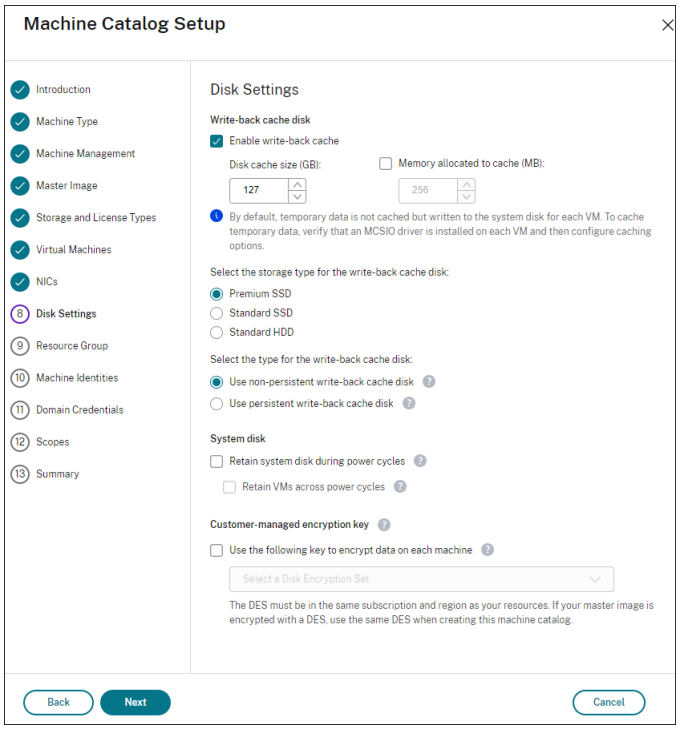
- https://docs.microsoft.com/en-us/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet
- https://docs.microsoft.com/en-us/azure/virtual-machines/linux/azure-hybrid-benefit-linux

Azure Compute Gallery (antes denominado Azure Shared Image Gallery) es un repositorio para administrar y compartir imágenes. Le permite poner sus imágenes a disposición de toda la organización. Le recomendamos almacenar una imagen en SIG al crear grandes catálogos de máquinas no persistentes, ya que, así, los discos del SO de VDA se pueden restablecer más rápidamente. Después de seleccionar **Colocar la imagen preparada en Azure Compute Gallery**, aparece la sección **Configuración de Azure Compute Gallery**, que le permite especificar más parámetros de Azure Computer Gallery:

- **Índice de máquinas virtuales por réplica de imagen**. Permite especificar la ratio de máquinas virtuales y réplicas de imagen que mantendrá Azure. De forma predeterminada, Azure mantiene una única réplica de imagen por cada 40 máquinas no persistentes. En el caso de máquinas persistentes, la cantidad predeterminada es de 1000 máquinas.

  - **Máximo de réplicas**. Permite especificar el máximo de réplicas de imagen que conservará Azure. El valor predeterminado es 100.

- En la página **Máquinas virtuales**, indique la cantidad de máquinas virtuales que quiere crear. Debe especificar al menos una y seleccionar un tamaño de máquina. Después de crear el catálogo, puede modificar el catálogo para cambiar el tamaño de la máquina.
- La página **Tarjetas NIC** no contiene información específica de Azure. Siga las instrucciones indicadas en el artículo Crear catálogos de máquinas.
- En la página **Parámetros del disco**, elija si quiere habilitar la caché de reescritura. Con la función de optimización del almacenamiento de MCS habilitada, puede configurar los siguientes parámetros al crear un catálogo: Esta configuración se aplica tanto a los entornos de Azure como a los de GCP.



Después de habilitar la caché de reescritura, puede hacer lo siguiente:

  - Puede configurar la RAM y el tamaño del disco utilizados para almacenar en caché datos temporales. Para obtener más información, consulte Configurar la caché de datos temporales.
  - Seleccione el tipo de almacenamiento del disco de caché de reescritura. Están disponibles las siguientes opciones de almacenamiento para uso con el disco de caché de reescritura:
    * SSD Premium
    * SSD estándar
    * HDD estándar

- Elija si prefiere que el disco de caché de reescritura sea persistente para las máquinas virtuales aprovisionadas. Seleccione **Habilitar caché de reescritura** para que estas opciones estén disponibles. De forma predeterminada, se selecciona **Usar disco no persistente de caché de reescritura**.
- Seleccione el tipo de disco de caché de reescritura.
  - **Usar disco no persistente de caché de reescritura**. Si se selecciona, el disco de caché de reescritura se elimina durante los ciclos de energía. Se perderán todos los datos redirigidos a él. Si el disco temporal de la VM tiene suficiente espacio, se usa para alojar el disco de caché de reescritura para reducir los costes. Tras la creación del catálogo, puede comprobar si las máquinas aprovisionadas utilizan el disco temporal. Para ello, haga clic en el catálogo y verifique la información de la ficha **Propiedades de plantilla**. Si se usa el disco temporal, verá **Disco no persistente de caché de reescritura**, y su valor es **Sí (con el disco temporal de la máquina virtual)**. De lo contrario, verá **Disco no persistente de caché de reescritura**, y su valor es **No (sin usar el disco temporal de la VM)**.
  - **Usar disco persistente de caché de reescritura**. Si se selecciona, el disco de caché de reescritura persiste en las máquinas virtuales aprovisionadas. Habilitar esta opción aumenta los costes de almacenamiento.
- Elija si quiere conservar las VM y los discos del sistema para los VDA durante los ciclos de energía.

  Conservar VM y disco del sistema durante los ciclos de energía. Disponible cuando se ha seleccionado **Habilitar caché de reescritura**. De forma predeterminada, las VM y los discos del sistema se eliminan al apagar la máquina y se crean de nuevo al iniciarla. Si quiere reducir los tiempos de reinicio de las máquinas virtuales, seleccione esta opción. Recuerde que habilitar esta opción también aumenta los costes de almacenamiento.
- Elija si quiere habilitar el **ahorro de costes de almacenamiento**. Si se habilita, para ahorrar costes de almacenamiento, revierta el disco de almacenamiento a un disco duro estándar cuando la máquina virtual se apague. La máquina virtual cambia a sus parámetros originales al reiniciarse. La opción se aplica tanto a los discos de almacenamiento como a los discos de caché de reescritura. También puede usar PowerShell. Consulte Cambiar el tipo de almacenamiento a un nivel inferior al apagar una máquina virtual.

  > **Nota:**
  >
  > Microsoft impone restricciones al cambiar el tipo de almacenamiento durante el apagado de máquinas virtuales. También es posible que, en el futuro, Microsoft bloquee cambios en el tipo de almacenamiento. Para obtener más información, consulte este artículo de Microsoft.
- Elija si quiere cifrar los datos de las máquinas aprovisionadas en el catálogo. El cifrado del

lado del servidor con una clave de cifrado administrada por el cliente permite administrar el cifrado a nivel de disco administrado y proteger los datos que contengan las máquinas del catálogo. Para obtener más información, consulte Cifrado del lado del servidor de Azure.

- En la página **Grupo de recursos**, elija si quiere crear grupos de recursos o usar los grupos existentes.
  - Si opta por crear grupos de recursos, seleccione **Siguiente**.
  - Si decide utilizar los grupos de recursos existentes, seleccione esos grupos en la lista **Grupos de recursos de aprovisionamiento disponibles**. **Recuerde:** Debe seleccionar grupos suficientes para las máquinas que está creando en el catálogo. Si no elige suficientes, aparecerá un mensaje. 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.
- En la página **Identidades de las máquinas**, elija un tipo de identidad y configure las identidades de las máquinas de este catálogo. Si selecciona las máquinas virtuales como **unidas a Azure Active Directory**, puede agregarlas a un grupo de seguridad de Azure AD. Estos son los pasos detallados:
  1. En el campo **Tipo de identidad**, seleccione **Unido a Azure Active Directory**. Aparecerá la opción **Grupo de seguridad de Azure AD (opcional)**.
  2. Haga clic en **Grupo de seguridad de Azure AD: Crear nuevo**.
  3. Introduzca un nombre de grupo y, a continuación, haga clic en **Crear**.
  4. Siga las instrucciones que aparecen en pantalla para iniciar sesión en Azure.
     Si el nombre del grupo no existe en Azure, aparecerá un icono verde. De lo contrario, aparecerá un mensaje de error en el que se le pide que introduzca un nombre nuevo.
  5. Introduzca el esquema de nomenclatura de las cuentas de máquina para las máquinas virtuales.

  Tras la creación del catálogo, Citrix Virtual Apps and Desktops accede a Azure en su nombre y crea el grupo de seguridad y una regla de pertenencia dinámica para el grupo. Según la regla, las máquinas virtuales con el esquema de nomenclatura especificado en este catálogo se agregan automáticamente al grupo de seguridad.

  Para agregar a este catálogo máquinas virtuales con un esquema de nomenclatura diferente, debe iniciar sesión en Azure. A continuación, Citrix Virtual Apps and Desktops puede acceder a Azure y crear una regla de pertenencia dinámica basada en el nuevo esquema de nomenclatura.

  Para poder eliminar el grupo de seguridad de Azure al eliminar este catálogo, también es necesario iniciar sesión en Azure.

- Las páginas **Credenciales de dominio** y **Resumen** no contienen información específica de Azure. Siga las instrucciones indicadas en el artículo Crear catálogos de máquinas.

Complete el asistente.

Condiciones para que el disco temporal de Azure sea apto como disco de caché de reescritura

Solamente puede usar el disco temporal de Azure como disco de caché de reescritura si se cumplen todas las condiciones siguientes:

- El disco de caché con escritura no debe persistir, ya que el disco temporal de Azure no es adecuado para datos persistentes.
- El tamaño de VM de Azure elegido debe incluir un disco temporal.
- No es necesario que el disco de SO efímero esté habilitado.
- Aceptar colocar el archivo de caché con escritura en el disco temporal de Azure.
- El tamaño del disco temporal de Azure debe ser mayor que el tamaño total de (tamaño del disco de caché de reescritura + espacio reservado para el archivo de paginación + 1 GB de espacio de búfer).

Casos de disco no persistente de caché de reescritura

En la siguiente tabla se describen tres casos diferentes en los que se utiliza un disco temporal para la caché de reescritura al crear un catálogo de máquinas.

Caso	Resultado
Se cumplen todas las condiciones para usar un disco temporal para la caché de reescritura.	El archivo WBC `mcsdif.vhdx` se coloca en el disco temporal.
El disco temporal no tiene suficiente espacio para uso de caché de reescritura.	Se crea un disco VHD `MCSWCDisk` y se coloca un archivo WBC `mcsdif.vhdx` en este disco.
El disco temporal tiene espacio suficiente para usar caché de reescritura, pero `UseTempDiskForWBC` está configurado como **false**.	Se crea un disco VHD `MCSWCDisk` y se coloca un archivo WBC `mcsdif.vhdx` en este disco.

Crear una especificación de plantilla de Azure

Puede crear una especificación de plantilla de Azure en Azure Portal y utilizarla en Web Studio y en los comandos de PowerShell para crear o actualizar catálogos de máquinas de MCS.

Para crear una especificación de plantilla de Azure para una máquina virtual existente:

1. Vaya a Azure Portal. Seleccione un grupo de recursos y, a continuación, seleccione la VM y la interfaz de red. En el menú **...** de la parte superior, haga clic en **Export template**.
2. Desmarque la casilla **Include parameters** si quiere crear una especificación de plantilla para el aprovisionamiento de catálogos.
3. Haga clic en **Add to library** para modificar la especificación de la plantilla más adelante.
4. En la página **Importing template**, introduzca la información requerida, como **Name**, **Subscription**, **Resource Group**, **Location** y **Version**. Haga clic en **Next: Edit Template**.
5. También necesita una interfaz de red como recurso independiente si quiere aprovisionar catálogos. Por lo tanto, debe quitar cualquier `dependsOn` especificado en la especificación de la plantilla. Por ejemplo:

   ```
   "dependsOn": [
   "[resourceId('Microsoft.Network/networkInterfaces', 'tnic937')]"
   ],
   ```

6. Haga clic en **Review+Create** y cree la especificación de la plantilla.
7. En la página **Template Specs**, compruebe la especificación de plantilla que acaba de crear. Haga clic en la especificación de la plantilla. En el panel de la izquierda, haga clic en **Versions**.
8. Para crear otra versión, haga clic en **Create new version**. Especifique un nuevo número de versión, modifique la especificación de la plantilla actual y haga clic en **Review+Create** para crear la otra versión de la especificación de plantilla.

Puede obtener información sobre la especificación y la versión de la plantilla mediante estos comandos de PowerShell:

- Para obtener información sobre la especificación de la plantilla, ejecute:

  ```
  get-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.
     resourcegroup\bggTemplateSpec.templatespec
  ```

- Para obtener información sobre la versión de la especificación de la plantilla, ejecute:

  ```
  get-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.
     resourcegroup\bggTemplateSpec.templatespec\bgg1.0.
     templatespecversion
  ```


Usar la especificación de la plantilla para crear o actualizar un catálogo

Puede crear o actualizar un catálogo de máquinas de MCS mediante una especificación de plantilla como entrada de datos de un perfil de máquina. Para ello, puede utilizar Web Studio o los comandos de PowerShell.

- Para Web Studio, consulte Crear un catálogo de máquinas con una imagen de Azure Resource Manager en Web Studio
- Para PowerShell, consulte Usar la especificación de la plantilla para crear o actualizar un catálogo con PowerShell

Cifrado del lado del servidor de Azure

Citrix Virtual Apps and Desktops admite claves de cifrado administradas por el cliente para los discos administrados por Azure a través de Azure Key Vault. Gracias a esta compatibilidad, puede satisfacer los requisitos organizativos y de conformidad mediante el cifrado de los discos administrados del catálogo de máquinas con su propia clave de cifrado. Para obtener más información, consulte Cifrado del lado del servidor de Azure Disk Storage.

Al utilizar esta función para discos administrados:

- Para cambiar la clave con la que está cifrado actualmente el disco, cámbiela en `DiskEncryptionSet`. Todos los recursos asociados a ese `DiskEncryptionSet` se cifrarán con la nueva clave.
- Cuando inhabilite o elimine la clave, todas las máquinas virtuales con discos que utilicen esa clave se apagarán automáticamente. Después de apagarse, las máquinas virtuales no se podrán utilizar, a menos que la clave se vuelva a habilitar o se asigne una nueva clave. Ningún catálogo que utilice la clave se podrá encender ni se le podrán agregar máquinas virtuales.

Consideraciones importantes al utilizar claves de cifrado administradas por el cliente

Tenga en cuenta lo siguiente al usar esta funcionalidad:

- Todos los recursos relacionados con las claves administradas por el cliente (instancias de Azure Key Vault, conjuntos de cifrado de disco, máquinas virtuales, discos e instantáneas) deben residir en la misma suscripción y región.
- Los discos, las instantáneas y las imágenes cifradas con claves administradas por el cliente no pueden transferirse a otro grupo de recursos y suscripción.
- Consulte el sitio de Microsoft para conocer las limitaciones de los conjuntos de cifrado de disco por región.

> **Nota:**
>
> Para obtener información acerca de la configuración del cifrado del lado del servidor de Azure, consulte Inicio rápido: Creación de un almacén de claves mediante Azure Portal.

Clave de cifrado administrada por el cliente de Azure

Al crear un catálogo de máquinas, puede elegir si cifrar los datos presentes en las máquinas aprovisionadas en el catálogo. El cifrado del lado del servidor con una clave de cifrado administrada por el cliente permite administrar el cifrado a nivel de disco administrado y proteger los datos que contengan las máquinas del catálogo. Un conjunto de cifrado de disco (Disk Encryption Set o DES) representa una clave administrada por el cliente. Para utilizar esta función, primero debe crear el DES en Azure. Un DES tiene este formato:

- `/subscriptions/12345678-1234-1234-1234-123456789012/resourceGroups/Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/SampleEncryption`

Seleccione un DES de la lista. El DES que seleccione debe estar en la misma suscripción y región que los recursos.

Consulte Crear un catálogo de máquinas con una clave administrada por el cliente.

Cifrado de discos de Azure en el host

Puede crear un catálogo de máquinas de MCS con capacidad de cifrado en el host. Actualmente, MCS solo admite el flujo de trabajo de perfiles de máquina para esta función. Puede utilizar una máquina virtual o una especificación de plantilla como entrada para un perfil de máquina.

Este método de cifrado no cifra los datos a través del almacenamiento de Azure. El servidor que aloja la máquina virtual cifra los datos y, a continuación, los datos cifrados fluyen a través del servidor de almacenamiento de Azure. Por lo tanto, este método de cifrado cifra los datos de extremo a extremo.

Restricciones:

El cifrado de discos de Azure en el host:

- No se admite con todos los tamaños de máquina de Azure
- Es incompatible con el cifrado de discos de Azure

Para crear un catálogo de máquinas con capacidad de cifrado en el host:

1. Compruebe si la suscripción tiene habilitada la funcionalidad de cifrado en el host o no. Para ello, consulte https://learn.microsoft.com/en-us/rest/api/resources/features/get?tabs=

HTTP/. Si no está habilitada, debe habilitar la funcionalidad para la suscripción. Para obtener información sobre cómo habilitar la funcionalidad para su suscripción, consulte https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/.

2. Compruebe si un tamaño de máquina virtual de Azure determinado admite el cifrado en el host o no. Para ello, en una ventana de PowerShell, ejecute uno de los siguientes comandos:

```
PS XDHyp:\Connections<your connection>\east us.region\
   serviceoffering.folder>
```

```
PS XDHyp:\HostingUnits<your hosting unit>\serviceoffering.folder>
```

3. Cree una máquina virtual o una especificación de plantilla, como entrada para el perfil de máquina, en Azure Portal con el cifrado en el host habilitado.

   - Si quiere crear una máquina virtual, seleccione un tamaño de máquina virtual que admita el cifrado en el host. Tras crear la máquina virtual, se habilita la propiedad **Encryption at host** (Cifrado en el host).
   - Si quiere utilizar una especificación de plantilla, asigne al parámetro `Encryption at Host` el valor **true** en `securityProfile`.

4. Cree un catálogo de máquinas de MCS con un flujo de trabajo de perfil de máquina. Para ello, seleccione una máquina virtual o una especificación de plantilla.

   - Disco del sistema operativo/disco de datos: Se cifra mediante una clave gestionada por el cliente y una clave gestionada por la plataforma
   - Disco de SO efímero: Se cifra solo mediante una clave administrada por la plataforma
   - Disco de caché: Se cifra mediante una clave administrada por el cliente y una clave administrada por la plataforma

   Puede crear el catálogo de máquinas a través de Web Studio o con los comandos de PowerShell.

Obtener la información de cifrado en el host desde un perfil de máquina

Puede recuperar la información de cifrado en el host desde un perfil de máquina al ejecutar el comando de PowerShell con el parámetro `AdditionalData`. Si el parámetro `EncryptionAtHost` es **True**, indica que el cifrado en el host está habilitado para el perfil de máquina.

Por ejemplo: Cuando la entrada del perfil de máquina sea una VM, ejecute el siguiente comando:

```
(get-item XDHyp:\HostingUnits\myAzureNetwork\machineprofile.folder\abc.
   resourcegroup\def.vm).AdditionalData
```

Por ejemplo: Cuando la entrada del perfil de máquina sea una especificación de plantilla, ejecute el siguiente comando:


```
(get-item XDHyp:\HostingUnits\myAzureNetwork\machineprofile.folder\abc.
    resourcegroup\def_templatespec.templatespec\EncryptionAtHost.
    templatespecversion).AdditionalData
```

Cifrado doble en disco administrado

Puede crear un catálogo de máquinas con doble cifrado. Todos los catálogos creados con esta función tienen todos los discos cifrados del lado del servidor con claves administradas por la plataforma y por el cliente. Usted posee y mantiene el Azure Key Vault, la clave de cifrado y los conjuntos de cifrado de disco (DES).

El cifrado doble es el cifrado del lado de la plataforma (predeterminado) y el cifrado administrado por el cliente (CMEK). Por lo tanto, si usted es un cliente altamente confidencial al que le preocupa el riesgo asociado a cualquier algoritmo de cifrado, implementación o claves comprometidas, puede optar por este doble cifrado. Los discos de datos y del SO persistentes, las instantáneas y las imágenes se cifran en REST con doble cifrado.

> **Nota:**
>
> - Puede crear y actualizar un catálogo de máquinas con doble cifrado mediante Web Studio y los comandos de PowerShell. Consulte Crear un catálogo de máquinas con doble cifrado para los comandos de PowerShell.
> - Puede utilizar un flujo de trabajo no basado en perfiles de máquina o un flujo de trabajo basado en perfiles de máquina para crear o actualizar un catálogo de máquinas con doble cifrado.
> - Si utiliza un flujo de trabajo no basado en perfiles de máquina para crear un catálogo de máquinas, puede reutilizar el `DiskEncryptionSetId` almacenado.
> - Si usa un perfil de máquina, puede usar una máquina virtual o una especificación de plantilla como entrada de perfil de máquina.

Limitaciones:

- No se admite el cifrado doble en los discos Ultra Disk ni en los discos Premium SSD v2.
- El cifrado doble no se admite en discos no administrados.
- Si inhabilita una clave DiskEncryptionSet asociada a un catálogo, se inhabilitan las máquinas virtuales del catálogo.
- Todos los recursos relacionados con las claves administradas por el cliente (instancias de Azure Key Vault, conjuntos de cifrado de disco, máquinas virtuales, discos e instantáneas) deben estar en la misma suscripción y región.
- Solo puede crear un máximo de 50 conjuntos de cifrado de disco por región y suscripción.

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 los grupos de recursos de Azure vacíos existentes cuando cree un catálogo de máquinas con MCS. También puede decidir que se creen nuevos grupos de recursos para usted. Para obtener información acerca de los grupos de recursos de Azure, consulte la documentación de Microsoft.

Uso del grupo de recursos de Azure

No hay límite en el número de máquinas virtuales, discos administrados, instantáneas e imágenes por grupo de recursos de Azure (se eliminó la limitación de 240 VM/800 discos administrados por grupo de recursos de Azure).

- Al utilizar la entidad de servicio de ámbito completo para crear un catálogo de máquinas, MCS crea solo un grupo de recursos de Azure y utiliza ese grupo para el catálogo.
- Al utilizar la entidad de servicio de ámbito restringido para crear un catálogo de máquinas, debe proporcionar un grupo de recursos de Azure vacío y creado previamente para el catálogo.

Discos efímeros de Azure

Un disco efímero de Azure le permite reutilizar el disco de caché o el disco temporal para almacenar el disco del sistema operativo de una máquina virtual habilitada para Azure. Esta funcionalidad es útil en entornos de Azure que requieren un disco SSD de mayor rendimiento, en lugar de un disco HDD estándar. Para obtener información sobre cómo crear un catálogo con un disco efímero de Azure, consulte Crear un catálogo con un disco efímero de Azure.

> **Nota:**
>
> Los catálogos persistentes no admiten discos de SO efímeros.

Los discos de SO efímeros requieren que el esquema de aprovisionamiento use discos administrados y una Shared Image Gallery.

Almacenamiento de un disco de SO efímero temporal

Tiene la posibilidad de almacenar un disco de SO efímero en el disco temporal de la VM o en un disco de recursos. Esta funcionalidad le permite usar un disco de SO efímero con una máquina virtual que no tenga caché o que no tenga suficiente caché. Estas VM tienen un disco temporal o de recursos para almacenar un disco de SO efímero, como Ddv4.

Se deben tener en cuenta las siguientes cuestiones:

- Un disco efímero se almacena en el disco de caché o en el disco temporal (de recursos) de la VM. Se prefiere el disco de caché antes que el disco temporal, a menos que el disco de caché no sea lo suficientemente grande como para albergar el contenido del disco del sistema operativo.
- En el caso de las actualizaciones, si una nueva imagen es más grande que el disco de caché, pero más pequeña que el disco temporal, el disco de SO efímero se sustituye por el disco temporal de la VM.

Optimización del almacenamiento (E/S de MCS) con discos efímeros de Azure y Machine Creation Services (MCS)

El disco de SO efímero de Azure y la E/S de MCS no se pueden habilitar al mismo tiempo.

Las consideraciones importantes son las siguientes:

- No puede crear un catálogo de máquinas con el disco de SO efímero y la E/S de MCS habilitados al mismo tiempo.
- Los parámetros de PowerShell (`UseWriteBackCache` y `UseEphemeralOsDisk`) fallan con el mensaje de error correspondiente si se establecen en **true** en `New-ProvScheme` o `Set-ProvScheme`.
- Para catálogos de máquinas existentes creados con ambas funciones habilitadas, aún puede:
  - actualizar un catálogo de máquinas;
  - agregar o eliminar máquinas virtuales;
  - eliminar un catálogo de máquinas.

Azure Compute Gallery

Utilice Azure Compute Gallery (antes denominado Azure Shared Image Gallery) como repositorio de imágenes publicadas para máquinas aprovisionadas por MCS en Azure. Puede almacenar una imagen publicada en la galería para acelerar la creación e hidratación de discos de SO, mejorando los tiempos de inicio y lanzamiento de aplicaciones en máquinas virtuales no persistentes. Shared Image Gallery contiene los tres elementos siguientes:

- *Galería*: El lugar donde se almacenan las imágenes. MCS crea una galería para cada catálogo de máquinas.
- *Definición de imagen de la galería*: Esta definición incluye información (el tipo y el estado del sistema operativo, la región de Azure) sobre la imagen publicada. MCS crea una definición de imagen para cada imagen creada para el catálogo.
- *Versión de la imagen de la galería*: Cada imagen de Shared Image Gallery puede tener varias versiones, y cada versión puede tener varias réplicas en diferentes regiones. Cada réplica es una copia completa de la imagen publicada.

> **Nota:**
>
> La funcionalidad Shared Image Gallery solo es compatible con discos administrados. No está disponible para catálogos de máquinas antiguos.

Para obtener más información, consulte Almacenamiento y uso compartido de imágenes en Azure Compute Gallery.

Para obtener información sobre cómo crear o actualizar un catálogo de máquinas con una imagen de Azure Compute Gallery con PowerShell, consulte Crear o actualizar un catálogo de máquinas con una imagen de Azure Compute Gallery.

Máquinas virtuales confidenciales de Azure

Las máquinas virtuales de computación confidencial de Azure garantizan que su escritorio virtual esté cifrado en memoria y protegido mientras se usa.

Puede usar MCS para crear un catálogo con máquinas virtuales confidenciales de Azure. Para crear dicho catálogo, debe usar el flujo de trabajo del perfil de máquina. Puede usar una máquina virtual o una especificación de plantilla de Azure Resource Manager como entrada para un perfil de máquina.

Consideraciones importantes acerca de las máquinas virtuales confidenciales

Las consideraciones importantes relativas a los tamaños de máquina virtual compatibles y la creación de catálogos de máquinas con VM confidenciales son las siguientes:

- Tamaños de VM compatibles: Las máquinas virtuales confidenciales admiten los siguientes tamaños:
  - Serie DCasv5
  - Serie DCadsv5
  - Serie ECasv5
  - Serie ECadsv5
- Crear catálogos de máquinas con VM confidenciales.
  - Puede crear un catálogo de máquinas con VM confidenciales de Azure mediante Web Studio y los comandos de PowerShell.
  - Para crear un catálogo de máquinas con VM confidenciales de Azure, debe usar un flujo de trabajo basado en perfiles de máquina. Puede usar una máquina virtual o una especificación de plantilla como entrada del perfil de máquina.

- La imagen maestra y la entrada del perfil de máquina deben estar habilitadas con el mismo tipo de seguridad confidencial. Los tipos de seguridad son:
  - **VMGuestStateOnly**: VM confidencial con solo el estado de invitado de VM cifrado
  - **DiskWithVMGuestState**: VM confidencial con disco de SO y estado de invitado de máquina virtual cifrados con una clave administrada por la plataforma o una clave administrada por el cliente. Se pueden cifrar tanto los discos de SO normales como los efímeros.
- Con el parámetro AdditionalData, puede obtener información de VM confidencial de varios tipos de recursos, como discos administrados, instantáneas, imágenes de Azure Compute Gallery, máquinas virtuales y especificaciones de plantilla de Azure Resource Manager. Por ejemplo:

```
PS C:\Users\username> (get-item XDHyp:\HostingUnits\mynetwork
    \image.folder\username-dev-testing-rg.resourcegroup\
    username-dev-tsvda.vm).AdditionalData
```

  Los campos de datos adicionales son:
  - DiskSecurityType
  - ConfidentialVMDiskEncryptionSetId
  - DiskSecurityProfiles

  Para obtener la propiedad de computación confidencial de un tamaño de una máquina, ejecute el siguiente comando: `(Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\abc.serviceoffering").AdditionalData`

  El campo de datos adicional es `ConfidentialComputingType`.
- No puede cambiar la imagen maestra ni el perfil de máquina de un tipo de seguridad confidencial a un tipo de seguridad no confidencial ni de un tipo de seguridad no confidencial a uno confidencial.
- Aparecerán los mensajes de error correspondientes a cualquier configuración incorrecta.

Preparar imágenes maestras y perfiles de máquina

Antes de crear un conjunto de máquinas virtuales confidenciales, siga estos pasos para preparar una imagen maestra y un perfil de máquina para ellas:

1. En el portal de Azure, cree una máquina virtual confidencial con parámetros específicos, como:
   - **Tipo de seguridad**: Máquinas virtuales confidenciales
   - **Cifrado de disco de SO confidencial**: Habilitado.

- **Administración de claves**: Cifrado de disco confidencial con una clave administrada por la plataforma
  Para obtener más información sobre la creación de máquinas virtuales confidenciales, consulte este artículo de Microsoft.

2. Prepare la imagen maestra en la máquina virtual creada. Instale las aplicaciones y VDA necesarios en la máquina virtual creada.

   > **Nota:**
   >
   > No se admite la creación de máquinas virtuales confidenciales mediante VHD. En su lugar, use Azure Compute Gallery, discos administrados o instantáneas para este fin.

3. Cree el perfil de la máquina de una de estas maneras:

   - Use la máquina virtual existente creada en el paso 1 si tiene las propiedades de máquina necesarias.
   - Si opta por una especificación de plantilla de ARM como perfil de máquina, cree la especificación de plantilla según sea necesario. En concreto, configure parámetros que cumplan con los requisitos de VM confidencial, como *SecurityEncryptionType* y *diskEncryptionSet* (para la clave administrada por el cliente). Para obtener más información, consulte Crear una especificación de plantilla de Azure.

     > **Nota:**
     >
     > - Asegúrese de que la imagen maestra y el perfil de la máquina tengan el mismo tipo de clave de seguridad.
     > - Para crear máquinas virtuales confidenciales que requieran cifrado de disco de SO confidencial con una clave administrada por el cliente, asegúrese de que los ID del conjunto de cifrado de disco tanto en la imagen maestra como en el perfil de la máquina sean idénticos.

Crear máquinas virtuales confidenciales mediante Web Studio o los comandos de PowerShell

Para crear un conjunto de máquinas virtuales confidenciales, cree un catálogo de máquinas con una imagen maestra y un perfil de máquina derivados de la máquina virtual confidencial deseada.

Para crear el catálogo con Web Studio, siga los pasos descritos en Crear catálogos de máquinas. Tenga en cuenta las siguientes consideraciones:

- En la página **Imagen**, seleccione una imagen maestra y un perfil de máquina que haya preparado para la creación de la máquina virtual confidencial. La selección del perfil de la máquina es obligatoria y solo están disponibles para selección los perfiles cuyo tipo de cifrado de seguridad coincida con el de la imagen maestra seleccionada.

- En la página **Máquinas virtuales**, solo aparecen para selección los tamaños de máquina compatibles con máquinas virtuales confidenciales.
- En la página **Parámetros del disco**, no puede especificar el conjunto de cifrado del disco porque se hereda del perfil de máquina seleccionado.

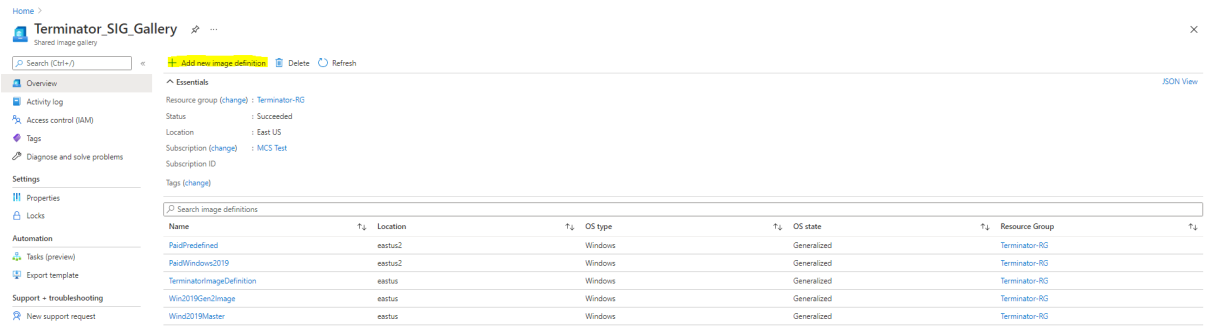
Azure Marketplace

Citrix Virtual Apps and Desktops admite el uso de una imagen maestra en Azure que contenga información del plan para crear un catálogo de máquinas. Para obtener más información, consulte Microsoft Azure Marketplace.

> **Sugerencia:**
>
> Algunas imágenes que se encuentran en Azure Marketplace, como la imagen estándar de Windows Server, no llevan anexa información del plan. La funcionalidad Citrix Virtual Apps and Desktops es para imágenes de pago.

Compruebe que la imagen creada en Shared Image Gallery contiene información del plan de Azure

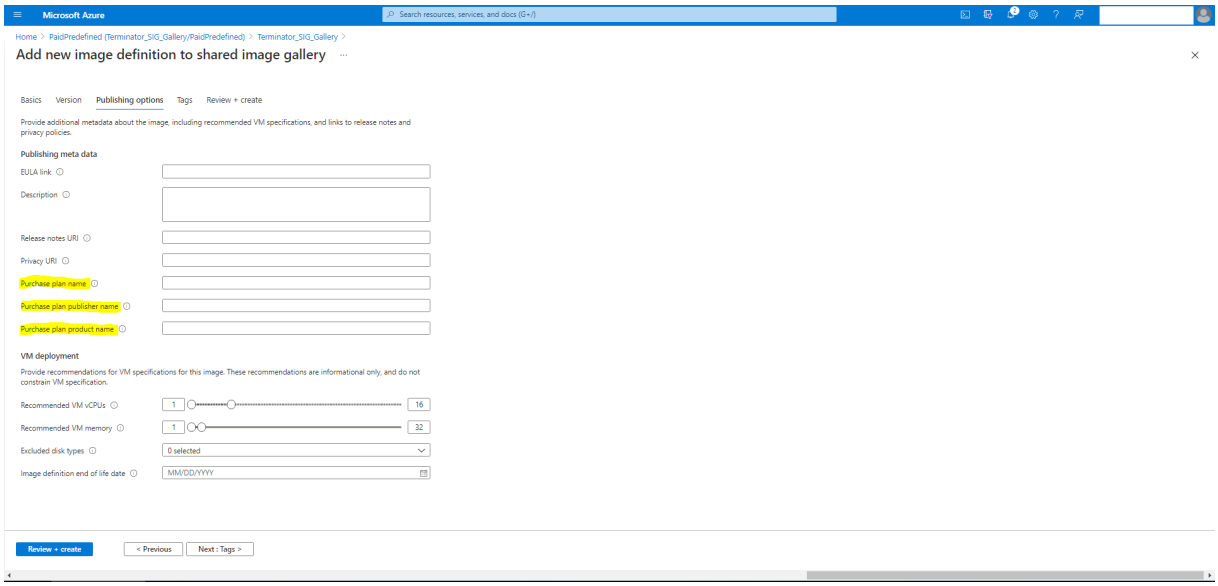
Use el procedimiento descrito en esta sección para ver las imágenes de Shared Image Gallery en Web Studio. Estas imágenes se pueden usar, opcionalmente, para una imagen maestra. Para colocar la imagen en Shared Image Gallery, cree una definición de imagen en una galería.



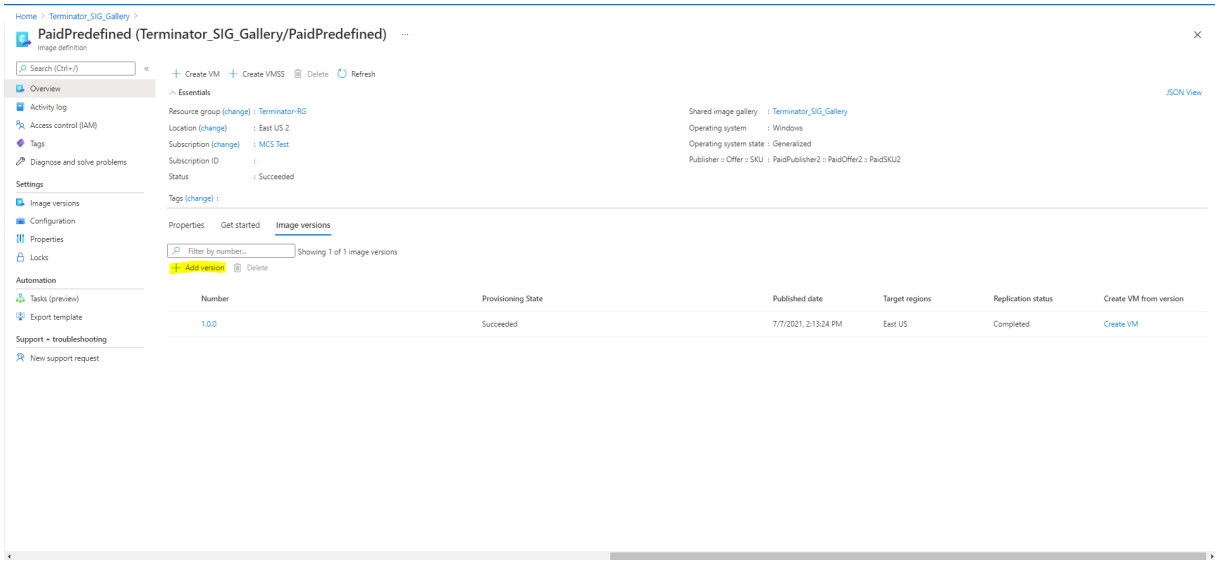
En la página **Publishing options**, verifique la información del plan de compra.

Los campos de información del plan de compra están vacíos inicialmente. Rellene esos campos con la información del plan de compra utilizada para la imagen. Si no se rellena la información del plan

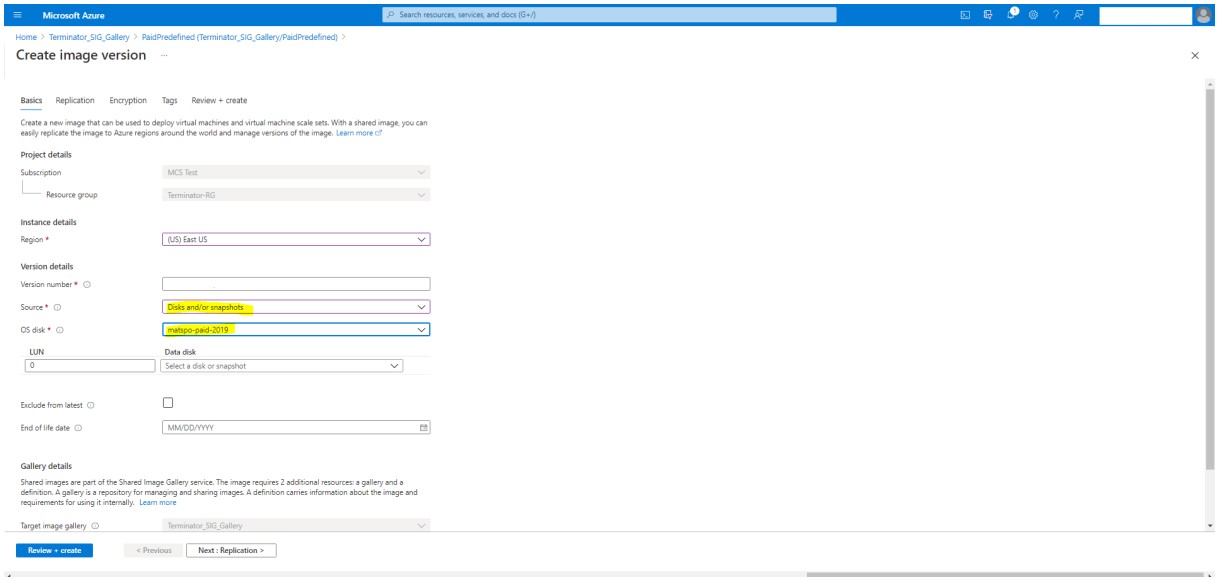
de compra, puede ocurrir un error en el procesamiento del catálogo de máquinas.



Después de verificar la información del plan de compra, cree una versión de la imagen dentro de la definición. Sirve de imagen maestra. Haga clic en **Add version**:



En la sección **Version details**, seleccione la instantánea de la imagen o el disco administrado como origen:



Virtualización anidada

Si configura la VM maestra con virtualización anidada habilitada, todas las VM del catálogo de máquinas de MCS creadas con esa VM maestra tienen habilitada la virtualización anidada. Esta función se aplica a máquinas virtuales persistentes y no persistentes. Puede actualizar un catálogo de máquinas de MCS existente y las máquinas virtuales existentes para que tengan una virtualización anidada mediante la actualización de imágenes.

Actualmente, solo los tamaños de VM Dv3 y Ev3 admiten la virtualización anidada.

Para obtener información sobre la virtualización anidada, consulte el blog de Microsoft Nested Virtualization in Azure.

Crear un catálogo de máquinas con PowerShell

En esta sección se detalla cómo puede crear catálogos con PowerShell:

- Crear un catálogo con un disco no persistente de caché de reescritura
- Crear un catálogo con un disco persistente de caché de reescritura
- Mejorar el rendimiento del arranque con E/S de MCS
- Usar la especificación de la plantilla para crear o actualizar un catálogo con PowerShell
- Catálogos de máquinas con inicio seguro
- Usar valores de propiedades de perfil de máquina
- Crear un catálogo de máquinas con una clave de cifrado administrada por el cliente
- Crear un catálogo de máquinas con doble cifrado
- Crear un catálogo con discos efímeros de Azure

- Hosts dedicados de Azure
- Crear o actualizar un catálogo de máquinas con una imagen de Azure Compute Gallery
- Configurar Shared Image Gallery
- Aprovisionar máquinas en zonas de disponibilidad especificadas
- Tipos de almacenamiento
- Actualizar la configuración del archivo de paginación
- Crear un catálogo con máquinas virtuales de Azure Spot
- Configurar los tamaños de las máquinas virtuales de seguridad
- Copiar etiquetas en todos los recursos
- Aprovisionar máquinas virtuales del catálogo con el agente de Azure Monitor instalado

Crear un catálogo con un disco no persistente de caché de reescritura

Para configurar un catálogo con disco no persistente de caché de reescritura, utilice el parámetro de PowerShell `New-ProvScheme CustomProperties`. La propiedad personalizada `UseTempDiskForWBC` indica si acepta usar el almacenamiento temporal de Azure para almacenar el archivo de caché de reescritura. Esto debe establecerse en "true"cuando se ejecuta `New-ProvScheme` si quiere usar el disco temporal como disco de caché de reescritura. Si no se especifica esta propiedad, el parámetro se establece en **false** de forma predeterminada.

Por ejemplo, así se usa el parámetro `CustomProperties` para configurar `UseTempDiskForWBC` en **true**:

```
-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com
   /2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/
   XMLSchema-instance"> `
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false"/> `
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false
   "/> `
<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS"/> `
<Property xsi:type="StringProperty" Name="WBCDiskStorageType" Value="
   Premium_LRS"/> `
<Property xsi:type="StringProperty" Name="LicenseType" Value="
   Windows_Client"/> `
<Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value="
   true"/> `
</CustomProperties>'
```

> **Nota:**
>
> Después de confirmar que el catálogo de máquinas use el almacenamiento temporal local de Azure para el archivo de caché de reescritura, no se puede cambiar para que use VHD más adelante.

Crear un catálogo con un disco persistente de caché de reescritura

Para configurar un catálogo con disco persistente de caché de reescritura, use el parámetro `New-ProvScheme CustomProperties` de PowerShell. 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. 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.

He aquí unos cuantos ejemplos de propiedades que se encuentran en el parámetro `CustomProperties` antes de optar por la propiedad `PersistWBC`:

```
<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="
   benvaldev5RG3" />
</CustomProperties>
```

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 Web 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 Web 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 Web Studio.

Por ejemplo, así se usa el parámetro `CustomProperties` para configurar `PersistWBC` en “true” :

```
<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="
    benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
</CustomProperties>
```

> **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 de reescritura cuando se apaga una máquina.

Por ejemplo, configure `New-ProvScheme` para utilizar la memoria caché de reescritura mientras configura la propiedad `PersistWBC` en "true":

```
New-ProvScheme
-CleanOnBoot
-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=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
    =`"PersistWBC`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
    GoldImages.resourcegroup\W10MCSIO-01
    _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
     CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
     adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
    folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
```

Mejorar el rendimiento del arranque con E/S de MCS

Puede mejorar el rendimiento de arranque de los discos administrados de Azure y GCP cuando E/S de MCS está habilitada. Utilice la propiedad personalizada `PersistOSDisk` de PowerShell en el comando `New-ProvScheme` para configurar esta función. Las opciones asociadas a `New-ProvScheme` son:


```
<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="Resource ``````<!--NeedCopy
    -->
````````Groups" Value="benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
    />
</CustomProperties>
```

Para habilitar esta función, establezca la propiedad personalizada `PersistOSDisk` en **`true`**. Por ejemplo:

```
New-ProvScheme
-CleanOnBoot
-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=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
    =`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
    GoldImages.resourcegroup\W10MCSIO-01
    _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
     CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
     adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
    folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
```

Usar la especificación de la plantilla para crear o actualizar un catálogo con PowerShell

Puede crear o actualizar un catálogo de máquinas de MCS mediante una especificación de plantilla como entrada de datos de un perfil de máquina. Para ello, puede utilizar Web Studio o los comandos


```

de PowerShell.

Para Web Studio, consulte Crear un catálogo de máquinas con una imagen de Azure Resource Manager en Web Studio

Mediante los comandos de PowerShell:

1. Abra la ventana de **PowerShell**.
2. Ejecute `asnp citrix*`.
3. Cree o actualice un catálogo.

    - Para crear un catálogo:

        a) Utilice el comando `New-ProvScheme` con una especificación de plantilla como entrada de datos de un perfil de máquina. Por ejemplo:

        ```
        New-ProvScheme -MasterImageVM "XDHyp:/HostingUnits/azure/
            image.folder/fgthj.resourcegroup/nab-ws-
            vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
        MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.
            folder/fgthj.resourcegroup/test.templatespec/V1.
            templatespecversion"
        -ProvisioningSchemeName <String>
        -HostingUnitName <String>
        -IdentityPoolName <String>
        [-ServiceOffering <String>][-CustomProperties <String>
        [-LoggingId <Guid>]
        [-BearerToken <String>][-AdminAddress <String>]
        [<CommonParameters>]
        ```

        b) Termine de crear el catálogo.

    - Para actualizar un catálogo, utilice el comando `Set-ProvScheme` con una especificación de plantilla como entrada de datos de un perfil de máquina. Por ejemplo:

    ```
    Set-ProvScheme -MasterImageVm 'XDHyp://Connections/Azure/East
        Us.region/vm.folder/MasterDisk.vm'
    MachineProfile 'XDHyp:/HostingUnits/azure/machineprofile.
        folder/fgthj.resourcegroup/testing.templatespec/V1.
        templatespecversion'
    [-ProvisioningSchemeName] <String>
    [-CustomProperties <String>][-ServiceOffering <String>] [-
        PassThru]
    [-LoggingId <Guid>] [-BearerToken <String>][-AdminAddress <
        String>] [<CommonParameters>]
    ```

Catálogos de máquinas con inicio seguro

Para crear correctamente un catálogo de máquinas con inicio seguro, utilice:

- Un perfil de máquina con inicio seguro

- Un tamaño de máquina virtual compatible con el inicio seguro
- Una versión de máquina virtual Windows que admita inicio seguro. En la actualidad, Windows 10, Windows 11 y Windows Server 2016, 2019 y 2022 admiten el inicio seguro.

> **Importante:**
>
> MCS admite la creación de un catálogo con máquinas virtuales habilitadas para inicio seguro. Sin embargo, para actualizar un catálogo persistente y las máquinas virtuales ya existentes, debe usar el portal de Azure. No puede actualizar el inicio seguro de un catálogo no persistente. Para obtener más información, consulte el documento de Microsoft Enable Trusted launch on existing Azure VMs.

Para ver los elementos de inventario que ofrecen Citrix Virtual Apps and Desktops y determinar si el tamaño de máquina virtual admite el inicio seguro, ejecute el siguiente comando:

1. Abra una ventana de PowerShell.
2. Ejecute **asnp citrix*** para cargar los módulos de PowerShell específicos de Citrix.
3. Ejecute este comando:

```
$s = (ls XDHyp:\HostingUnits<name of hosting unit>\serviceoffering
    .folder"<VM size>.serviceoffering)
```

4. Ejecute `$s | select -ExpandProperty Additionaldata`
5. Compruebe el valor del atributo `SupportsTrustedLaunch`.
    - Si `SupportsTrustedLaunch` es **True**, el tamaño de máquina virtual admite el inicio seguro.
    - Si `SupportsTrustedLaunch` es **False**, el tamaño de máquina virtual no admite el inicio seguro.

Según la instancia de PowerShell de Azure, puede usar este comando para determinar los tamaños de máquina virtual que admiten el inicio seguro:

```
(Get-AzComputeResourceSku | where {
 $_.Locations.Contains($region) -and ($_.Name -eq "<VM size>")  }
 )[0].Capabilities
```

A continuación, se muestran ejemplos que describen si el tamaño de máquina virtual admite el inicio seguro después de ejecutar el comando de Azure PowerShell.

- *Ejemplo 1*: Si la máquina virtual de Azure solo admite la generación 1, esa máquina virtual no admite el inicio seguro. Por lo tanto, la funcionalidad `TrustedLaunchDisabled` no se muestra después de ejecutar el comando de Azure PowerShell.

- *Ejemplo 2*: Si la máquina virtual de Azure solo admite la generación 2 y la funcionalidad `TrustedLaunchDisabled` es **True**, el tamaño de máquina virtual de la generación 2 no se admite para el inicio seguro.
- *Ejemplo 3*: Si la máquina virtual de Azure solo admite la generación 2 y la funcionalidad `TrustedLaunchDisabled` no se muestra después de ejecutar el comando de PowerShell, se admite el tamaño de máquina virtual de generación 2 para el inicio seguro.

Para obtener más información sobre el inicio seguro para máquinas virtuales de Azure, consulte el documento Trusted Launch for Azure Virtual Machines de Microsoft.

Crear un catálogo de máquinas con inicio seguro

1. Cree una imagen maestra habilitada para inicio seguro. Consulte la documentación Trusted Launch VM Images de Microsoft.
2. Cree una especificación de plantilla o máquina virtual con el tipo de seguridad **máquinas virtuales con inicio seguro**. Para obtener más información sobre cómo crear una especificación de plantilla o VM, consulte el documento Deploy a Trusted Launch VM de Microsoft.
3. Cree un catálogo de máquinas con Web Studio o los comandos de PowerShell.

   - Si quiere usar Web Studio, consulte Crear un catálogo de máquinas con una imagen de Azure Resource Manager en Web Studio.
   - Si quiere usar los comandos de PowerShell, utilice el comando `New-ProvScheme` con la especificación de plantilla o VM como entrada de perfil de máquina. Para ver la lista completa de comandos para crear un catálogo, consulte Creación de un catálogo.

     Ejemplo de `New-ProvScheme` con VM como entrada del perfil de máquina:

     ```
     New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
        IdentityPoolName "name" -InitialBatchSizeHint 1
     -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/fgthj.
        resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
     -MachineProfile "XDHyp:\HostingUnits<adnet>\machineprofile.
        folder<def.resourcegroup><machine profile vm.vm>"
     -ProvisioningSchemeName <String>
     -HostingUnitName <String>
     -IdentityPoolName <String>
     [-ServiceOffering <String>][-CustomProperties <String>]
     [<CommonParameters>]
     ```

     Ejemplo de `New-ProvScheme` con especificación de plantilla como entrada del perfil de máquina:

     ```
     New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
        IdentityPoolName "name" -InitialBatchSizeHint 1
     ```



```
2   -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/fgthj.
        resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
3   MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.
        folder/fgthj.resourcegroup/test.templatespec/V1.
        templatespecversion"
4   -ProvisioningSchemeName <String>
5   -HostingUnitName <String>
6   -IdentityPoolName <String>
7   [-ServiceOffering <String>][-CustomProperties <String>]
8   [<CommonParameters>]
```

Errores al crear catálogos de máquinas con inicio seguro

Al crear un catálogo de máquinas con inicio seguro en los siguientes casos, se obtienen los errores correspondientes:

Caso	Error
Si selecciona un perfil de máquina al crear un catálogo no administrado	MachineProfileNotSupportedForUnmanagedCata
Si selecciona un perfil de máquina que admite el inicio seguro al crear un catálogo con un disco no administrado como imagen maestra	SecurityTypeNotSupportedForUnmanagedDisk
Si no selecciona un perfil de máquina al crear un catálogo administrado con una imagen maestra de origen que tenga inicio seguro como tipo de seguridad	MachineProfileNotFoundForTrustedLaunchMaste
Si selecciona un perfil de máquina con un tipo de seguridad diferente del tipo de seguridad de la imagen maestra	SecurityTypeConflictBetweenMasterImageAndMa
Si selecciona un tamaño de máquina virtual que no admite el inicio seguro, pero usa una imagen maestra que sí admite el inicio seguro al crear un catálogo	MachineSizeNotSupportTrustedLaunch

Usar valores de propiedades de perfil de máquina

El catálogo de máquinas utiliza las siguientes propiedades que se definen en las propiedades personalizadas:

- Zona de disponibilidad

- ID de grupo de hosts dedicado
- ID del conjunto de cifrado de disco
- Tipo de SO
- Tipo de licencia
- Tipo de almacenamiento

Si estas propiedades personalizadas no se definen explícitamente, los valores de propiedad se establecen a partir de la especificación de plantilla de ARM o de la VM, lo que se utilice como perfil de máquina. Además, si no se especifica `ServiceOffering`, se establecerá a partir del perfil de máquina.

> **Nota:**
>
> Si faltan algunas propiedades en el perfil de la máquina (MachineProfile) y no están definidas en las propiedades personalizadas (CustomProperties), se utilizan los valores por defecto de las propiedades siempre que sea aplicable.

En la siguiente sección se describen algunos casos de `New-ProvScheme` y `Set-ProvScheme` en los que `CustomProperties` tiene definidas todas las propiedades o los valores se derivan de MachineProfile.

- Casos de New-ProvScheme
  - MachineProfile tiene todas las propiedades y CustomProperties no está definido. Ejemplo:

    ```
    New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
    \machineprofile.folder\azure.resourcegroup\mpA.vm"
    ```

    Estos valores se definen como propiedades personalizadas del catálogo:

    ```
    1  Get-ProvScheme | select CustomProperties
    2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
           machinecreation" xmlns:xsi="http://www.w3.org/2001/
           XMLSchema-instance">
    3  <Property xsi:type="StringProperty" Name="StorageAccountType"
           Value="<mpA-value>"/>
    4  <Property xsi:type="StringProperty" Name="OSType" Value="<mpA
           -value>"/>
    5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
           "<mpA-value>"/>
    6  <Property xsi:type="StringProperty" Name="DiskEncryptionSetId
           " Value="<mpA-value>"/>
    7  <Property xsi:type="StringProperty" Name="
           DedicatedHostGroupId" Value="<mpA-value>"/>
    8  <Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
           value>"/>
    9  </CustomProperties>
    ```


- MachineProfile tiene algunas propiedades y CustomProperties no está definido. Ejemplo: MachineProfile solo tiene LicenseType y OsType.

  ```
  New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
  \machineprofile.folder\azure.resourcegroup\mpA.vm"
  ```

  Estos valores se definen como propiedades personalizadas del catálogo:

  ```
  1  Get-ProvScheme | select CustomProperties
  2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
        machinecreation" xmlns:xsi="http://www.w3.org/2001/
        XMLSchema-instance">
  3  <Property xsi:type="StringProperty" Name="OSType" Value="<mpA
        -value>"/>
  4  <Property xsi:type="StringProperty" Name="LicenseType" Value=
        "<mpA-value>"/>
  5  </CustomProperties>
  ```

- Tanto MachineProfile como CustomProperties definen todas las propiedades. Ejemplo:

  ```
  New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
  \machineprofile.folder\azure.resourcegroup\mpA.vm"-CustomProperties
   $CustomPropertiesA
  ```

  Las propiedades personalizadas tienen prioridad. Estos valores se definen como propiedades personalizadas del catálogo:

  ```
  1  Get-ProvScheme | select CustomProperties
  2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
        machinecreation" xmlns:xsi="http://www.w3.org/2001/
        XMLSchema-instance">
  3  <Property xsi:type="StringProperty" Name="StorageAccountType"
         Value="<CustomPropertiesA-value>"/>
  4  <Property xsi:type="StringProperty" Name="OSType" Value="<
        CustomPropertiesA-value>"/>
  5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
        "<CustomPropertiesA-value>"/>
  6  <Property xsi:type="StringProperty" Name="DiskEncryptionSetId
        " Value="<CustomPropertiesA-value>"/>
  7  <Property xsi:type="StringProperty" Name="
        DedicatedHostGroupId" Value="<CustomPropertiesA-value>"/>
  8  <Property xsi:type="StringProperty" Name="Zones" Value="<
        CustomPropertiesA-value>"/>
  9  </CustomProperties>
  ```

- Algunas propiedades se definen en MachineProfile y otras se definen en CustomProperties. Ejemplo:

  * CustomProperties define LicenseType y StorageAccountType
  * MachineProfile define LicenseType, OsType y Zones

  ```
  New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
  ```



```
\machineprofile.folder\azure.resourcegroup\mpA.vm"-CustomProperties
 $CustomPropertiesA
```

Estos valores se definen como propiedades personalizadas del catálogo:

```
Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
    Value="<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="OSType" Value="<mpA
   -value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
   "<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
   value>"/>
</CustomProperties>
```

- Algunas propiedades se definen en MachineProfile y otras se definen en CustomProperties. Además, ServiceOffering no está definido. Ejemplo:
  - CustomProperties define StorageType
  - MachineProfile define LicenseType

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
   \machineprofile.folder\azure.resourcegroup\mp.vm"
-ServiceOffering "XDHyp:\HostingUnits\azureunit\
   serviceoffering.folder<explicit-machine-size>.
   serviceoffering"
```

Estos valores se definen como propiedades personalizadas del catálogo:

```
Get-ProvScheme | select ServiceOffering
serviceoffering.folder<explicit-machine-size>.serviceoffering

Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
    Value="explicit-storage-type"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
   "value-from-machineprofile"/>
</CustomProperties>
```

- Si OsType no está ni en CustomProperties ni en MachineProfile, entonces:
  - El valor se lee de la imagen maestra.
  - Si la imagen maestra es un disco no administrado, OsType se establece en Windows. Ejemplo:


```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpA.vm"-MasterImageVM
 "XDHyp:\HostingUnits\azureunit\image.folder\linux-master-
image.manageddisk"
```

El valor de la imagen maestra se escribe en las propiedades personalizadas, en este caso Linux.

```
1  Get-ProvScheme | select CustomProperties
2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
      machinecreation" xmlns:xsi="http://www.w3.org/2001/
      XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="OSType" Value="
      Linux"/>
4  </CustomProperties>
```

- Casos de Set-ProvScheme
  - Un catálogo con:
    - CustomProperties para `StorageAccountType` y OsType
    - MachineProfile `mpA.vm` que define zonas
  - Actualizaciones:
    - MachineProfile mpB.vm que define StorageAccountType
    - Un nuevo conjunto de propiedades personalizadas $CustomPropertiesB que define LicenseType y OsType

```
Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpB.vm"-CustomProperties
 $CustomPropertiesB
```

Estos valores se definen como propiedades personalizadas del catálogo:

```
1  Get-ProvScheme | select CustomProperties
2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
      machinecreation" xmlns:xsi="http://www.w3.org/2001/
      XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="StorageAccountType"
       Value="<mpB-value>"/>
4  <Property xsi:type="StringProperty" Name="OSType" Value="<
      CustomPropertiesB-value>"/>
5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
      "<CustomPropertiesB-value>"/>
6      </CustomProperties>
```

  - Un catálogo con:
    - Propiedades personalizadas para `StorageAccountType` y OsType.

    - MachineProfile `mpA.vm` que define StorageAccountType y LicenseType

- Actualizaciones:

    - Un nuevo conjunto de propiedades personalizadas $CustomPropertiesB que define StorageAccountType y OsType.

```
Set-ProvScheme -CustomProperties $CustomPropertiesB
```

Estos valores se definen como propiedades personalizadas del catálogo:

```
Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
    Value="<CustomPropertiesB-value>"/>
<Property xsi:type="StringProperty" Name="OSType" Value="<
   CustomPropertiesB-value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
   "<mp-A-value>"/>
</CustomProperties>
```

- Un catálogo con:

    - CustomProperties para `StorageAccountType` y OsType
    - MachineProfile `mpA.vm` que define zonas

- Actualizaciones:

    - MachineProfile mpB.vm que define StorageAccountType y LicenseType
    - `ServiceOffering` está sin especificar

```
Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpB.vm"
```

Estos valores se definen como propiedades personalizadas del catálogo:

```
Get-ProvScheme | select ServiceOffering
serviceoffering.folder<value-from-machineprofile>.
   serviceoffering

Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
    Value="<mpB-value>"/>
<Property xsi:type="StringProperty" Name="OSType" Value="<
   prior-CustomProperties-value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
   "<mpB-value>"/>
</CustomProperties>
```


Aprovisionar máquinas virtuales del catálogo con el agente de Azure Monitor instalado

La supervisión de Azure es un servicio que puede utilizar para recopilar, analizar y responder a datos de telemetría de sus entornos locales y de Azure.

El agente de Azure Monitor (AMA) recopila datos de supervisión de recursos de procesamiento, como máquinas virtuales, y los entrega a Azure Monitor. Actualmente, permite la recopilación de registros de eventos y métricas de Syslog y rendimiento, y los envía a los orígenes de datos de las Métricas de Azure Monitor y los Registros de Azure Monitor.

Para habilitar la supervisión mediante la identificación exclusiva de las máquinas virtuales en los datos de supervisión, puede aprovisionar las máquinas virtuales de un catálogo de máquinas de MCS con AMA instalado como extensión.

Requisitos

- Permisos: Asegúrese de tener los permisos mínimos de Azure especificados en Permisos de Azure requeridos y estos permisos para usar Azure Monitor:
  - `Microsoft.Compute/virtualMachines/extensions/read`
  - `Microsoft.Compute/virtualMachines/extensions/write`
  - `Microsoft.Insights/DataCollectionRuleAssociations/Read`
  - `Microsoft.Insights/dataCollectionRuleAssociations/write`
  - `Microsoft.Insights/DataCollectionRules/Read`
- Regla de recopilación de datos: Configure una regla de recopilación de datos (DCR) en Azure Portal. Para obtener información sobre cómo configurar una DCR, consulte Creación de una regla de recopilación de datos. Las DCR son específicas de cada plataforma (Windows o Linux). Asegúrese de crear una DCR según la plataforma requerida.
  El AMA utiliza las reglas de recopilación de datos (DCR) para administrar la asignación entre los recursos, como las máquinas virtuales, y los orígenes de datos, como las Métricas de Azure Monitor y los Registros de Azure Monitor.
- Espacio de trabajo predeterminado: Cree un espacio de trabajo en Azure Portal. Para obtener información sobre cómo crear un espacio de trabajo, consulte Creación de un área de trabajo de Log Analytics. Al recopilar registros y datos, la información se almacena en un espacio de trabajo. Un espacio de trabajo tiene un ID de espacio de trabajo y un ID de recurso únicos. El nombre del espacio de trabajo debe ser único para un grupo de recursos determinado. Después de crear un espacio de trabajo, configure los orígenes de datos y las soluciones para almacenar sus datos en el espacio de trabajo.
- Extensión de supervisión en la lista de permitidos: Las extensiones `AzureMonitorWindowsAgent` y `AzureMonitorLinuxAgent` son extensiones de la lista de permitidos definida por Citrix.

Para ver la lista de extensiones incluidas en la lista de permitidos, utilice el comando PoSH `Get-ProvMetadataConfiguration`.

- Imagen maestra: Microsoft recomienda quitar extensiones de una máquina existente antes de crear otra máquina a partir de ella. Si no se quitan las extensiones, es posible que queden archivos sobrantes y que se produzca un comportamiento inesperado. Para obtener más información, consulte Si la máquina virtual se vuelve a crear a partir de una máquina virtual existente.

Para aprovisionar máquinas virtuales de catálogo con el AMA activado:

1. Configure una plantilla de perfil de máquina.
    - Si quiere usar una máquina virtual como plantilla de perfil de máquina:
        a) Cree una máquina virtual en Azure Portal.
        b) Encienda la máquina virtual.
        c) Agregue la máquina virtual a la regla de recopilación de datos en **Recursos**. Esto invoca la instalación del agente en la máquina virtual de la plantilla.

    > **Nota:**
    >
    > Si debe crear un catálogo de Linux, configure una máquina Linux.

    - Si quiere utilizar la especificación de plantilla como plantilla de perfil de máquina:
        a) Configure una especificación de plantilla.
        b) Agregue esta asociación de extensiones y reglas de recopilación de datos a la especificación de plantilla generada:

```
{

"type": "Microsoft.Compute/virtualMachines/extensions",
"apiVersion": "2022-03-01",
"name": "<vm-name>/AzureMonitorWindowsAgent",
"dependsOn": [
    "Microsoft.Compute/virtualMachines/<vm-name>"
],
"location": "<azure-region>",
"properties": {

    "publisher": "Microsoft.Azure.Monitor",
    "type": "AzureMonitorWindowsAgent",
    "typeHandlerVersion": "1.0",
    "autoUpgradeMinorVersion": true,
    "enableAutomaticUpgrade": true
 }

 }
 ,
```



```
{

   "type": "Microsoft.Insights/
      dataCollectionRuleAssociations",
   "apiVersion": "2021-11-01",
   "name": "<associatio-name>",
   "scope": "Microsoft.Compute/virtualMachines/<vm-name>",
   "dependsOn": [
    "Microsoft.Compute/virtualMachines/<vm-name>",
   "Microsoft.Compute/virtualMachines/<vm-name>/extensions
      /AzureMonitorWindowsAgent"
   ],
   "properties": {

      "description": "Association of data collection rule.
          Deleting this association will break the data
         collection for this Arc server.",
    "dataCollectionRuleId": "/subscriptions/<azure-
       subscription>/resourcegroups/<azure-resource-group
       >/providers/microsoft.insights/datacollectionrules
       /<azure-data-collection-rule>"
     }

    }
```

2. Cree o actualice un catálogo de máquinas de MCS existente.

   - Para crear otro catálogo de MCS:

     a) Seleccione esa especificación de máquina virtual o plantilla como perfil de máquina en Web Studio.
     b) Continúe con los pasos siguientes para crear el catálogo.

   - Para actualizar un catálogo de MCS existente, utilice estos comandos de PoSH:

     - Para que las nuevas máquinas virtuales obtengan la plantilla de perfil de máquina actualizada, ejecute este comando:

       ```
       Set-ProvScheme -ProvisioningSchemeName "name"
       -MachineProfile "XDHyp:\HostingUnits\Unit1\machineprofile.
          folder\abc.resourcegroup\ab-machine-profile.vm"
       ```

     - Para actualizar máquinas virtuales existentes con la plantilla de perfil de máquina actualizada:

       ```
       Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-
          catalog -StartsNow -DurationInMinutes -1
       ```

3. Encienda las máquinas virtuales del catálogo.
4. Vaya a Azure Portal y compruebe si la extensión de supervisión está instalada en la máquina

virtual y si la máquina virtual aparece en los recursos de la DCR. Después de unos minutos, los datos de supervisión se muestran en Azure Monitor.

Solución de problemas

Para obtener información sobre la guía de solución de problemas del agente de Azure Monitor, consulte lo siguiente:

- https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/
- https://learn.microsoft.com/en-us/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/

Crear un catálogo de máquinas con una clave de cifrado administrada por el cliente

Los pasos detallados para crear un catálogo de máquinas con una clave de cifrado administrada por el cliente son:

1. Abra una ventana de PowerShell.
2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
3. Escriba `cd xdhyp:/.`
4. Escriba `cd .\HostingUnits\(your hosting unit).`
5. Escriba `cd diskencryptionset.folder.`
6. Escriba `dir` para obtener la lista de conjuntos de cifrado de disco.
7. Copie el ID de un conjunto de cifrado de disco.
8. Cree una cadena de propiedades personalizada para incluir el ID del conjunto de cifrado de disco. Por ejemplo:

```
$customProperties = "<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`" Value=`"Standard_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"persistWBC`" Value=`"False`" />
<Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`" Value=`"false`" />
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"true`" />
```



```
<Property xsi:type=`"StringProperty`" Name=`"DiskEncryptionSetId`"
     Value=`"/subscriptions/0xxx4xxx-xxb-4bxx-xxxx-xxxxxxxx/
    resourceGroups/abc/providers/Microsoft.Compute/
    diskEncryptionSets/abc-des`"/>
</CustomProperties>
```

9. Cree un grupo de identidades si aún no se ha creado. Por ejemplo:

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms## -
    Domain def.local -NamingSchemeType Numeric
```

10. Ejecute el comando New-ProvScheme. Por ejemplo:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
    IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits\azure-res2\image.folder\def.
    resourcegroup\def.snapshot"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure-res2\virtualprivatecloud.folder\
     def.resourcegroup\def-vnet.virtualprivatecloud\subnet1.network
     " }

-ProvisioningSchemeName "name"
-ServiceOffering "XDHyp:\HostingUnits\azure-res2\serviceoffering.
    folder\Standard_DS2_v2.serviceoffering"
-MachineProfile "XDHyp:\HostingUnits<adnet>\machineprofile.folder<
    def.resourcegroup><machine profile vm.vm>"
-CustomProperties $customProperties
```

11. Termine de crear el catálogo de máquinas.

Crear un catálogo de máquinas con doble cifrado

Puede crear y actualizar un catálogo de máquinas con doble cifrado mediante Web Studio y los comandos de PowerShell.

Los pasos detallados para crear un catálogo de máquinas con doble cifrado son:

1. Cree un Azure Key Vault y un DES con claves administradas por la plataforma y por el cliente. Para obtener información sobre cómo crear un Azure Key Vault y un DES, consulte Uso de Azure Portal para habilitar el cifrado doble en reposo para discos administrados.
2. Para buscar DiskEncryptionSets en su conexión de alojamiento:
   a) Abra una ventana de **PowerShell**.
   b) Ejecute los siguientes comandos de PowerShell:
      i. `asnp citrix*`
      ii. `cd xdhyp:`
      iii. `cd HostingUnits`

iv. `cd YourHostingUnitName` (por ejemplo, azul-este)
v. `cd diskencryptionset.folder`
vi. `dir`

Puede usar un ID del `DiskEncryptionSet` para crear o actualizar un catálogo mediante propiedades personalizadas.

3. Si quiere utilizar el flujo de trabajo del perfil de máquina, cree una especificación de máquina virtual o plantilla como entrada de perfil de máquina.

   - Si quiere utilizar una máquina virtual como entrada de perfil de máquina:
     a) Cree una máquina virtual en Azure Portal.
     b) Vaya a **Disks > Key Management** para cifrar la máquina virtual directamente con cualquier otro `DiskEncryptionSetID`.
   - Si quiere utilizar una especificación de plantilla como entrada de perfil de máquina:
     a) En la plantilla, en `properties>storageProfile>osDisk>managedDisk`, agregue el parámetro `diskEncryptionSet` y agregue el ID del DES de doble cifrado.

4. Cree el catálogo de máquinas

   - Si usa Web Studio, realice una de estas acciones, además de los pasos de Crear catálogos de máquinas.
     - Si no usa un flujo de trabajo basado en perfiles de máquina, en la página **Parámetros del disco**, seleccione **Utilice esta clave para cifrar datos en cada máquina**. A continuación, seleccione su DES de doble cifrado en el menú desplegable. Siga con la creación del catálogo.
     - Si usa un flujo de trabajo de perfil de máquina, en la página **Imagen**, seleccione una imagen maestra y un perfil de máquina. Asegúrese de que el perfil de la máquina tenga un ID de conjunto de cifrado de disco en sus propiedades.

     Todas las máquinas creadas en el catálogo se cifran con doble cifrado mediante la clave asociada al DES que haya seleccionado.
   - Si usa comandos de PowerShell, realice una de estas acciones:
     - Si no utiliza un flujo de trabajo basado en perfiles de máquina, agregue la propiedad personalizada `DiskEncryptionSetId` en el comando `New-ProvScheme`. Por ejemplo:

```
New-ProvScheme -CleanOnBoot -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="
   DiskEncryptionSetId" Value="/subscriptions/12345678-
   xxxx-1234-1234-123456789012/resourceGroups/Sample-RG/
   providers/Microsoft.Compute/diskEncryptionSets/
   SampleEncryptionSet" />
</CustomProperties>'
-HostingUnitName "Redacted"
-IdentityPoolName "Redacted"
-InitialBatchSizeHint 1
-MasterImageVM "Redacted"
-NetworkMapping @{
"0"="Redacted" }

-ProvisioningSchemeName "Redacted"
-ServiceOffering "Redacted"
```

- Si utiliza un flujo de trabajo basado en perfiles de máquina, utilice una entrada de perfil de máquina en el comando `New-ProvScheme`. Por ejemplo:

```
New-ProvScheme -CleanOnBoot
-HostingUnitName azure-east
-IdentityPoolName aio-ip
-InitialBatchSizeHint 1
-MasterImageVM XDHyp:\HostingUnits\azure-east\image.folder
   \abc.resourcegroup\fgb-vda-snapshot.snapshot
-NetworkMapping @{
"0"="XDHyp:\HostingUnits\azure-east\virtualprivatecloud.
   folder\apa-resourceGroup.resourcegroup\apa-
   resourceGroup-vnet.virtualprivatecloud\default.network"
    }

-ProvisioningSchemeName aio-test
-MachineProfile XDHyp:\HostingUnits\azure-east\
   machineprofile.folder\abc.resourcegroup\abx-mp.
   templatespec\1.0.0.templatespecversion
```

5. Termine de crear un catálogo mediante el SDK de PowerShell remoto. Para obtener información sobre cómo crear un catálogo con el SDK de PowerShell remoto, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/. Todas las máquinas creadas en el catálogo se cifran con doble cifrado mediante la clave asociada al DES que haya seleccionado.

Convertir un catálogo sin cifrar para usar el cifrado doble

Puede actualizar el tipo de cifrado de un catálogo de máquinas (mediante propiedades personalizadas o un perfil de la máquina).

- Si no utiliza un flujo de trabajo basado en perfiles de máquina, agregue la propiedad personalizada DiskEncryptionSetId en el comando `Set-ProvScheme`. Por ejemplo:

```
1  Set-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
2  -CustomProperties '<CustomProperties xmlns="http://schemas.citrix
       .com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org
       /2001/XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
       Value="/subscriptions/12345678-xxxx-1234-1234-123456789012/
       resourceGroups/Sample-RG/providers/Microsoft.Compute/
       diskEncryptionSets/SampleEncryptionSet" />
4  </CustomProperties>'
```

- Si utiliza un flujo de trabajo basado en perfiles de máquina, utilice una entrada de perfil de máquina en el comando `Set-ProvScheme`. Por ejemplo:

```
1  Set-ProvScheme -ProvisioningSchemeName mxiao-test -MachineProfile
        XDHyp:\HostingUnits\azure-east\machineprofile.folder\aelx.
       resourcegroup\elx-mp.templatespec\1.0.0.templatespecversion
```

Cuando se haya completado correctamente, todas las máquinas virtuales nuevas que agregue al catálogo se cifrarán con cifrado doble con la clave asociada al DES que haya seleccionado.

Verificar que el catálogo tenga un cifrado doble

- En Web Studio:
  1. Vaya a **Catálogos de máquinas**.
  2. Seleccione el catálogo que quiere verificar. Haga clic en la ficha **Propiedades de plantilla** situada cerca de la parte inferior de la pantalla.
  3. En **Detalles de Azure**, verifique el ID del conjunto de cifrado de disco en **Conjunto de cifrado de disco**. Si el ID del DES del catálogo está vacío, el catálogo no está cifrado.
  4. En Azure Portal, compruebe que el tipo de cifrado del DES asociado al ID del DES sean claves administradas por la plataforma y por el cliente.
- Mediante el comando de PowerShell:
  1. Abra la ventana de **PowerShell**.
  2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
  3. Use `Get-ProvScheme` para obtener la información de su catálogo de máquinas. Por ejemplo:


```
Get-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
```

4. Obtenga la propiedad personalizada del ID del DES del catálogo de máquinas. Por ejemplo:

```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="/subscriptions
   /12345678-1234-1234-1234-123456789012/resourceGroups/Sample
   -RG/providers/Microsoft.Compute/diskEncryptionSets/
   SampleEncryptionSet" />
```

5. En Azure Portal, compruebe que el tipo de cifrado del DES asociado al ID del DES sean claves administradas por la plataforma y por el cliente.

Crear un catálogo con discos efímeros de Azure

Para utilizar discos efímeros, debe establecer la propiedad personalizada `UseEphemeralOsDisk` en **true** al ejecutar `New-ProvScheme`.

> **Nota:**
>
> Si la propiedad personalizada `UseEphemeralOsDisk` se establece en **false** o no se especifica un valor, todos los VDA aprovisionados seguirán utilizando un disco de SO aprovisionado.

A continuación, se muestra un conjunto de ejemplo de propiedades personalizadas para uso en el esquema de aprovisionamiento:

```
"CustomProperties": [
            {

                "Name": "UseManagedDisks",
                "Value": "true"
             }
 ,
            {

                "Name": "StorageType",
                "Value": "Standard_LRS"
             }
 ,
            {

                "Name": "UseSharedImageGallery",
                "Value": "true"
             }
 ,
            {

                "Name": "SharedImageGalleryReplicaRatio",
```



```
                    "Value": "40"
                }
    ,
                {

                    "Name": "SharedImageGalleryReplicaMaximum",
                    "Value": "10"
                }
    ,
                {

                    "Name": "LicenseType",
                    "Value": "Windows_Server"
                }
    ,
                {

                    "Name": "UseEphemeralOsDisk",
                    "Value": "true"
                }

            ],
```

Configurar un disco efímero para un catálogo

Para configurar un disco de SO efímero de Azure para un catálogo, utilice el parámetro `UseEphemeralOsDisk` de `Set-ProvScheme`. Establezca el valor del parámetro `UseEphemeralOsDisk` en **true**.

> **Nota:**
>
> Para utilizar esta función, también debe habilitar los parámetros `UseManagedDisks` y `UseSharedImageGallery`.

Por ejemplo:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -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="UseSharedImageGallery" Value=
    "true" />
<Property xsi:type="StringProperty" Name="UseEphemeralOsDisk" Value="
    true" />
</CustomProperties>'
```


Consideraciones importantes con relación a los discos efímeros

Para aprovisionar discos de SO efímeros con `New-ProvScheme`, tenga en cuenta las siguientes restricciones:

- El tamaño de VM utilizado para el catálogo debe admitir discos de SO efímeros.
- El tamaño de la memoria caché o del disco temporal asociado al tamaño de la máquina virtual debe ser mayor o igual que el tamaño del disco del sistema operativo.
- El tamaño del disco temporal debe ser mayor que el tamaño del disco de la memoria caché.

Tenga en cuenta también estos aspectos al:

- Crear el esquema de aprovisionamiento.
- Modificar el esquema de aprovisionamiento.
- Actualizar la imagen.

Hosts dedicados de Azure

Puede usar MCS para aprovisionar VM en los hosts dedicados de Azure. Antes de aprovisionar VM en hosts dedicados de Azure:

- Cree un grupo de hosts.
- Cree hosts en ese grupo de hosts.
- Compruebe que haya suficiente capacidad de host reservada para crear catálogos y máquinas virtuales.

Puede crear un catálogo de máquinas con arrendamiento de hosts definido a través del siguiente script de PowerShell:

```
1 New-ProvScheme <otherParameters> -CustomProperties '<CustomProperties
     xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi
     ="http://www.w3.org/2001/XMLSchema-instance">
2  <Property xsi:type="StringProperty" Name="HostGroupId" Value="
      myResourceGroup/myHostGroup" />
3  ...other Custom Properties...
4  </CustomProperties>
```

Cuando utilice MCS para aprovisionar máquinas virtuales en hosts dedicados de Azure, tenga en cuenta que:

- Un *host dedicado* es una propiedad del catálogo y no se puede cambiar una vez creado dicho catálogo. Actualmente, el arrendamiento dedicado no está disponible en Azure.
- Se requiere un grupo de hosts de Azure preconfigurado, en la región de la unidad de alojamiento, al utilizar el parámetro `HostGroupId`.

- Se requiere la ubicación automática de Azure. Esta funcionalidad realiza una solicitud para incorporar la suscripción asociada al grupo de hosts. Para obtener más información, consulte VM Scale Set on Azure Dedicated Hosts - Public Preview. Si la ubicación automática no está habilitada, MCS genera un error durante la creación del catálogo.

Crear o actualizar un catálogo de máquinas con una imagen de Azure Compute Gallery

Al seleccionar una imagen para utilizarla para crear un catálogo de máquinas, puede seleccionar las imágenes que haya creado en Azure Compute Gallery.

Para que aparezcan estas imágenes, haga lo siguiente:

1. Configurar un sitio de Citrix Virtual Apps and Desktops.
2. Conéctese a Azure Resource Manager.
3. En Azure Portal, cree un grupo de recursos. Para obtener información detallada, consulte Creación de una galería de Azure Compute mediante el portal.
4. En el grupo de recursos, cree una galería Azure Compute Gallery.
5. En Azure Compute Gallery, cree una definición de imagen.
6. En la definición de imagen, cree una versión de imagen.

Use los siguientes comandos de PowerShell para crear o actualizar un catálogo de máquinas con una imagen de Azure Compute Gallery:

1. Abra una ventana de PowerShell.
2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
3. Seleccione un grupo de recursos y, a continuación, enumere todas las galerías de ese grupo de recursos.

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\testresource\
    image.folder\sharedImageGalleryTest.resourcegroup")
```

4. Seleccione una galería y, a continuación, enumere todas las definiciones de imágenes de esa galería.

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\testresource\
    image.folder\sharedImageGalleryTest.resourcegroup\
    sharedImageGallery.sharedimagegallery")
```

5. Seleccione una definición de imagen y, a continuación, enumere todas las versiones de imagen de esa definición de imagen.

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\testresource\
    image.folder\sharedImageGalleryTest.resourcegroup\
    sharedImageGallery.sharedimagegallery\sigtestimage.
    imagedefinition")
```


6. Cree y actualice un catálogo de MCS con los siguientes elementos:

    - Resource group
    - Galería
    - Definición de imagen de la galería
    - Versión de la imagen de la galería

    Para obtener información sobre cómo crear un catálogo con el SDK de PowerShell remoto, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Configurar Shared Image Gallery

Utilice el comando `New-ProvScheme` para crear un esquema de aprovisionamiento que permita usar Shared Image Gallery. Utilice el comando `Set-ProvScheme` para habilitar o inhabilitar esta función en los esquemas de aprovisionamiento y para cambiar el índice de réplicas y los valores máximos de las réplicas.

Se agregaron tres propiedades personalizadas a los esquemas de aprovisionamiento para admitir la función Shared Image Gallery:

`UseSharedImageGallery`

- Define si se va a utilizar Shared Image Gallery para almacenar las imágenes publicadas. Si se establece en **True**, la imagen se almacena como una imagen de Shared Image Gallery; de lo contrario, la imagen se almacena como una instantánea.
- Los valores válidos son **True** y **False**.
- Si la propiedad no está definida, el valor predeterminado es **False**.

`SharedImageGalleryReplicaRatio`

- Define el índice entre máquinas y réplicas de versiones de imágenes de la galería.
- Los valores válidos son números enteros mayores que 0.
- Si la propiedad no está definida, se utilizan los valores predeterminados. El valor predeterminado para los discos de SO persistentes es 1000, y el valor predeterminado para los discos de SO no persistentes es 40.

`SharedImageGalleryReplicaMaximum`

- Define el máximo de réplicas para cada versión de imagen de la galería.
- Si la propiedad no está definida, el valor predeterminado es 100.
- Si la propiedad no está definida, el valor predeterminado es 100.

> **Sugerencia:**
>
> Al utilizar Shared Image Gallery para almacenar una imagen publicada de catálogos aprovisionados con MCS, MCS establece el recuento de réplicas de versiones de imágenes de la galería en función de la cantidad de máquinas del catálogo, el índice de réplicas y el máximo de réplicas. El recuento de réplicas se calcula al dividir la cantidad de máquinas del catálogo entre el índice de réplicas (se redondea al valor entero más cercano). A continuación, se limita el valor al recuento máximo de réplicas. Por ejemplo, con un índice de réplicas de 20 y un máximo de 5, entre 0 y 20 máquinas tienen una réplica creada, entre 21 y 40 tienen 2 réplicas, entre 41 y 60 tienen 3 réplicas, entre 61 y 80 tienen 4 réplicas, y más de 81 tienen 5 réplicas.

Caso de uso: Actualizar el índice de réplicas y el máximo de réplicas de Shared Image Gallery

El catálogo de máquinas existente utiliza Shared Image Gallery. Utilice el comando `Set-ProvScheme` para actualizar las propiedades personalizadas de todas las máquinas existentes del catálogo y de futuras máquinas:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"> <Property xsi:type="StringProperty" Name="StorageType"
    Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
    UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
    Name="UseSharedImageGallery" Value="True"/> <Property xsi:type="
    IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/> <
    Property xsi:type="IntProperty" Name="
    SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'
```

Caso de uso: Convertir un catálogo de instantáneas en un catálogo de Shared Image Gallery

Para este caso de uso:

1. Ejecute `Set-ProvScheme` con el indicador `UseSharedImageGallery` establecido en **True**. Si quiere, incluya las propiedades `SharedImageGalleryReplicaRatio` y `SharedImageGalleryReplicaMaximum`.
2. Actualice el catálogo.
3. Apague y encienda las máquinas para forzar una actualización.

Por ejemplo:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"> <Property xsi:type="StringProperty" Name="StorageType"
    Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
```



```
UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
Name="UseSharedImageGallery" Value="True"/> <Property xsi:type="
IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/> <
Property xsi:type="IntProperty" Name="
SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'
```

> **Sugerencia:**
>
> Los parámetros `SharedImageGalleryReplicaRatio` y `SharedImageGalleryReplicaMaximum` no son necesarios. Una vez finalizado el comando `Set-ProvScheme`, aún no se ha creado la imagen de Shared Image Gallery. Una vez configurado el catálogo para utilizar la galería, la siguiente operación de actualización del catálogo almacena la imagen publicada en la galería. El comando de actualización del catálogo crea la galería, la imagen de la galería y la versión de la imagen. Apagar y encender las máquinas las actualiza, momento en el que se actualiza el recuento de réplicas, si procede. A partir de ese momento, todas las máquinas no persistentes existentes se restablecen mediante la imagen de Shared Image Gallery, y todas las máquinas recién aprovisionadas se crean mediante la imagen. La antigua instantánea se borra automáticamente en unas horas.

Caso de uso: Convertir un catálogo de Shared Image Gallery en un catálogo de instantáneas

Para este caso de uso:

1. Ejecute `Set-ProvScheme` con el indicador `UseSharedImageGallery` establecido en **False** o sin definir.
2. Actualice el catálogo.
3. Apague y encienda las máquinas para forzar una actualización.

Por ejemplo:

```
1 Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"> <Property xsi:type="StringProperty" Name="StorageType"
    Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
    UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
    Name="UseSharedImageGallery" Value="False"/></CustomProperties>'
```

> **Sugerencia:**
>
> A diferencia de actualizar una instantánea a un catálogo de Shared Image Gallery, los datos personalizados de cada máquina aún no se actualizan para reflejar las nuevas propiedades personalizadas. Ejecute el siguiente comando para ver las propiedades personalizadas originales de Shared Image Gallery: `Get-ProvVm -ProvisioningSchemeName catalog-name`. Una vez finalizado el comando `Set-ProvScheme`, aún no se ha creado la instantánea de la

> imagen publicada. Una vez configurado el catálogo para que no utilice la galería, la siguiente operación de actualización del catálogo almacena la imagen publicada como una instantánea. A partir de ese momento, todas las máquinas no persistentes existentes se restablecen mediante la instantánea, y todas las máquinas recién aprovisionadas se crean a partir de la instantánea. Apagar y encender las máquinas las actualiza, momento en el que los datos personalizados de las máquinas se actualizan para reflejar que `UseSharedImageGallery` está establecido en **False**. Los antiguos elementos de Shared Image Gallery (la galería, la imagen y la versión) se borran automáticamente en unas horas.

Aprovisionar máquinas en zonas de disponibilidad especificadas

En entornos de Azure, es posible aprovisionar máquinas en zonas de disponibilidad específicas. Puede hacerlo con PowerShell.

> **Nota:**
>
> Si no se especifica ninguna zona, MCS permite a Azure colocar las máquinas dentro de la región. Si se especifica más de una zona, MCS distribuye aleatoriamente las máquinas entre ellas.

Configurar zonas de disponibilidad a través de PowerShell

Con PowerShell, puede ver la oferta de elementos de inventario mediante `Get-Item`. Por ejemplo, para ver la oferta de servicio de la *región oriental de EE. UU.* `Standard_B1ls`:

```
1 $serviceOffering = Get-Item -path "XDHyp:\Connections\my-connection-
     name\East US.region\serviceoffering.folder\Standard_B1ls.
     serviceoffering"
```

Para ver las zonas, utilice el parámetro `AdditionalData` para el elemento:

```
$serviceOffering.AdditionalData
```

Si no se especifican zonas de disponibilidad, no hay ningún cambio en la forma en que se aprovisionan las máquinas.

Para configurar las zonas de disponibilidad a través de PowerShell, utilice la propiedad personalizada **Zonas** disponible con la operación `New-ProvScheme`. La propiedad **Zonas** define una lista de zonas de disponibilidad en las que aprovisionar máquinas. Esas zonas pueden incluir una o más zonas de disponibilidad. Por ejemplo, `<Property xsi:type="StringProperty"Name="Zones" Value="1, 3"/>` para las zonas 1 y 3.

Utilice el comando `Set-ProvScheme` para actualizar las zonas de un esquema de aprovisionamiento.

Si se proporciona una zona no válida, el esquema de aprovisionamiento no se actualiza y aparece un mensaje de error con instrucciones sobre cómo corregir el comando no válido.

> **Sugerencia:**
>
> Si especifica una propiedad personalizada no válida, el esquema de aprovisionamiento no se actualiza y aparece un mensaje de error al respecto.

Tipos de almacenamiento

Seleccione distintos tipos de almacenamiento para máquinas virtuales en entornos Azure que utilizan MCS. Para las máquinas virtuales de destino, MCS admite:

- Disco de SO: SSD Premium, SSD o HDD
- Disco de memoria caché con escritura: SSD Premium, SSD o HDD

Al utilizar estos tipos de almacenamiento, tenga en cuenta lo siguiente:

- Asegúrese de que su máquina virtual sea compatible con el tipo de almacenamiento seleccionado.
- Si su configuración usa un disco efímero de Azure, no tiene la posibilidad de configurar el disco de caché de reescritura.

> **Sugerencia:**
>
> `StorageType` está configurado para un tipo de SO y una cuenta de almacenamiento. `WBCDiskStorageType` está configurado para el tipo de almacenamiento de memoria caché de escritura. Para un catálogo normal, se requiere `StorageType`. Si `WBCDiskStorageType` no está configurado, `StorageType` se utiliza como predeterminado para `WBCDiskStorageType` .

Si WBCDiskStorageType no está configurado, StorageType se utiliza como predeterminado para WBCDiskStorageType.

Configurar los tipos de almacenamiento

Para configurar los tipos de almacenamiento para VM, utilice el parámetro `StorageType` en `New-ProvScheme`. Establezca el valor del parámetro `StorageType` en uno de los tipos de almacenamiento admitidos.

A continuación, se muestra un conjunto de ejemplo del parámetro `CustomProperties` en un esquema de aprovisionamiento:

```
1 Set-ProvScheme -ProvisioningSchemeName catalog-name -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="StorageType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
   Windows_Client" />
</CustomProperties>'
```

Habilitar el almacenamiento con redundancia de zonas

Puede seleccionar almacenamiento con redundancia de zonas durante la creación de catálogos. Replica sincrónicamente su disco administrado de Azure en varias zonas de disponibilidad, lo que le permite recuperarse de un error en una zona al usar la redundancia en otras.

Puede especificar **Premium_ZRS** y **StandardSSD_ZRS** en las propiedades personalizadas del tipo de almacenamiento. El almacenamiento ZRS se puede configurar mediante propiedades personalizadas existentes o mediante la plantilla **MachineProfile**. El almacenamiento ZRS también es compatible con el comando `Set-ProvVMUpdateTimeWindow` mediante los parámetros `-StartsNow` y `-DurationInMinutes -1`, y usted puede cambiar el almacenamiento de la máquina existente de LRS a ZRS.

Limitaciones:

- Compatible solo para discos administrados
- Compatible únicamente con unidades de estado sólido (SSD) estándar y premium
- No es compatible con `StorageTypeAtShutdown`
- Disponible solo en determinadas regiones.
- El rendimiento de Azure disminuye al crear discos ZRS a escala. Por lo tanto, al encenderlas por primera vez, encienda las máquinas en lotes más pequeños (menos de 300 máquinas a la vez)

Definir el almacenamiento con redundancia de zonas como tipo de almacenamiento en disco

Puede seleccionar un almacenamiento con redundancia de zonas durante la creación de catálogos inicial o puede actualizar el tipo de almacenamiento en un catálogo existente.

Seleccionar el almacenamiento con redundancia de zonas mediante los comandos de PowerShell Al crear un catálogo en Azure mediante el comando `New-ProvScheme` de PowerShell, use `Standard_ZRS` como valor en `StorageAccountType`.
Por ejemplo:

```
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   StandardSSD_ZRS" />
```


Al definir este valor, se valida mediante una API dinámica que determina si se puede utilizar correctamente. Se pueden producir estas excepciones si el uso de ZRS no es válido para su catálogo:

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: La propiedad personalizada StorageTypeAtShutdown no se puede utilizar con el almacenamiento ZRS.
- **StorageAccountTypeNotSupportedInRegion**: Esta excepción se produce si intenta utilizar el almacenamiento ZRS en una región de Azure que no admite ZRS.
- **ZrsRequiresManagedDisks**: Solo puede utilizar el almacenamiento con redundancia de zonas con discos administrados.

Puede configurar el tipo de almacenamiento en disco mediante estas propiedades personalizadas:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`

> **Nota:**
>
> Durante la creación de catálogos, se utiliza el `StorageType` del disco del sistema operativo del perfil de máquina si las propiedades personalizadas no están configuradas.

Capture la configuración de diagnóstico en máquinas virtuales y NIC desde un perfil de máquina

Puede capturar la configuración de diagnóstico de las máquinas virtuales y las NIC desde un perfil de máquina mientras crea un catálogo de máquinas, actualiza un catálogo de máquinas existente y actualiza las máquinas virtuales existentes.

Puede crear una máquina virtual o una especificación de plantilla como fuente del perfil de máquina.

Pasos clave

1. Configure los ID necesarios en Azure. Debe proporcionar estos ID en la especificación de la plantilla.
    - Cuenta de almacenamiento
    - Espacio de trabajo de analíticas de registros
    - Espacio de nombres del centro de eventos con el precio del nivel estándar
2. Cree un origen de perfil de máquina.
3. Cree un nuevo catálogo de máquinas, actualice un catálogo existente o actualice las máquinas virtuales existentes.

Configurar los ID necesarios en Azure

Configure una de las siguientes opciones en Azure:

- Cuenta de almacenamiento
- Espacio de trabajo de analíticas de registros
- Espacio de nombres del centro de eventos con el precio del nivel estándar

Configurar una cuenta de almacenamiento Cree una cuenta de almacenamiento estándar en Azure. En la especificación de la plantilla, indique el resourceId completo de la cuenta de almacenamiento como el `storageAccountId`.

Una vez que las máquinas virtuales estén configuradas para registrar los datos en la cuenta de almacenamiento, los datos se pueden encontrar en el contenedor `insights-metrics-pt1m`.

Configurar un espacio de trabajo de análisis de registros Cree un espacio de trabajo de análisis de registros. En la especificación de la plantilla, indique el resourceId completo para el espacio de trabajo de análisis de registros como workspaceId.

Una vez que las máquinas virtuales estén configuradas para registrar datos en el espacio de trabajo, los datos se pueden consultar en Registros en Azure. Puede ejecutar el siguiente comando en Azure en Registros para mostrar un recuento de todas las métricas registradas por un recurso:

‘AzureMetrics
| summarize Count=count() by ResourceId# Crear un catálogo de Microsoft Azure

> **Nota:**
>
> Desde julio de 2023, Microsoft cambió el nombre de Azure Active Directory (Azure AD) a Microsoft Entra ID. En este documento, cualquier referencia a Azure Active Directory, Azure AD o AAD ahora se refiere a Microsoft Entra ID.

Crear catálogos de máquinas describe los asistentes con los que se crea un catálogo de máquinas. La siguiente información incluye detalles específicos de los entornos de nube de Microsoft Azure Resource Manager.

> **Nota:**
>
> Antes de crear un catálogo de Microsoft Azure, debe terminar de crear una conexión con Microsoft Azure. Consulte Conexión con Microsoft Azure.

Creación de un catálogo de máquinas

Puede crear un catálogo de máquinas de dos maneras:

- Crear un catálogo de máquinas con una imagen de Azure Resource Manager en Web Studio
- Crear un catálogo de máquinas con PowerShell

Crear un catálogo de máquinas con una imagen de Azure Resource Manager en Web Studio

Una imagen puede ser un disco, una instantánea o la versión de una imagen de una definición de imagen en Azure Compute Gallery que se usa para crear las máquinas virtuales en un catálogo de máquinas. Antes de crear el catálogo de máquinas, cree una imagen en Azure Resource Manager. Para obtener información general acerca de las imágenes, consulte Crear catálogos de máquinas.

> **Nota:**
>
> Se retiró la compatibilidad con el uso de una imagen maestra de una región diferente a la configurada en la conexión del host. Use Azure Compute Gallery para replicar la imagen maestra en la región deseada.

Durante la preparación de la imagen, se crea una VM de preparación basada en la máquina virtual original. Esta máquina virtual de preparación está desconectada de la red. Para desconectar la red de la máquina virtual de preparación, se crea un grupo de seguridad de red para denegar todo el tráfico entrante y saliente. El grupo de seguridad de red se crea automáticamente una vez por catálogo. El nombre del grupo de seguridad de red es <!JEKYLL@5300@0>, donde el GUID se genera aleatoriamente. Por ejemplo, <!JEKYLL@5300@1>.

En el asistente para la creación de catálogos de máquinas:

- Las páginas **Tipo de máquina** y **Administración de máquinas** no contienen información específica de Azure. Siga las instrucciones indicadas en el artículo Crear catálogos de máquinas.
- En la página **Imagen**, elija una imagen que quiera usar como plantilla para crear máquinas en este catálogo.

  Si selecciona **Imagen maestra** como el tipo de imagen que va a usar, haga clic en **Seleccionar una imagen** y siga estos pasos para seleccionar una imagen maestra según sea necesario:

  1. (Aplicable solo a las conexiones configuradas con imágenes compartidas en o entre arrendatarios). Seleccione una suscripción en la que resida la imagen.
  2. Seleccione un grupo de recursos.
  3. Vaya a Azure VHD, Azure Compute Gallery o la versión de imagen de Azure. Si es necesario, agregue una nota a la imagen seleccionada.

  Al seleccionar una imagen, tenga en cuenta lo siguiente:

  - Compruebe que hay un VDA de Citrix instalado en la imagen.
  - Si selecciona un disco duro virtual (VHD) conectado a una máquina virtual, debe apagar esta antes de continuar con el siguiente paso.

Nota:

- La suscripción correspondiente a la conexión (host) que creó las máquinas del catálogo se indica con un punto verde. Las demás suscripciones son aquellas en las que se comparte Azure Compute Gallery con esa suscripción. En esas suscripciones, solo se muestran las galerías compartidas. Para obtener información sobre cómo configurar las suscripciones compartidas, consulte Compartir imágenes con un arrendatario (entre suscripciones) y Compartir imágenes entre arrendatarios.
- Es obligatorio usar un perfil de máquina con Inicio seguro como **Tipo de seguridad** al seleccionar una imagen o una instantánea que tenga habilitado el inicio seguro. A continuación, para habilitar o inhabilitar SecureBoot y vTPM, especifique sus valores en el perfil de la máquina. El inicio de confianza no se admite en Shared Image Gallery. Para obtener información sobre el inicio de confianza de Azure, consulte https://docs.microsoft.com/en-us/azure/virtual-machines/trusted-launch.
- Puede crear un esquema de aprovisionamiento mediante un disco de SO efímero en Windows con inicio seguro. Al seleccionar una imagen con inicio seguro, debe seleccionar un perfil de máquina con inicio seguro que esté habilitado con vTPM. Para crear catálogos de máquinas con un disco de SO efímero, consulte Cómo crear máquinas con discos de SO efímeros.
- Durante la replicación de imágenes, puede continuar y seleccionar la imagen como imagen maestra y completar la configuración. Sin embargo, es posible que la creación de catálogos tarde más tiempo en completarse mientras se replica la imagen. MCS necesita que la replicación se complete en una hora a partir de la creación de catálogos. Si la replicación tarda más, no se crean los catálogos. Puede verificar el estado de la replicación en Azure. Inténtelo de nuevo si la replicación sigue pendiente o después de que se haya completado.
- Al seleccionar una imagen maestra para catálogos de máquinas en Azure, MCS identifica el tipo de SO en función de la imagen maestra y el perfil de máquina que seleccione. Si MCS no puede identificarlo, seleccione el tipo de SO que coincida con el de la imagen maestra.
- Puede aprovisionar un catálogo de máquinas virtuales de 2.ª generación mediante una imagen de 2.ª generación para mejorar el rendimiento del tiempo de arranque. Sin embargo, no se admite la creación de catálogos de máquinas de 2.ª generación con una imagen de 1.ª generación. Del mismo modo, tampoco se admite la creación de catálogos de máquinas de 1.ª generación con una imagen de 2.ª generación. Además, cualquier imagen antigua que no tenga información de generación es una imagen de 1.ª generación.

Si selecciona **Imagen preparada** como el tipo de imagen que va a usar, haga clic en **Seleccionar una imagen** y seleccione una imagen preparada según sea necesario.

Para garantizar la creación correcta de la máquina virtual, verifique que la imagen tenga instalado Citrix VDA 2311 o una versión posterior y que E/S de MCS esté presente en el VDA.

Tras seleccionar una imagen, la casilla **Usar un perfil de máquina (obligatoria para Azure Active Directory)** se selecciona automáticamente. Haga clic en **Seleccione un perfil de máquina** para buscar una VM o una especificación de plantilla de ARM en una lista de grupos de recursos. Las máquinas virtuales del catálogo pueden heredar configuraciones del perfil de máquina seleccionado.

Valide la especificación de plantilla ARM para asegurarse de que se puede utilizar como perfil de máquina para crear un catálogo de máquinas. Hay dos formas de validar la especificación de la plantilla ARM:

- Después de seleccionar la especificación de plantilla ARM en la lista de grupos de recursos, haga clic en **Siguiente**. Aparecen mensajes de error si la especificación de plantilla ARM contiene errores.
- Ejecute uno de estos comandos de PowerShell:
  - <!JEKYLL@5300@2>
  - <!JEKYLL@5300@3>

Algunos ejemplos de configuraciones que las máquinas virtuales pueden heredar de un perfil de máquina incluyen:

- Redes aceleradas
- Diagnóstico de arranque
- Almacenamiento en caché de discos de host (relacionado con discos de SO y de E/S de MCS)
- Tamaño de máquina (a menos que se especifique lo contrario)
- Etiquetas colocadas en la máquina virtual

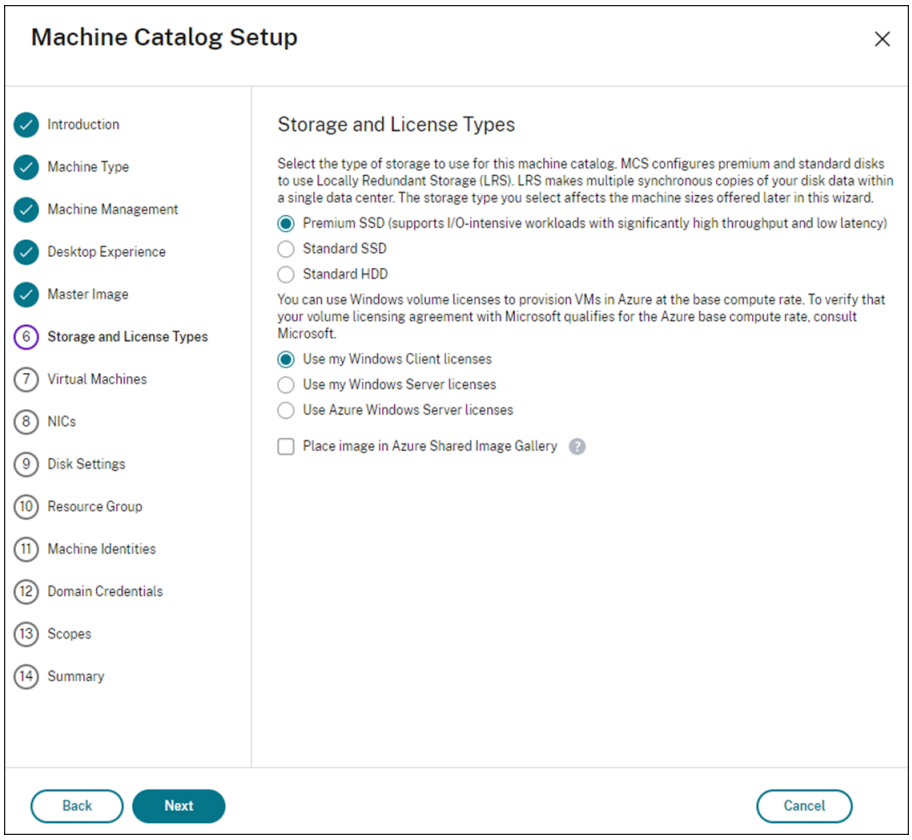
Tras crear el catálogo, podrá ver las configuraciones que la imagen hereda del perfil de máquina. En el nodo **Catálogos de máquinas**, seleccione el catálogo para ver sus detalles en el panel inferior. A continuación, haga clic en la ficha **Propiedades de plantilla** para ver las propiedades del perfil de máquina. La sección **Etiquetas** muestra hasta tres etiquetas. Para ver todas las etiquetas colocadas en la máquina virtual, haga clic en **Ver todo**.

Si quiere que MCS aprovisione máquinas virtuales en un host dedicado de Azure, active la casilla de verificación **Usar un grupo de hosts dedicado** y, a continuación, seleccione un grupo de hosts de la lista. Un grupo de hosts es un recurso que representa un conjunto de hosts dedicados. Un host dedicado es un servicio que proporciona servidores físicos que alojan una o más VM. Su servidor está dedicado a su suscripción de Azure, no se comparte con otros suscriptores. Cuando utiliza un host dedicado, Azure garantiza que sus máquinas virtuales sean las únicas máquinas activas en ese host. Esta función es adecuada para situaciones en las que debe

cumplir con requisitos normativos o de seguridad interna. Para obtener más información sobre los grupos de hosts y las consideraciones para usarlos, consulte Hosts dedicados de Azure.

> **Importante:**
>
> - Solo se muestran los grupos de hosts que tienen habilitada la ubicación automática de Azure.
> - El uso de un grupo de hosts cambia la página **Máquinas virtuales** que se ofrece más adelante en el asistente. En esa página, solo se muestran los tamaños de máquina que contiene el grupo de hosts seleccionado. Además, las zonas de disponibilidad se seleccionan automáticamente y no están disponibles para selección manual.

- La página **Tipos de licencia y almacenamiento** solo aparece cuando se usa una imagen de Azure Resource Manager.



Puede utilizar los siguientes tipos de almacenamiento para el catálogo de máquinas:

- **SSD Premium**. Ofrece una opción de almacenamiento en disco de alto rendimiento y baja latencia, adecuada para máquinas virtuales con cargas de trabajo intensivas de E/S.
- **SSD estándar**. Ofrece una opción de almacenamiento rentable, adecuada para cargas de trabajo que necesitan un rendimiento uniforme a niveles de IOPS más bajos.
- **HDD estándar**. Ofrece una opción de almacenamiento en disco fiable y de bajo coste,

adecuada para máquinas virtuales que ejecutan cargas de trabajo donde no importa la latencia.

- **Disco de SO efímero de Azure**. Ofrece una opción de almacenamiento rentable que reutiliza el disco local de las VM para alojar el disco del sistema operativo. Como alternativa, puede usar PowerShell para crear máquinas que usen discos de SO efímeros. Para obtener más información, consulte Discos efímeros de Azure. Tenga en cuenta las siguientes consideraciones cuando utilice un disco de SO efímero:
  * El disco de SO efímero de Azure y la E/S de MCS no se pueden habilitar al mismo tiempo.
  * Para actualizar máquinas que usan discos de SO efímeros, debe seleccionar una imagen cuyo tamaño no exceda el tamaño del disco de caché o el disco temporal de la VM.
  * No puede usar la opción **Conservar VM y disco del sistema durante los ciclos de energía** que se ofrece más adelante en el asistente.

> **Nota:**
>
> El disco de identidad siempre se crea con un SSD estándar, independientemente del tipo de almacenamiento que elija.

El tipo de almacenamiento determina el tamaño de las máquinas que se ofrecen en la página **Máquinas virtuales** del asistente. MCS configura discos premium y estándar para uso de almacenamiento con redundancia local (LRS). LRS hace varias copias sincrónicas de los datos en un único centro de datos. Los discos de SO efímeros de Azure usan el disco local de las VM para almacenar el sistema operativo. 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 licencias de Windows o de Linux existentes.

- Licencias de Windows: El uso de licencias de Windows junto con imágenes de Windows (imágenes que admita la plataforma Azure o imágenes personalizadas) permite ejecutar máquinas virtuales de Windows en Azure a un coste reducido. Existen dos tipos de licencias:
  * **Licencia de Windows Server**. Le permite utilizar sus licencias de Windows Server o Azure Windows Server, con lo que puede usar las ventajas híbridas de Azure. Para obtener información detallada, consulte https://azure.microsoft.com/en-us/pricing/hybrid-benefit/. Las ventajas híbridas de Azure reducen los costes de ejecución

de máquinas virtuales en Azure a la tarifa básica de procesamiento, lo que elimina el gasto en licencias de Windows Server adicionales desde la galería de Azure.

* **Licencia de cliente de Windows**. Le permite llevar sus licencias de Windows 10 y Windows 11 a Azure, con lo que puede usar máquinas virtuales con Windows 10 y Windows 11 en Azure sin necesidad de licencias adicionales. Para obtener más información, consulte Licencias de acceso de cliente y licencias de administración.

Para comprobar que la máquina virtual aprovisionada aprovecha los beneficios de las licencias, ejecute este comando de PowerShell: <!JEKYLL@5300@4>.

- Para el tipo de licencia de Windows Server, 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/.
- Para el tipo de licencia de cliente de Windows, compruebe que el tipo de licencia es **Windows_Client**. Encontrará instrucciones adicionales en https://docs.microsoft.com/en-us/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/.

También puede usar el SDK de PowerShell <!JEKYLL@5300@5> para hacer la verificación. Por ejemplo: <!JEKYLL@5300@6>. Para obtener más información sobre este cmdlet, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/.

- Licencias de Linux: Con las licencias de Linux de su propia suscripción (BYOS), no tiene que pagar por el software. El cargo de las licencias BYOS solo incluye la tarifa de hardware del procesamiento. Existen dos tipos de licencias:

  * **RHEL_BYOS**: Para usar correctamente el tipo RHEL_BYOS, habilite Red Hat Cloud Access en su suscripción de Azure.
  * **SLES_BYOS**: Las versiones de BYOS de SLES permiten el uso de SUSE.

  Puede establecer el valor de LicenseType en opciones de Linux con <!JEKYLL@5300@7> y <!JEKYLL@5300@8>.

  Ejemplo de configuración de LicenseType en RHEL_BYOS con <!JEKYLL@5300@9>:

  <!JEKYLL@5300@10>

  Ejemplo de configuración de LicenseType en SLES_BYOS con <!JEKYLL@5300@11>:

  <!JEKYLL@5300@12>

  > **Nota:**

> Si el valor <!JEKYLL@5300@13> está vacío, los valores predeterminados son Azure Windows Server License o Azure Linux License, según el valor de OsType.

Ejemplo de configuración de LicenseType vacío:

<!JEKYLL@5300@14>

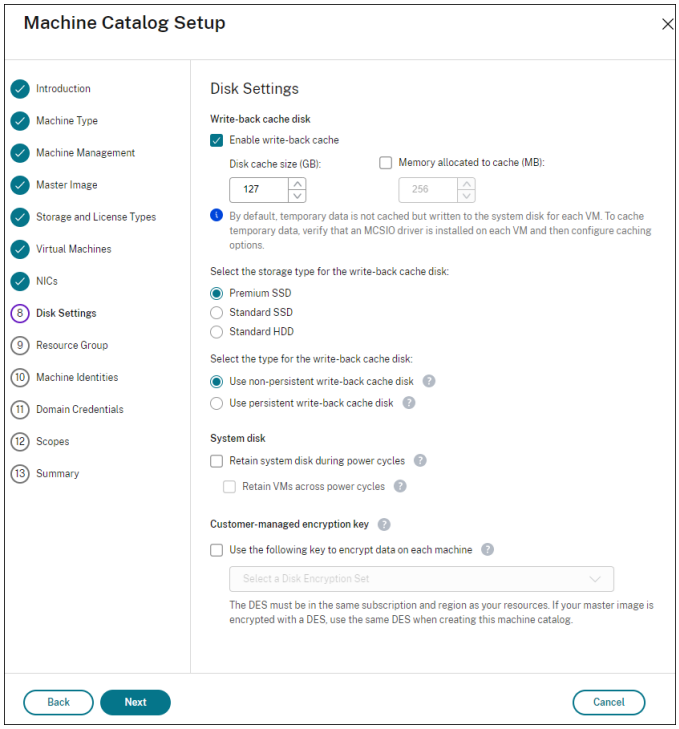
Consulte estos documentos para comprender los tipos de licencias y sus beneficios:

- https://docs.microsoft.com/en-us/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet
- https://docs.microsoft.com/en-us/azure/virtual-machines/linux/azure-hybrid-benefit-linux

Azure Compute Gallery (antes denominado Azure Shared Image Gallery) es un repositorio para administrar y compartir imágenes. Le permite poner sus imágenes a disposición de toda la organización. Le recomendamos almacenar una imagen en SIG al crear grandes catálogos de máquinas no persistentes, ya que, así, los discos del SO de VDA se pueden restablecer más rápidamente. Después de seleccionar **Colocar la imagen preparada en Azure Compute Gallery**, aparece la sección **Configuración de Azure Compute Gallery**, que le permite especificar más parámetros de Azure Computer Gallery:

- **Índice de máquinas virtuales por réplica de imagen**. Permite especificar la ratio de máquinas virtuales y réplicas de imagen que mantendrá Azure. De forma predeterminada, Azure mantiene una única réplica de imagen por cada 40 máquinas no persistentes. En el caso de máquinas persistentes, la cantidad predeterminada es de 1000 máquinas.
- **Máximo de réplicas**. Permite especificar el máximo de réplicas de imagen que conservará Azure. El valor predeterminado es 100.

- En la página **Máquinas virtuales**, indique la cantidad de máquinas virtuales que quiere crear. Debe especificar al menos una y seleccionar un tamaño de máquina. Después de crear el catálogo, puede modificar el catálogo para cambiar el tamaño de la máquina.
- La página **Tarjetas NIC** no contiene información específica de Azure. Siga las instrucciones indicadas en el artículo Crear catálogos de máquinas.
- En la página **Parámetros del disco**, elija si quiere habilitar la caché de reescritura. Con la función de optimización del almacenamiento de MCS habilitada, puede configurar los siguientes parámetros al crear un catálogo: Esta configuración se aplica tanto a los entornos de Azure como a los de GCP.



Después de habilitar la caché de reescritura, puede hacer lo siguiente:

- Puede configurar la RAM y el tamaño del disco utilizados para almacenar en caché datos temporales. Para obtener más información, consulte Configurar la caché de datos temporales.
- Seleccione el tipo de almacenamiento del disco de caché de reescritura. Están disponibles las siguientes opciones de almacenamiento para uso con el disco de caché de reescritura:
  - SSD Premium
  - SSD estándar
  - HDD estándar
- Elija si prefiere que el disco de caché de reescritura sea persistente para las máquinas virtuales aprovisionadas. Seleccione **Habilitar caché de reescritura** para que estas opciones estén disponibles. De forma predeterminada, se selecciona **Usar disco no persistente de caché de reescritura**.
- Seleccione el tipo de disco de caché de reescritura.
  - **Usar disco no persistente de caché de reescritura**. Si se selecciona, el disco de caché de reescritura se elimina durante los ciclos de energía. Se perderán todos los datos redirigidos a él. Si el disco temporal de la VM tiene suficiente espacio, se usa para alojar el disco de caché de reescritura para reducir los costes. Tras la creación del catálogo, puede comprobar si las máquinas aprovisionadas utilizan el disco temporal. Para ello, haga clic en el catálogo y verifique la información de la ficha **Propiedades**

de plantilla. Si se usa el disco temporal, verá **Disco no persistente de caché de reescritura**, y su valor es **Sí (con el disco temporal de la máquina virtual)**. De lo contrario, verá **Disco no persistente de caché de reescritura**, y su valor es **No (sin usar el disco temporal de la VM)**.

* **Usar disco persistente de caché de reescritura**. Si se selecciona, el disco de caché de reescritura persiste en las máquinas virtuales aprovisionadas. Habilitar esta opción aumenta los costes de almacenamiento.

- Elija si quiere conservar las VM y los discos del sistema para los VDA durante los ciclos de energía.

  Conservar VM y disco del sistema durante los ciclos de energía. Disponible cuando se ha seleccionado **Habilitar caché de reescritura**. De forma predeterminada, las VM y los discos del sistema se eliminan al apagar la máquina y se crean de nuevo al iniciarla. Si quiere reducir los tiempos de reinicio de las máquinas virtuales, seleccione esta opción. Recuerde que habilitar esta opción también aumenta los costes de almacenamiento.

- Elija si quiere habilitar el **ahorro de costes de almacenamiento**. Si se habilita, para ahorrar costes de almacenamiento, revierta el disco de almacenamiento a un disco duro estándar cuando la máquina virtual se apague. La máquina virtual cambia a sus parámetros originales al reiniciarse. La opción se aplica tanto a los discos de almacenamiento como a los discos de caché de reescritura. También puede usar PowerShell. Consulte Cambiar el tipo de almacenamiento a un nivel inferior al apagar una máquina virtual.

  > **Nota:**
  >
  > Microsoft impone restricciones al cambiar el tipo de almacenamiento durante el apagado de máquinas virtuales. También es posible que, en el futuro, Microsoft bloquee cambios en el tipo de almacenamiento. Para obtener más información, consulte este artículo de Microsoft.

- Elija si quiere cifrar los datos de las máquinas aprovisionadas en el catálogo. El cifrado del lado del servidor con una clave de cifrado administrada por el cliente permite administrar el cifrado a nivel de disco administrado y proteger los datos que contengan las máquinas del catálogo. Para obtener más información, consulte Cifrado del lado del servidor de Azure.

- En la página **Grupo de recursos**, elija si quiere crear grupos de recursos o usar los grupos existentes.

  - Si opta por crear grupos de recursos, seleccione **Siguiente**.
  - Si decide utilizar los grupos de recursos existentes, seleccione esos grupos en la lista **Grupos de recursos de aprovisionamiento disponibles**. **Recuerde:** Debe seleccionar grupos suficientes para las máquinas que está creando en el catálogo. Si no elige suficientes,

aparecerá un mensaje. 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.

- En la página **Identidades de las máquinas**, elija un tipo de identidad y configure las identidades de las máquinas de este catálogo. Si selecciona las máquinas virtuales como **unidas a Azure Active Directory**, puede agregarlas a un grupo de seguridad de Azure AD. Estos son los pasos detallados:

  1. En el campo **Tipo de identidad**, seleccione **Unido a Azure Active Directory**. Aparecerá la opción **Grupo de seguridad de Azure AD (opcional)**.
  2. Haga clic en **Grupo de seguridad de Azure AD: Crear nuevo**.
  3. Introduzca un nombre de grupo y, a continuación, haga clic en **Crear**.
  4. Siga las instrucciones que aparecen en pantalla para iniciar sesión en Azure.
     Si el nombre del grupo no existe en Azure, aparecerá un icono verde. De lo contrario, aparecerá un mensaje de error en el que se le pide que introduzca un nombre nuevo.
  5. Introduzca el esquema de nomenclatura de las cuentas de máquina para las máquinas virtuales.

  Tras la creación del catálogo, Citrix Virtual Apps and Desktops accede a Azure en su nombre y crea el grupo de seguridad y una regla de pertenencia dinámica para el grupo. Según la regla, las máquinas virtuales con el esquema de nomenclatura especificado en este catálogo se agregan automáticamente al grupo de seguridad.

  Para agregar a este catálogo máquinas virtuales con un esquema de nomenclatura diferente, debe iniciar sesión en Azure. A continuación, Citrix Virtual Apps and Desktops puede acceder a Azure y crear una regla de pertenencia dinámica basada en el nuevo esquema de nomenclatura.

  Para poder eliminar el grupo de seguridad de Azure al eliminar este catálogo, también es necesario iniciar sesión en Azure.

- Las páginas **Credenciales de dominio** y **Resumen** no contienen información específica de Azure. Siga las instrucciones indicadas en el artículo Crear catálogos de máquinas.

Complete el asistente.

Condiciones para que el disco temporal de Azure sea apto como disco de caché de reescritura

Solamente puede usar el disco temporal de Azure como disco de caché de reescritura si se cumplen todas las condiciones siguientes:

- El disco de caché con escritura no debe persistir, ya que el disco temporal de Azure no es adecuado para datos persistentes.
- El tamaño de VM de Azure elegido debe incluir un disco temporal.
- No es necesario que el disco de SO efímero esté habilitado.
- Aceptar colocar el archivo de caché con escritura en el disco temporal de Azure.
- El tamaño del disco temporal de Azure debe ser mayor que el tamaño total de (tamaño del disco de caché de reescritura + espacio reservado para el archivo de paginación + 1 GB de espacio de búfer).

Casos de disco no persistente de caché de reescritura

En la siguiente tabla se describen tres casos diferentes en los que se utiliza un disco temporal para la caché de reescritura al crear un catálogo de máquinas.

Caso	Resultado
Se cumplen todas las condiciones para usar un disco temporal para la caché de reescritura.	El archivo WBC <!JEKYLL@5300@15> se coloca en el disco temporal.
El disco temporal no tiene suficiente espacio para uso de caché de reescritura.	Se crea un disco VHD <!JEKYLL@5300@16> y se coloca un archivo WBC <!JEKYLL@5300@17> en este disco.
El disco temporal tiene espacio suficiente para usar caché de reescritura, pero <!JEKYLL@5300@18> está configurado como **false**.	Se crea un disco VHD <!JEKYLL@5300@19> y se coloca un archivo WBC <!JEKYLL@5300@20> en este disco.

Crear una especificación de plantilla de Azure

Puede crear una especificación de plantilla de Azure en Azure Portal y utilizarla en Web Studio y en los comandos de PowerShell para crear o actualizar catálogos de máquinas de MCS.

Para crear una especificación de plantilla de Azure para una máquina virtual existente:

1. Vaya a Azure Portal. Seleccione un grupo de recursos y, a continuación, seleccione la VM y la interfaz de red. En el menú **...** de la parte superior, haga clic en **Export template**.
2. Desmarque la casilla **Include parameters** si quiere crear una especificación de plantilla para el aprovisionamiento de catálogos.
3. Haga clic en **Add to library** para modificar la especificación de la plantilla más adelante.

4. En la página **Importing template**, introduzca la información requerida, como **Name**, **Subscription**, **Resource Group**, **Location** y **Version**. Haga clic en **Next: Edit Template**.
5. También necesita una interfaz de red como recurso independiente si quiere aprovisionar catálogos. Por lo tanto, debe quitar cualquier <!JEKYLL@5300@21> especificado en la especificación de la plantilla. Por ejemplo:

   <!JEKYLL@5300@22>
6. Haga clic en **Review+Create** y cree la especificación de la plantilla.
7. En la página **Template Specs**, compruebe la especificación de plantilla que acaba de crear. Haga clic en la especificación de la plantilla. En el panel de la izquierda, haga clic en **Versions**.
8. Para crear otra versión, haga clic en **Create new version**. Especifique un nuevo número de versión, modifique la especificación de la plantilla actual y haga clic en **Review+Create** para crear la otra versión de la especificación de plantilla.

Puede obtener información sobre la especificación y la versión de la plantilla mediante estos comandos de PowerShell:

- Para obtener información sobre la especificación de la plantilla, ejecute:

  <!JEKYLL@5300@23>
- Para obtener información sobre la versión de la especificación de la plantilla, ejecute:

  <!JEKYLL@5300@24>

Usar la especificación de la plantilla para crear o actualizar un catálogo

Puede crear o actualizar un catálogo de máquinas de MCS mediante una especificación de plantilla como entrada de datos de un perfil de máquina. Para ello, puede utilizar Web Studio o los comandos de PowerShell.

- Para Web Studio, consulte Crear un catálogo de máquinas con una imagen de Azure Resource Manager en Web Studio
- Para PowerShell, consulte Usar la especificación de la plantilla para crear o actualizar un catálogo con PowerShell

Cifrado del lado del servidor de Azure

Citrix Virtual Apps and Desktops admite claves de cifrado administradas por el cliente para los discos administrados por Azure a través de Azure Key Vault. Gracias a esta compatibilidad, puede satisfacer los requisitos organizativos y de conformidad mediante el cifrado de los discos administrados del

catálogo de máquinas con su propia clave de cifrado. Para obtener más información, consulte Cifrado del lado del servidor de Azure Disk Storage.

Al utilizar esta función para discos administrados:

- Para cambiar la clave con la que está cifrado actualmente el disco, cámbiela en <!JEKYLL@5300@25>. Todos los recursos asociados a ese <!JEKYLL@5300@26> se cifrarán con la nueva clave.
- Cuando inhabilite o elimine la clave, todas las máquinas virtuales con discos que utilicen esa clave se apagarán automáticamente. Después de apagarse, las máquinas virtuales no se podrán utilizar, a menos que la clave se vuelva a habilitar o se asigne una nueva clave. Ningún catálogo que utilice la clave se podrá encender ni se le podrán agregar máquinas virtuales.

Consideraciones importantes al utilizar claves de cifrado administradas por el cliente

Tenga en cuenta lo siguiente al usar esta funcionalidad:

- Todos los recursos relacionados con las claves administradas por el cliente (instancias de Azure Key Vault, conjuntos de cifrado de disco, máquinas virtuales, discos e instantáneas) deben residir en la misma suscripción y región.
- Los discos, las instantáneas y las imágenes cifradas con claves administradas por el cliente no pueden transferirse a otro grupo de recursos y suscripción.
- Consulte el sitio de Microsoft para conocer las limitaciones de los conjuntos de cifrado de disco por región.

> **Nota:**
>
> Para obtener información acerca de la configuración del cifrado del lado del servidor de Azure, consulte Inicio rápido: Creación de un almacén de claves mediante Azure Portal.

Clave de cifrado administrada por el cliente de Azure

Al crear un catálogo de máquinas, puede elegir si cifrar los datos presentes en las máquinas aprovisionadas en el catálogo. El cifrado del lado del servidor con una clave de cifrado administrada por el cliente permite administrar el cifrado a nivel de disco administrado y proteger los datos que contengan las máquinas del catálogo. Un conjunto de cifrado de disco (Disk Encryption Set o DES) representa una clave administrada por el cliente. Para utilizar esta función, primero debe crear el DES en Azure. Un DES tiene este formato:

- <!JEKYLL@5300@27>

Seleccione un DES de la lista. El DES que seleccione debe estar en la misma suscripción y región que los recursos.

Consulte Crear un catálogo de máquinas con una clave administrada por el cliente.

Cifrado de discos de Azure en el host

Puede crear un catálogo de máquinas de MCS con capacidad de cifrado en el host. Actualmente, MCS solo admite el flujo de trabajo de perfiles de máquina para esta función. Puede utilizar una máquina virtual o una especificación de plantilla como entrada para un perfil de máquina.

Este método de cifrado no cifra los datos a través del almacenamiento de Azure. El servidor que aloja la máquina virtual cifra los datos y, a continuación, los datos cifrados fluyen a través del servidor de almacenamiento de Azure. Por lo tanto, este método de cifrado cifra los datos de extremo a extremo.

Restricciones:

El cifrado de discos de Azure en el host:

- No se admite con todos los tamaños de máquina de Azure
- Es incompatible con el cifrado de discos de Azure

Para crear un catálogo de máquinas con capacidad de cifrado en el host:

1. Compruebe si la suscripción tiene habilitada la funcionalidad de cifrado en el host o no. Para ello, consulte https://learn.microsoft.com/en-us/rest/api/resources/features/get?tabs=HTTP/. Si no está habilitada, debe habilitar la funcionalidad para la suscripción. Para obtener información sobre cómo habilitar la funcionalidad para su suscripción, consulte https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/.
2. Compruebe si un tamaño de máquina virtual de Azure determinado admite el cifrado en el host o no. Para ello, en una ventana de PowerShell, ejecute uno de los siguientes comandos:

   <!JEKYLL@5300@28>

   <!JEKYLL@5300@29>

3. Cree una máquina virtual o una especificación de plantilla, como entrada para el perfil de máquina, en Azure Portal con el cifrado en el host habilitado.

   - Si quiere crear una máquina virtual, seleccione un tamaño de máquina virtual que admita el cifrado en el host. Tras crear la máquina virtual, se habilita la propiedad **Encryption at host** (Cifrado en el host).
   - Si quiere utilizar una especificación de plantilla, asigne al parámetro <!JEKYLL@5300@30> el valor **true** en <!JEKYLL@5300@31>.

4. Cree un catálogo de máquinas de MCS con un flujo de trabajo de perfil de máquina. Para ello, seleccione una máquina virtual o una especificación de plantilla.

   - Disco del sistema operativo/disco de datos: Se cifra mediante una clave gestionada por el cliente y una clave gestionada por la plataforma

- Disco de SO efímero: Se cifra solo mediante una clave administrada por la plataforma
- Disco de caché: Se cifra mediante una clave administrada por el cliente y una clave administrada por la plataforma

Puede crear el catálogo de máquinas a través de Web Studio o con los comandos de PowerShell.

Obtener la información de cifrado en el host desde un perfil de máquina

Puede recuperar la información de cifrado en el host desde un perfil de máquina al ejecutar el comando de PowerShell con el parámetro <!JEKYLL@5300@32>. Si el parámetro <!JEKYLL@5300@33> es **True**, indica que el cifrado en el host está habilitado para el perfil de máquina.

Por ejemplo: Cuando la entrada del perfil de máquina sea una VM, ejecute el siguiente comando:

<!JEKYLL@5300@34>

Por ejemplo: Cuando la entrada del perfil de máquina sea una especificación de plantilla, ejecute el siguiente comando:

<!JEKYLL@5300@35>

Cifrado doble en disco administrado

Puede crear un catálogo de máquinas con doble cifrado. Todos los catálogos creados con esta función tienen todos los discos cifrados del lado del servidor con claves administradas por la plataforma y por el cliente. Usted posee y mantiene el Azure Key Vault, la clave de cifrado y los conjuntos de cifrado de disco (DES).

El cifrado doble es el cifrado del lado de la plataforma (predeterminado) y el cifrado administrado por el cliente (CMEK). Por lo tanto, si usted es un cliente altamente confidencial al que le preocupa el riesgo asociado a cualquier algoritmo de cifrado, implementación o claves comprometidas, puede optar por este doble cifrado. Los discos de datos y del SO persistentes, las instantáneas y las imágenes se cifran en REST con doble cifrado.

> **Nota:**
>
> - Puede crear y actualizar un catálogo de máquinas con doble cifrado mediante Web Studio y los comandos de PowerShell. Consulte Crear un catálogo de máquinas con doble cifrado para los comandos de PowerShell.
> - Puede utilizar un flujo de trabajo no basado en perfiles de máquina o un flujo de trabajo basado en perfiles de máquina para crear o actualizar un catálogo de máquinas con doble cifrado.
> - Si utiliza un flujo de trabajo no basado en perfiles de máquina para crear un catálogo de máquinas, puede reutilizar el <!JEKYLL@5300@36> almacenado.

> - Si usa un perfil de máquina, puede usar una máquina virtual o una especificación de plantilla como entrada de perfil de máquina.

Limitaciones:

- No se admite el cifrado doble en los discos Ultra Disk ni en los discos Premium SSD v2.
- El cifrado doble no se admite en discos no administrados.
- Si inhabilita una clave DiskEncryptionSet asociada a un catálogo, se inhabilitan las máquinas virtuales del catálogo.
- Todos los recursos relacionados con las claves administradas por el cliente (instancias de Azure Key Vault, conjuntos de cifrado de disco, máquinas virtuales, discos e instantáneas) deben estar en la misma suscripción y región.
- Solo puede crear un máximo de 50 conjuntos de cifrado de disco por región y suscripción.

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 los grupos de recursos de Azure vacíos existentes cuando cree un catálogo de máquinas con MCS. También puede decidir que se creen nuevos grupos de recursos para usted. Para obtener información acerca de los grupos de recursos de Azure, consulte la documentación de Microsoft.

Uso del grupo de recursos de Azure

No hay límite en el número de máquinas virtuales, discos administrados, instantáneas e imágenes por grupo de recursos de Azure (se eliminó la limitación de 240 VM/800 discos administrados por grupo de recursos de Azure).

- Al utilizar la entidad de servicio de ámbito completo para crear un catálogo de máquinas, MCS crea solo un grupo de recursos de Azure y utiliza ese grupo para el catálogo.
- Al utilizar la entidad de servicio de ámbito restringido para crear un catálogo de máquinas, debe proporcionar un grupo de recursos de Azure vacío y creado previamente para el catálogo.

Discos efímeros de Azure

Un disco efímero de Azure le permite reutilizar el disco de caché o el disco temporal para almacenar el disco del sistema operativo de una máquina virtual habilitada para Azure. Esta funcionalidad es útil en entornos de Azure que requieren un disco SSD de mayor rendimiento, en lugar de un disco HDD estándar. Para obtener información sobre cómo crear un catálogo con un disco efímero de Azure, consulte Crear un catálogo con un disco efímero de Azure.

> **Nota:**
>
> Los catálogos persistentes no admiten discos de SO efímeros.

Los discos de SO efímeros requieren que el esquema de aprovisionamiento use discos administrados y una Shared Image Gallery.

Almacenamiento de un disco de SO efímero temporal

Tiene la posibilidad de almacenar un disco de SO efímero en el disco temporal de la VM o en un disco de recursos. Esta funcionalidad le permite usar un disco de SO efímero con una máquina virtual que no tenga caché o que no tenga suficiente caché. Estas VM tienen un disco temporal o de recursos para almacenar un disco de SO efímero, como <!JEKYLL@5300@37>.

Se deben tener en cuenta las siguientes cuestiones:

- Un disco efímero se almacena en el disco de caché o en el disco temporal (de recursos) de la VM. Se prefiere el disco de caché antes que el disco temporal, a menos que el disco de caché no sea lo suficientemente grande como para albergar el contenido del disco del sistema operativo.
- En el caso de las actualizaciones, si una nueva imagen es más grande que el disco de caché, pero más pequeña que el disco temporal, el disco de SO efímero se sustituye por el disco temporal de la VM.

Optimización del almacenamiento (E/S de MCS) con discos efímeros de Azure y Machine Creation Services (MCS)

El disco de SO efímero de Azure y la E/S de MCS no se pueden habilitar al mismo tiempo.

Las consideraciones importantes son las siguientes:

- No puede crear un catálogo de máquinas con el disco de SO efímero y la E/S de MCS habilitados al mismo tiempo.
- Los parámetros de PowerShell (<!JEKYLL@5300@38> y <!JEKYLL@5300@39>) fallan con el mensaje de error correspondiente si se establecen en **true** en <!JEKYLL@5300@40> o <!JEKYLL@5300@41>.
- Para catálogos de máquinas existentes creados con ambas funciones habilitadas, aún puede:
  - actualizar un catálogo de máquinas;
  - agregar o eliminar máquinas virtuales;
  - eliminar un catálogo de máquinas.

Azure Compute Gallery

Utilice Azure Compute Gallery (antes denominado Azure Shared Image Gallery) como repositorio de imágenes publicadas para máquinas aprovisionadas por MCS en Azure. Puede almacenar una imagen publicada en la galería para acelerar la creación e hidratación de discos de SO, mejorando los tiempos de inicio y lanzamiento de aplicaciones en máquinas virtuales no persistentes. Shared Image Gallery contiene los tres elementos siguientes:

- *Galería*: El lugar donde se almacenan las imágenes. MCS crea una galería para cada catálogo de máquinas.
- *Definición de imagen de la galería*: Esta definición incluye información (el tipo y el estado del sistema operativo, la región de Azure) sobre la imagen publicada. MCS crea una definición de imagen para cada imagen creada para el catálogo.
- *Versión de la imagen de la galería*: Cada imagen de Shared Image Gallery puede tener varias versiones, y cada versión puede tener varias réplicas en diferentes regiones. Cada réplica es una copia completa de la imagen publicada.

> **Nota:**
>
> La funcionalidad Shared Image Gallery solo es compatible con discos administrados. No está disponible para catálogos de máquinas antiguos.

Para obtener más información, consulte Almacenamiento y uso compartido de imágenes en Azure Compute Gallery.

Para obtener información sobre cómo crear o actualizar un catálogo de máquinas con una imagen de Azure Compute Gallery con PowerShell, consulte Crear o actualizar un catálogo de máquinas con una imagen de Azure Compute Gallery.

Máquinas virtuales confidenciales de Azure

Las máquinas virtuales de computación confidencial de Azure garantizan que su escritorio virtual esté cifrado en memoria y protegido mientras se usa.

Puede usar MCS para crear un catálogo con máquinas virtuales confidenciales de Azure. Para crear dicho catálogo, debe usar el flujo de trabajo del perfil de máquina. Puede usar una máquina virtual o una especificación de plantilla de Azure Resource Manager como entrada para un perfil de máquina.

Consideraciones importantes acerca de las máquinas virtuales confidenciales

Las consideraciones importantes relativas a los tamaños de máquina virtual compatibles y la creación de catálogos de máquinas con VM confidenciales son las siguientes:

- Tamaños de VM compatibles: Las máquinas virtuales confidenciales admiten los siguientes tamaños:
  - Serie DCasv5
  - Serie DCadsv5
  - Serie ECasv5
  - Serie ECadsv5
- Crear catálogos de máquinas con VM confidenciales.
  - Puede crear un catálogo de máquinas con VM confidenciales de Azure mediante Web Studio y los comandos de PowerShell.
  - Para crear un catálogo de máquinas con VM confidenciales de Azure, debe usar un flujo de trabajo basado en perfiles de máquina. Puede usar una máquina virtual o una especificación de plantilla como entrada del perfil de máquina.
  - La imagen maestra y la entrada del perfil de máquina deben estar habilitadas con el mismo tipo de seguridad confidencial. Los tipos de seguridad son:
    - **VMGuestStateOnly**: VM confidencial con solo el estado de invitado de VM cifrado
    - **DiskWithVMGuestState**: VM confidencial con disco de SO y estado de invitado de máquina virtual cifrados con una clave administrada por la plataforma o una clave administrada por el cliente. Se pueden cifrar tanto los discos de SO normales como los efímeros.
  - Con el parámetro AdditionalData, puede obtener información de VM confidencial de varios tipos de recursos, como discos administrados, instantáneas, imágenes de Azure Compute Gallery, máquinas virtuales y especificaciones de plantilla de Azure Resource Manager. Por ejemplo:

    <!JEKYLL@5300@42>

    Los campos de datos adicionales son:

    - DiskSecurityType
    - ConfidentialVMDiskEncryptionSetId
    - DiskSecurityProfiles

    Para obtener la propiedad de computación confidencial de un tamaño de una máquina, ejecute el siguiente comando: <!JEKYLL@5300@43>

    El campo de datos adicional es <!JEKYLL@5300@44>.
  - No puede cambiar la imagen maestra ni el perfil de máquina de un tipo de seguridad confidencial a un tipo de seguridad no confidencial ni de un tipo de seguridad no confidencial a uno confidencial.
  - Aparecerán los mensajes de error correspondientes a cualquier configuración incorrecta.

Preparar imágenes maestras y perfiles de máquina

Antes de crear un conjunto de máquinas virtuales confidenciales, siga estos pasos para preparar una imagen maestra y un perfil de máquina para ellas:

1. En el portal de Azure, cree una máquina virtual confidencial con parámetros específicos, como:
   - **Tipo de seguridad**: Máquinas virtuales confidenciales
   - **Cifrado de disco de SO confidencial**: Habilitado.
   - **Administración de claves**: Cifrado de disco confidencial con una clave administrada por la plataforma
     Para obtener más información sobre la creación de máquinas virtuales confidenciales, consulte este artículo de Microsoft.
2. Prepare la imagen maestra en la máquina virtual creada. Instale las aplicaciones y VDA necesarios en la máquina virtual creada.

   > **Nota:**
   >
   > No se admite la creación de máquinas virtuales confidenciales mediante VHD. En su lugar, use Azure Compute Gallery, discos administrados o instantáneas para este fin.

3. Cree el perfil de la máquina de una de estas maneras:
   - Use la máquina virtual existente creada en el paso 1 si tiene las propiedades de máquina necesarias.
   - Si opta por una especificación de plantilla de ARM como perfil de máquina, cree la especificación de plantilla según sea necesario. En concreto, configure parámetros que cumplan con los requisitos de VM confidencial, como *SecurityEncryptionType* y *diskEncryptionSet* (para la clave administrada por el cliente). Para obtener más información, consulte Crear una especificación de plantilla de Azure.

     > **Nota:**
     >
     > - Asegúrese de que la imagen maestra y el perfil de la máquina tengan el mismo tipo de clave de seguridad.
     > - Para crear máquinas virtuales confidenciales que requieran cifrado de disco de SO confidencial con una clave administrada por el cliente, asegúrese de que los ID del conjunto de cifrado de disco tanto en la imagen maestra como en el perfil de la máquina sean idénticos.

Crear máquinas virtuales confidenciales mediante Web Studio o los comandos de PowerShell

Para crear un conjunto de máquinas virtuales confidenciales, cree un catálogo de máquinas con una imagen maestra y un perfil de máquina derivados de la máquina virtual confidencial deseada.

Para crear el catálogo con Web Studio, siga los pasos descritos en Crear catálogos de máquinas. Tenga en cuenta las siguientes consideraciones:

- En la página **Imagen**, seleccione una imagen maestra y un perfil de máquina que haya preparado para la creación de la máquina virtual confidencial. La selección del perfil de la máquina es obligatoria y solo están disponibles para selección los perfiles cuyo tipo de cifrado de seguridad coincida con el de la imagen maestra seleccionada.
- En la página **Máquinas virtuales**, solo aparecen para selección los tamaños de máquina compatibles con máquinas virtuales confidenciales.
- En la página **Parámetros del disco**, no puede especificar el conjunto de cifrado del disco porque se hereda del perfil de máquina seleccionado.

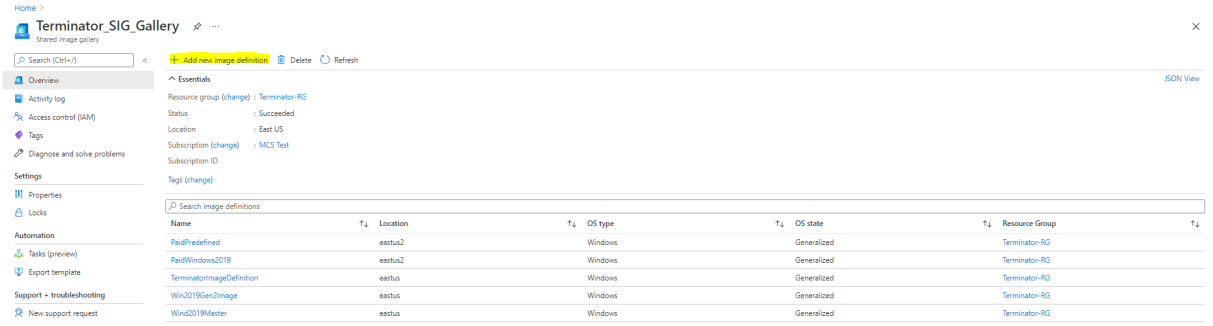
Azure Marketplace

Citrix Virtual Apps and Desktops admite el uso de una imagen maestra en Azure que contenga información del plan para crear un catálogo de máquinas. Para obtener más información, consulte Microsoft Azure Marketplace.

> **Sugerencia:**
>
> Algunas imágenes que se encuentran en Azure Marketplace, como la imagen estándar de Windows Server, no llevan anexa información del plan. La funcionalidad Citrix Virtual Apps and Desktops es para imágenes de pago.

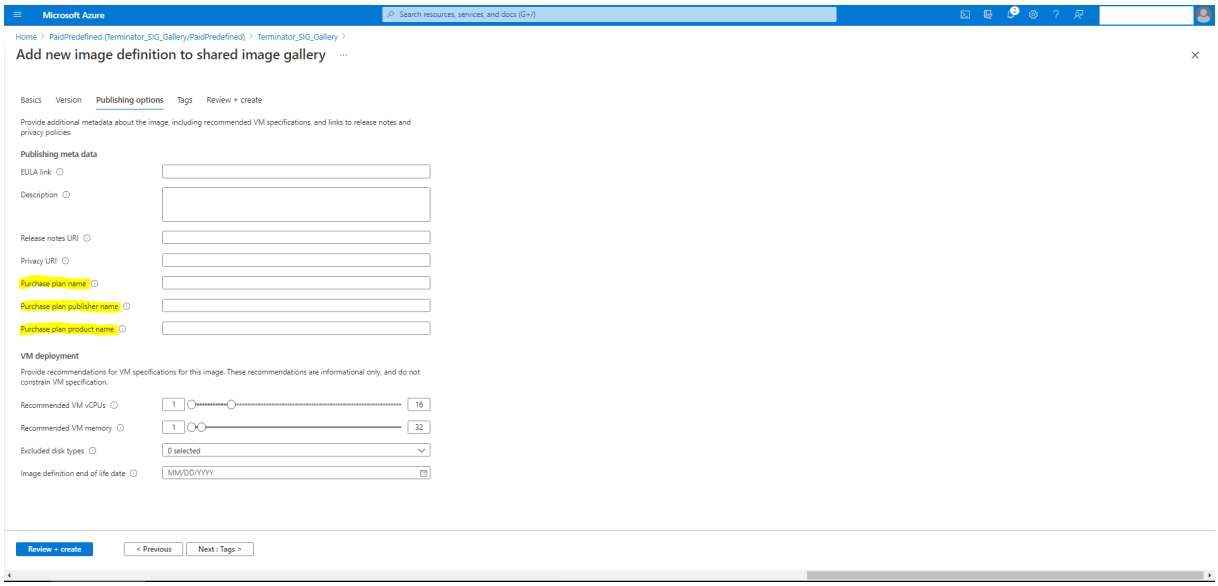
Compruebe que la imagen creada en Shared Image Gallery contiene información del plan de Azure

Use el procedimiento descrito en esta sección para ver las imágenes de Shared Image Gallery en Web Studio. Estas imágenes se pueden usar, opcionalmente, para una imagen maestra. Para colocar la imagen en Shared Image Gallery, cree una definición de imagen en una galería.

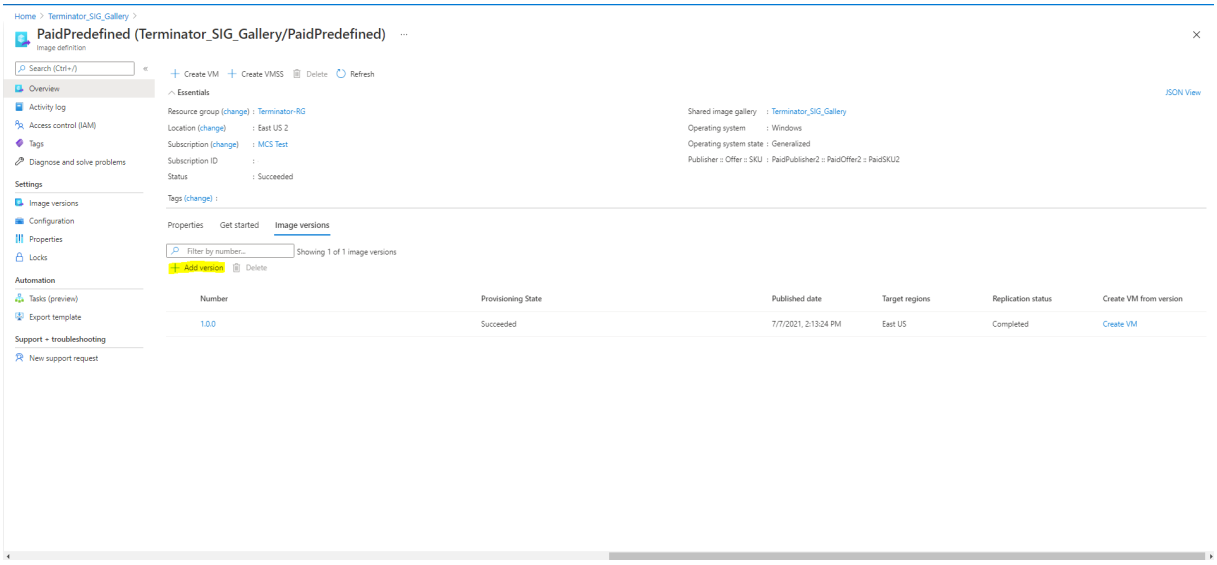


En la página **Publishing options**, verifique la información del plan de compra.

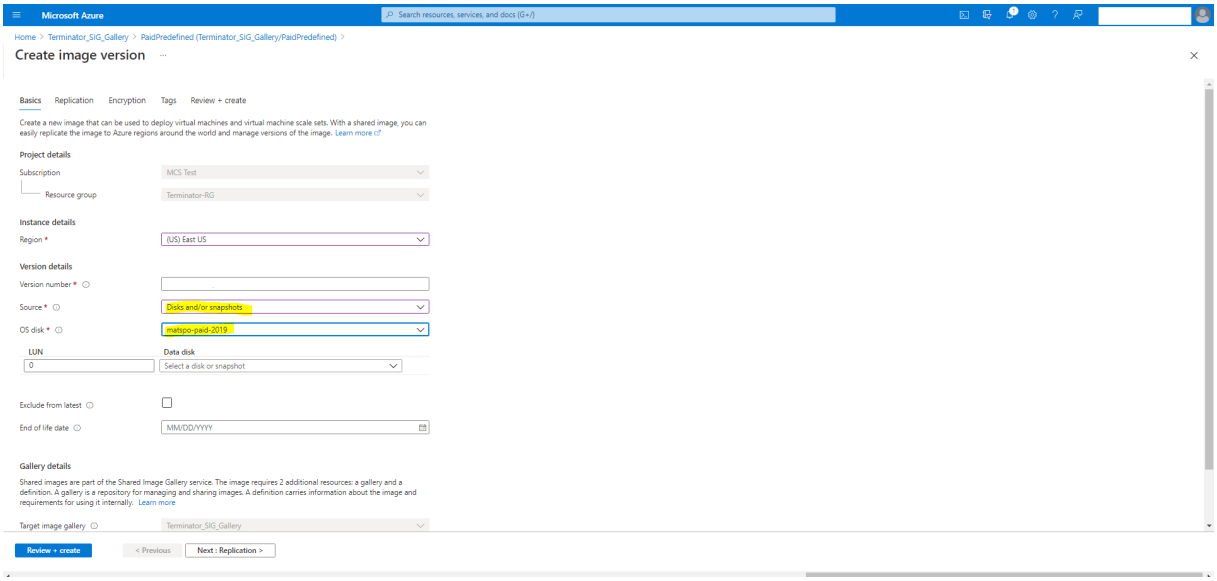
Los campos de información del plan de compra están vacíos inicialmente. Rellene esos campos con la información del plan de compra utilizada para la imagen. Si no se rellena la información del plan de compra, puede ocurrir un error en el procesamiento del catálogo de máquinas.



Después de verificar la información del plan de compra, cree una versión de la imagen dentro de la definición. Sirve de imagen maestra. Haga clic en **Add version**:



En la sección **Version details**, seleccione la instantánea de la imagen o el disco administrado como origen:



Virtualización anidada

Si configura la VM maestra con virtualización anidada habilitada, todas las VM del catálogo de máquinas de MCS creadas con esa VM maestra tienen habilitada la virtualización anidada. Esta función se aplica a máquinas virtuales persistentes y no persistentes. Puede actualizar un catálogo de máquinas de MCS existente y las máquinas virtuales existentes para que tengan una virtualización anidada mediante la actualización de imágenes.

Actualmente, solo los tamaños de VM Dv3 y Ev3 admiten la virtualización anidada.

Para obtener información sobre la virtualización anidada, consulte el blog de Microsoft Nested Virtualization in Azure.

Crear un catálogo de máquinas con PowerShell

En esta sección se detalla cómo puede crear catálogos con PowerShell:

- Crear un catálogo con un disco no persistente de caché de reescritura
- Crear un catálogo con un disco persistente de caché de reescritura
- Mejorar el rendimiento del arranque con E/S de MCS
- Usar la especificación de la plantilla para crear o actualizar un catálogo con PowerShell
- Catálogos de máquinas con inicio seguro
- Usar valores de propiedades de perfil de máquina
- Crear un catálogo de máquinas con una clave de cifrado administrada por el cliente
- Crear un catálogo de máquinas con doble cifrado
- Crear un catálogo con discos efímeros de Azure
- Hosts dedicados de Azure
- Crear o actualizar un catálogo de máquinas con una imagen de Azure Compute Gallery
- Configurar Shared Image Gallery
- Aprovisionar máquinas en zonas de disponibilidad especificadas
- Tipos de almacenamiento
- Actualizar la configuración del archivo de paginación
- Crear un catálogo con máquinas virtuales de Azure Spot
- Configurar los tamaños de las máquinas virtuales de seguridad
- Copiar etiquetas en todos los recursos
- Aprovisionar máquinas virtuales del catálogo con el agente de Azure Monitor instalado

Crear un catálogo con un disco no persistente de caché de reescritura

Para configurar un catálogo con disco no persistente de caché de reescritura, utilice el parámetro de PowerShell <!JEKYLL@5300@45>. La propiedad personalizada <!JEKYLL@5300@46> indica si acepta usar el almacenamiento temporal de Azure para almacenar el archivo de caché de reescritura. Esto debe establecerse en “true”cuando se ejecuta <!JEKYLL@5300@47> si quiere usar el disco temporal como disco de caché de reescritura. Si no se especifica esta propiedad, el parámetro se establece en **false** de forma predeterminada.

Por ejemplo, así se usa el parámetro <!JEKYLL@5300@48> para configurar <!JEKYLL@5300@49> en **true**:

<!JEKYLL@5300@50>

> **Nota:**
>
> Después de confirmar que el catálogo de máquinas use el almacenamiento temporal local de Azure para el archivo de caché de reescritura, no se puede cambiar para que use VHD más adelante.

Crear un catálogo con un disco persistente de caché de reescritura

Para configurar un catálogo con disco persistente de caché de reescritura, use el parámetro <!JEKYLL@5300@51> de PowerShell. Este parámetro ofrece una propiedad adicional, <!JEKYLL@5300@52>, que se utiliza para determinar cómo el disco de caché de reescritura persiste en máquinas aprovisionadas con MCS. La propiedad <!JEKYLL@5300@53> solo se utiliza cuando se especifica el parámetro <!JEKYLL@5300@54> y cuando se establece el parámetro <!JEKYLL@5300@55> para indicar que se ha creado un disco.

He aquí unos cuantos ejemplos de propiedades que se encuentran en el parámetro <!JEKYLL@5300@56> antes de optar por la propiedad <!JEKYLL@5300@57>:

<!JEKYLL@5300@58>

Al utilizar estas propiedades, tenga en cuenta que contienen valores predeterminados si las propiedades se omiten del parámetro <!JEKYLL@5300@59>. La propiedad <!JEKYLL@5300@60> tiene dos valores posibles: **true** o **false**.

Cuando la propiedad <!JEKYLL@5300@61> es **true**, el disco de caché de reescritura no se elimina cuando el administrador de Citrix Virtual Apps and Desktops apaga la máquina mediante Web Studio.

Cuando la propiedad <!JEKYLL@5300@62> es **false**, el disco de caché de reescritura se elimina cuando el administrador de Citrix Virtual Apps and Desktops apaga la máquina mediante Web Studio.

> **Nota:**
>
> Si se omite la propiedad <!JEKYLL@5300@63>, su valor predeterminado es **false**, y la memoria caché de reescritura se elimina cuando la máquina se apaga mediante Web Studio.

Por ejemplo, así se usa el parámetro <!JEKYLL@5300@64> para configurar <!JEKYLL@5300@65> en "true":

<!JEKYLL@5300@66>

> **Importante:**
>
> La propiedad <!JEKYLL@5300@67> solo se puede configurar mediante el cmdlet de PowerShell <!JEKYLL@5300@68>. Si se intenta modificar <!JEKYLL@5300@69> de un esquema de aprovi-

> sionamiento después de la creación, esto no afecta al catálogo de máquinas ni a la persistencia del disco de caché de reescritura cuando se apaga una máquina.

Por ejemplo, configure <!JEKYLL@5300@70> para utilizar la memoria caché de reescritura mientras configura la propiedad <!JEKYLL@5300@71> en "true":

<!JEKYLL@5300@72>

Mejorar el rendimiento del arranque con E/S de MCS

Puede mejorar el rendimiento de arranque de los discos administrados de Azure y GCP cuando E/S de MCS está habilitada. Utilice la propiedad personalizada <!JEKYLL@5300@73> de PowerShell en el comando <!JEKYLL@5300@74> para configurar esta función. Las opciones asociadas a <!JEKYLL@5300@75> son:

<!JEKYLL@5300@76><!JEKYLL@5300@77><!JEKYLL@5300@78>

Para habilitar esta función, establezca la propiedad personalizada <!JEKYLL@5300@79> en <!JEKYLL@5300@80>. Por ejemplo:

<!JEKYLL@5300@81>

Usar la especificación de la plantilla para crear o actualizar un catálogo con PowerShell

Puede crear o actualizar un catálogo de máquinas de MCS mediante una especificación de plantilla como entrada de datos de un perfil de máquina. Para ello, puede utilizar Web Studio o los comandos de PowerShell.

Para Web Studio, consulte Crear un catálogo de máquinas con una imagen de Azure Resource Manager en Web Studio

Mediante los comandos de PowerShell:

1. Abra la ventana de **PowerShell**.
2. Ejecute <!JEKYLL@5300@82>.
3. Cree o actualice un catálogo.
    - Para crear un catálogo:
        a) Utilice el comando <!JEKYLL@5300@83> con una especificación de plantilla como entrada de datos de un perfil de máquina. Por ejemplo:

        <!JEKYLL@5300@84>

        b) Termine de crear el catálogo.

- Para actualizar un catálogo, utilice el comando <!JEKYLL@5300@85> con una especificación de plantilla como entrada de datos de un perfil de máquina. Por ejemplo:

  <!JEKYLL@5300@86>

Catálogos de máquinas con inicio seguro

Para crear correctamente un catálogo de máquinas con inicio seguro, utilice:

- Un perfil de máquina con inicio seguro
- Un tamaño de máquina virtual compatible con el inicio seguro
- Una versión de máquina virtual Windows que admita inicio seguro. En la actualidad, Windows 10, Windows 11 y Windows Server 2016, 2019 y 2022 admiten el inicio seguro.

> **Importante:**
>
> MCS admite la creación de un catálogo con máquinas virtuales habilitadas para inicio seguro. Sin embargo, para actualizar un catálogo persistente y las máquinas virtuales ya existentes, debe usar el portal de Azure. No puede actualizar el inicio seguro de un catálogo no persistente. Para obtener más información, consulte el documento de Microsoft Enable Trusted launch on existing Azure VMs.

Para ver los elementos de inventario que ofrecen Citrix Virtual Apps and Desktops y determinar si el tamaño de máquina virtual admite el inicio seguro, ejecute el siguiente comando:

1. Abra una ventana de PowerShell.
2. Ejecute **asnp citrix*** para cargar los módulos de PowerShell específicos de Citrix.
3. Ejecute este comando:

   <!JEKYLL@5300@87>
4. Ejecute <!JEKYLL@5300@88>
5. Compruebe el valor del atributo <!JEKYLL@5300@89>.

   - Si <!JEKYLL@5300@90> es **True**, el tamaño de máquina virtual admite el inicio seguro.
   - Si <!JEKYLL@5300@91> es **False**, el tamaño de máquina virtual no admite el inicio seguro.

Según la instancia de PowerShell de Azure, puede usar este comando para determinar los tamaños de máquina virtual que admiten el inicio seguro:

<!JEKYLL@5300@92>

A continuación, se muestran ejemplos que describen si el tamaño de máquina virtual admite el inicio seguro después de ejecutar el comando de Azure PowerShell.

- *Ejemplo 1*: Si la máquina virtual de Azure solo admite la generación 1, esa máquina virtual no admite el inicio seguro. Por lo tanto, la funcionalidad <!JEKYLL@5300@93> no se muestra después de ejecutar el comando de Azure PowerShell.
- *Ejemplo 2*: Si la máquina virtual de Azure solo admite la generación 2 y la funcionalidad <!JEKYLL@5300@94> es **True**, el tamaño de máquina virtual de la generación 2 no se admite para el inicio seguro.
- *Ejemplo 3*: Si la máquina virtual de Azure solo admite la generación 2 y la funcionalidad <!JEKYLL@5300@95> no se muestra después de ejecutar el comando de PowerShell, se admite el tamaño de máquina virtual de generación 2 para el inicio seguro.

Para obtener más información sobre el inicio seguro para máquinas virtuales de Azure, consulte el documento Trusted Launch for Azure Virtual Machines de Microsoft.

Crear un catálogo de máquinas con inicio seguro

1. Cree una imagen maestra habilitada para inicio seguro. Consulte la documentación Trusted Launch VM Images de Microsoft.
2. Cree una especificación de plantilla o máquina virtual con el tipo de seguridad **máquinas virtuales con inicio seguro**. Para obtener más información sobre cómo crear una especificación de plantilla o VM, consulte el documento Deploy a Trusted Launch VM de Microsoft.
3. Cree un catálogo de máquinas con Web Studio o los comandos de PowerShell.

    - Si quiere usar Web Studio, consulte Crear un catálogo de máquinas con una imagen de Azure Resource Manager en Web Studio.
    - Si quiere usar los comandos de PowerShell, utilice el comando <!JEKYLL@5300@96> con la especificación de plantilla o VM como entrada de perfil de máquina. Para ver la lista completa de comandos para crear un catálogo, consulte Creación de un catálogo.

      Ejemplo de <!JEKYLL@5300@97> con VM como entrada del perfil de máquina:

      <!JEKYLL@5300@98>

      Ejemplo de <!JEKYLL@5300@99> con especificación de plantilla como entrada del perfil de máquina:

      <!JEKYLL@5300@100>

Errores al crear catálogos de máquinas con inicio seguro

Al crear un catálogo de máquinas con inicio seguro en los siguientes casos, se obtienen los errores correspondientes:

Caso	Error
Si selecciona un perfil de máquina al crear un catálogo no administrado	<!JEKYLL@5300@101>
Si selecciona un perfil de máquina que admite el inicio seguro al crear un catálogo con un disco no administrado como imagen maestra	<!JEKYLL@5300@102>
Si no selecciona un perfil de máquina al crear un catálogo administrado con una imagen maestra de origen que tenga inicio seguro como tipo de seguridad	<!JEKYLL@5300@103>
Si selecciona un perfil de máquina con un tipo de seguridad diferente del tipo de seguridad de la imagen maestra	<!JEKYLL@5300@104>
Si selecciona un tamaño de máquina virtual que no admite el inicio seguro, pero usa una imagen maestra que sí admite el inicio seguro al crear un catálogo	<!JEKYLL@5300@105>

Usar valores de propiedades de perfil de máquina

El catálogo de máquinas utiliza las siguientes propiedades que se definen en las propiedades personalizadas:

- Zona de disponibilidad
- ID de grupo de hosts dedicado
- ID del conjunto de cifrado de disco
- Tipo de SO
- Tipo de licencia
- Tipo de almacenamiento

Si estas propiedades personalizadas no se definen explícitamente, los valores de propiedad se establecen a partir de la especificación de plantilla de ARM o de la VM, lo que se utilice como perfil de máquina. Además, si no se especifica <!JEKYLL@5300@106>, se establecerá a partir del perfil de máquina.

> **Nota:**
>
> Si faltan algunas propiedades en el perfil de la máquina (MachineProfile) y no están definidas en las propiedades personalizadas (CustomProperties), se utilizan los valores por defecto de las

> propiedades siempre que sea aplicable.

En la siguiente sección se describen algunos casos de <!JEKYLL@5300@107> y <!JEKYLL@5300@108> en los que <!JEKYLL@5300@109> tiene definidas todas las propiedades o los valores se derivan de MachineProfile.

- Casos de New-ProvScheme
  - MachineProfile tiene todas las propiedades y CustomProperties no está definido. Ejemplo:

    <!JEKYLL@5300@110>

    Estos valores se definen como propiedades personalizadas del catálogo:

    <!JEKYLL@5300@111>
  - MachineProfile tiene algunas propiedades y CustomProperties no está definido. Ejemplo: MachineProfile solo tiene LicenseType y OsType.

    <!JEKYLL@5300@112>

    Estos valores se definen como propiedades personalizadas del catálogo:

    <!JEKYLL@5300@113>
  - Tanto MachineProfile como CustomProperties definen todas las propiedades. Ejemplo:

    <!JEKYLL@5300@114>

    Las propiedades personalizadas tienen prioridad. Estos valores se definen como propiedades personalizadas del catálogo:

    <!JEKYLL@5300@115>
  - Algunas propiedades se definen en MachineProfile y otras se definen en CustomProperties. Ejemplo:
    - CustomProperties define LicenseType y StorageAccountType
    - MachineProfile define LicenseType, OsType y Zones

    <!JEKYLL@5300@116>

    Estos valores se definen como propiedades personalizadas del catálogo:

    <!JEKYLL@5300@117>
  - Algunas propiedades se definen en MachineProfile y otras se definen en CustomProperties. Además, ServiceOffering no está definido. Ejemplo:
    - CustomProperties define StorageType
    - MachineProfile define LicenseType

<!JEKYLL@5300@118>

Estos valores se definen como propiedades personalizadas del catálogo:

<!JEKYLL@5300@119>

- Si OsType no está ni en CustomProperties ni en MachineProfile, entonces:
  - El valor se lee de la imagen maestra.
  - Si la imagen maestra es un disco no administrado, OsType se establece en Windows. Ejemplo:

<!JEKYLL@5300@120>

El valor de la imagen maestra se escribe en las propiedades personalizadas, en este caso Linux.

<!JEKYLL@5300@121>

- Casos de Set-ProvScheme
  - Un catálogo con:
    - CustomProperties para <!JEKYLL@5300@122> y OsType
    - MachineProfile <!JEKYLL@5300@123> que define zonas
  - Actualizaciones:
    - MachineProfile mpB.vm que define StorageAccountType
    - Un nuevo conjunto de propiedades personalizadas $CustomPropertiesB que define LicenseType y OsType

<!JEKYLL@5300@124>

Estos valores se definen como propiedades personalizadas del catálogo:

<!JEKYLL@5300@125>

  - Un catálogo con:
    - Propiedades personalizadas para S<!JEKYLL@5300@126> y OsType.
    - MachineProfile <!JEKYLL@5300@127> que define StorageAccountType y LicenseType
  - Actualizaciones:
    - Un nuevo conjunto de propiedades personalizadas $CustomPropertiesB que define StorageAccountType y OsType.

<!JEKYLL@5300@128>

Estos valores se definen como propiedades personalizadas del catálogo:

<!JEKYLL@5300@129>

- Un catálogo con:
  - CustomProperties para <!JEKYLL@5300@130> y OsType
  - MachineProfile <!JEKYLL@5300@131> que define zonas
- Actualizaciones:
  - MachineProfile mpB.vm que define StorageAccountType y LicenseType
  - <!JEKYLL@5300@132> está sin especificar

<!JEKYLL@5300@133>

Estos valores se definen como propiedades personalizadas del catálogo:

<!JEKYLL@5300@134>

Aprovisionar máquinas virtuales del catálogo con el agente de Azure Monitor instalado

La supervisión de Azure es un servicio que puede utilizar para recopilar, analizar y responder a datos de telemetría de sus entornos locales y de Azure.

El agente de Azure Monitor (AMA) recopila datos de supervisión de recursos de procesamiento, como máquinas virtuales, y los entrega a Azure Monitor. Actualmente, permite la recopilación de registros de eventos y métricas de Syslog y rendimiento, y los envía a los orígenes de datos de las Métricas de Azure Monitor y los Registros de Azure Monitor.

Para habilitar la supervisión mediante la identificación exclusiva de las máquinas virtuales en los datos de supervisión, puede aprovisionar las máquinas virtuales de un catálogo de máquinas de MCS con AMA instalado como extensión.

Requisitos

- Permisos: Asegúrese de tener los permisos mínimos de Azure especificados en Permisos de Azure requeridos y estos permisos para usar Azure Monitor:
  - <!JEKYLL@5300@135>
  - <!JEKYLL@5300@136>
  - <!JEKYLL@5300@137>
  - <!JEKYLL@5300@138>
  - <!JEKYLL@5300@139>
- Regla de recopilación de datos: Configure una regla de recopilación de datos (DCR) en Azure Portal. Para obtener información sobre cómo configurar una DCR, consulte Creación de una regla de recopilación de datos. Las DCR son específicas de cada plataforma (Windows o Linux). Asegúrese de crear una DCR según la plataforma requerida.

El AMA utiliza las reglas de recopilación de datos (DCR) para administrar la asignación entre los recursos, como las máquinas virtuales, y los orígenes de datos, como las Métricas de Azure Monitor y los Registros de Azure Monitor.

- Espacio de trabajo predeterminado: Cree un espacio de trabajo en Azure Portal. Para obtener información sobre cómo crear un espacio de trabajo, consulte Creación de un área de trabajo de Log Analytics. Al recopilar registros y datos, la información se almacena en un espacio de trabajo. Un espacio de trabajo tiene un ID de espacio de trabajo y un ID de recurso únicos. El nombre del espacio de trabajo debe ser único para un grupo de recursos determinado. Después de crear un espacio de trabajo, configure los orígenes de datos y las soluciones para almacenar sus datos en el espacio de trabajo.
- Extensión de supervisión en la lista de permitidos: Las extensiones <!JEKYLL@5300@140> y <!JEKYLL@5300@141> son extensiones de la lista de permitidos definida por Citrix. Para ver la lista de extensiones incluidas en la lista de permitidos, utilice el comando PoSH <!JEKYLL@5300@142>.
- Imagen maestra: Microsoft recomienda quitar extensiones de una máquina existente antes de crear otra máquina a partir de ella. Si no se quitan las extensiones, es posible que queden archivos sobrantes y que se produzca un comportamiento inesperado. Para obtener más información, consulte Si la máquina virtual se vuelve a crear a partir de una máquina virtual existente.

Para aprovisionar máquinas virtuales de catálogo con el AMA activado:

1. Configure una plantilla de perfil de máquina.
    - Si quiere usar una máquina virtual como plantilla de perfil de máquina:
        a) Cree una máquina virtual en Azure Portal.
        b) Encienda la máquina virtual.
        c) Agregue la máquina virtual a la regla de recopilación de datos en **Recursos**. Esto invoca la instalación del agente en la máquina virtual de la plantilla.

    > **Nota:**
    >
    > Si debe crear un catálogo de Linux, configure una máquina Linux.

    - Si quiere utilizar la especificación de plantilla como plantilla de perfil de máquina:
        a) Configure una especificación de plantilla.
        b) Agregue esta asociación de extensiones y reglas de recopilación de datos a la especificación de plantilla generada:

        <!JEKYLL@5300@143>
2. Cree o actualice un catálogo de máquinas de MCS existente.

- Para crear otro catálogo de MCS:
  a) Seleccione esa especificación de máquina virtual o plantilla como perfil de máquina en Web Studio.
  b) Continúe con los pasos siguientes para crear el catálogo.
- Para actualizar un catálogo de MCS existente, utilice estos comandos de PoSH:
  - Para que las nuevas máquinas virtuales obtengan la plantilla de perfil de máquina actualizada, ejecute este comando:

    <!JEKYLL@5300@144>
  - Para actualizar máquinas virtuales existentes con la plantilla de perfil de máquina actualizada:

    <!JEKYLL@5300@145>

3. Encienda las máquinas virtuales del catálogo.
4. Vaya a Azure Portal y compruebe si la extensión de supervisión está instalada en la máquina virtual y si la máquina virtual aparece en los recursos de la DCR. Después de unos minutos, los datos de supervisión se muestran en Azure Monitor.

Solución de problemas

Para obtener información sobre la guía de solución de problemas del agente de Azure Monitor, consulte lo siguiente:

- https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/
- https://learn.microsoft.com/en-us/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/

Crear un catálogo de máquinas con una clave de cifrado administrada por el cliente

Los pasos detallados para crear un catálogo de máquinas con una clave de cifrado administrada por el cliente son:

1. Abra una ventana de PowerShell.
2. Ejecute <!JEKYLL@5300@146> para cargar los módulos de PowerShell específicos de Citrix.
3. Escriba <!JEKYLL@5300@147>.
4. Escriba <!JEKYLL@5300@148>.

5. Escriba <!JEKYLL@5300@149>.
6. Escriba <!JEKYLL@5300@150> para obtener la lista de conjuntos de cifrado de disco.
7. Copie el ID de un conjunto de cifrado de disco.
8. Cree una cadena de propiedades personalizada para incluir el ID del conjunto de cifrado de disco. Por ejemplo:

   <!JEKYLL@5300@151>
9. Cree un grupo de identidades si aún no se ha creado. Por ejemplo:

   <!JEKYLL@5300@152>
10. Ejecute el comando New-ProvScheme. Por ejemplo:

    <!JEKYLL@5300@153>
11. Termine de crear el catálogo de máquinas.

Crear un catálogo de máquinas con doble cifrado

Puede crear y actualizar un catálogo de máquinas con doble cifrado mediante Web Studio y los comandos de PowerShell.

Los pasos detallados para crear un catálogo de máquinas con doble cifrado son:

1. Cree un Azure Key Vault y un DES con claves administradas por la plataforma y por el cliente. Para obtener información sobre cómo crear un Azure Key Vault y un DES, consulte Uso de Azure Portal para habilitar el cifrado doble en reposo para discos administrados.
2. Para buscar DiskEncryptionSets en su conexión de alojamiento:

   a) Abra una ventana de **PowerShell**.
   b) Ejecute los siguientes comandos de PowerShell:
      i. <!JEKYLL@5300@154>
      ii. <!JEKYLL@5300@155>
      iii. <!JEKYLL@5300@156>
      iv. <!JEKYLL@5300@157> (por ejemplo, azul-este)
      v. <!JEKYLL@5300@158>
      vi. <!JEKYLL@5300@159>

   Puede usar un ID del <!JEKYLL@5300@160> para crear o actualizar un catálogo mediante propiedades personalizadas.
3. Si quiere utilizar el flujo de trabajo del perfil de máquina, cree una especificación de máquina virtual o plantilla como entrada de perfil de máquina.

- Si quiere utilizar una máquina virtual como entrada de perfil de máquina:
  a) Cree una máquina virtual en Azure Portal.
  b) Vaya a **Disks > Key Management** para cifrar la máquina virtual directamente con cualquier otro <!JEKYLL@5300@161>.
- Si quiere utilizar una especificación de plantilla como entrada de perfil de máquina:
  a) En la plantilla, en <!JEKYLL@5300@162>, agregue el parámetro <!JEKYLL@5300@163> y agregue el ID del DES de doble cifrado.

4. Cree el catálogo de máquinas

   - Si usa Web Studio, realice una de estas acciones, además de los pasos de Crear catálogos de máquinas.

     – Si no usa un flujo de trabajo basado en perfiles de máquina, en la página **Parámetros del disco**, seleccione **Utilice esta clave para cifrar datos en cada máquina**. A continuación, seleccione su DES de doble cifrado en el menú desplegable. Siga con la creación del catálogo.
     – Si usa un flujo de trabajo de perfil de máquina, en la página **Imagen**, seleccione una imagen maestra y un perfil de máquina. Asegúrese de que el perfil de la máquina tenga un ID de conjunto de cifrado de disco en sus propiedades.

     Todas las máquinas creadas en el catálogo se cifran con doble cifrado mediante la clave asociada al DES que haya seleccionado.

   - Si usa comandos de PowerShell, realice una de estas acciones:

     – Si no utiliza un flujo de trabajo basado en perfiles de máquina, agregue la propiedad personalizada <!JEKYLL@5300@164> en el comando <!JEKYLL@5300@165>. Por ejemplo:

       <!JEKYLL@5300@166>

     – Si utiliza un flujo de trabajo basado en perfiles de máquina, utilice una entrada de perfil de máquina en el comando <!JEKYLL@5300@167>. Por ejemplo:

       <!JEKYLL@5300@168>

5. Termine de crear un catálogo mediante el SDK de PowerShell remoto. Para obtener información sobre cómo crear un catálogo con el SDK de PowerShell remoto, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/. Todas las máquinas creadas en el catálogo se cifran con doble cifrado mediante la clave asociada al DES que haya seleccionado.

Convertir un catálogo sin cifrar para usar el cifrado doble

Puede actualizar el tipo de cifrado de un catálogo de máquinas (mediante propiedades personalizadas o un perfil de la máquina).

- Si no utiliza un flujo de trabajo basado en perfiles de máquina, agregue la propiedad personalizada DiskEncryptionSetId en el comando <!JEKYLL@5300@169>. Por ejemplo:

  <!JEKYLL@5300@170>

- Si utiliza un flujo de trabajo basado en perfiles de máquina, utilice una entrada de perfil de máquina en el comando <!JEKYLL@5300@171>. Por ejemplo:

  <!JEKYLL@5300@172>

Cuando se haya completado correctamente, todas las máquinas virtuales nuevas que agregue al catálogo se cifrarán con cifrado doble con la clave asociada al DES que haya seleccionado.

Verificar que el catálogo tenga un cifrado doble

- En Web Studio:

  1. Vaya a **Catálogos de máquinas**.
  2. Seleccione el catálogo que quiere verificar. Haga clic en la ficha **Propiedades de plantilla** situada cerca de la parte inferior de la pantalla.
  3. En **Detalles de Azure**, verifique el ID del conjunto de cifrado de disco en **Conjunto de cifrado de disco**. Si el ID del DES del catálogo está vacío, el catálogo no está cifrado.
  4. En Azure Portal, compruebe que el tipo de cifrado del DES asociado al ID del DES sean claves administradas por la plataforma y por el cliente.

- Mediante el comando de PowerShell:

  1. Abra la ventana de **PowerShell**.
  2. Ejecute <!JEKYLL@5300@173> para cargar los módulos de PowerShell específicos de Citrix.
  3. Use <!JEKYLL@5300@174> para obtener la información de su catálogo de máquinas. Por ejemplo:

     <!JEKYLL@5300@175>

  4. Obtenga la propiedad personalizada del ID del DES del catálogo de máquinas. Por ejemplo:

     <!JEKYLL@5300@176>

  5. En Azure Portal, compruebe que el tipo de cifrado del DES asociado al ID del DES sean claves administradas por la plataforma y por el cliente.

Crear un catálogo con discos efímeros de Azure

Para utilizar discos efímeros, debe establecer la propiedad personalizada <!JEKYLL@5300@177> en **true** al ejecutar <!JEKYLL@5300@178>.

> **Nota:**
>
> Si la propiedad personalizada <!JEKYLL@5300@179> se establece en **false** o no se especifica un valor, todos los VDA aprovisionados seguirán utilizando un disco de SO aprovisionado.

A continuación, se muestra un conjunto de ejemplo de propiedades personalizadas para uso en el esquema de aprovisionamiento:

<!JEKYLL@5300@180>

Configurar un disco efímero para un catálogo

Para configurar un disco de SO efímero de Azure para un catálogo, utilice el parámetro <!JEKYLL@5300@181> de <!JEKYLL@5300@182>. Establezca el valor del parámetro <!JEKYLL@5300@183> en **true**.

> **Nota:**
>
> Para utilizar esta función, también debe habilitar los parámetros <!JEKYLL@5300@184> y <!JEKYLL@5300@185>.

Por ejemplo:

<!JEKYLL@5300@186>

Consideraciones importantes con relación a los discos efímeros

Para aprovisionar discos de SO efímeros con <!JEKYLL@5300@187>, tenga en cuenta las siguientes restricciones:

- El tamaño de VM utilizado para el catálogo debe admitir discos de SO efímeros.
- El tamaño de la memoria caché o del disco temporal asociado al tamaño de la máquina virtual debe ser mayor o igual que el tamaño del disco del sistema operativo.
- El tamaño del disco temporal debe ser mayor que el tamaño del disco de la memoria caché.

Tenga en cuenta también estos aspectos al:

- Crear el esquema de aprovisionamiento.
- Modificar el esquema de aprovisionamiento.
- Actualizar la imagen.

Hosts dedicados de Azure

Puede usar MCS para aprovisionar VM en los hosts dedicados de Azure. Antes de aprovisionar VM en hosts dedicados de Azure:

- Cree un grupo de hosts.
- Cree hosts en ese grupo de hosts.
- Compruebe que haya suficiente capacidad de host reservada para crear catálogos y máquinas virtuales.

Puede crear un catálogo de máquinas con arrendamiento de hosts definido a través del siguiente script de PowerShell:

<!JEKYLL@5300@188>

Cuando utilice MCS para aprovisionar máquinas virtuales en hosts dedicados de Azure, tenga en cuenta que:

- Un *host dedicado* es una propiedad del catálogo y no se puede cambiar una vez creado dicho catálogo. Actualmente, el arrendamiento dedicado no está disponible en Azure.
- Se requiere un grupo de hosts de Azure preconfigurado, en la región de la unidad de alojamiento, al utilizar el parámetro <!JEKYLL@5300@189>.
- Se requiere la ubicación automática de Azure. Esta funcionalidad realiza una solicitud para incorporar la suscripción asociada al grupo de hosts. Para obtener más información, consulte VM Scale Set on Azure Dedicated Hosts - Public Preview. Si la ubicación automática no está habilitada, MCS genera un error durante la creación del catálogo.

Crear o actualizar un catálogo de máquinas con una imagen de Azure Compute Gallery

Al seleccionar una imagen para utilizarla para crear un catálogo de máquinas, puede seleccionar las imágenes que haya creado en Azure Compute Gallery.

Para que aparezcan estas imágenes, haga lo siguiente:

1. Configurar un sitio de Citrix Virtual Apps and Desktops.
2. Conéctese a Azure Resource Manager.
3. En Azure Portal, cree un grupo de recursos. Para obtener información detallada, consulte Creación de una galería de Azure Compute mediante el portal.
4. En el grupo de recursos, cree una galería Azure Compute Gallery.
5. En Azure Compute Gallery, cree una definición de imagen.
6. En la definición de imagen, cree una versión de imagen.

Use los siguientes comandos de PowerShell para crear o actualizar un catálogo de máquinas con una imagen de Azure Compute Gallery:

1. Abra una ventana de PowerShell.
2. Ejecute <!JEKYLL@5300@190> para cargar los módulos de PowerShell específicos de Citrix.
3. Seleccione un grupo de recursos y, a continuación, enumere todas las galerías de ese grupo de recursos.

   <!JEKYLL@5300@191>

4. Seleccione una galería y, a continuación, enumere todas las definiciones de imágenes de esa galería.

   <!JEKYLL@5300@192>

5. Seleccione una definición de imagen y, a continuación, enumere todas las versiones de imagen de esa definición de imagen.

   <!JEKYLL@5300@193>

6. Cree y actualice un catálogo de MCS con los siguientes elementos:

   - Resource group
   - Galería
   - Definición de imagen de la galería
   - Versión de la imagen de la galería

   Para obtener información sobre cómo crear un catálogo con el SDK de PowerShell remoto, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Configurar Shared Image Gallery

Utilice el comando <!JEKYLL@5300@194> para crear un esquema de aprovisionamiento que permita usar Shared Image Gallery. Utilice el comando <!JEKYLL@5300@195> para habilitar o inhabilitar esta función en los esquemas de aprovisionamiento y para cambiar el índice de réplicas y los valores máximos de las réplicas.

Se agregaron tres propiedades personalizadas a los esquemas de aprovisionamiento para admitir la función Shared Image Gallery:

<!JEKYLL@5300@196>

- Define si se va a utilizar Shared Image Gallery para almacenar las imágenes publicadas. Si se establece en **True**, la imagen se almacena como una imagen de Shared Image Gallery; de lo contrario, la imagen se almacena como una instantánea.
- Los valores válidos son **True** y **False**.
- Si la propiedad no está definida, el valor predeterminado es **False**.

<!JEKYLL@5300@197>

- Define el índice entre máquinas y réplicas de versiones de imágenes de la galería.
- Los valores válidos son números enteros mayores que 0.
- Si la propiedad no está definida, se utilizan los valores predeterminados. El valor predeterminado para los discos de SO persistentes es 1000, y el valor predeterminado para los discos de SO no persistentes es 40.

<!JEKYLL@5300@198>

- Define el máximo de réplicas para cada versión de imagen de la galería.
- Si la propiedad no está definida, el valor predeterminado es 100.
- Si la propiedad no está definida, el valor predeterminado es 100.

> **Sugerencia:**
>
> Al utilizar Shared Image Gallery para almacenar una imagen publicada de catálogos aprovisionados con MCS, MCS establece el recuento de réplicas de versiones de imágenes de la galería en función de la cantidad de máquinas del catálogo, el índice de réplicas y el máximo de réplicas. El recuento de réplicas se calcula al dividir la cantidad de máquinas del catálogo entre el índice de réplicas (se redondea al valor entero más cercano). A continuación, se limita el valor al recuento máximo de réplicas. Por ejemplo, con un índice de réplicas de 20 y un máximo de 5, entre 0 y 20 máquinas tienen una réplica creada, entre 21 y 40 tienen 2 réplicas, entre 41 y 60 tienen 3 réplicas, entre 61 y 80 tienen 4 réplicas, y más de 81 tienen 5 réplicas.

Caso de uso: Actualizar el índice de réplicas y el máximo de réplicas de Shared Image Gallery

El catálogo de máquinas existente utiliza Shared Image Gallery. Utilice el comando <!JEKYLL@5300@199> para actualizar las propiedades personalizadas de todas las máquinas existentes del catálogo y de futuras máquinas:

<!JEKYLL@5300@200>

Caso de uso: Convertir un catálogo de instantáneas en un catálogo de Shared Image Gallery

Para este caso de uso:

1. Ejecute <!JEKYLL@5300@201> con el indicador <!JEKYLL@5300@202> establecido en **True**. Si quiere, incluya las propiedades <!JEKYLL@5300@203> y <!JEKYLL@5300@204>.
2. Actualice el catálogo.
3. Apague y encienda las máquinas para forzar una actualización.

Por ejemplo:

<!JEKYLL@5300@205>

> **Sugerencia:**
>
> Los parámetros <!JEKYLL@5300@206> y <!JEKYLL@5300@207> no son necesarios. Una vez finalizado el comando <!JEKYLL@5300@208>, aún no se ha creado la imagen de Shared Image Gallery. Una vez configurado el catálogo para utilizar la galería, la siguiente operación de actualización del catálogo almacena la imagen publicada en la galería. El comando de actualización del catálogo crea la galería, la imagen de la galería y la versión de la imagen. Apagar y encender las máquinas las actualiza, momento en el que se actualiza el recuento de réplicas, si procede. A partir de ese momento, todas las máquinas no persistentes existentes se restablecen mediante la imagen de Shared Image Gallery, y todas las máquinas recién aprovisionadas se crean mediante la imagen. La antigua instantánea se borra automáticamente en unas horas.

Caso de uso: Convertir un catálogo de Shared Image Gallery en un catálogo de instantáneas

Para este caso de uso:

1. Ejecute <!JEKYLL@5300@209> con el indicador <!JEKYLL@5300@210> establecido en **False** o sin definir.
2. Actualice el catálogo.
3. Apague y encienda las máquinas para forzar una actualización.

Por ejemplo:

<!JEKYLL@5300@211>

> **Sugerencia:**
>
> A diferencia de actualizar una instantánea a un catálogo de Shared Image Gallery, los datos personalizados de cada máquina aún no se actualizan para reflejar las nuevas propiedades personalizadas. Ejecute el siguiente comando para ver las propiedades personalizadas originales de Shared Image Gallery: <!JEKYLL@5300@212>. Una vez finalizado el comando <!JEKYLL@5300@213>, aún no se ha creado la instantánea de la imagen publicada. Una vez configurado el catálogo para que no utilice la galería, la siguiente operación de actualización del catálogo almacena la imagen publicada como una instantánea. A partir de ese momento, todas las máquinas no persistentes existentes se restablecen mediante la instantánea, y todas las máquinas recién aprovisionadas se crean a partir de la instantánea. Apagar y encender las máquinas las actualiza, momento en el que los datos personalizados de las máquinas se actualizan para reflejar que <!JEKYLL@5300@214> está establecido en **False**. Los antiguos elementos

> de Shared Image Gallery (la galería, la imagen y la versión) se borran automáticamente en unas horas.

Aprovisionar máquinas en zonas de disponibilidad especificadas

En entornos de Azure, es posible aprovisionar máquinas en zonas de disponibilidad específicas. Puede hacerlo con PowerShell.

> **Nota:**
>
> Si no se especifica ninguna zona, MCS permite a Azure colocar las máquinas dentro de la región. Si se especifica más de una zona, MCS distribuye aleatoriamente las máquinas entre ellas.

Configurar zonas de disponibilidad a través de PowerShell

Con PowerShell, puede ver la oferta de elementos de inventario mediante <!JEKYLL@5300@215>. Por ejemplo, para ver la oferta de servicio de la *región oriental de EE. UU.* <!JEKYLL@5300@216>:

<!JEKYLL@5300@217>

Para ver las zonas, utilice el parámetro <!JEKYLL@5300@218> para el elemento:

<!JEKYLL@5300@219>

Si no se especifican zonas de disponibilidad, no hay ningún cambio en la forma en que se aprovisionan las máquinas.

Para configurar las zonas de disponibilidad a través de PowerShell, utilice la propiedad personalizada **Zonas** disponible con la operación <!JEKYLL@5300@220>. La propiedad **Zonas** define una lista de zonas de disponibilidad en las que aprovisionar máquinas. Esas zonas pueden incluir una o más zonas de disponibilidad. Por ejemplo, <!JEKYLL@5300@221> para las zonas 1 y 3.

Utilice el comando <!JEKYLL@5300@222> para actualizar las zonas de un esquema de aprovisionamiento.

Si se proporciona una zona no válida, el esquema de aprovisionamiento no se actualiza y aparece un mensaje de error con instrucciones sobre cómo corregir el comando no válido.

> **Sugerencia:**
>
> Si especifica una propiedad personalizada no válida, el esquema de aprovisionamiento no se actualiza y aparece un mensaje de error al respecto.

Tipos de almacenamiento

Seleccione distintos tipos de almacenamiento para máquinas virtuales en entornos Azure que utilizan MCS. Para las máquinas virtuales de destino, MCS admite:

- Disco de SO: SSD Premium, SSD o HDD
- Disco de memoria caché con escritura: SSD Premium, SSD o HDD

Al utilizar estos tipos de almacenamiento, tenga en cuenta lo siguiente:

- Asegúrese de que su máquina virtual sea compatible con el tipo de almacenamiento seleccionado.
- Si su configuración usa un disco efímero de Azure, no tiene la posibilidad de configurar el disco de caché de reescritura.

> **Sugerencia:**
>
> <!JEKYLL@5300@223> está configurado para un tipo de SO y una cuenta de almacenamiento. <!JEKYLL@5300@224> está configurado para el tipo de almacenamiento de memoria caché de escritura. Para un catálogo normal, se requiere <!JEKYLL@5300@225>. Si <!JEKYLL@5300@226> no está configurado, <!JEKYLL@5300@227> se utiliza como predeterminado para <!JEKYLL@5300@228>.

Si WBCDiskStorageType no está configurado, StorageType se utiliza como predeterminado para WBCDiskStorageType.

Configurar los tipos de almacenamiento

Para configurar los tipos de almacenamiento para VM, utilice el parámetro <!JEKYLL@5300@229> en <!JEKYLL@5300@230>. Establezca el valor del parámetro <!JEKYLL@5300@231> en uno de los tipos de almacenamiento admitidos.

A continuación, se muestra un conjunto de ejemplo del parámetro <!JEKYLL@5300@232> en un esquema de aprovisionamiento:

<!JEKYLL@5300@233>

Habilitar el almacenamiento con redundancia de zonas

Puede seleccionar almacenamiento con redundancia de zonas durante la creación de catálogos. Replica sincrónicamente su disco administrado de Azure en varias zonas de disponibilidad, lo que le permite recuperarse de un error en una zona al usar la redundancia en otras.

Puede especificar **Premium_ZRS** y **StandardSSD_ZRS** en las propiedades personalizadas del tipo de almacenamiento. El almacenamiento ZRS se puede configurar mediante propiedades personalizadas existentes o mediante la plantilla **MachineProfile**. El almacenamiento ZRS también es compatible con el comando <!JEKYLL@5300@234> mediante los parámetros <!JEKYLL@5300@235> y <!JEKYLL@5300@236>, y usted puede cambiar el almacenamiento de la máquina existente de LRS a ZRS.

Limitaciones:

- Compatible solo para discos administrados
- Compatible únicamente con unidades de estado sólido (SSD) estándar y premium
- No es compatible con <!JEKYLL@5300@237>
- Disponible solo en determinadas regiones.
- El rendimiento de Azure disminuye al crear discos ZRS a escala. Por lo tanto, al encenderlas por primera vez, encienda las máquinas en lotes más pequeños (menos de 300 máquinas a la vez)

Definir el almacenamiento con redundancia de zonas como tipo de almacenamiento en disco
Puede seleccionar un almacenamiento con redundancia de zonas durante la creación de catálogos inicial o puede actualizar el tipo de almacenamiento en un catálogo existente.

Seleccionar el almacenamiento con redundancia de zonas mediante los comandos de PowerShell Al crear un catálogo en Azure mediante el comando <!JEKYLL@5300@238> de PowerShell, use <!JEKYLL@5300@239> como valor en <!JEKYLL@5300@240>.
Por ejemplo:

<!JEKYLL@5300@241>

Al definir este valor, se valida mediante una API dinámica que determina si se puede utilizar correctamente. Se pueden producir estas excepciones si el uso de ZRS no es válido para su catálogo:

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: La propiedad personalizada StorageTypeAtShutdown no se puede utilizar con el almacenamiento ZRS.
- **StorageAccountTypeNotSupportedInRegion**: Esta excepción se produce si intenta utilizar el almacenamiento ZRS en una región de Azure que no admite ZRS.
- **ZrsRequiresManagedDisks**: Solo puede utilizar el almacenamiento con redundancia de zonas con discos administrados.

Puede configurar el tipo de almacenamiento en disco mediante estas propiedades personalizadas:

- <!JEKYLL@5300@242>
- <!JEKYLL@5300@243>
- <!JEKYLL@5300@244>

> **Nota:**
>
> Durante la creación de catálogos, se utiliza el <!JEKYLL@5300@245> del disco del sistema operativo del perfil de máquina si las propiedades personalizadas no están configuradas.

Capture la configuración de diagnóstico en máquinas virtuales y NIC desde un perfil de máquina

Puede capturar la configuración de diagnóstico de las máquinas virtuales y las NIC desde un perfil de máquina mientras crea un catálogo de máquinas, actualiza un catálogo de máquinas existente y actualiza las máquinas virtuales existentes.

Puede crear una máquina virtual o una especificación de plantilla como fuente del perfil de máquina.

Pasos clave

1. Configure los ID necesarios en Azure. Debe proporcionar estos ID en la especificación de la plantilla.
    - Cuenta de almacenamiento
    - Espacio de trabajo de analíticas de registros
    - Espacio de nombres del centro de eventos con el precio del nivel estándar
2. Cree un origen de perfil de máquina.
3. Cree un nuevo catálogo de máquinas, actualice un catálogo existente o actualice las máquinas virtuales existentes.

Configurar los ID necesarios en Azure

Configure una de las siguientes opciones en Azure:

- Cuenta de almacenamiento
- Espacio de trabajo de analíticas de registros
- Espacio de nombres del centro de eventos con el precio del nivel estándar

Configurar una cuenta de almacenamiento Cree una cuenta de almacenamiento estándar en Azure. En la especificación de la plantilla, indique el resourceId completo de la cuenta de almacenamiento como el <!JEKYLL@5300@246>.

Una vez que las máquinas virtuales estén configuradas para registrar los datos en la cuenta de almacenamiento, los datos se pueden encontrar en el contenedor <!JEKYLL@5300@247>.

Configurar un espacio de trabajo de análisis de registros Cree un espacio de trabajo de análisis de registros. En la especificación de la plantilla, indique el resourceId completo para el espacio de trabajo de análisis de registros como workspaceId.

Una vez que las máquinas virtuales estén configuradas para registrar datos en el espacio de trabajo, los datos se pueden consultar en Registros en Azure. Puede ejecutar el siguiente comando en Azure en Registros para mostrar un recuento de todas las métricas registradas por un recurso:

‘AzureMetrics

Configurar un centro de eventos Haga lo siguiente para configurar un centro de eventos en Azure Portal:

1. Crea un espacio de nombres para centros de eventos con los precios del nivel estándar.
2. Cree un centro de eventos debajo del espacio de nombres.
3. Vaya a **Capturar** en el centro de eventos. Encienda el interruptor para capturar con el tipo de salida Avro.
4. Cree un contenedor nuevo en una cuenta de almacenamiento existente para capturar los registros.
5. En la especificación de la plantilla, especifique el `eventHubAuthorizationRuleId` en el siguiente formato: `/subscriptions/093f4c12-704b-4b1d-8339-f339e7557f60/resourcegroups/matspo/providers/Microsoft.EventHub/namespaces/matspoeventhub/authorizationrules/RootManageSharedAccessKey`
6. Especifique el nombre del centro de eventos.

Una vez que las máquinas virtuales están configuradas para registrar datos en el centro de eventos, los datos se capturan en el contenedor de almacenamiento configurado.

Crear una fuente de perfil de máquina

Puede crear una máquina virtual o una especificación de plantilla como fuente del perfil de máquina.

Cree un perfil de máquina basado en máquinas virtuales con parámetros de diagnóstico Si quiere crear una máquina virtual como perfil de máquina, primero configure los parámetros de diagnóstico en la propia máquina virtual de plantilla. Puede consultar las instrucciones detalladas que se proporcionan en la documentación de Microsoft Parámetros de diagnóstico en Azure Monitor.

Puede ejecutar los siguientes comandos para verificar que ahora hay una configuración de diagnóstico asociada a la máquina virtual o a la NIC:


```
az monitor diagnostic-settings list --resource-group matspo --resource
    matspo-tog-cc2659 --resource-type microsoft.network/
    networkInterfaces
```

```
az monitor diagnostic-settings list --resource-group matspo --resource
    matspo-tog-cc2 --resource-type microsoft.compute/virtualMachines
```

Cree una plantilla de perfil de máquina basada en especificaciones con parámetros de diagnóstico Si quiere usar una máquina virtual que ya tenga habilitada la configuración de diagnóstico y exportarla a una especificación de plantilla ARM, esta configuración no se incluirá automáticamente en la plantilla. Debe agregar o modificar manualmente la configuración de diagnóstico en la plantilla ARM.

Sin embargo, si quiere una máquina virtual como perfil de máquina, MCS se asegura de que la configuración de diagnóstico crítica se capture y aplique con precisión a los recursos de su catálogo de MCS.

1. Cree una especificación de plantilla estándar que defina una máquina virtual y una NIC.
2. Agregue recursos adicionales para implementar la configuración de diagnóstico de acuerdo con la especificación: Microsoft.Insights diagnosticSettings. Para conocer el ámbito, haga referencia a una máquina virtual o NIC que esté en la plantilla por su nombre con un identificador parcial. Por ejemplo, para crear una configuración de diagnóstico adjunta a una máquina virtual denominada Test-VM en la especificación de la plantilla, especifique el ámbito de la siguiente manera:

   ```
   "scope": "microsoft.compute/virtualMachines/test-VM",
   ```

3. Use la especificación de la plantilla como fuente del perfil de máquina.

Crear o actualizar un catálogo con parámetros de diagnóstico

Después de crear un origen de perfiles de máquinas, ahora puede crear un catálogo de máquinas mediante un comando `New-ProvScheme`, actualizar un catálogo de máquinas existente mediante un comando `Set-ProvScheme` y actualizar las máquinas virtuales existentes mediante un comando `Request-ProvVMUpdate`.

Determinación de la ubicación del archivo de paginación

La ubicación del archivo de paginación se determina según el siguiente supuesto:

> **Nota:**
>
> La ubicación predeterminada del archivo de paginación está en el disco del SO.

Caso	Location
La configuración del archivo de paginación se especifica en las propiedades personalizadas	Según se especifica en las propiedades personalizadas
El disco de SO efímero o la hibernación están habilitados	Disco de SO
La máquina virtual tiene un disco temporal	Disco temporal
E/S de MCS está habilitada	Disco WBC

Casos de configuración de archivos de paginación

En esta tabla se describen algunos casos posibles de configuración de archivos de paginación durante la preparación de imágenes y la actualización del esquema de aprovisionamiento:

Durante	Caso	Resultado
Preparación de imágenes	El archivo de paginación de la imagen de origen se establece en el disco temporal, mientras que el tamaño de la máquina virtual que especifique en el esquema de aprovisionamiento no tiene disco temporal	El archivo de paginación se coloca en el SO
Preparación de imágenes	El archivo de paginación de la imagen de origen se establece en el disco de SO, mientras que el tamaño de la máquina virtual que se especifica en el esquema de aprovisionamiento tiene un disco temporal	El archivo de paginación se coloca en el disco temporal

Durante	Caso	Resultado
Preparación de imágenes	Establezca el archivo de paginación de la imagen de origen en el disco temporal y habilite el disco de SO efímero en el esquema de aprovisionamiento.	El archivo de paginación se coloca en el disco del sistema operativo
Actualización del esquema de aprovisionamiento	Intenta actualizar el esquema de aprovisionamiento cuando la versión del VDA es anterior a la 2311	Modifica la configuración del archivo de paginación con una advertencia
Actualización del esquema de aprovisionamiento	Intenta actualizar el esquema de aprovisionamiento cuando la versión del VDA es 2311 o posterior	Determina la ubicación del archivo de paginación según la determinación de la ubicación del archivo de paginación

Especificar los parámetros del archivo de páginación

Con los comandos de PowerShell, puede especificar los parámetros del archivo de paginación, incluidos la ubicación y el tamaño. Esto supedita los parámetros del archivo de paginación determinados por MCS según la determinación de la ubicación del archivo de paginación. Para ello, ejecute este comando `New-ProvScheme` durante la creación del catálogo de máquinas.

Consideraciones importantes

Tenga en cuenta lo siguiente antes de continuar con la creación del catálogo:

- Debe proporcionar todas las propiedades personalizadas (“PageFileDiskDriveLetterOverride” , “InitialPageFileSizeInMB”y “MaxPageFileSizeInMB”) en el comando `New-ProvScheme` o ninguna de ellas.
- Esta función no está disponible a través de Citrix Studio.
- El tamaño del archivo de paginación inicial debe estar entre 16 MB y 16777216 MB.
- El tamaño del archivo de paginación máximo debe ser superior o igual al tamaño del archivo de paginación inicial e inferior a 16777216 MB.
- Puede establecer el tamaño inicial del archivo de paginación y el tamaño máximo del archivo de paginación en cero al mismo tiempo.

> **Nota:**
>
> Puede modificar los parámetros del archivo de paginación de las máquinas virtuales recién agregadas de un catálogo existente sin actualizar la imagen maestra. Para modificar los parámetros del archivo de paginación, necesita la versión 2311 o posterior del VDA. Puede modificar los parámetros del archivo de paginación mediante los comandos de PowerShell. Para obtener más información, consulte Modificar los parámetros del archivo de paginación.

```
New-ProvScheme -CleanOnBoot `
-HostingUnitName "zijinnet" `
-IdentityPoolName "PageFileSettingExample" `
-ProvisioningSchemeName "PageFileSettingExample" `
-InitialBatchSizeHint 1 `
-MasterImageVM "XDHyp:\HostingUnits\zijinnet\image.folder\neal-
   zijincloud-resources.resourcegroup\
   CustomWin10VDA_OsDisk_1_9473d7c8a6174b2c8284c7d3efeea88f.manageddisk
   " `
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\zijinnet\virtualprivatecloud.folder\East US.
    region\virtualprivatecloud.folder\neal-zijincloud-resources.
    resourcegroup\neal-zijincloud-resources-vnet.virtualprivatecloud\
    default.network" }
  `
-ServiceOffering "XDHyp:\HostingUnits\zijinnet\serviceoffering.folder\
   Standard_B2ms.serviceoffering" `
-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com
   /2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/
   XMLSchema-instance"> `
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false
   "/> `
<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `
<Property xsi:type="StringProperty" Name="
   PageFileDiskDriveLetterOverride" Value="d"/> `
<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
   Value="2048"/> `
<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB" Value
   ="8196"/> `
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS"/> `
<Property xsi:type="StringProperty" Name="LicenseType" Value="
   Windows_Client"/> `
</CustomProperties>'
```

Modificar los parámetros del archivo de páginación

Puede modificar los parámetros del archivo de paginación de las máquinas virtuales recién agregadas a un catálogo existente sin actualizar la imagen maestra. Esta función se aplica actualmente a los entornos de Azure solamente.

Para modificar los parámetros del archivo de paginación, necesita la versión 2311 o posterior del VDA. Puede modificar los parámetros del archivo de paginación mediante los comandos de PowerShell.

A continuación se muestran los distintos parámetros del archivo de paginación que puede modificar en el entorno de Azure:

- `PageFileDiskDriveLetterOverride`
- `InitialPageFileSizeInMB`
- `MaxPageFileSizeInMB`

Modificar los parámetros del archivo de paginación de un catálogo existente

Para modificar los parámetros del archivo de paginación de un catálogo de máquinas existente, ejecute el comando `Set-ProvScheme`. En este caso, las actualizaciones se aplican solo a las nuevas máquinas virtuales agregadas al catálogo. Por ejemplo:

```
1  Set-ProvScheme -ProvisioningSchemeName $schemeName -CustomProperties '<
       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="OsType" Value="Windows" />
4  <Property xsi:type="StringProperty" Name="StorageType" Value="
       StandardSSD_LRS" />
5  <Property xsi:type="StringProperty" Name="
       PageFileDiskDriveLetterOverride" Value="D" />
6  <Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
       Value="2048" />
7  <Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB" Value
       ="8196" />
8  <Property xsi:type="StringProperty" Name="LicenseType" Value="
       Windows_Client" />
9  <Property  xsi:type="StringProperty" Name="Zones" Value="1" />
10 <Property xsi:type="StringProperty" Name="ResourceGroups" Value="neal-
       test-group1" />
11 <Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
12 </CustomProperties>'
```

> **Nota:**
>
> Si habilita la caché de reescritura e intenta asignar a `PageFileDiskDriveLetterOverride` el valor `C:` con el comando de PowerShell, el controlador de E/S de MCS redirige automáticamente el archivo de paginación a la unidad de disco correcta, en vez de a `C:`.

Crear un catálogo con máquinas virtuales de Azure Spot

Las máquinas virtuales Azure Spot le permiten aprovechar la capacidad informática no usada de Azure con un importante ahorro de costes. Sin embargo, la capacidad de asignar una máquina virtual Azure Spot depende de la capacidad y los precios actuales. Por lo tanto, Azure podría desalojar la máquina virtual en ejecución, no crear la máquina virtual o no encenderla según la directiva de desalojo. Por lo tanto, las máquinas virtuales de Azure Spot son buenas para algunas aplicaciones y escritorios no son críticos. Para obtener más información, consulte Usar máquinas virtuales de Azure Spot.

Limitaciones

- Las máquinas virtuales de Azure Spot no presentan compatibilidad con todos los tamaños de máquinas virtuales. Para obtener más información, consulte Limitaciones.

  Puede ejecutar el siguiente comando de PowerShell para comprobar si el tamaño de una máquina virtual es compatible con máquinas virtuales puntuales o no. Si el tamaño de una máquina virtual es compatible con máquinas virtuales Spot, entonces `SupportsSpotVM` es **True**.

  ```
  1   (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\serviceoffering.
         folder\Standard_D2ds_v4.serviceoffering"). AdditionalData
  ```

- Actualmente, las máquinas virtuales de Azure Spot no tienen disponible la función de hibernación.

Requisito

Al crear el origen del perfil de máquina (especificación de máquina virtual o plantilla) para el catálogo de máquinas virtuales de Azure Spot, debe seleccionar Azure Spot Instance (si usa una máquina virtual) o configurar `priority` como `Spot` (si usa una especificación de plantilla).

Pasos para crear un catálogo con máquinas virtuales de Azure Spot

1. Cree un origen de perfil de máquina (máquina virtual o plantilla de inicio).
   - Para crear una máquina virtual con Azure Portal, consulte Implementar máquinas virtuales Azure Spot con Azure Portal.
   - Para crear una especificación de plantilla, agregue las siguientes propiedades en **recursos > tipo: Microsoft.Compute/virtualMachines > propiedades** en la especificación de plantilla. Por ejemplo:


```
"priority": "Spot",
"evictionPolicy": "Deallocate",
"billingProfile": {

"maxPrice": 0.01
 }
```

Nota:

- La directiva de desalojo puede **desasignarse** o **eliminarse**.
  - Para las máquinas virtuales no persistentes, MCS siempre establece la directiva de desalojo como **Eliminar**. Si se desaloja la máquina virtual, se elimina junto con todos los discos no persistentes (por ejemplo, el disco del sistema operativo). No se elimina ningún disco persistente (por ejemplo, el disco de identidad). Sin embargo, un disco del sistema operativo es persistente si el tipo de catálogo es persistente o si la propiedad personalizada `PersistOsDisk` está establecida en True. Del mismo modo, un disco WBC es persistente si la propiedad personalizada `PersistWbc` se establece en **True**.
  - Para las máquinas virtuales persistentes, MCS siempre establece la directiva de desalojo como Desasignar. Si se desaloja la máquina virtual, se desasigna. No se realizan cambios en los discos.
- El precio máximo es el precio que está dispuesto a pagar por hora. Si está usando **Solo capacity** , entonces es **-1**. El precio máximo solo puede ser nulo, -1 o un decimal mayor que cero. Para obtener más información, consulte Precios.

2. Puede ejecutar el siguiente comando de PowerShell para comprobar si un perfil de máquina está habilitado para Azure Spot VM o no. Si el parámetro `SpotEnabled` es **True** y `SpotEvictionPolicy` está establecido en **Desasignar** o **Eliminar**, el perfil de la máquina está habilitado para Azure Spot VM. Por ejemplo,

   - Si la fuente del perfil de la máquina es una máquina virtual, ejecute el siguiente comando:

   ```
   (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\machineprofile
       .folder\fifthcolumn.resourcegroup\kb-spot-delete.vm").
       AdditionalData
   ```

   - Si el origen del perfil de la máquina es una especificación de plantilla, ejecute el siguiente comando:

   ```
   (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\machineprofile
       .folder\fifthcolumn.resourcegroup\fc-aeh-templatespec.
       templatespec\14.0.0-spot-delete.templatespecversion").
       AdditionalData
   ```


3. Cree un catálogo de máquinas mediante un perfil de máquina con el comando `New-ProvScheme` PowerShell.

Puede actualizar un catálogo mediante el comando `Set-ProvScheme`. También puede actualizar las máquinas virtuales existentes mediante el comando PowerShell `Set-ProvVmUpdateTimeWindow`. El perfil de la máquina se actualiza la próxima vez que se enciende.

Desalojos en una máquina virtual Azure Spot en ejecución

Si la capacidad de procesamiento no está disponible o el precio por hora es superior al precio máximo configurado, Azure desaloja una máquina virtual de Spot en ejecución. De forma predeterminada, no se le notifica ningún desalojo. La máquina virtual simplemente se congela y se desaloja. Microsoft recomienda usar eventos programados para supervisar los desalojos. Consulte Supervisar continuamente el desalojo. También puede ejecutar scripts desde una máquina virtual para recibir una notificación antes del desalojo. Por ejemplo, Microsoft tiene un script de sondeo en Python ScheduledEvents.cs.

Solución de problemas

- Puede ver las propiedades de la máquina virtual Spot en customMachineData de la máquina virtual aprovisionada mediante el comando `Get-ProvVM`. Si el campo de prioridad está establecido en **Spot**, significa que Spot está en uso.
- Puede comprobar si una máquina virtual usa Spot en Azure Portal:

    1. Busque la máquina virtual en Azure Portal.
    2. Vaya a la página **Descripción general**.
    3. Desplácese hacia abajo y localice la sección **Azure Spot**.

        - Si Spot no está en uso, este campo está vacío.
        - Si se está usando, se establecen los campos de **directiva de desalojo de Azure Spot** y **Azure Spot**.

1. Puede comprobar el perfil de facturación o el precio máximo por hora de la máquina virtual en la página de configuración.

Configurar los tamaños de las máquinas virtuales de seguridad

En ocasiones, las nubes públicas pueden quedarse sin capacidad para un tamaño de máquina virtual específico. Además, si usa máquinas virtuales de Azure Spot, las máquinas virtuales se desalojan en cualquier momento en función de las necesidades de capacidad de Azure. En el caso

de que la capacidad de Azure sea insuficiente o de que una máquina virtual puntual no se encienda, MCS recurre a los tamaños de las máquinas virtuales de seguridad. Puede proporcionar una lista de los tamaños de las máquinas virtuales de seguridad mediante una propiedad personalizada `BackupVmConfiguration` al crear o actualizar un catálogo de máquinas MCS. MCS intenta usar los tamaños de las máquinas virtuales de seguridad en el orden indicado por usted en la lista.

Cuando MCS usa una configuración de seguridad en particular para la máquina virtual, continúa usando esa configuración hasta el próximo cierre. La próxima vez que se encienda, MCS intentará iniciar la configuración de la máquina virtual principal. En caso de error, MCS intenta iniciar de nuevo una configuración de tamaño de máquina virtual de seguridad según la lista.

Esta función está disponible para:

- un catálogo que usa un perfil de máquina
- Catálogos de máquinas de MCS persistentes y no persistentes
- Entornos de Azure actualmente

Consideraciones importantes

- Puede proporcionar más de un tamaño de máquina virtual de seguridad en la lista.
- La lista debe ser única.
- Puede agregar la propiedad del tipo de instancia para cada una de las máquinas virtuales de la lista. El tipo es **Spot** o **Regular**. Si no se especifica el tipo, MCS considera que la máquina virtual es **Regular**.
- Puede cambiar la lista de tamaños de máquinas virtuales de seguridad de un catálogo existente mediante los comandos de PowerShell `Set-ProvScheme`.
- Puede actualizar las máquinas virtuales existentes creadas a partir del esquema de aprovisionamiento asociado al catálogo mediante el comando `Set-ProvVMUpdateTimeWindow`.
- Puede configurar la lista de tamaños de máquinas virtuales de seguridad para un número seleccionado de máquinas virtuales MCS existentes mediante el comando `Set-ProvVM`. Sin embargo, para aplicar las actualizaciones, establezca una ventana de tiempo de actualización para las máquinas virtuales que usan `Set-ProvVMUpdateTimeWindow` e inicie las máquinas virtuales dentro de la ventana. Si el comando `Set-ProvVm` se usa en una máquina virtual, la máquina virtual continúa usando la lista de tamaños de máquinas virtuales de seguridad establecida en esa máquina virtual en particular, incluso sila lista del esquema de aprovisionamiento se actualiza más adelante. Puede usar `Set-ProvVM` con `-RevertToProvSchemeConfiguration` para hacer que la máquina virtual use la lista de seguridad del esquema de aprovisionamiento.

Cree un catálogo con tamaños de máquinas virtuales de seguridad

1. Abra una ventana de **PowerShell**.
2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
3. Cree un catálogo de brokers. Este catálogo contiene máquinas que están a punto de crearse.
4. Crear un grupo de identidades. Se convierte en un contenedor para las cuentas de AD creadas para las máquinas que se van a crear.
5. Cree un esquema de aprovisionamiento con el perfil de la máquina. Por ejemplo:

   - Si quiere proporcionar una lista solo de los tamaños de máquinas virtuales regulares, ejecute lo siguiente:

```
New-ProvScheme -ProvisioningSchemeName "azure-catalog" -
    MasterImageVM "XDHyp:\HostingUnits\azure-zones\image.
    folder\helenli.resourcegroup\helenli-master1-mcsio-
    snapshot.snapshot"
-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=`"LicenseType`"
    Value=`"Windows_Server`"/>
<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`"
    Value=`"true`"/>  <Property xsi:type=`"StringProperty`"
    Name=`"BackupVmConfiguration`" Value=`"['ServiceOffering':
     'Standard_D2as_v4', 'ServiceOffering': 'Standard_D2s_v3',
     'ServiceOffering': 'C']`"/>
</CustomProperties>"
```

   - Si quiere proporcionar una lista de tamaños de máquinas virtuales mixtos (máquinas virtuales normales y puntuales), ejecute lo siguiente:

```
New-ProvScheme -ProvisioningSchemeName "azure-catalog" -
    MasterImageVM "XDHyp:\HostingUnits\azure-zones\image.
    folder\helenli.resourcegroup\helenli-master1-mcsio-
    snapshot.snapshot"
-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=`"LicenseType`"
   Value=`"Windows_Server`"/>
<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`"
   Value=`"true`"/>  <Property xsi:type=`"StringProperty`"
   Name=`"BackupVmConfiguration`" Value=`"[{
'ServiceOffering': 'Standard_D2as_v4', 'Type': 'Spot' }
, {
'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Regular' }
, {
'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Spot' }
]`"/>
</CustomProperties>"
```

6. Actualice el BrokerCatalog con el identificador único del esquema de aprovisionamiento.
7. Cree máquinas virtuales y agréguelas al catálogo.

Actualizar un catálogo existente

Puede actualizar un esquema de aprovisionamiento mediante el comando `Set-ProvScheme`. Por ejemplo:

```
Set-ProvScheme -ProvisioningSchemeName "azure-catalog"
-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=`"LicenseType`" Value=`"
   Windows_Server`"/>
<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"true`
   "/>
<Property xsi:type=`"StringProperty`" Name=`"BackupVmConfiguration`"
   Value=`"[{
 'ServiceOffering': 'Standard_D2as_v4', 'Type': 'Spot' }
 , {
 'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Regular' }
 , {
 'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Spot' }
 ]`"/>
</CustomProperties>"
```

Actualizar las máquinas virtuales existentes

Puede actualizar las máquinas virtuales existentes en un catálogo mediante el comando de PowerShell `Set-ProvVMUpdateTimeWindow`. El comando actualiza las máquinas virtuales creadas a

partir del esquema de aprovisionamiento asociado al catálogo la próxima vez que se encienda dentro del período de tiempo determinado. Por ejemplo:

- `Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -StartTimeInUTC "3/12/2022 3am"-DurationInMinutes 60`
- `Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -StartsNow -DurationInMinutes 60`

> **Nota:**
>
> `StartsNow` indica la hora de inicio programada. `DurationInMinutes` es el periodo de tiempo de la programación.

Puede configurar la lista de tamaños de máquinas virtuales de seguridad para un número seleccionado de máquinas virtuales MCS existentes mediante el comando `Set-ProvVM`. Sin embargo, para aplicar las actualizaciones, establezca una ventana de tiempo de actualización para las máquinas virtuales que usan `Set-ProvVMUpdateTimeWindow` e inicie las máquinas virtuales dentro de la ventana. Por ejemplo:

1. Ejecute el comando `Set-ProvVM` para configurar la lista de tamaños de máquinas virtuales de seguridad para una máquina virtual MCS existente seleccionada. Por ejemplo:

```
Set-ProvVM -VMName "Vm-001"
-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=`"LicenseType`" Value=`"Windows_Server`"/>
<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"true`"/>
<Property xsi:type=`"StringProperty`" Name=`"BackupVmConfiguration`" Value=`"[{
 'ServiceOffering': 'Standard_D2as_v4', 'Type': 'Spot' }
 , {
 'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Regular' }
 , {
 'ServiceOffering': 'Standard_D2s_v3', 'Type': 'Spot' }
 ]`"/>
</CustomProperties>"
```

2. Ejecute el comando `Set-ProvVMUpdateTimeWindow` para aplicar las actualizaciones. Por ejemplo:


```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -
    StartsNow -DurationInMinutes 60
```

Copiar etiquetas en todos los recursos

Puede copiar las etiquetas especificadas en un perfil de máquina en todos los recursos, como varias NIC y discos (disco del sistema operativo, disco de identidad y disco de caché de reescritura), de una máquina virtual nueva o existente de un catálogo de máquinas. La fuente del perfil de máquina puede ser una VM o una especificación de plantilla de Azure Resource Manager.

> **Nota:**
>
> Debe agregar la directiva a las etiquetas (consulte Assign policy definitions for tag compliance) o agregar las etiquetas en un origen de perfil de máquina para conservar las etiquetas en los recursos.

Requisitos previos

Cree el origen del perfil de máquina (VM o especificación de plantilla de Azure Resource Manager) para tener etiquetas en la VM, los discos y las tarjetas NIC de esa VM.

- Si quiere usar una VM como entrada del perfil de máquina, aplique etiquetas a VM y a todos los recursos de Azure Portal. Consulte Apply tags with Azure portal.
- Si quiere usar una especificación de plantilla de Azure Resource Manager como entrada del perfil de la máquina, agregue el siguiente bloque de etiquetas bajo cada recurso.

```
 "tags": {

"TagC": "Value3"
 }
,
```

> **Nota:**
>
> Puede tener un máximo de un disco y al menos una tarjeta NIC en la especificación de plantilla.

Copie las etiquetas en los recursos de una VM de un nuevo catálogo de máquinas

1. Cree un catálogo persistente o no persistente con una VM o una especificación de plantilla de Azure Resource Manager como entrada del perfil de máquina.
2. Agregue una VM al catálogo y enciéndala. Debería poder ver que las etiquetas especificadas en el perfil de máquina se han copiado en los recursos correspondientes de esa VM.

> **Nota:**
>
> Aparecerá un error si la cantidad de tarjetas NIC proporcionadas en el perfil de máquina no coincide con la cantidad de tarjetas NIC que quiere que usen las VM.

Modificar las etiquetas de los recursos de una VM existente

1. Cree un perfil de máquina con las etiquetas de todos los recursos.
2. Actualice el catálogo de máquinas existente con el perfil de máquina actualizado. Por ejemplo:

```
Set-ProvScheme -ProvisioningSchemeName <YourCatalogName> -
    MachineProfile <PathToYourMachineProfile>
```

3. Apague la máquina virtual en la que quiera aplicar las actualizaciones.
4. Solicite una actualización programada para la máquina virtual. Por ejemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <
    YourCatalogName>  -VMName machine1 -StartsNow -
    DurationInMinutes -1
```

5. Encienda la máquina virtual.
6. Debería poder ver que las etiquetas especificadas en el perfil de máquina se han copiado en los recursos correspondientes.

> **Nota:**
>
> Aparecerá un error si la cantidad de tarjetas NIC proporcionadas en el perfil de máquina no coincide con la cantidad de tarjetas NIC proporcionadas en `Set-ProvScheme`.

Qué hacer a continuación

- Si este es el primer catálogo creado, Web Studio le guiará para crear un grupo de entrega
- Para revisar todo el proceso de configuración, consulte Instalar y configurar
- Para administrar catálogos, consulte Administrar catálogos de máquinas y Administrar un catálogo de Microsoft Azure

Más información

- Crear y administrar conexiones y recursos
- Conexión con Microsoft Azure Resource Manager
- Crear catálogos de máquinas

Crear un catálogo de Microsoft System Center Virtual Machine Manager

August 17, 2024

Crear catálogos de máquinas describe los asistentes con los que se crea un catálogo de máquinas. La siguiente información incluye detalles específicos de los entornos de virtualización de Microsoft System Center Virtual Machine Manager (VMM).

> **Nota:**
>
> Antes de crear un catálogo de VMM, debe terminar de crear una conexión con VMM. Consulte Conexión con Microsoft System Center Virtual Machine Manager.

Crear una VM maestra

1. Instale un agente Virtual Desktop Agent en la VM maestra y seleccione la opción de optimizar el escritorio y así mejorar el rendimiento.
2. Tome una instantánea de la VM maestra para usarla como copia de seguridad.
3. Cree escritorios virtuales.

MCS en recursos compartidos de archivos SMB 3

Para catálogos de máquinas creados con MCS en recursos compartidos de archivos SMB 3 para almacenamiento de VM, compruebe que las credenciales cumplan los siguientes requisitos. Estos requisitos garantizan que las llamadas de la biblioteca de comunicaciones de hipervisor (HCL) del Controller se conecten correctamente al almacenamiento de 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.

Cuando utilice el almacenamiento de SMB, habilite el proveedor de compatibilidad para seguridad de credenciales de autenticación (CredSSP) desde el Controller a máquinas Hyper-V individuales. Use este proceso para VMM 2012 SP1 con Hyper-V en Windows Server 2012. Para obtener más información, consulte CTX137465.

La biblioteca HCL utiliza `CredSSP` para abrir una conexión a la máquina Hyper-V. Esta función pasa las credenciales de usuario cifradas por Kerberos a la máquina Hyper-V. 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, para que los comandos de comunicación con el 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 imagen maestra:** Una imagen maestra crea un esquema de aprovisionamiento (catálogo de máquinas) de MCS. Clona y deja la VM maestra lista para crear máquinas virtuales 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:

```
$ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
$result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)
$result
```

- **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:

```
$ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
$result = $ims.CreateVirtualHardDisk($vhdastext);
$result
```

- **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.

  1. La HCL carga la identidad en la máquina Hyper-V mediante el recurso compartido de administrador.
  2. 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).
  3. La biblioteca HCL elimina el archivo del recurso compartido de administrador.
  4. Cuando la HCL termina de cargar el disco de identidad en la máquina Hyper-V, la sesión remota de PowerShell copia los discos de identidad al almacenamiento de SMB. A continuación, lo 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.

  1. La máquina Hyper-V copia el disco desde el almacenamiento de SMB al almacenamiento de Hyper-V local mediante un script de PowerShell. Este script se ejecuta en la sesión remota de PowerShell V3.
  2. La HCL lee el disco desde el recurso compartido de administrador de la máquina Hyper-V y lo copia en memoria.
  3. La HCL elimina el archivo del recurso compartido de administrador.

Crear un catálogo con un perfil de máquina

Puede usar un perfil de máquina para crear y actualizar un catálogo de máquinas MCS en entornos de System Center Virtual Machine Manager (SCVMM). Puede habilitar vTPM. También puede agregar etiquetas personalizadas de una VM de perfil de máquina a las VM aprovisionadas.

Consideraciones importantes

- La imagen maestra solo puede ser una instantánea y no una máquina virtual.
- Solo puede usar una máquina virtual como origen de perfil de máquina.
- Puede configurar VTPM desde la consola de Hyper-V y no desde la consola SCVMM.
- Si la imagen maestra tiene el vTPM habilitado, debe habilitar el vTPM en el origen del perfil de la máquina.
- vTPM solo es compatible en máquinas de 2.ª generación.
- Los siguientes parámetros sobrescriben los valores capturados en un perfil de máquina si se proporcionan por separado:
  - VMCpuCount
  - VMMemoryMB
  - Almacenamiento en disco
- Las etiquetas personalizadas solo se heredan del perfil de máquina, y no de la imagen maestra. La etiqueta `CitrixProvisioningSchemeId` se agrega de forma predeterminada a la máquina virtual. Si no quiere incluir la etiqueta `CitrixProvisioningSchemeId`, agregue el parámetro `-NoVmTagging` al crear una unidad de alojamiento. Ejemplo:


```
New-Item -HypervisorConnectionName $ConnectionName ` -NetworkPath
 @($NetworkPath)` -Path @($HostingUnitPath)` -PersonalvDiskStoragePath
 @()` -RootPath $RootPath ` -StoragePath @($StoragePath)` -
NoVmTagging
```

- Puede actualizar un catálogo existente mediante el comando `Set-ProvScheme`.

Crear un catálogo de máquinas mediante un perfil de máquina

1. Cree una máquina virtual para que sea un origen de perfiles de máquina. Para obtener más información, consulte Aprovisionar máquinas virtuales en el tejido de VMM. No puede cambiar la **generación** después de seleccionarla. Puede hacer lo siguiente en SCVMM:
    - Para habilitar vTPM:
        a) Después de crear la máquina virtual, inicie sesión en el host de Hyper-V y busque su máquina virtual en el **administrador de Hyper-V**.
        b) Haga clic con el botón derecho en la máquina virtual y, a continuación, vaya a **Parámetros**.
        c) En **Seguridad**, seleccione la casilla **Habilitar el módulo de plataforma segura**.
2. Abra una ventana de **PowerShell**.
3. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
4. Cree un catálogo de brokers. Este catálogo contiene máquinas que están a punto de crearse.
5. Crear un grupo de identidades. Se convierte en un contenedor para las cuentas de AD creadas para las máquinas que se van a crear.
6. Cree un esquema de aprovisionamiento con el perfil de la máquina. Por ejemplo:

```
1 New-ProvScheme -HostingUnitName "<hostingunit name>"
2 -IdentityPoolName "ID1" -MasterImageVM "XDHyp:\HostingUnits\HU1<
     path to the checkpoint/snapshot>"
3 -ProvisioningSchemeName "<catalogname>"  -MachineProfile "XDHyp:<
     path to the machine profile VM>"
```

7. Actualiza el catálogo de Broker con el identificador único del esquema de aprovisionamiento.
8. Cree máquinas virtuales y agréguelas al catálogo.

Actualizar un catálogo existente

Puede actualizar un catálogo existente mediante el comando Set-ProvScheme. Por ejemplo:

```
1 Set-ProvScheme -ProvisioningSchemeName "<catalogname>" -MachineProfile
     "XDHyp:<path to the machine profile VM>"
```


Quitar una máquina virtual

Puede optar por quitar una máquina virtual de un catálogo, pero no puede eliminarla de SCVMM. En este caso, la etiqueta `CitrixProvisioningSchemeId` solo se quita de la máquina virtual. Las etiquetas personalizadas no se eliminan de la máquina virtual. Puede quitar una máquina virtual desde la interfaz de Configuración completa o usar los comandos de PowerShell.

Quitar una máquina virtual mediante la interfaz de Configuración completa

1. Seleccione y haga clic con el botón secundario en la máquina virtual.
2. Haga clic en **Eliminar**.
3. Seleccione **Quitar las máquinas virtuales del catálogo pero no eliminarlas**.

Mediante los comandos de PowerShell `Remove-ProvVM` con el parámetro `ForgetVM`. Para obtener más información, consulte:

- Quitar etiquetas
- Eliminar máquinas sin acceder al hipervisor

Qué hacer a continuación

- Si este es el primer catálogo creado, Web Studio le guiará para crear un grupo de entrega
- Para revisar todo el proceso de configuración, consulte Instalar y configurar
- Para administrar catálogos, consulte Administrar catálogos de máquinas y Administrar un catálogo de Microsoft System Center Virtual Machine Manager

Más información

- Crear y administrar conexiones y recursos
- Conexión con Microsoft System Center Virtual Machine Manager
- Crear catálogos de máquinas

Crear un catálogo de Nutanix

August 17, 2024

Crear catálogos de máquinas describe los asistentes con los que se crea un catálogo de máquinas. La siguiente información incluye detalles específicos de los entornos de virtualización de Nutanix.

> **Nota:**
>
> Antes de crear un catálogo de Nutanix, debe terminar de crear una conexión con Nutanix. Consulte Conexión con Nutanix.

Crear un catálogo de máquinas mediante una instantánea de Nutanix

La instantánea que seleccione es la plantilla que se utiliza para crear las máquinas virtuales del catálogo. Antes de crear el catálogo de máquinas, cree las imágenes y las instantáneas en Nutanix. Para obtener más información, consulte la documentación de Nutanix.

En el asistente para la creación de catálogos:

- Las páginas **Sistema operativo** y **Administración de máquinas** no contienen información específica de Nutanix.
- La página **Contenedor** o **Cluster and Container** es exclusiva de Nutanix.

  Si implementa máquinas mediante Nutanix AHV XI como recursos, aparecerá la página **Contenedor**. Seleccione un contenedor en el que se colocarán los discos de identidad de las máquinas virtuales.

  Si implementa máquinas mediante Nutanix AHV Prism Central (PC) como recursos, aparecerá la página **Cluster and Container**. Seleccione el clúster que se utilizará para la implementación de las máquinas virtuales y, a continuación, un contenedor.
- En la página **Imagen**, 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 de creación de 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.
- En la página **Tarjetas de red**, seleccione el tipo de tarjeta de interfaz de red (NIC) para filtrar las redes asociadas. Hay dos tipos de NIC: **VLAN** y **SUPERPOSICIÓN**. Seleccione una o varias NIC que contengan la imagen maestra y, a continuación, seleccione una red virtual asociada para cada NIC.
- Las páginas **Identidades de las máquinas**, **Credenciales de dominio**, **Ámbitos** y **Resumen** no contienen información específica de Nutanix.

Limitación

Al crear un catálogo de MCS con una conexión de host de Nutanix (específicamente, el plug-in 2.7.1 de Nutanix AHV), el tamaño del disco duro de las máquinas virtuales aprovisionadas no se muestra correctamente en Web Studio. El tamaño que se muestra es mucho más pequeño (1 GB) que el tamaño de almacenamiento real (50 GB). El tamaño del disco duro se muestra correctamente en la consola de Nutanix.

Qué hacer a continuación

- Si este es el primer catálogo creado, Web Studio le guiará para crear un grupo de entrega
- Para revisar todo el proceso de configuración, consulte Instalar y configurar
- Para administrar catálogos, consulte Administrar catálogos de máquinas

Más información

- Crear y administrar conexiones y recursos
- Conexión con Nutanix
- Conexión con soluciones de Nutanix Cloud y de partners
- Crear catálogos de máquinas

Crear un catálogo de VMware

August 17, 2024

Crear catálogos de máquinas describe los asistentes con los que se crea un catálogo de máquinas. La siguiente información incluye detalles específicos de los entornos de virtualización de VMware.

> **Nota:**
>
> Antes de crear un catálogo de VMware, debe terminar de crear una conexión con VMware. Consulte Conexión con VMware.

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.

> **Nota:**
>
> Puede usar MCS para aprovisionar máquinas virtuales en un entorno de vSAN 8.0.

Crear un catálogo de máquinas mediante un perfil de máquina

Puede crear un catálogo de máquinas de MCS mediante un perfil de máquina. El origen de la entrada del perfil de la máquina es una plantilla de VMware. El perfil de la máquina captura las propiedades del hardware de una plantilla de VMware y las aplica a las máquinas virtuales recién aprovisionadas del catálogo.

> **Nota:**
>
> - La entrada de la imagen maestra (instantánea) y la entrada del perfil de la máquina (plantilla de VMware) deben tener las dos vTPM habilitado o inhabilitado. Esta regla se aplica tanto a `New-ProvScheme` como a `Set-ProvScheme`.
> - Si la imagen maestra tiene vTPM habilitado, la plantilla de VMware solo puede provenir del mismo origen de máquina virtual que la imagen maestra.
> - La directiva de almacenamiento cifrado solo admite la clonación completa.

La plantilla de VMware en el perfil de máquina debe existir durante el ciclo de vida del catálogo para permitir el aprovisionamiento de máquinas virtuales en el catálogo. Sin una plantilla de VMware, no puede aprovisionar nuevas máquinas virtuales. Al eliminar una plantilla de VMware, debe proporcionar una plantilla nueva mediante el comando `Set-ProvScheme`.

- MCS captura las propiedades de las plantillas de VMware. Puede crear otra plantilla de VMware que haga referencia a las propiedades almacenadas de la plantilla de VMware mediante el comando Get-Provscheme.
- Igualmente, si existen el catálogo de máquinas y las máquinas virtuales aprovisionadas, se puede usar una máquina aprovisionada de MCS para crear otra plantilla de VMware.

En función de cada sistema operativo, puede crear un catálogo de máquinas con diferentes configuraciones:

- Si Windows 11 está instalado en la imagen maestra, es necesario tener habilitado vTPM para la imagen maestra. Por lo tanto, la plantilla de VMware, que es el origen del perfil de la máquina, debe tener el vTPM conectado.
- Si Windows 10 está instalado en la imagen maestra sin ningún vTPM conectado, puede crear un catálogo de máquinas con una plantilla de VMware que no sea vTPM como origen para el perfil de la máquina.

Hay otra configuración en la que puede crear un catálogo de máquinas mediante el modo de disco de copia completa con una plantilla de perfil de máquina aplicada con una directiva de almacenamiento cifrado.

Para crear un catálogo de máquinas mediante los comandos de PowerShell con el perfil de la máquina como entrada:

1. Abra una ventana de **PowerShell**.
2. Ejecute `asnp citrix*`.
3. Ejecute los comandos siguientes:

   - Para crear un catálogo de máquinas con una plantilla de VMware con un vTPM conectado como origen para la entrada del perfil de la máquina y la imagen maestra instalada en Windows 11:

```
$identityPool = New-AcctIdentityPool  -IdentityPoolName "<
    string>"
-NamingScheme "<string>-###"
-NamingSchemeType Numeric
-Domain "<domain name"
-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme  -CleanOnBoot
-HostingUnitName "vSanRg"
-IdentityPoolName "<string>"
-InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits<hosting unit name><
    snapshot name>.snapshot"
-NetworkMapping @{
"0"="XDHyp:\HostingUnits<hosting unit name>\<network name>.
    network" }

-ProvisioningSchemeName "<string>"
-Scope @() -VMCpuCount 4
-VMMemoryMB 6144
-MachineProfile "XDHyp:\HostingUnits<hosting unit name><
    template name>.template" -TenancyType Shared
-FunctionalLevel "L7_20"
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"
-Description "<string>"
-IsRemotePC $False
-MinimumFunctionalLevel 'L7_9'
-Name "<catalog name>"
-ProvisioningType 'MCS'
-Scope @()
-SessionSupport "SingleSession" -ZoneUid "<Uid>"
```



```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- Para crear un catálogo de máquinas con una plantilla de VMware sin un vTPM como origen para el perfil de la máquina y la imagen maestra instalada en Windows 10:

```
$identityPool = New-AcctIdentityPool
-IdentityPoolName "<string>"
-NamingScheme "<string>-###" -NamingSchemeType Numeric
-Domain "<domain name>"
-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme
-CleanOnBoot -HostingUnitName "<string>"
-IdentityPoolName "<string>"
-InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits<hosting unit name><
   snapshot name>.snapshot
-NetworkMapping @{
"0"="XDHyp:\HostingUnits<hosting unit name>\<string>.network"
    }

-ProvisioningSchemeName "<string>"  -Scope @() -VMCpuCount 4
    -VMMemoryMB 8192
-MachineProfile "XDHyp:\HostingUnits<hosting unit name><
   template name>.template"
-TenancyType Shared  -FunctionalLevel "L7_20"
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"
-Description "<string>"
-IsRemotePC $False
-MinimumFunctionalLevel 'L7_9' -Name "<string>" -
   ProvisioningType 'MCS' -Scope @()
-SessionSupport "SingleSession" -ZoneUid "<Uid"
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

- Para crear un catálogo de máquinas mediante el modo de disco de copia completa con una plantilla de perfil de máquina aplicada con una directiva de almacenamiento cifrado:

```
$identityPool = New-AcctIdentityPool
-IdentityPoolName "<string>"
-NamingScheme "<string>-###"
-NamingSchemeType Numeric
-Domain "<domain name>"
-ZoneUid "<Uid>"  -Scope @()
```

```
$provScheme =New-ProvScheme
```



```
-HostingUnitName "<string>"
-IdentityPoolName "<string>"
-InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits<hosting unit name><
    snapshot name>.snapshot"
-NetworkMapping @{
"0"="XDHyp:\HostingUnits<hosting unit name>\<string>.network"
     }

-ProvisioningSchemeName "<string>"
-Scope @() -VMCpuCount 4  -VMMemoryMB 8192 -MachineProfile "
    XDHyp:\HostingUnits<hosting unit name><template name>.
    template"
-TenancyType Shared
-FunctionalLevel "L7_20" -UseFullDiskCloneProvisioning
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"
-Description "<string>"  -IsRemotePC $False
-MinimumFunctionalLevel 'L7_9'
-Name "<string>" -ProvisioningType 'MCS' -Scope @()
-SessionSupport "SingleSession" -ZoneUid "<Uid>"
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
```

Para actualizar un perfil de máquina, utilice el comando Set-ProvScheme. Por ejemplo:

```
Set-ProvScheme -ProvisioningSchemeName 'name' -IdentityPoolName 'name'
    -MachineProfile 'XDHyp:\HostingUnits<hosting unit name><template
    name>.template'
```

Comprobar la presencia de varias tarjetas NIC

Aparecen diversos mensajes de error durante las comprobaciones preliminares sobre presencia de varias tarjetas NIC cuando se usa un perfil de máquina y el parámetro `NetworkMapping` en los comandos `New-ProvScheme` y `Set-ProvScheme`.

La lista de verificación preliminar para detectar la presencia de varias tarjetas NIC es la siguiente:

- Solo se usa y valida el recuento de tarjetas NIC de la plantilla de perfil de la máquina. La red a la que apuntan estas tarjetas NIC no se usa ni se valida con respecto a las redes de la unidad de alojamiento.
- Si el recuento de tarjetas NIC en la plantilla de perfil de la máquina es mayor que el número de redes de la unidad de alojamiento, aparecerá un mensaje de error.

- Si el recuento de tarjetas NIC en la plantilla de perfil de la máquina es cero, aparecerá un mensaje de error.
  Cuando el recuento de tarjetas NIC en la plantilla de perfil de la máquina es uno, entonces:
  - If no network mapping is specified in the `New-ProvScheme` or `Set-ProvScheme` command, and the hosting unit network is one, then the hosting unit network is used.
  - If network mapping is specified, then the specified network mapping is used if it is valid.
- Cuando el recuento de tarjetas NIC en la plantilla de perfil de la máquina es superior a 1 o el recuento de redes de la unidad de alojamiento es superior a 1, entonces:
  - El comando requiere una asignación de red válida y debe proporcionar una asignación para cada tarjeta NIC (es decir, el recuento de NetworkMapping debe ser el mismo que el recuento de tarjetas NIC del perfil de máquina).
  - No se pueden asignar varias tarjetas NIC a la misma red en la unidad de alojamiento.
  - El recuento de `NetworkMapping` y el recuento de tarjetas NIC del perfil de máquina debe ser inferior o igual al recuento de redes de la unidad de alojamiento.
  - Se debe proporcionar `NetworkMapping` para cada ID comprendido entre 0 y n-1, donde n es el número de adaptadores de red de la plantilla del perfil de máquina.

Solución de problemas

Si no se puede crear el catálogo, consulte CTX294978.

Qué hacer a continuación

- Si este es el primer catálogo creado, Web Studio le guiará para crear un grupo de entrega
- Para revisar todo el proceso de configuración, consulte Instalar y configurar
- Para administrar catálogos, consulte Administrar catálogos de máquinas y Administrar un catálogo de VMware

Más información

- Crear y administrar conexiones y recursos
- Conexión con VMware
- Crear catálogos de máquinas

Crear catálogos de diferentes tipos de unión

August 17, 2024

Con MCS, puede aprovisionar máquinas como unidas a AD locales o unidas a Azure AD híbrido.

Para obtener información sobre cómo configurar identidades de máquinas en la interfaz de Web Studio, consulte Crear catálogos de máquinas.

Para obtener información específica sobre cómo crear catálogos unidos de identidades de máquinas, consulte lo siguiente:

- Crear catálogos unidos a Azure Active Directory híbrido

Crear catálogos unidos a Azure Active Directory híbrido

August 17, 2024

> **Nota:**
>
> Desde julio de 2023, Microsoft cambió el nombre de Azure Active Directory (Azure AD) a Microsoft Entra ID. En este documento, cualquier referencia a Azure Active Directory, Azure AD o AAD ahora se refiere a Microsoft Entra ID.

En este artículo se describe cómo crear catálogos unidos a Azure Active Directory (AD) híbrido.

Puede crear catálogos unidos a Azure AD mediante Web Studio o PowerShell.

Para obtener información sobre los requisitos, las limitaciones y los aspectos a tener en cuenta, consulte Unidos a Azure Active Directory híbrido.

Usar Web Studio

La información siguiente complementa a las instrucciones del artículo Crear catálogos de máquinas. Para crear catálogos unidos a Azure AD híbrido, siga las instrucciones generales de ese artículo y tenga en cuenta los detalles específicos sobre los catálogos unidos a Azure AD híbrido.

En el asistente para la creación de catálogos:

- En la página **Identidades de máquinas**, seleccione **Unido a Azure Active Directory híbrido**. Las máquinas creadas son propiedad de una organización en las que se ha iniciado sesión con una cuenta de Active Directory Dominio Services perteneciente a esa organización. Existen en la nube y en instancias locales.

> **Nota:**
>
> Si selecciona **Unido a Azure Active Directory híbrido** como el tipo de identidad, cada máquina del catálogo debe tener una cuenta de equipo de AD correspondiente.

Usar PowerShell

Estos son los pasos en PowerShell equivalentes a las operaciones en Web Studio. Para obtener información sobre cómo crear un catálogo con el SDK de PowerShell remoto, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

La diferencia entre los catálogos unidos a AD local y los unidos a Azure AD híbrido radica en la creación del grupo de identidades y las cuentas de máquina.

Para crear un grupo de identidades junto con las cuentas de los catálogos unidos a Azure AD híbrido:

```
1 New-AcctIdentityPool -AllowUnicode -IdentityType "HybridAzureAD" -
    Domain "corp.local" -IdentityPoolName "HybridAADJoinedCatalog" -
    NamingScheme "HybridAAD-VM-##" -NamingSchemeType "Numeric" -OU "CN=
    AADComputers,DC=corp,DC=local" -Scope @() -ZoneUid "81291221-d2f2-49
    d2-ab12-bae5bbd0df05"
2 New-AcctADAccount -IdentityPoolName "HybridAADJoinedCatalog" -Count 10
    -ADUserName "corp\admin1" -ADPassword $password
3 Set-AcctAdAccountUserCert -IdentityPoolName "HybridAADJoinedCatalog" -
    All -ADUserName "corp\admin1" -ADPassword $password
```

> **Nota:**
>
> `$password` es la contraseña correspondiente de una cuenta de usuario de AD con permisos de escritura.

Todos los demás comandos que se utilizan para crear catálogos unidos a Azure AD híbrido son los mismos que se usan para los catálogos tradicionales unidos a AD local.

Ver el estado del proceso de unión a Azure AD híbrido

En Web Studio, el estado del proceso de unión a Azure AD híbrido es visible cuando las máquinas unidas a Azure AD híbrido de un grupo de entrega están encendidas. Para ver el estado, utilice Buscar para identificar esas máquinas y, a continuación, para cada una de ellas, compruebe la **identidad de la máquina** en la ficha **Detalles** del panel inferior. Esta información puede aparecer en **Identidad de la máquina**:

- Unida a Azure AD híbrido
- Aún no se ha unido a Azure AD

> **Nota:**
>
> - Es posible que se produzca una demora en la unión a Azure AD híbrido cuando la máquina se enciende por primera vez. Esto se debe al intervalo de sincronización de identidad de máquina predeterminado (30 minutos de Azure AD Connect). La máquina se halla en estado unido a Azure AD híbrido solamente después de que las identidades de máquina se hayan sincronizado con Azure AD a través de Azure AD Connect.
> - Si las máquinas no están unidas a Azure AD híbrido, no se registran en el Delivery Controller. Su estado de registro aparece como **Inicialización**.

Además, mediante la interfaz de Web Studio, puede averiguar por qué las máquinas no están disponibles. Para ello, haga clic en una máquina del nodo **Buscar**, marque **Registro** en la ficha **Detalles** del panel inferior y, a continuación, lea el texto de ayuda para obtener información adicional.

Solucionar problemas

Si las máquinas no logran unirse a Azure AD híbrido, haga lo siguiente:

- Compruebe si la cuenta de máquina se ha sincronizado con Azure AD a través del portal de Microsoft Azure AD. Si se ha sincronizado, aparece **Aún no se ha unido a Azure AD**, que indica que el estado de registro está pendiente.

  Para sincronizar las cuentas de máquina con Azure AD, asegúrese de lo siguiente:

  - La cuenta de máquina está en la OU configurada para sincronizarse con Azure AD. Las cuentas de máquina sin el atributo **userCertificate** no se sincronizan con Azure AD aunque estén en la OU configurada para sincronizarse.
  - El atributo **userCertificate** se rellena en la cuenta de la máquina. Utilice Active Directory Explorer para ver el atributo.
  - Azure AD Connect debe haberse sincronizado al menos una vez después de haber creado la cuenta de máquina. Si no es el caso, ejecute manualmente el comando `Start-ADSyncSyncCycle -PolicyType Delta` en la consola de PowerShell de la máquina de Azure AD Connect para activar una sincronización inmediata.

- Para comprobar si el par de claves de dispositivos administrados por Citrix para la unión a Azure AD híbrido se ha insertado correctamente en la máquina, consulte el valor de **DeviceKeyPairRestored** en **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix**.

  Verifique que el valor sea 1. Si no es así, he aquí una serie de posibles razones:

  - `IdentityType` del grupo de identidades asociado al esquema de aprovisionamiento no está configurado en `HybridAzureAD`. Para comprobarlo, ejecute `Get-AcctIdentityPool`.

  - La máquina no se aprovisiona con el mismo esquema de aprovisionamiento del catálogo de máquinas.
  - La máquina no está unida al dominio local. La unión al dominio local es un requisito previo para la unión a Azure AD híbrido.

- Para comprobar los mensajes de diagnóstico, ejecute el comando `dsregcmd /status /debug` en la máquina aprovisionada por MCS.

  - Si la unión a Azure AD híbrido se realiza correctamente, **AzureAdJoined** y **DomainJoined** son **YES** en el resultado de la línea de comandos.
  - Si no es así, consulte la documentación de Microsoft para solucionar los problemas: https://docs.microsoft.com/en-us/azure/active-directory/devices/troubleshoot-hybrid-join-windows-current.
  - Si recibe el mensaje de error **Server Message: The user certificate is not found on the device with id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx**, ejecute el siguiente comando de PowerShell para reparar el certificado de usuario:

    ```
    1  Repair-AcctIdentity -IdentityAccountName TEST\VM1 -Target
          UserCertificate
    ```

    Para obtener más información sobre el problema del certificado de usuario, consulte CTX566696.

Administrar catálogos de máquinas

August 20, 2024

> **Nota:**
>
> Puede administrar la implementación de Citrix Virtual Apps and Desktops mediante dos consolas de administración: Web Studio (basada en la web) y Citrix Studio (basada en Windows). Este artículo se refiere únicamente a Web Studio. Para obtener información sobre Citrix Studio, consulte el artículo equivalente en Citrix Virtual Apps and Desktops 7 2212 o versiones anteriores.

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.

El mantenimiento de catálogos también puede incluir comprobar que cada máquina tenga las últimas actualizaciones del sistema operativo. Aquí se incluyen las actualizaciones de antivirus y del sistema operativo o los cambios de configuración.

- 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 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 Web 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 para alojar hipervisores, 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.

Administrar catálogos de máquinas

Puede administrar un catálogo de máquinas de dos maneras:

- Mediante Web Studio
- Uso de PowerShell

Usar Web Studio

En esta sección se detalla cómo puede administrar los catálogos con Web Studio:

- Administrar catálogos de máquinas
  - Introducción
  - Acerca de las instancias persistentes
- Administrar catálogos de máquinas
- Usar Web Studio
- Ver detalles de un catálogo
  - Agregar máquinas a un catálogo
  - Eliminar máquinas de un catálogo
- Modificar un catálogo
- Cambiar el nombre de un catálogo
- Mover un catálogo a otra zona
- Eliminar un catálogo
- Administrar cuentas de equipo de Active Directory en un catálogo
- Actualizar un catálogo
  - Actualizar o crear una imagen maestra
  - Cambiar la imagen maestra
  - Revertir la imagen maestra
- Cambiar el nivel funcional o deshacer el cambio
- Clonar un catálogo
- Organizar los catálogos por medio de carpetas
  - Crear una carpeta de catálogo
  - Mover un catálogo
  - Administrar carpetas de catálogos
- Reintentar la creación de catálogos
- Inscribir agentes VDA no aprovisionados por MCS mediante tokens (Technical Preview)
- Usar PowerShell
- Recuperar advertencias y errores asociados a un catálogo
- Habilitar la programación de reinicios únicos
- Agregar descripciones a una imagen

- Restablecer disco de SO
- Cambiar el parámetro de red de un esquema de aprovisionamiento existente
- Administrar versiones de un catálogo de máquinas
- Convertir un catálogo de máquinas no basado en perfiles de máquina en un catálogo de máquinas basado en perfiles de máquina
- Reparar la información de identidad de las cuentas de equipo activas
  - Condiciones
  - Restablecer disco de identidad
- Cambiar la configuración de la caché en un catálogo de máquinas existente
  - Requisitos
  - Cambiar la configuración de caché
- Compatibilidad con la actualización de VDA mediante acceso a recursos compartidos de archivos locales
  - Cmdlets de PowerShell
  - Requisitos previos
  - Cómo configurar los permisos de los recursos compartidos de archivos
  - Actualizaciones de VDA desde un recurso compartido de archivos local
- Solucionar problemas
- Qué hacer a continuación

Ver detalles de un catálogo

1. Use la función de búsqueda para localizar un catálogo de máquinas específico. Para obtener instrucciones, consulte Buscar instancias.
2. En los resultados de la búsqueda, seleccione un catálogo según sea necesario.
3. Consulte la siguiente tabla para ver las descripciones de las columnas del catálogo.
4. Haga clic en una ficha del panel de detalles inferior para obtener más información sobre este catálogo.

Columna	Descripción
Catálogo de máquinas	El nombre y el tipo de asignación del catálogo. Los tipos de asignación incluyen Aleatoria: Las máquinas del catálogo se asignan a un usuario de forma aleatoria. Permanente: Las máquinas del catálogo se asignan a un usuario de forma permanente.
Tipo de máquina	El tipo de sesión admitido de las máquinas del catálogo. Los posibles valores incluyen Tipo de sistema operativo: SO multisesión (virtual); Datos de usuario: Descartar. Tipo de sistema operativo: SO multisesión (virtual); Datos de usuario: En disco local Tipo de sistema operativo: SO de sesión única (acceso con Remote PC)

Columna	Descripción
Recuento de máquinas	El recuento de máquinas en el catálogo y el método de aprovisionamiento. Los métodos de aprovisionamiento posibles incluyen: Machine Creation Services (máquina de MCS), Manual y Citrix Provisioning Services.
Recuento asignado	La cantidad de máquinas del catálogo asignadas a un grupo de entrega.
Carpeta	La ubicación del catálogo en el árbol de **Catálogos de máquinas**. Muestra el nombre de la carpeta en la que se encuentra el catálogo (incluida la barra invertida al final) o − si el catálogo está en el nivel raíz.
Actualización de versión de VDA	Estado de la actualización de versión de VDA. Entre los valores posibles se incluyen: No configurado, Programado, Disponible y Actualizado.
Estado de la imagen	El estado de actualización de la imagen del catálogo. Solo se aplica a los catálogos de máquinas no persistentes. Los valores posibles incluyen: Totalmente actualizada, Parcialmente actualizada, Actualizaciones pendientes y En preparación

Agregar máquinas a un catálogo

Antes de comenzar:

- Compruebe que el host de virtualización 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 Web 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. Inicie sesión en Web Studio.
2. Seleccione **Catálogos de máquinas** en el panel de la izquierda.
3. Seleccione un catálogo de máquinas y, a continuación, seleccione **Agregar máquinas** en la barra de acciones.
4. Seleccione la cantidad de máquinas virtuales que se van a agregar.
5. 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 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.
6. 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. Web Studio administra estas cuentas. Por eso, permita que Web 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 Web 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. Inicie sesión en Web Studio.
2. Seleccione **Catálogos de máquinas** en el panel de la izquierda.
3. Seleccione un catálogo y, a continuación, seleccione **Ver máquinas** en la barra de acciones.

4. Seleccione una o varias máquinas y, a continuación, seleccione **Eliminar** en la barra de acciones.

Elija si se eliminarán las máquinas que se van a quitar. Si opta por eliminar las máquinas, indique si las cuentas de Active Directory de esas máquinas deberán conservarse, inhabilitarse o eliminarse.

Modificar un catálogo

1. En la página **Descripción**, cambie la descripción del catálogo.
2. Seleccione **Catálogos de máquinas** en el panel de la izquierda.
3. Seleccione un catálogo y, a continuación, seleccione **Modificar catálogo de máquinas** en la barra de acciones.
4. En la página **Ámbitos**, cambie los ámbitos.
5. En la página de tarjetas **NIC**, haga lo siguiente:

   - Para cambiar la asignación de subredes de una NIC, seleccione una red en el campo **Red asociada**.
   - Para agregar una asignación de subred, seleccione **Agregar NIC**, seleccione una red en el campo **Red asociada** y haga clic en **Guardar**.

   Solo las subredes presentes en el host asociado al catálogo aparecen en el campo **Red asociada**.

   Solo se puede agregar NIC a los catálogos de máquinas de Azure sin perfiles de máquina.

   > **Nota:**
   >
   > - En el caso de los catálogos de máquinas de AWS, no se puede asignar la misma subred a más de una NIC.
   > - En el caso de los catálogos de máquinas con perfiles de máquina, la cantidad de NIC del catálogo debe ser igual a la cantidad de NIC del perfil de la máquina.
   > - Esta función no es compatible con los hipervisores de IBM Cloud.
   > - Esta función solo es compatible con Nutanix Prism Element en el caso de los hipervisores Nutanix.

6. Es posible que aparezcan otras páginas, según el tipo de catálogo.

   Para los catálogos creados con una imagen de Azure Resource Manager, se ven las siguientes páginas. Tenga en cuenta que los cambios que haga se aplican solo a las máquinas que agregue al catálogo más adelante. Las máquinas existentes permanecen sin cambios.

   - En la página **Máquinas virtuales**, cambie el tamaño de la máquina y las zonas de disponibilidad donde quiera crear máquinas.

> **Nota:**
>
> – Solo se muestran los tamaños de máquina que admite el catálogo.
> – Si es necesario, seleccione **Mostrar solo los tamaños de máquinas utilizados en otros catálogos de máquinas** para filtrar la lista de tamaños de máquinas.

- En la página **Perfil de máquina**, elija si quiere usar o cambiar un perfil de máquina.
- (Solo visible cuando el catálogo está configurado con un host de grupo dedicado) En la página **Grupo de hosts dedicado**, elija si quiere cambiar un grupo de hosts.
- En la página **Tipos de almacenamiento y licencias**, elija si quiere cambiar el tipo de almacenamiento, el tipo de licencia y los parámetros de Azure Computer Gallery (disponibles solo cuando se usa **Colocar la imagen preparada en Azure Gallery**).

> **Nota:**
>
> Si el parámetro recién seleccionado no es compatible con el tamaño actual de la máquina, aparece un cuadro de diálogo de advertencia que le informa de que, al cambiar el parámetro, se restablecerá el parámetro de tamaño de la máquina. Si decide continuar, aparecerá un punto rojo junto al menú **Máquinas virtuales** que le pedirá que seleccione un nuevo tamaño de máquina.

- En la página **Tipo de licencia**, elija si quiere cambiar la configuración de la licencia de Windows o de Linux.

Para los catálogos de acceso con Remote PC, se muestran las siguientes páginas:

- En la página **Administración de energía**, cambie los parámetros de administración de energía y seleccione una conexión de administración de energía.
- En la página **Unidades organizativas**, agregue o quite unidades organizativas de Active Directory.

7. Haga clic en **Aplicar** para aplicar los cambios realizados y haga clic en **Guardar** para salir.

Cambiar el nombre de un catálogo

1. Inicie sesión en Web Studio.
2. Seleccione **Catálogos de máquinas** en el panel de la izquierda.
3. Seleccione un catálogo y, a continuación, seleccione **Cambiar nombre de catálogo de máquinas** en la barra de acciones.
4. 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.

Mover un catálogo a otra zona que no sea el hipervisor que contiene las máquinas virtuales de ese catálogo puede afectar al rendimiento.

1. Inicie sesión en Web Studio.
2. Seleccione **Catálogos de máquinas** en el panel de la izquierda.
3. Seleccione un catálogo y, a continuación, seleccione **Mover** en la barra de acciones.
4. 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. Inicie sesión en Web Studio.
2. Seleccione **Catálogos de máquinas** en el panel de la izquierda.
3. Seleccione un catálogo y, a continuación, seleccione **Eliminar catálogo de máquinas** en la barra de acciones.
4. Indique si las máquinas del catálogo deberán eliminarse. Si opta por eliminar máquinas, indique si las cuentas de equipo de Active Directory de esas máquinas deberán 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. Inicie sesión en Web Studio.
2. Seleccione **Catálogos de máquinas** en el panel de la izquierda.
3. Seleccione un catálogo y, a continuación, seleccione **Administrar cuentas de AD** en la barra de acciones.
4. 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. Al introducir una contraseña, cambiará la contraseña en las cuentas a medida que se importan. Al eliminar una cuenta, deberá elegir si la cuenta de Active Directory debe mantenerse, inhabilitarse o eliminarse.

Indique si las cuentas de Active Directory se deberán conservar, inhabilitar o eliminar cuando quite máquinas de un catálogo o elimine un catálogo.

Actualizar un catálogo

Se 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. Revierta 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. De esta forma, se minimiza el tiempo de inactividad de los usuarios. No elimine, mueva o cambie el nombre de las imágenes maestras. No se puede revertir un catálogo para utilizarlas.

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, 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. Apague la máquina virtual.
5. Cree una instantánea de la máquina virtual. Asígnele un nombre significativo fácilmente reconocible cuando el catálogo se actualice en Web Studio. Aunque Web Studio puede crear una instantánea, Citrix recomienda crearla desde la consola de administración del hipervisor. A continuación, seleccione esa instantánea en Web Studio. Este proceso 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 XenCenter de XenServer.

Cambiar la imagen maestra

Para preparar y aplicar la actualización a todas las máquinas de un catálogo:

1. Inicie sesión en Web Studio.
2. Seleccione **Catálogos de máquinas** en el panel de la izquierda.
3. Seleccione un catálogo y, a continuación, seleccione **Cambiar imagen maestra** en la barra de acciones.
4. En la página **Imagen**, seleccione el host y la imagen que quiere implantar.

   > **Sugerencia:**
   >
   > Para un catálogo creado con MCS, puede anotar su imagen agregando una nota para la imagen. Una nota puede contener hasta 500 caracteres. Cada vez que cambia la imagen maestra, se crea una entrada con una nota relacionada, independientemente de si agrega o no una nota. Si actualiza un catálogo sin agregar una nota, la entrada aparece como nula (-). Para ver el historial de notas de la imagen, seleccione el catálogo, haga clic en **Propiedades de plantilla** en el panel inferior y, a continuación, haga clic en **Ver historial de notas**.

5. 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).

   > **Nota:**
   >
   > La página **Estrategia de implementación** no está disponible para las máquinas virtuales persistentes porque la implementación solo se aplica a las máquinas virtuales no persistentes.

6. En la página **Resumen**, revise la información y haga clic en **Finalizar**. Cada máquina se reiniciará automáticamente después de actualizarse.

Para hacer un seguimiento del progreso de la actualización, busque el catálogo en **Catálogos de máquinas** para ver la barra de progreso integrada y el gráfico de progreso detallado.

Al actualizar un catálogo directamente mediante el SDK de PowerShell, en lugar de Web Studio, especifique una plantilla de hipervisor (**VMTemplates**). Esto sirve de alternativa a una imagen o a una instantánea de una imagen.

Estrategia de implantación:

La actualización de las imágenes 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 SO de sesión única se actualizan inmediatamente cuando no se están usando o cuando los usuarios no han iniciado sesión en ellas.
- Para un SO multisesión 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 habilitar la programación de reinicios únicos mediante PowerShell, consulte Habilitar la programación de reinicios únicos.

Revertir la imagen maestra

Después de aplicar una imagen maestra nueva o actualizada, puede revertirla. Este proceso 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 están disponibles. Al igual que en la implantación, la reversión de una máquina implica un reinicio.

1. Inicie sesión en Web Studio.
2. Seleccione **Catálogos de máquinas** en el panel de la izquierda.
3. Seleccione el catálogo y, a continuación, seleccione **Revertir imagen maestra** en la barra de acciones.
4. Puede especificar cuándo se aplicará la versión anterior de la imagen maestra a las máquinas, de la manera que se describe en la sección anterior, en la operación de implantación.

La reversión solo se aplica a máquinas que deben revertirse. Las máquinas que no se actualizan con la imagen maestra nueva o actualizada no reciben mensajes de notificación y no se ven obligadas a cerrar la sesión.

Para hacer un seguimiento del progreso de la reversión, busque el catálogo en **Catálogos de máquinas** para ver la barra de progreso integrada y el gráfico de progreso detallado.

Cambiar el nivel funcional o deshacer el cambio

Cambie el nivel funcional del catálogo de máquinas después de actualizar la versión de 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 cambiar el nivel funcional de un catálogo de máquinas:

- Inicie las máquinas actualizadas para que se registren con el Controller. Este proceso permite a Web Studio determinar si las máquinas del catálogo necesitan actualización.

Para cambiar el nivel funcional de un catálogo:

1. Inicie sesión en Web Studio.
2. Seleccione **Catálogos de máquinas** en el panel de la izquierda.
3. Seleccione el catálogo. En la ficha **Detalles** del panel inferior, se muestra la información de versión.
4. Seleccione **Cambiar nivel funcional**. Si Web 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. Para garantizar que todas las máquinas funcionen correctamente, Citrix recomienda resolver los problemas de la máquina antes de hacer clic en **Cambiar**.

Después de completar el cambio del catálogo, puede revertir las máquinas a sus versiones anteriores de VDA. Para ello, seleccione el catálogo y, a continuación, seleccione **Deshacer cambio de nivel funcional** en la barra de acciones.

Clonar un catálogo

Antes de clonar un catálogo, tenga en cuenta esto:

- No se pueden cambiar los parámetros asociados a la administración de máquinas y al sistema operativo. El catálogo clonado hereda esos parámetros del original.
- La clonación de un catálogo puede tardar en completarse. Si es necesario, selecciona **Ocultar progreso** para realizar la clonación en segundo plano.

- El catálogo clonado hereda el nombre del original y tiene el sufijo Copy. Puede cambiarle el nombre. Consulte Cambiar el nombre de un catálogo.
- Una vez finalizada la clonación, asegúrese de asignar el catálogo clonado a un grupo de entrega.

1. Inicie sesión en Web Studio y, a continuación, seleccione **Catálogos de máquinas** en el panel de la izquierda.
2. Seleccione un catálogo y, a continuación, seleccione **Clonar** en la barra de acciones.
3. En la ventana **Clonar catálogo de máquinas seleccionado**, consulte los parámetros del catálogo clonado y configúrelos según corresponda. Seleccione **Siguiente** para pasar a la página siguiente.
4. En la página **Resumen**, verá un resumen de los parámetros. Seleccione **Finalizar** para iniciar la clonación.
5. Si es necesario, selecciona **Ocultar progreso** para realizar la clonación en segundo plano.

Organizar los catálogos por medio de carpetas

Puede crear carpetas para organizar los catálogos y acceder a ellos fácilmente. Por ejemplo, puede organizar los catálogos por tipo de imagen o por estructura organizativa.

Crear una carpeta de catálogo

Antes de empezar, planifique cómo organizar sus catálogos. Se deben tener en cuenta las siguientes cuestiones:

- Puede anidar carpetas con hasta cinco niveles de profundidad (excluyendo la carpeta raíz predeterminada).
- Una carpeta de catálogo puede contener catálogos y subcarpetas.
- Todos los nodos de Web Studio (como los nodos **Catálogos de máquinas** y **Aplicaciones**) comparten un árbol de carpetas en el back-end. Para evitar conflictos de nombres con otros nodos al cambiar el nombre de las carpetas o moverlas, le recomendamos que asigne nombres diferentes a las carpetas de primer nivel de los distintos nodos.

Para crear una carpeta de catálogo, siga estos pasos:

1. Seleccione **Catálogos de máquinas** en el panel de la izquierda.
2. En la jerarquía de carpetas, seleccione una carpeta y, a continuación, seleccione **Crear carpeta** en la barra de **acciones**.
3. Introduzca un nombre para la nueva carpeta y, a continuación, haga clic en **Listo**.

> **Sugerencia:**
>
> Si crea una carpeta en una ubicación no deseada, puede arrastrarla a la ubicación correcta.

Mover un catálogo

Puede mover un catálogo entre carpetas. Estos son los pasos detallados:

1. Seleccione **Catálogos de máquinas** en el panel de la izquierda.
2. Ver los catálogos por carpeta. También puede activar **Ver todo** por encima de la jerarquía de carpetas para ver todos los catálogos a la vez.
3. Haga clic con el botón secundario en un catálogo y, a continuación, seleccione **Mover catálogo de máquinas**.
4. Seleccione la carpeta a la que quiere mover el catálogo y, a continuación, haga clic en **Listo**.

> **Sugerencia:**
>
> Puede arrastrar un catálogo a una carpeta.

Administrar carpetas de catálogos

Puede eliminar, cambiar el nombre y mover las carpetas de catálogos.

Solo puede eliminar una carpeta si esta y sus subcarpetas no contienen catálogos.

Para administrar una carpeta, siga estos pasos:

1. Seleccione **Catálogos de máquinas** en el panel de la izquierda.
2. En la jerarquía de carpetas, seleccione una carpeta y, a continuación, seleccione una acción en la barra de **acciones**:
   - Para cambiar el nombre de la carpeta, seleccione **Cambiar nombre de carpeta**.
   - Para eliminar la carpeta, seleccione **Eliminar carpeta**.
   - Para mover la carpeta, seleccione **Mover carpeta**.
3. Siga las instrucciones que aparecen en pantalla para completar los pasos restantes.

Reintentar la creación de catálogos

> **Nota:**
>
> Esta función solo se aplica a catálogos de MCS.

Los catálogos con errores se marcan con un icono de error. Para ver los detalles, vaya a la ficha **Solucionar problemas** de cada catálogo. Antes de reintentar la creación de catálogos, tenga en cuenta estas consideraciones:

- Compruebe primero la información sobre la solución de problemas y resuelva los problemas. La información describe los problemas encontrados y proporciona recomendaciones para resolverlos.
- No se pueden cambiar los parámetros asociados a la administración de máquinas y al sistema operativo. El catálogo hereda esos parámetros del original.
- La creación puede tardar un tiempo en completarse. Si es necesario, seleccione **Ocultar progreso** para realizar la creación en segundo plano.

Para intentar de nuevo la creación de un catálogo, haga lo siguiente:

1. En Web Studio, seleccione **Catálogos de máquinas** en el panel de la izquierda.
2. Seleccione el catálogo y, a continuación, vaya a la ficha **Solucionar problemas**.
3. Haga clic en el hipervínculo Reintentar para intentar crear el catálogo de nuevo.
4. En el asistente que aparece, cambie los parámetros donde sea necesario. Si no necesita realizar ningún cambio, puede ir directamente a la página **Resumen**.
5. Cuando termine, seleccione **Finalizar** para iniciar la creación.

Inscribir agentes VDA no aprovisionados por MCS mediante tokens (Technical Preview)

Ahora puede generar y administrar tokens de inscripción para los VDA no aprovisionados por MCS. Esta implementación permite el registro de VDA a través de WebSocket sin aprovisionar los VDA con MCS. Esta función también es compatible con Linux Virtual Delivery Agent, Citrix Virtual Delivery Agent para macOS y agentes VDA no unidos a un dominio con Citrix Virtual Apps and Desktops.

Antes de comenzar

1. Configure el sitio. Para obtener más información, consulte Crear un sitio.
2. Instale los certificados TLS en los Delivery Controllers. Para obtener más información, consulte Instalar certificados de servidor TLS en los Controllers.
3. Instale la CA raíz y la CA intermedia en el VDA para confiar en el Delivery Controller.
4. Habilite la conexión WebSocket en el Delivery Controller. Ejecute el siguiente comando en cada Delivery Controller presente en su sitio:

```
New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\WorkerProxy"
    -Name "WebSocket_Enabled" -PropertyType "DWord" -Value 1 -
   Force
```


> **Nota:**
>
> Asegúrese de reiniciar los Delivery Controllers después de habilitar el WebSocket.

Generar tokens de inscripción

Cuando decida habilitar la inscripción basada en tokens para máquinas aprovisionadas que no sean de Citrix, primero debe generar tokens por catálogo de máquinas y después compartirlos con los administradores de instalación de VDA.

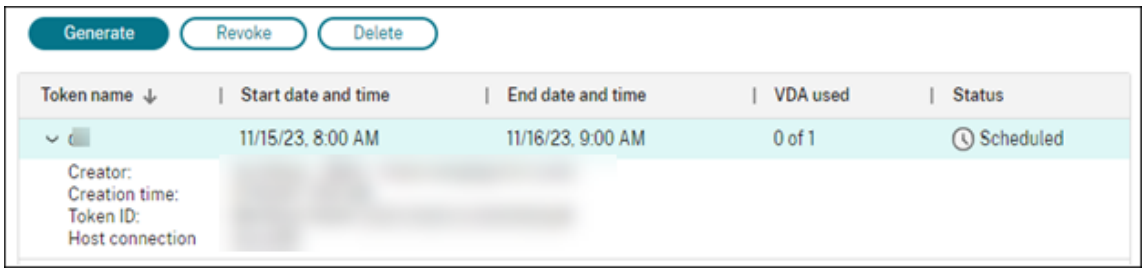
Un token de inscripción incluye:

- Rango de registro: de 1 a 100 máquinas VDA
- Periodo de validez: hasta 14 días

Para generar un token para un catálogo mediante Web Studio, siga estos pasos:

1. En **Web Studio > Catálogos de máquinas**, busque un catálogo que no esté aprovisionado por MCS y que muestre **Método de aprovisionamiento: Manual** en la columna **Recuento de máquinas**.
2. Haga clic con el botón secundario en el catálogo y después seleccione **Administrar tokens de inscripción**.
3. En la página **Generar token de inscripción** que se muestra, introduzca la siguiente información sobre el token:
   - Escriba un nombre para el token.
   - Introduzca su período de validez. El período no debe ser superior a 14 días. El token solo es válido durante el período especificado.
   - (Opcional) Seleccione una conexión de host para administrar la energía de los VDA inscritos con el token. Las opciones incluyen todas las conexiones de host de la zona de este catálogo.
   - Introduzca los límites de uso del token (entre 1 y 100).
4. Haga clic en **Generar**.
5. En la ventana **Token generado correctamente** que se muestra, cópielo y guárdelo en un lugar seguro, o haga clic en **Descargar** para descargarlo en la carpeta **Descargas**.

   Se muestra un registro de token en la lista de tokens.



6. Comparta el token con los administradores de instalación del VDA.

   Para obtener más información sobre cómo instalar un VDA y un token en las máquinas, consulte Instalar agentes VDA.

Administrar tokens

Tiene dos opciones para revocar un token y hacer que no esté disponible para la inscripción de VDA:

- Revocar: revoca el token pero lo conserva en la lista para fines de registro.
- Eliminar: revoca el token y lo elimina de la lista.

> **Nota:**
>
> Los tokens caducados se eliminan automáticamente en 14 días.

Inscribir máquinas en catálogos mediante la herramienta de inscripción de VDA de WebSocket

La herramienta de inscripción de VDA de WebSocket facilita la inscripción basada en tokens para máquinas VDA. Esta herramienta le ayuda a convertir una conexión en una conexión de WebSocket agregando el VDA al catálogo de máquinas mediante el token de inscripción.

> **Nota:**
>
> Esta herramienta está diseñada para inscribir máquinas VDA que no se han inscrito en ningún catálogo de máquinas.

Siga las instrucciones para ejecutar la herramienta de inscripción:

1. Inicie sesión en el VDA.
2. Localice la herramienta `EnrollMachine.exe`, en `C:\Program Files\Citrix\Virtual Desktop Agent\Web Socket Vda Enrollment Tool`.
3. Ejecute la herramienta con los parámetros de entrada apropiados. Por ejemplo, `EnrollMachine.exe -websocket_token_string:xxxxxxxxx`

En la siguiente tabla se describen los parámetros de entrada de la herramienta de inscripción:

Nombre del parámetro	Si son necesarias	Descripción	Ejemplo
-websocket_token_stdin	Sí	Lee el token de inscripción.	.\EnrollMachine.exe -websocket_token_stdin
-websocket_token_string		Lee el token de inscripción directamente desde el parámetro de la línea de comandos.	.\EnrollMachine.exe -websocket_token_string:<token>
-websocket_token_file:[token-file-path]		Lee el token de inscripción de la ruta proporcionada.	.\EnrollMachine.exe -websocket_token_file:C:\token\test2.txt
log:[log-file-path]	No	Muestra los registros de la herramienta de inscripción.	.\EnrollMachine.exe log:[C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt]
-help	No	Muestra un breve texto de ayuda.	.\EnrollMachine.exe -help

Una vez que se haya inscrito correctamente, recibirá un mensaje de confirmación en la herramienta y en los registros. Asegúrese de iniciar sesión en Web Studio para verificar que la máquina VDA se ha agregado al catálogo y que el estado de la máquina está registrado.

Solución de problemas De forma predeterminada, puede encontrar los registros de la herramienta de inscripción en:

`C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt`

Si ha especificado una ruta diferente para los registros, puede usar `log:[log-file-path]` para recuperarlos.

En la siguiente tabla se enumeran los códigos devueltos por la herramienta de inscripción:

Código	Cadena	Descripción
0	Success	Un VDA se agregó correctamente al catálogo de máquinas.
-1	InvalidArgument	El parámetro de entrada del token de inscripción no es válido.
-2	BrokerAgentNotFound	No se encuentra el servicio de agente intermediario.
-3	TokenInvalid	El token introducido no es válido.
-4	TokenMissingRequiredClaims	Faltan las notificaciones necesarias para el token, por ejemplo, CustomerId o los URI de inscripción.
-5	InternalError	Se ha producido un error general.
-6	TimedOut	Se ha agotado el tiempo de espera de la tarea.
-7	FailedToDetermineMachineADJoinStatus	El servicio que devuelve el estado de unión al AD de la máquina falló.
-8	ADMachineFailedToFindSid	El servicio que devuelve el Sid de la máquina de AD falló.
-9	EnrollRequestFailed	La solicitud falló debido a un error de HTTP.
-10	EnrollResponseMissingRequiredFields	A la respuesta de la herramienta de inscripción le falta el parámetro `VirtualSiteId`.
-11	InsufficientPermission	No tiene los permisos necesarios para ejecutar la tarea.
-12	FailedToDetermineMachineAadJoinStatus	El servicio que comprueba el estado de unión al AD de la máquina devuelve un error.

Código	Cadena	Descripción
-13	AadMachineFailedToFindDeviceId	El parámetro adicional `AAD device id` agregado por el sistema está vacío.
-14	AadDeviceIdNotValid	El parámetro adicional `AAD device id` agregado por el sistema no es un GUID válido.
-15	NoValidMacAddress	Dirección MAC no válida.
-16	FailedToGetComputerHostNameForVdaInstanceName	No se pudo obtener el nombre de host del equipo para establecer el parámetro adicional `VdaInstanceName`.
-17	VirtualDesktopAgentRegistryKeyFailedToOpen	No se pudo abrir la clave de registro del VDA para escribir la lista de los Delivery Controller.
-18	Se alcanzó el recuento máximo de token fallidos	Se alcanzó el recuento máximo de token fallidos.

Usar PowerShell

En esta sección se detalla cómo puede administrar catálogos con PowerShell:

- Recuperar advertencias y errores asociados a un catálogo
- Habilitar la programación de reinicios únicos
- Agregar descripciones a una imagen
- Restablecer disco de SO
- Cambiar el parámetro de red de un esquema de aprovisionamiento existente
- Administrar versiones de un catálogo de máquinas
- Convertir un catálogo de máquinas no basado en perfiles de máquina en un catálogo de máquinas basado en perfiles de máquina
- Reparar la información de identidad de las cuentas de equipo activas
- Cambiar la configuración de la caché en un catálogo de máquinas existente
- Compatibilidad con la actualización de VDA mediante acceso a recursos compartidos de archivos locales

Recuperar advertencias y errores asociados a un catálogo

Puede obtener advertencias y errores históricos para comprender los problemas de su catálogo de máquinas de MCS y corregirlos.

Con los comandos de PowerShell, puede:

- Obtener una lista de errores o advertencias
- Cambiar el estado de una advertencia de **New** a **Acknowledged**
- Eliminar los errores o las advertencias

Para ejecutar los comandos de PowerShell:

1. Abra una ventana de PowerShell.
2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.

Para obtener una lista de errores y advertencias:

Ejecute el comando `Get-ProvOperationEvent`.

- Sin parámetros: Obtiene todas las advertencias.
- Con los parámetros `LinkedObjectType` y `LinkedObjectUid`: Obtiene todos los errores y advertencias asociados a un esquema de aprovisionamiento específico.
- Con el parámetro `EventId`: Obtiene errores o advertencias específicos que coinciden con este ID de evento.
- Con el parámetro `Filter`: Obtiene errores o advertencias mediante un filtro personalizado.

Para cambiar el estado de los errores o advertencias de **New** a **Acknowledged**:

Ejecute el comando `Confirm-ProvOperationEvent`.

- Con el parámetro `EventId`: Configura el estado de errores o advertencias específicos que coinciden con este ID de evento. Puede obtener el `EventId` de un error o advertencia específico como resultado del comando `Get-ProvOperationEvent`
- Con los parámetros `LinkedObjectType` y `LinkedObjectUid`: Configura el estado de todos los errores y advertencias asociados a un esquema de aprovisionamiento específico.
- Con el parámetro `All`: Configura el estado de todos los errores y advertencias como **Acknowledged**.

Para eliminar los errores o advertencias:

Ejecute el comando `Remove-ProvOperationEvent`.

- Con el parámetro `EventId`: Quita errores o advertencias específicos que coinciden con este ID de evento Puede obtener el `EventId` de un error o advertencia específico como resultado del comando `Get-ProvOperationEvent`

- Con los parámetros `LinkedObjectType` y `LinkedObjectUid`: Quita todos los errores y advertencias asociados a un esquema de aprovisionamiento específico.
- Con el parámetro `All`: Quita todas las advertencias.

Para obtener más información, consulte SDK de PowerShell de Citrix.

Eliminar máquinas sin acceder al hipervisor

Al eliminar una máquina virtual o un esquema de aprovisionamiento, MCS necesita quitar etiquetas de la máquina virtual y, a veces, también del disco base, para que MCS deje de rastrear o identificar los recursos incluidos en las opciones de eliminación. Sin embargo, algunos de estos recursos solo son accesibles a través del hipervisor. Utilice la opción `PurgeDBOnly` de PowerShell `Remove-ProvVM` para eliminar de la base de datos objetos de recursos de VM, como la máquina virtual, el disco base o la imagen en ACG incluso cuando no se pueda acceder al hipervisor.

Esta opción está habilitada en:

- Todos los hipervisores compatibles
- Máquinas virtuales persistentes y no persistentes

Limitaciones

No puede usar los comandos -PurgeDBOnly y -ForgetVM al mismo tiempo.

Usar el comando PurgeDBOnly

Al ejecutar el comando de PowerShell `Remove-ProvVM -ProvisioningSchemeName SCVMM -MC -VMName SCVMM01 -ForgetVM`, es posible que la operación de eliminación falle en estos casos:

- La conexión de host está en modo de mantenimiento
- Credenciales no válidas
- Fallo de autenticación
- Operación no autorizada
- No se puede contactar con el hipervisor

> **Nota:**
>
> Remove-provVM -ForgetVM se dirige solamente a máquinas virtuales persistentes. Si una de las máquinas virtuales de la lista no es persistente, se produce un error en la operación.

Cuando la operación falla porque no se puede contactar con el hipervisor, aparece este mensaje:

```
Try to use -PurgeDBOnly option to clean DDC database.
```

Utilice la opción `-PurgeDBOnly` del comando `Remove-ProvVM` de PowerShell para eliminar de la base de datos de MCS referencias de máquinas virtuales. Por ejemplo,

```
Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -
PurgeDBOnly
```

Habilitar la programación de reinicios únicos

Si quiere habilitar la programación de reinicio único con PowerShell, use estos comandos `BrokerCatalogRebootSchedule` de PowerShell para crear, modificar y eliminar una programación de reinicio:

- Get-BrokerCatalogRebootSchedule
- New-BrokerCatalogRebootSchedule
- Set-BrokerCatalogRebootSchedule
- Remove-BrokerCatalogRebootSchedule
- Rename-BrokerCatalogRebootSchedule

Por ejemplo,

- Para crear una programación de reinicio de las máquinas virtuales del catálogo denominado **Cajeros** que comience el 3 de febrero de 2022, entre las 2:00 y las 4:00.

```
C:\PS> New-BrokerCatalogRebootSchedule -Name BankTellers -
    CatalogName BankTellers  -StartDate "2022-02-03" -StartTime "
    02:00" -Enabled $true -RebootDuration 120
```

- Para crear una programación de reinicio de las máquinas virtuales del catálogo con el UID 17 que comience el 3 de febrero de 2022, entre la 1:00 y las 5:00. 10 minutos antes del reinicio, cada máquina virtual está configurada para mostrar un cuadro de mensaje con el título **ADVERTENCIA: Reinicio pendiente** y el mensaje **Guarde su trabajo** en cada sesión de usuario.

```
C:\PS> New-BrokerCatalogRebootSchedule -Name 'Update reboot' -
    CatalogUid 17 -StartDate "2022-02-03" -StartTime "01:00" -
    Enabled $true -RebootDuration 240 -WarningTitle "WARNING:
    Reboot pending" -WarningMessage "Save your work" -
    WarningDuration 10
```

- Para cambiar el nombre de la programación de reinicio del catálogo denominado **Nombre antiguo** a **Nombre nuevo**.

```
C:\PS> Rename-BrokerCatalogRebootSchedule -Name "Old Name" -
    NewName "New Name"
```


- Para mostrar todas las programaciones de reinicio del catálogo con el UID 1 y, a continuación, cambiar el nombre de la programación de reinicio del catálogo con el UID 1 a **Nuevo nombre**.

```
C:\PS> Get-BrokerCatalogRebootSchedule -Uid 1 | Rename-
    BrokerCatalogRebootSchedule -NewName "New Name" -PassThru
```

- Para configurar la programación de reinicios del catálogo denominado **Contabilidad**, se mostrará un mensaje con el título **ADVERTENCIA: Reinicio pendiente y el mensaje Guarde su trabajo** 10 minutos antes del reinicio de cada máquina virtual. El mensaje aparece en todas las sesiones de usuario de esa máquina virtual.

  “‘

  C:\PS> Set-BrokerCatalogRebootSchedule -Name Accounting -WarningMessage “Guarde su trabajo”-WarningDuration 10 -WarningTitle “ADVERTENCIA: Reinicio pendiente”

- Para mostrar todas las programaciones de reinicio que están inhabilitadas y, a continuación, habilitar todas las programaciones de reinicio inhabilitadas.

```
C:\PS> Get-BrokerCatalogRebootSchedule -Enabled $false | Set-
    BrokerCatalogRebootSchedule -Enabled $true
```

- Para configurar la programación de reinicio del catálogo con UID 17, muestre el mensaje **Reiniciando en %m% min** 15, 10 y 5 minutos antes del reinicio de cada máquina virtual.

```
C:\PS> Set-BrokerCatalogRebootSchedule 17 -WarningMessage "
    Rebooting in %m% minutes." -WarningDuration 15 -
    WarningRepeatInterval 5
```

- Para configurar la zona horaria del catálogo denominado **MiCatálogo**.

```
C:\PS> Set-BrokerCatalog -Name "MyCatalog" -TimeZone <TimeZone>
```

Agregar descripciones a una imagen

Puede agregar descripciones informativas acerca de los cambios relacionados con las actualizaciones de imágenes de los catálogos de máquinas. Utilice esta función para agregar una descripción al crear un catálogo o al actualizar una imagen maestra existente de un catálogo. También puede mostrar información de cada imagen maestra del catálogo. Utilice los siguientes comandos para agregar o ver descripciones de imágenes:

- Para agregar una nota al crear un catálogo de máquinas con una imagen maestra, utilice el parámetro `MasterImageNote` en el comando `NewProvScheme`. Por ejemplo:

```
C:\PS>New-ProvScheme -ProvisioningSchemeName <name> -
    HostingUnitName <name> -IdentityPoolName <name> -MasterImageVM
XDHyp:\HostingUnits<hosting unit name><vm name>.vm\Base.snapshot
    -MasterImageNote "Note"
```


- Para actualizar la imagen maestra asociada a un catálogo de máquinas, utilice el parámetro `MasterImageNote` en el comando `Publish-ProvMasterVMImage`. Por ejemplo:

```
C:\PS>Publish-ProvMasterVMImage -ProvisioningSchemeName <name> -
    MasterImageVM XDHyp:\HostingUnits<hosting unit name><vm name>.
    vm\base.snapshot -MasterImageNote "Note"
```

- Para mostrar la información de cada imagen, utilice el comando Get-ProvSchemeMasterVMImageHistory. Por ejemplo:

```
C:\PS>Get-ProvSchemeMasterVMImageHistory -ProvisioningSchemeName
    MyScheme -Showall
```

Para hacer un seguimiento del progreso de la reversión, busque el catálogo en **Catálogos de máquinas** para ver la barra de progreso integrada y el gráfico de progreso detallado.

La reversión no es posible en ciertos casos, como estos (la opción **Revertir imagen maestra** no se ve).

- No tiene permiso para revertir.
- El catálogo no se creó con MCS.
- El catálogo se creó con una imagen del disco del SO.
- La instantánea utilizada para crear el catálogo está dañada.
- Los cambios de los usuarios en las máquinas del catálogo no se conservan.
- Hay máquinas del catálogo que se están ejecutando.

Restablecer disco de SO

Use el comando `Reset-ProvVMDisk` de PowerShell para restablecer el disco del sistema operativo de una máquina virtual persistente en un catálogo de máquinas creado con MCS. Actualmente, esta función se aplica a AWS, Azure, XenServer y Google Cloud. Entornos de virtualización de SCVMM y VMware.

Para ejecutar correctamente el comando de PowerShell, asegúrese de que:

- Las máquinas virtuales de destino están en un catálogo de MCS persistente.
- El catálogo de máquinas MCS funciona correctamente.
- Esto implica que el esquema de aprovisionamiento y el host existen y que el esquema de aprovisionamiento tiene las entradas correctas.
- El hipervisor no está en modo de mantenimiento.
- Las máquinas virtuales de destino están apagadas y en modo de mantenimiento.

Siga estos pasos para restablecer el disco del sistema operativo:

1. Abra una ventana de PowerShell.

2. Ejecute **asnp citrix*** para cargar los módulos de PowerShell específicos de Citrix.
3. Ejecute el comando `Reset-ProvVMDisk` de PowerShell de cualquiera de las siguientes maneras:

   - Especifique la lista de máquinas virtuales en forma de lista separada por comas y efectúe el restablecimiento en cada máquina virtual:

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName ("abc"
         ,"def") -OS
     ```

   - Especifique la lista de máquinas virtuales como resultado del comando `Get-ProvVM` y efectúe el restablecimiento en cada máquina virtual:

     ```
     (Get-ProvVM -ProvisioningSchemeName "xxx") | Reset-ProvVMDisk
         "abc" -OS
     ```

   - Especifique una sola máquina virtual por nombre:

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
         -OS
     ```

   - Cree tareas de restablecimiento independientes para cada una de las máquinas virtuales que devuelva el comando `Get-ProvVM`. Este método es menos eficiente, ya que cada tarea realizará las mismas comprobaciones redundantes, como la comprobación de la capacidad del hipervisor o la comprobación de la conexión para cada máquina virtual.

     ```
     Get-ProvVM -ProvisioningSchemeName "xxx" | Reset-ProvVMDisk -
         ProvisioningSchemeName "xxx" -OS
     ```

4. Aparecerá un mensaje de confirmación con una lista de las máquinas virtuales que se restablecerán, junto con un mensaje de advertencia que indica que se trata de una operación irrecuperable. Si no proporciona una respuesta y pulsa **Intro**, no tendrá lugar ninguna otra acción.

   > **Nota:**
   >
   > No saque las máquinas virtuales del modo de mantenimiento ni las encienda hasta que finalice el proceso de restablecimiento.

   Puede ejecutar el comando `-WhatIf` de PowerShell para imprimir la acción que tendría lugar y salir sin realizar dicha acción.

   También puede omitir el mensaje de confirmación mediante uno de los siguientes métodos:

   - Indique el parámetro `-Force`:

     ```
     Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
         -OS -Force
     ```


- Indique el parámetro `-Confirm:$false`:

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
    -OS -Confirm:$false
```

- Antes de ejecutar `Reset-ProvVMDisk`, cambie `$ConfirmPreference` a **None**:

```
PS C:\Windows\system32> $ConfirmPreference='None'
PS C:\Windows\system32> $ConfirmPreference
None
PS C:\Windows\system32> Reset-ProvVMDisk -
    ProvisioningSchemeName "xxx" -VMName "abc" -OS
```

5. Ejecute `Get-ProvTask` para obtener el estado de las tareas devueltas por el comando `Reset-ProvVMDisk`.

Cambiar el parámetro de red de un esquema de aprovisionamiento existente

Puede cambiar el parámetro de red de un esquema de aprovisionamiento existente para que las nuevas máquinas virtuales se creen en la nueva subred. Utilice el parámetro `-NetworkMapping` del comando `Set-ProvScheme` para cambiar el parámetro de la red.

> **Nota:**
>
> Esta función se admite en Citrix Virtual Apps and Desktops 2203 LTSR CU3 y versiones posteriores.

Para cambiar el parámetro de red de un esquema de aprovisionamiento existente, haga lo siguiente:

1. En la ventana de PowerShell, ejecute el comando `asnp citrix*` para cargar los módulos de PowerShell.
2. Ejecute `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` para ir a la ruta de red que quiere cambiar.
3. Asigne una variable al nuevo parámetro de red. Por ejemplo:

```
$NewNetworkMap = @{
 "0"= "XDHYP:\HostingUnits\MyNetworks\Network 0.network" }
```

4. Ejecute `Set-ProvScheme -ProvisioningSchemeName "name"-NetworkMapping $NewNetworkMap`.
5. Ejecute `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` para verificar el nuevo parámetro de red para el esquema de aprovisionamiento existente.

Administrar versiones de un catálogo de máquinas

Cuando se actualiza un catálogo de máquinas de MCS con el comando `Set-ProvScheme`, la configuración actual se guarda como una versión. A continuación, puede administrar las distintas versiones del catálogo de máquinas mediante los comandos de PowerShell. Puede hacer lo siguiente:

- Consulte la lista de versiones de un catálogo de máquinas
- Use cualquier versión anterior para actualizar el catálogo de máquinas
- Eliminar manualmente una versión si no la usa una máquina virtual de ese catálogo de máquinas
- Cambiar el número máximo de versiones que debe conservar el catálogo de máquinas (el valor predeterminado es 99)

Una versión incluye la siguiente información de un catálogo de máquinas:

- VMCpuCount
- VMMemoryMB
- CustomProperties
- ServiceOffering
- MachineProfile
- NetworkMapping
- SecurityGroup

Ejecute los siguientes comandos (se indican como ejemplos) para administrar las distintas versiones de un catálogo de máquinas.

- Para ver los detalles de configuración de las distintas versiones de un catálogo de máquinas:

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog
```

- Para ver los detalles de configuración de una versión concreta de un catálogo de máquinas:

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -
    Version 2
```

- Para ver el número total de versiones asociadas a un catálogo de máquinas:

  “‘

  (Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog).Count

- Para usar cualquier versión anterior para actualizar el catálogo de máquinas:

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -Version 2
```

- Para eliminar manualmente una versión si no la usa una máquina virtual de ese catálogo de máquinas


```
Remove-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -
    Version 3
```

- Para cambiar el número máximo de versiones que debe conservar el catálogo de máquinas (el valor predeterminado es 99). Esta configuración se aplica en todos los catálogos. Por ejemplo, en este caso, se conservará un máximo de 15 versiones para todos los catálogos aprovisionados por MCS.

```
Set-ProvServiceConfigurationData -Name "MaxProvSchemeVersions" -
    Value 15
```

Si el número de versiones alcanza el número máximo de versiones, no se puede crear una nueva versión si alguna de las máquinas virtuales del catálogo de máquinas está usando versiones anteriores. En ese caso, realice una de las siguientes acciones:

- Aumente el límite del número máximo de versiones que debe conservar el catálogo de máquinas.
- Actualice algunas máquinas virtuales que están en versiones anteriores para que ninguna máquina virtual deje de hacer referencia a esas versiones anteriores y pueda eliminarlas.

Convertir un catálogo de máquinas no basado en perfiles de máquina en un catálogo de máquinas basado en perfiles de máquina

Puede usar una VM, una especificación de plantilla (en el caso de Azure) o una plantilla de inicio (en el caso de AWS) como entrada del perfil de máquina para convertir un catálogo de máquinas no basado en perfiles de máquina en un catálogo de máquinas basado en perfiles de máquina. Las máquinas virtuales nuevas agregadas al catálogo toman los valores de las propiedades del perfil de la máquina a menos que se sobrescriban con una propiedad personalizada explícita.

> **Nota:**
>
> Un catálogo de máquinas existente basado en perfiles de máquina no se puede cambiar a un catálogo de máquinas no basado en perfiles de máquina.

Para hacerlo:

1. Cree un catálogo de máquinas persistente o no persistente con máquinas virtuales y sin un perfil de máquina.
2. Abra la ventana de **PowerShell**.
3. Ejecute el comando `Set-ProvScheme` para aplicar los valores de las propiedades del perfil de la máquina a las nuevas máquinas virtuales agregadas al catálogo de máquinas. Por ejemplo:
    - En el caso de Azure:


```
Set-ProvScheme = Set-ProvScheme -ProvisioningSchemeName xxxx
    -MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
    machineprofile.folder<ResourceGroupName><TemplateSpecName
    ><VersionName>
```

- En el caso de AWS:

```
Set-ProvScheme = Set-ProvScheme -ProvisioningSchemeName xxxx
    -MachineProfile "XDHyp:\HostingUnits<hosting-unit><launch-
    template>.launchtemplate<launch-template-version>.
    launchtemplateversion"
```

Reparar la información de identidad de las cuentas de equipo activas

Puede restablecer la información de identidad de las cuentas de equipo activas que tengan problemas relacionados con la identidad. Puede elegir restablecer solo la contraseña de la máquina y las claves de confianza, o bien restablecer toda la configuración del disco de identidad. Esta implementación se aplica tanto a catálogos de máquinas de MCS persistentes como no persistentes.

> **Nota:**
>
> En la actualidad, la función solo es compatible con los entornos de virtualización de AWS, GCP, Azure, XenServer y VMware.

Condiciones

Para restablecer correctamente el disco de identidad:

- Apague y ponga la VM en modo de mantenimiento
- No incluya el parámetro -OS en el comando de PowerShell

Restablecer disco de identidad

Para restablecer un disco de identidad:

1. Abra la ventana de **PowerShell**.
2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
3. Restablezca la información de identidad.
    - Para restablecer únicamente la contraseña de la máquina y las claves de confianza, ejecute los siguientes comandos en este orden:


```
Repair-AcctIdentity -IdentityAccountName TEST\VM1 -
    PrivilegedUserName TEST\admin1 -PrivilegedUserPassword
    $password -Target IdentityInfo
```

La descripción de los parámetros usados en el comando es la siguiente:

- `IdentityAccountName`: El nombre de la cuenta de identidad que se debe reparar.
- `PrivilegedUserName`: La cuenta de usuario que tiene permiso de escritura en el proveedor de identidades (AD o AzureAD).
- `PrivilegedUserPassword`: Contraseña para PrivilegedUserName.
- `Target`: Objetivo de la acción de reparación. Puede ser IdentityInfo para reparar la contraseña o la clave de confianza de la cuenta y UserCertificate para reparar los atributos del certificado de usuario de las identidades de máquinas híbridas unidas a AzureAD.

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMname <name
    > -Identity -ResetIdentityInfo
```

El parámetro `ResetIdentityInfo` restablece lo siguiente:

- Contraseña y claves de confianza: Si la VM está unida a un dominio de AD (solo para documentos de DaaS)
- Solo claves de confianza: Si la máquina virtual no está unida a un dominio de AD (solo para documentos de DaaS)
- Solo contraseña: si la máquina virtual está unida a un dominio de AD (solo para documentos locales de CVAD)

- Para restablecer toda la configuración del disco de identidad, ejecute los siguientes comandos en este orden:

```
Repair-AcctIdentity -IdentityAccountName TEST\VM1 -
    PrivilegedUserName TEST\admin1 -PrivilegedUserPassword
    $password -Target IdentityInfo
```

```
Reset-ProvVMDisk ProvisioningSchemeName <name> -VMName <name>
     -Identity
```

4. Escriba **y** para confirmar la acción. También puede omitir el mensaje de confirmación mediante el parámetro `-Force`. Por ejemplo:

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMName <name> -
    Identity -Force
```

5. Ejecute `Get-ProvVM -ProvisioningSchemeName <name -VMName <name>` para comprobar la configuración actualizada del disco de identidad. Los atributos del disco de identidad (por ejemplo, `IdentityDiskId`) deben actualizarse. `StorageId` y `IdentityDiskIndex` no deben cambiar.

Cambiar la configuración de la caché en un catálogo de máquinas existente

Después de crear un catálogo no persistente con E/S de MCS habilitada, puede usar el comando Set-ProvScheme para modificar los siguientes parámetros:

- WriteBackCacheMemorySize
- WriteBackCacheDiskSize

Esta función se aplica actualmente a:

- Entornos de GCP y Microsoft Azure, y
- un catálogo no persistente con E/S de MCS habilitada

Requisitos

Los requisitos para modificar la configuración de caché son:

- Actualizar a la versión más reciente de VDA (2308 o posterior).
- Habilitar el parámetro `UseWriteBackCache` para el catálogo de máquinas existente. Use `New-ProvScheme` para crear un catálogo de máquinas con la opción `UseWriteBackCache` habilitada. Por ejemplo:

```
New-ProvScheme -ProvisioningSchemeName $CatalogName -
   HostingUnitUid $HostingUnitUid `
-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `
-MasterImageVM $MasterImage `
-ServiceOffering $ServiceOffering `
-NetworkMap $NetworkMap `
-SecurityGroup $SecurityGroup `
-UseWriteBackCache -WriteBackCacheDiskSize 8
```

Cambiar la configuración de caché

Ejecute el comando Set-ProvScheme. Por ejemplo:

```
Set-ProvScheme -ProvisioningSchemeName $provScheme.
   ProvisioningSchemeName -WriteBackCacheDisk32 -
   WriteBackCacheMemorySize 128
```

> **Nota:**
>
> - El valor de `WriteBackCacheDiskSize` debe ser mayor que cero porque se requiere al menos 1 GB de almacenamiento en disco de caché.
> - El valor de `WriteBackCacheMemorySize` debe ser menor que el tamaño de la memoria del catálogo de máquinas.

> - Estos cambios solo afectan a las nuevas VM que se agreguen al catálogo después de realizar el cambio. Estos cambios no afectan a las VM existentes.

Compatibilidad con la actualización de VDA mediante acceso a recursos compartidos de archivos locales

Especifique la ubicación del instalador del VDA mediante los cmdlets de PowerShell, lo que reduce la necesidad de proporcionar reglas de red para permitir que cada VDA obtenga el nuevo instalador de VDA en la CDN de Azure administrada por Citrix.

Cmdlets de PowerShell

Se han agregado dos nuevos parámetros opcionales a los cmdlets **New-VusCatalogSchedule** y **New-VusMachineUpgrade** que permiten usar instaladores desde un recurso compartido de archivos local

- **VdaWorkstationPackageUri**: para especificar la ruta UNC al instalador de VDA del sistema operativo de la estación de trabajo
- **VdaServerPackageUri**: para especificar la ruta UNC al instalador de VDA del sistema operativo del servidor

Requisitos previos

- Instalador de VUS Agent incluido con VDA 2311
- Agente de actualización de VDA a la versión 7.40.0.35 o posterior (con la versión 2311 o posterior del instalador de VDA)
- Virtual Apps and Desktops Remote PowerShell SDK versión 7.40 o posterior (publicada el 10 de enero de 2024 o posterior)

Cómo configurar los permisos de los recursos compartidos de archivos

Los recursos compartidos de red que contienen los paquetes de instalación de VDA deben tener acceso de lectura para el servicio Agente de actualización de VDA, que se ejecuta como sistema local (entidad principal NT AUTHORITY\SYSTEM).

- **Permiso para recursos compartidos de archivos con unión a un dominio**

  Cuando la máquina VDA está unida a un dominio, la cuenta del **sistema local** (VUA se ejecuta como sistema local) usa las credenciales del equipo al acceder a los recursos compartidos de red.

El permiso de privilegio mínimo se puede establecer concediendo acceso de **lectura** a los equipos del dominio.

1. Elija a las personas de su red con las que quiere compartir el archivo.
2. Haga clic en **Advanced Sharing Settings** y active **File and Printer Sharing**.

- **Permiso para recursos compartidos de archivos sin unión a un dominio**

  Cuando la máquina VDA no está unida a un dominio, la cuenta **Local System** (VUA se ejecuta como Local System) usa **ANONYMOUS LOGON** al acceder a los recursos compartidos de red.

  1. Seleccione una carpeta compartida.
  2. Inhabilite la protección con contraseña.
     a) Vaya a la ficha **Properties** de la carpeta.
     b) Seleccione **Network and Sharing Center**.
     c) Desactive **Password Protected Sharing**.
  3. Haga clic en **Advanced Sharing** para conceder un permiso para compartir.
     a) Seleccione **Permissions**.
     b) Conceda un permiso de lectura (**Read**) para el recurso compartido a **ANONYMOUS LOGON**.
  4. Seleccione la ficha **Security** para conceder permisos a la carpeta
     a) Haga clic en **Edit** para agregar permisos a la carpeta compartida
     b) Seleccione la carpeta compartida para conceder permisos de carpeta a **ANONYMOUS LOGON**.
  5. Haga clic en **Advanced** para activar **File and Printer Sharing**.
  6. Agregue el nombre de la carpeta compartida a **Network Access Security Policy**.

  > **Nota:**
  >
  > Reinicie el equipo para que el cambio surta efecto inmediatamente.

Actualizaciones de VDA desde un recurso compartido de archivos local

1. Descargue el instalador del VDA y colóquelo en el recurso compartido de archivos.

   > **Nota:**
   >
   > Con el servicio Virtual Upgrade Service, puede seleccionar entre la pista Current Release o la pista LTSR.
   >
   > **Por ejemplo:** Si el catálogo de máquinas está establecido en la versión Current Release, es decir, 2311, y la versión del VDA es 2305, debe actualizar el VDA a la versión 2311.

   a) Vaya a la página **Descargas** de nuestro sitio web.

b) Seleccione **Citrix Virtual Apps and Desktops** como producto.
c) Seleccione **Citrix Virtual Apps and Desktops 7 2311, All Editions**.
d) Seleccione el instalador del VDA en el nodo **Components that are on the product ISO but also packaged separately**.

2. Seleccione el instalador de VDA correspondiente según el tipo de catálogo.

   - Descargue el **instalador de VDA para SO multisesión** si el tipo de catálogo es **multisesión**
   - Descargue el **instalador de VDA para SO de sesión única** si el tipo de catálogo es de **sesión única**
   - Descargue el **instalador de VDA de servicios básicos para SO de sesión única** si el tipo de catálogo es **Acceso con Remote PC**

> **Nota:**
>
> La versión del instalador de recursos compartidos de archivos debe coincidir **exactamente** con la versión del instalador más reciente publicada por VUS en la nube.

Solucionar 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.

Qué hacer a continuación

Para obtener información sobre la administración de catálogos de servicios en la nube específicos, consulte:

- Administrar un catálogo de AWS
- Administrar un catálogo de XenServer
- Administrar un catálogo de Google Cloud Platform
- Administrar un catálogo de Microsoft Azure
- Administrar un catálogo de Microsoft System Center Virtual Machine Manager
- Administrar un catálogo de VMware

Administrar un catálogo de AWS

August 17, 2024

Administrar catálogos de máquinas describe los asistentes con los que se administra un catálogo de máquinas. La siguiente información incluye detalles específicos de los entornos de nube de AWS.

> **Nota:**
>
> Antes de administrar un catálogo de AWS, debe terminar de crear un catálogo de AWS. Consulte Crear un catálogo de AWS.

Quitar etiquetas

Al crear un catálogo o una máquina virtual, se crean etiquetas de MCS en estos recursos:

- Máquina virtual
- Volumen del disco raíz
- Volumen del disco de identidad
- NIC
- Imagen del disco raíz (AMI)
- Plantilla de inicio
- Instantánea de la AMI o del disco raíz

Puede quitar máquinas virtuales y catálogos de máquinas de la base de datos de Citrix y quitar etiquetas de MCS. Puede usar:

- `Remove-ProvVM` con el parámetro `ForgetVM` para quitar máquinas virtuales y etiquetas de MCS de una sola máquina virtual o una lista de máquinas virtuales de un catálogo de máquinas.
- `Remove-ProvScheme` con el parámetro `ForgetVM` para quitar un catálogo de máquinas de la base de datos de Citrix y recursos de un catálogo de máquinas.

Esta función solo se puede aplicar a máquinas virtuales persistentes.

Para hacerlo:

1. Abra una ventana de **PowerShell**.
2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
3. Desbloquee la máquina virtual antes de quitarlas. Por ejemplo:

```
1 Unlock-ProvVM -ProvisioningSchemeName "<name>" -VMID "<id"
```

4. Ejecute uno de estos comandos para quitar máquinas virtuales, el catálogo de máquinas y las etiqueta de MCS de los recursos.
    - Ejecute `Remove-ProvVM` con `ForgetVM` para quitar máquinas virtuales de la base de datos de Citrix y las etiquetas de las máquinas virtuales. Por ejemplo:


```
Remove-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name
    >" -ForgetVM
```

- Ejecute `Remove-ProvScheme` para quitar un catálogo de máquinas de la base de datos de Citrix y los recursos de dicho catálogo de máquinas. Por ejemplo:

```
Run Remove-ProvScheme -ProvisioningSchemeName "<name>" -
    ForgetVM
```

5. Sin embargo, verifique que la máquina virtual se haya quitado del Delivery Controller, no del hipervisor.
   a) Ejecute `Get-ProvVM -ProvisioningSchemeName "<name>"-VMName "<name>"`. Esto no debe devolver nada.
   b) Vaya a la consola de Amazon EC2. Debería ver las máquinas virtuales. Ahora, las etiquetas se han quitado. Se quitan las etiquetas de estos recursos:
      - Máquina virtual
      - Volumen del disco raíz
      - Volumen del disco de identidad
      - NIC
6. Si quita el catálogo de máquinas, verifique que el catálogo se haya quitado del Delivery Controller.
   a) Ejecute `Get-ProvScheme -ProvisioningSchemeName "forgetvmdemo"`. Esto debe devolver un error.
   b) Verifique en la consola de Amazon EC2 que se hayan quitado estos recursos.
      - Imagen del disco raíz (AMI)
      - Plantilla de inicio
      - Instantánea de la AMI o del disco raíz

Identificar los recursos creados por MCS

A continuación, se muestran las etiquetas que MCS agrega a los recursos. Las etiquetas de la tabla se representan como "clave": "valor".

Resource name	Etiqueta
Disco de ID	"Name": "VMName_IdentityDisk" "XdConfig": "XdProvisioned=true"

Resource name	Etiqueta
Imagen	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “XdConfig”: “XdProvisioned=true”
NIC	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “Description”: “XD NIC” “XdConfig”: “XdProvisioned=true”
Disco de SO	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “Name”: “VMName_rootDisk” “XdConfig”: “XdProvisioned=True”
PrepVM	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [cuando AwsCaptureInstanceProperties = true] “Citrix Resource”: “” [cuando AwsCaptureInstanceProperties = true y AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “” “Name”: “Preparation - CatalogName - xxxxxxxxxx” “XdConfig”: “XdProvisioned=true”
Instantánea publicada	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [cuando AwsCaptureInstanceProperties = true] “Citrix Resource”: “” [cuando AwsCaptureInstanceProperties = true y AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “” “XdConfig”: “XdProvisioned=true”
Plantilla	Si no se trata de una instantánea para la AMI de Volume Worker, “CitrixProvisioningSchemeId”es: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [cuando AwsCaptureInstanceProperties = true] “XdConfig”: “XdProvisioned=true”

Resource name	Etiqueta
VM en catálogo	[cuando AwsCaptureInstanceProperties = true] “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [cuando AwsCaptureInstanceProperties = true] “CitrixResource”: “” [cuando AwsCaptureInstanceProperties = true y AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “” “XdConfig”: “XdProvisioned=true”
AMI de trabajador de volumen	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [cuando AwsCaptureInstanceProperties = true] “CitrixResource”: “” [cuando AwsCaptureInstanceProperties = true] “aws:ec2launchtemplate:id”:”lt-xxxx” [cuando AwsCaptureInstanceProperties = true] “aws:ec2launchtemplate:version”: “n” [cuando AwsCaptureInstanceProperties = true y AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “” “XdConfig”: “XdProvisioned=true”
Programa previo (bootstrapper) de trabajador por volumen	“Name”: “XenDesktop Temp” “XdConfig”: “XdProvisioned=true”
Instancia de trabajador de volumen	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [cuando AwsCaptureInstanceProperties = true y AwsOperationalResourcesTagging = true] “CitrixVolumeWorkerBootstrapper”: “” “Name”: “Citrix.XD.Volumeworker-xxxx-xx-xx-xx-xxxx” “XdConfig”: “XdProvisioned=true”

Más información

- Crear y administrar conexiones y recursos

- Conexión con AWS
- Crear catálogos de máquinas
- Crear un catálogo de AWS
- Administrar catálogos de máquinas

Administrar un catálogo de XenServer

August 17, 2024

Administrar catálogos de máquinas describe los asistentes con los que se administra un catálogo de máquinas. La siguiente información incluye detalles específicos de los entornos de virtualización de XenServer.

> **Nota:**
>
> Antes de administrar un catálogo de XenServer, debe terminar de crear un catálogo de XenServer. Consulte Crear un catálogo de XenServer.

Identificar los recursos creados por MCS

A continuación, se muestran las etiquetas que MCS agrega a los recursos. Las etiquetas de la tabla se representan como "clave": "valor".

Resource name	Etiqueta
Disco base publicado y su copia en cada red o almacenamiento local	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Disco de ID	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Disco de SO	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Máquina virtual de preparación	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
VM en catálogo	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Disco WBC	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

Más información

- Crear y administrar conexiones y recursos
- Conexión a XenServer
- Crear catálogos de máquinas
- Crear un catálogo de XenServer
- Administrar catálogos de máquinas

Administrar un catálogo de Google Cloud Platform

August 17, 2024

Administrar catálogos de máquinas describe los asistentes con los que se administra un catálogo de máquinas. La siguiente información incluye detalles específicos de los entornos de Google Cloud.

> **Nota:**
>
> Antes de administrar un catálogo de Google Cloud Platform, debe terminar de crear un catálogo de Google Cloud Platform. Consulte Crear un catálogo de Google Cloud Platform.

Administrar catálogos de máquinas

Para agregar máquinas a un catálogo, actualizar máquinas y revertir una actualización, consulte Administrar catálogos de máquinas.

Administración de energía

Citrix DaaS le permite administrar la energía de las máquinas de Google Cloud. Utilice el nodo **Buscar** del panel de la izquierda para localizar la máquina que quiere administrar. Estas son las acciones de energía que hay disponibles:

- Eliminar
- Iniciar
- Reiniciar
- Forzar reinicio
- Apagar
- Forzar apagado
- Agregar a grupo de entrega
- Administrar etiquetas

- Activar modo de mantenimiento

También puede administrar la energía de las máquinas de Google Cloud mediante Autoscale. Para ello, agregue las máquinas de Google Cloud a un grupo de entrega y, a continuación, habilite Autoscale para dicho grupo de entrega. Para obtener más información sobre Autoscale, consulte Autoscale.

Actualizar las máquinas aprovisionadas mediante PowerShell

El comando `Set-ProvScheme` cambia el esquema de aprovisionamiento. Sin embargo, no afecta a las máquinas existentes. Ahora, con el comando `Set-ProvVMUpdateTimeWindow` de PowerShell, puede aplicar el esquema de aprovisionamiento actual a una máquina o un conjunto de máquinas persistentes o no persistentes. Actualmente, en Google Cloud Platform, la actualización de propiedades que admite esta función es el perfil de máquina.

Puede actualizar:

- Una sola máquina virtual
- Una lista de máquinas virtuales específicas o todas las máquinas virtuales asociadas a un ID de esquema de aprovisionamiento
- Una lista de máquinas virtuales específicas o todas las máquinas virtuales asociadas a un nombre de esquema de aprovisionamiento

Para actualizar las máquinas virtuales:

1. Compruebe la configuración de las máquinas. Por ejemplo,

```
Get-ProvScheme | select ProvisioningSchemeName,
    ProvisioningSchemeVersion
```

2. Actualice el esquema de aprovisionamiento. Por ejemplo,

```
`Set-ProvScheme –ProvisioningSchemeName "my-catalog" –
    MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
    machineprofileinstance.vm"
```

3. Compruebe si la propiedad actual de la máquina virtual coincide con el esquema de aprovisionamiento actual y si hay alguna acción de actualización pendiente en la máquina virtual. Por ejemplo,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeVersion
```

   También puede encontrar máquinas con una versión en particular. Por ejemplo,

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select
    VMName, ProvisioningSchemeVersion
```


4. Actualice las máquinas existentes.

   - Para actualizar todas las máquinas:

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
       -StartsNow -DurationInMinutes -1
   ```

   - Para actualizar una lista de máquinas específicas:

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
       -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes
      -1
   ```

   - Para actualizar las máquinas según el resultado de `Get-ProvVM`:

   ```
   Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
      ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
      -StartsNow -DurationInMinutes -1
   ```

5. Busque las máquinas que tienen una actualización programada. Por ejemplo,

   ```
   Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName
      , ProvisioningSchemeUpdateAfter
   ```

6. Reinicie las máquinas. En el siguiente encendido, los cambios en las propiedades se aplicarán a las máquinas existentes. Puede comprobar el estado de la actualización con el siguiente comando:

   ```
   Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
      ProvisioningSchemeVersion
   ```

Cambiar las propiedades personalizadas relacionadas con el disco de un catálogo existente

Puede cambiar estas propiedades personalizadas relacionadas con el disco de un catálogo existente y de máquinas virtuales existentes del catálogo:

- `PersistOSDisk`
- `PersistWBC`
- `StorageType`
- `IdentityDiskStorageType`
- `WbcDiskStorageType`

> **Nota:**
>
> - La propiedad `StorageType` es para el disco del sistema operativo
> - La propiedad `PersistOsDisk` solo se puede configurar para catálogos no persistentes

> con caché de reescritura habilitada

Esta implementación le ayuda a seleccionar diferentes tipos de almacenamiento para diferentes discos incluso después de crear un catálogo y, por lo tanto, a equilibrar los precios asociados a los diferentes tipos de almacenamiento.

Para hacer esto, utilice los comandos de PowerShell `Set-ProvScheme` y `Set-ProvVMUpdateTimeWindow`.

1. Abra una ventana de **PowerShell**.
2. Ejecute `asnp citrix*`.
3. Ejecute `Get-ProvVM -VMName <VM name>` para obtener las propiedades personalizadas.
4. Cambie la cadena de propiedades personalizada:
   a) Copie las propiedades personalizadas en un bloc de notas y cámbieles las propiedades personalizadas.
   b) En la ventana de **PowerShell**, pegue las propiedades personalizadas modificadas del Bloc de notas y asigne una variable a las propiedades personalizadas modificadas. Por ejemplo:

```
$cp =  '<CustomProperties xmlns=http://schemas.citrix.com
   /2014/xd/machinecreation xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="CatalogZones" Value
   ="" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="
   true" />
<Property xsi:type="StringProperty" Name="PersistOSDisk" Value
   ="true" />
<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
   Value="pd-standard" />
<Property xsi:type="StringProperty" Name="StorageType" Value="
   pd-standard" />
</CustomProperties>'
```

5. Actualice el catálogo existente. Por ejemplo:

```
Set-ProvScheme -ProvisioningSchemeName <yourCatalogName> -
   CustomProperties $cp
```

6. Actualice las máquinas virtuales existentes. Por ejemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
   VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

7. Reinicie las máquinas virtuales. En el siguiente encendido, los cambios en las propiedades personalizadas se aplicarán a las máquinas virtuales existentes.

Proteger contra la eliminación accidental de máquinas

Citrix DaaS le permite proteger los recursos de MCS en Google Cloud para evitar la eliminación accidental. Configure la máquina virtual aprovisionada estableciendo el indicador `deletionProtection` en TRUE.

De forma predeterminada, las VM aprovisionadas a través del plug-in de Google Cloud o MCS se crean con "InstanceProtection"habilitada. La implementación se aplica tanto a catálogos persistentes como no persistentes. Los catálogos no persistentes se actualizan cuando las instancias se vuelven a crear a partir de la plantilla. Para las máquinas persistentes, se puede establecer el indicador en la consola de Google Cloud. Para obtener más información sobre cómo establecer el indicador, consulte el sitio de documentación de Google. Las nuevas máquinas que se agregan a catálogos persistentes se crean con la opción `deletionProtection` habilitada.

Si intenta eliminar una instancia de VM para la que estableció el indicador `deletionProtection`, la solicitud falla. Sin embargo, si se le concede el permiso `compute.instances.setDeletionProtection` o se le asigna el rol de **administrador de procesos** (Compute Admin) de IAM, puede restablecer el indicador para permitir la eliminación del recurso.

Identificar los recursos creados por MCS

A continuación, se muestran las etiquetas que MCS agrega a los recursos. Las etiquetas de la tabla se representan como "clave": "valor".

Resource name	Etiqueta
Disco de ID	"CitrixResource": "internal" "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Imagen	"CitrixResource": "internal" "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Disco de SO	"CitrixResource": "internal" "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
PrepVM	"CitrixResource": "internal" "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
Instantánea publicada	"CitrixResource": "internal"
Depósito de almacenamiento	"Citrixresource": "internal"

Resource name	Etiqueta
Plantilla	“CitrixResource”: “internal” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”
VM en catálogo	“CitrixResource”: “internal” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”. El plug-in también agrega esta etiqueta para las VM aprovisionadas con MCS: “citrix-provisioning-scheme-id”: “provSchemeId”. Puede usar esta etiqueta para filtrar por catálogo en la consola de GCP.
Disco WBC	“CitrixResource”: “internal” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”

> **Nota:**
>
> Una máquina virtual no está visible en el inventario de Citrix si se agrega una etiqueta **CitrixResource** para identificarla como un recurso creado por MCS. Puede quitar la etiqueta o cambiarle el nombre para que sea visible.

Más información

- Crear y administrar conexiones y recursos
- Conexión con entornos de Google Cloud
- Crear catálogos de máquinas
- Crear un catálogo de Google Cloud Platform
- Administrar catálogos de máquinas

Administrar un catálogo de HPE Moonshot

August 17, 2024

Administrar catálogos de máquinas describe los asistentes con los que se administra un catálogo de máquinas. La siguiente información incluye detalles específicos del catálogo de HPE Moonshot.

> **Nota:**
>
> Antes de administrar un catálogo de HPE Moonshot, debe terminar de un catálogo de HPE Moonshot.

Administración de energía

Citrix Virtual Apps and Desktops le permite administrar la energía de las máquinas HPE Moonshot. Utilice el nodo **Buscar** del panel de navegación para localizar la máquina que quiere administrar. Estas son las acciones de energía que hay disponibles:

- Iniciar
- Apagar
- Forzar apagado
- Reiniciar
- Restablecer

> **Nota:**
>
> No se admiten las acciones de energía **Suspender** y **Reanudar**.

Más información

- Crear y administrar conexiones y recursos
- Conexión a HPE Moonshot
- Crear catálogos de máquinas
- Crear un catálogo de máquinas de HPE Moonshot
- Administrar catálogos de máquinas

Administrar un catálogo de Microsoft Azure

August 17, 2024

> **Nota:**
>
> Desde julio de 2023, Microsoft cambió el nombre de Azure Active Directory (Azure AD) a Microsoft Entra ID. En este documento, cualquier referencia a Azure Active Directory, Azure AD o AAD ahora se refiere a Microsoft Entra ID.

Administrar catálogos de máquinas describe los asistentes con los que se administra un catálogo de máquinas. La siguiente información incluye detalles específicos de los entornos de nube de Microsoft Azure Resource Manager.

> **Nota:**
>
> Antes de administrar un catálogo de Microsoft Azure, debe terminar de crear un catálogo de Microsoft Azure. Consulte Crear un catálogo de Microsoft Azure.

Cambio del tipo de almacenamiento a un nivel inferior al apagar una máquina virtual

Puede ahorrar costes de almacenamiento al cambiar el tipo de almacenamiento de un disco administrado a un nivel inferior cuando apaga una máquina virtual. Para ello, utilice la propiedad `StorageTypeAtShutdown` personalizada.

El tipo de almacenamiento del disco pasa a un nivel inferior (tal y como se especifica en la propiedad personalizada `StorageTypeAtShutdown`) al apagar la máquina virtual. Tras encender la máquina virtual, el tipo de almacenamiento vuelve a ser el original (tal y como se especifica en la propiedad `StorageType` personalizada o en la propiedad `WBCDiskStorageType` personalizada).

> **Importante:**
>
> El disco no existe hasta que la máquina virtual se encienda al menos una vez. Por lo tanto, no puede cambiar el tipo de almacenamiento la primera vez que enciende la máquina virtual.

Requisitos

- Aplicable a un disco administrado. Esto implica establecer la propiedad personalizada `UseManagedDisks` en true.
- Aplicable a un catálogo persistente y no persistente con un disco de sistema operativo persistente. Esto implica establecer la propiedad personalizada `persistOsDisk` en true.
- Aplicable a un catálogo no persistente con un disco WBC persistente. Esto implica establecer la propiedad personalizada `persistWBC` en true.

Restricción

- Según informa Microsoft, solo se puede cambiar el tipo de disco dos veces al día. Consulte el documento de Microsoft. Según informa Citrix, la actualización de `StorageType` tiene lugar cada vez que hay una acción de inicio o desasignación para la máquina virtual. Por lo tanto, limite la cantidad de acciones de energía por máquina virtual a dos veces al día. Por ejemplo, una acción de energía por la mañana para iniciar la máquina virtual y otra por la noche para desasignarla.

Cambiar el tipo de almacenamiento a un nivel inferior

Antes de continuar con los pasos, consulte los Requisitos y la Restricción.

1. Agregue la propiedad personalizada `StorageTypeAtShutdown`, establezca el valor en Standard_LRS (HDD) y cree un catálogo mediante `New-ProvScheme`. Para obtener información sobre la creación de catálogos mediante PowerShell, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

   > **Nota:**
   >
   > Si `StorageTypeAtShutdown` tiene algún valor que no esté vacío o no sea Standard_LRS (HDD), la operación fallará.

   Ejemplo de configuración de propiedades personalizadas al crear un catálogo persistente:

```
$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="StorageType" Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown" Value="Standard_LRS" />
</CustomProperties>'
```

   Ejemplo de configuración de propiedades personalizadas al crear un catálogo no persistente:

```
$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="StorageType" Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="WbcDiskStorageType" Value="Standard_SSD_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
```



```
<Property xsi:type="StringProperty" Name="OsType" Value="Windows"
    />
<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true
    />
<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=
    true />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
    Value="Standard_LRS" />
</CustomProperties>'
```

> **Nota:**
>
> Al utilizar un perfil de máquina, la propiedad personalizada tiene prioridad sobre la propiedad definida en `MachineProfile`.

2. Apague la máquina virtual y compruebe el tipo de almacenamiento de la máquina virtual en Azure Portal. El tipo de almacenamiento del disco pasa a un nivel inferior, tal y como se especifica en la propiedad `StorageTypeAtShutdown` personalizada.
3. Encienda la máquina virtual. El tipo de almacenamiento del disco vuelve al tipo de almacenamiento mencionado en:
    - Propiedad `StorageType` personalizada para el disco del sistema operativo
    - Propiedad `WBCDiskStorageType` personalizada para el disco WBC solo si la especifica en `CustomProperties`. De lo contrario, vuelve al tipo de almacenamiento mencionado en `StorageType`.

Aplicar `StorageTypeAtShutdown` a un catálogo existente

Antes de continuar con los pasos, consulte los Requisitos y la Restricción.

Use `Set-ProvScheme` para agregar una máquina virtual a un catálogo existente. La función se aplica a las nuevas máquinas virtuales que se agregan después de ejecutar `Set-ProvScheme`. Las máquinas existentes no se ven afectadas.

Ejemplo de configuración de propiedades personalizadas al agregar una máquina virtual a un catálogo existente:

```
$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="StorageType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="WbcDiskStorageType" Value="
    Standard_SSD_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />
```



```
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />
<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown" Value
    ="Standard_LRS" />
</CustomProperties>'

$ProvScheme = Get-Provscheme -ProvisioningSchemeName $CatalogName

Set-ProvScheme -ProvisioningSchemeName $ProvScheme.
    ProvisioningSchemeName -CustomProperties $customProperties
```

Cambiar el tipo de almacenamiento de las máquinas virtuales existentes a un nivel inferior al apagarlas

Antes de continuar con los pasos, consulte los Requisitos y la Restricción.

Puede ahorrar costes de almacenamiento si cambia el tipo de almacenamiento de las máquinas virtuales existentes a un nivel inferior cuando estas están apagadas. Para ello, utilice la propiedad `StorageTypeAtShutdown` personalizada.

Para cambiar el tipo de almacenamiento de las máquinas de un catálogo a un nivel inferior cuando las VM estén apagadas:

1. Abra una ventana de PowerShell.
2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
3. Ejecute `Get-Provscheme -ProvisioningSchemeName $CatalogName`.
4. Cambie la cadena de propiedades personalizada.

   ```
   $customProperties = '<CustomProperties xmlns="http://schemas.
       citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
       org/2001/XMLSchema-instance">
   <Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
       Value="Standard_LRS" />
   </CustomProperties>'
   ```

5. Actualice el esquema de aprovisionamiento del catálogo existente. La actualización se aplica a las nuevas máquinas virtuales que se agregan después de ejecutar `Set-ProvScheme`.

   ```
   Set-ProvScheme -ProvisioningSchemeName $CatalogName -
       CustomProperties $customProperties
   ```

6. Actualice las máquinas virtuales existentes para habilitar `StorageTypeAtShutdown`.


```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName $CatalogName -
    StartsNow -DurationInMinutes -1
```

7. La próxima vez que encienda las máquinas, se actualizará la propiedad `StorageTypeAtShutdown` de las máquinas. El tipo de almacenamiento cambiará la próxima vez que se apague.
8. Ejecute el siguiente comando para ver el valor `StorageTypeAtShutdown` de cada máquina virtual de un catálogo:

```
Get-ProvVM -ProvisioningSchemeName <catalog-name> | foreach {
  $vmName = $_.VMName; $storageTypeAtShutdown = ($_.CustomVmData |
      ConvertFrom-Json).StorageTypeAtShutdown.
     DiskStorageAccountType; return New-Object psobject -Property
     @{
  "VMName" = $vmName; "StorageTypeAtShutdown" =
     $storageTypeAtShutdown  }
   }
```

Actualizar las máquinas aprovisionadas al estado actual del esquema de aprovisionamiento

El comando `Set-ProvScheme` cambia el esquema de aprovisionamiento. Sin embargo, no afecta a las máquinas existentes. Con el comando `Set-ProvVMUpdateTimeWindow` de PowerShell, puede aplicar el esquema de aprovisionamiento actual a una máquina o un conjunto de máquinas persistentes o no persistentes. También puede programar un intervalo de tiempo para las actualizaciones de configuración de las máquinas aprovisionadas por MCS existentes. Cualquier encendido o reinicio durante el intervalo de tiempo programado aplica una actualización programada del esquema de aprovisionamiento a una máquina. Actualmente, en Azure, puede actualizar `ServiceOffering`, `MachineProfile` y estas propiedades personalizadas:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`
- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`

> **Nota:**
>
> - Solo puede actualizar las propiedades personalizadas `StorageType`, `WBCDiskStorageType` y `IdentityDiskStorageType` de un catálogo mediante un disco administrado en

> entornos de Azure.
> - Si ejecuta `Set-ProvVMUpdateTimeWindow` dos veces, se aplicará el comando más reciente.

Puede actualizar:

- Una sola máquina virtual
- Una lista de máquinas virtuales específicas o todas las máquinas virtuales asociadas a un ID de esquema de aprovisionamiento
- Una lista de máquinas virtuales específicas o todas las máquinas virtuales asociadas a un nombre de esquema de aprovisionamiento (nombre del catálogo de máquinas)

Tras realizar los siguientes cambios en el esquema de aprovisionamiento, la instancia de máquina virtual se vuelve a crear para los catálogos persistentes en Azure:

- Cambiar `MachineProfile`
- Quitar `LicenseType`
- Quitar `DedicatedHostGroupId`

> **Nota:**
>
> El disco del sistema operativo de las máquinas existentes, junto con todos sus datos, permanecen tal cual y una nueva máquina virtual se conecta al disco.

Antes de actualizar las máquinas virtuales existentes:

1. Compruebe la configuración de las máquinas. Por ejemplo,

```
Get-ProvScheme | select ProvisioningSchemeName,
    ProvisioningSchemeVersion
```

2. Actualice el esquema de aprovisionamiento. Por ejemplo,

   - Con VM como entrada de perfil de máquina:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
    MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
    machineprofile.folder<resource-group>.resourcegroup<
    virtual-machine>.vm"
```

   - Con la especificación de plantilla como entrada del perfil de la máquina:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog"
-MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
    machineprofile.folder<resource-group>.resourcegroup<
    template-spec>.templatespec<template-spec-version>.
    templatespecversion"
-ServiceOffering "XDHyp:\HostingUnits<hosting-unit>\
    serviceoffering.folder<service-offering>.serviceoffering"
```


- Con solo oferta de servicios:

```
Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
    ServiceOffering "XDHyp:\HostingUnits<hosting-unit>\
    serviceoffering.folder<service-offering>.serviceoffering"
```

3. Compruebe si la propiedad actual de la máquina virtual coincide con el esquema de aprovisionamiento actual y si hay alguna acción de actualización pendiente en la máquina virtual. Por ejemplo,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeVersion
```

También puede encontrar máquinas con una versión en particular. Por ejemplo,

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select
    VMName, ProvisioningSchemeVersion
```

Para solicitar que las actualizaciones de las máquinas existentes se apliquen en el próximo reinicio:

1. Ejecute estos comandos para actualizar las máquinas existentes y hacer que las actualizaciones se apliquen en el próximo reinicio.

   - Para actualizar todas las máquinas. Por ejemplo,

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -StartsNow -DurationInMinutes -1
```

   - Para actualizar una lista de máquinas específicas. Por ejemplo,

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes
    -1
```

   - Para actualizar las máquinas según el resultado de Get-ProvVM. Por ejemplo,

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
    ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -StartsNow -DurationInMinutes -1
```

> **Nota:**
>
> - `StartsNow` indica que la hora de inicio programada es la hora actual.
> - `DurationInMinutes` con un número negativo (por ejemplo, -1) indica que no hay ningún límite superior en la ventana de tiempo de la programación.

2. Busque las máquinas que tienen una actualización programada. Por ejemplo,

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName
    , ProvisioningSchemeUpdateAfter
```


3. Reinicie las máquinas. En el siguiente encendido, los cambios en las propiedades se aplicarán a las máquinas existentes. Puede comprobar el estado de la actualización con el siguiente comando. Por ejemplo,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeVersion
```

Para programar la actualización de una máquina virtual a los parámetros de aprovisionamiento más recientes la próxima vez que se inicie en la franja horaria programada:

1. Ejecute los comandos siguientes:

   - Para programar una actualización con la hora de inicio como la hora actual

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -VMName vm1 -StartsNow -DurationInMinutes 120
```

   - Para programar una actualización en un fin de semana

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-
    catalog" -VMName "vm1" -StartTimeInUTC "10/15/2022
    9:00am" -DurationInMinutes (New-TimeSpan -Days 2).
    TotalMinutes
```

> **Nota:**
>
> - `VMName` es opcional. Si no se especifica, la actualización se programa para todo el catálogo.
> - En lugar de `StartTimeInUTC`, use `StartsNow` para indicar que la hora de inicio de la programación es la hora actual.
> - `DurationInMinutes` es opcional. El valor predeterminado es de 120 minutos. Un número negativo (por ejemplo, -1) indica que no hay ningún límite superior en la ventana de tiempo de la programación.

2. Compruebe el estado de la actualización.

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeUpdateUntil, ProvisioningSchemeVersion
```

3. Encienda la máquina virtual. Si enciende la máquina después de la franja horaria programada, no se aplica la actualización de la configuración. Si enciende la máquina durante la franja horaria programada

   - Si la máquina está apagada y:
     - No enciende la máquina, no se aplica la actualización de la configuración
     - Enciende la máquina, se aplica la actualización de la configuración

- Si la máquina está encendida y:
  - No reinicia la máquina, no se aplica la actualización de la configuración
  - Reinicia la máquina, se aplica la actualización de la configuración

Para cancelar la actualización de configuración:

También puede cancelar una actualización de configuración de una sola máquina virtual, varias máquinas virtuales o todo un catálogo. Para cancelar una actualización de configuración:

1. Ejecute `Clear-ProvVMUpdateTimeWindow`. Por ejemplo:
   - Para cancelar la actualización de configuración programada para una sola máquina virtual:

     ```
     Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName “ my-catalog “ -VMName “ vm1 ”
     ```

   - Para cancelar la actualización de configuración programada para varias máquinas virtuales:

     ```
     Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-catalog" -VMName "vm1","vm2"
     ```

     > **Nota:**
     >
     > Las máquinas virtuales deben ser del mismo catálogo.

Actualizar propiedades de máquinas virtuales individuales

Puede actualizar propiedades de máquinas virtuales individuales en catálogos de máquinas de MCS persistentes mediante el comando de PowerShell `Set-ProvVM`. Sin embargo, las actualizaciones no se aplican de forma inmediata. Debe configurar el intervalo de tiempo mediante el comando de PowerShell `Set-ProvVMUpdateTimeWindow` para que se apliquen las actualizaciones.

Esta implementación le ayuda a administrar máquinas virtuales individuales de manera eficiente sin actualizar todo el catálogo de máquinas. Actualmente, esta función solo se aplica al entorno de Azure.

Actualmente, las propiedades que puede actualizar son:

- `CustomProperties`
- `ServiceOffering`
- `MachineProfile`

Con esta función, puede:

- Actualizar las propiedades de una máquina virtual

- Conservar las propiedades actualizadas en una máquina virtual después de actualizar el catálogo de máquinas
- Revertir las actualizaciones de configuración aplicadas a una máquina virtual

Antes de actualizar las propiedades de una máquina virtual:

1. Abra una ventana de **PowerShell**.
2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
3. Compruebe la configuración del catálogo de máquinas existente. Por ejemplo:

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
```

4. Compruebe la configuración de la máquina virtual en la que quiere aplicar las actualizaciones. Por ejemplo:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

Actualizar propiedades de una máquina virtual

Haga lo siguiente para actualizar las propiedades de una máquina virtual:

1. Apague la máquina virtual en la que quiera aplicar las actualizaciones.
2. Actualice las propiedades de la máquina virtual. Por ejemplo, si quiere actualizar la propiedad personalizada de tipo de almacenamiento (`StorageType`) de la máquina virtual, ejecute lo siguiente:

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
    CustomProperties "...<Property Name='StorageType' Value='
    Premium_LRS' />..."
```

Puede actualizar propiedades de dos máquinas virtuales de un catálogo de máquinas simultáneamente. Por ejemplo:

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
    CustomProperties "...<Property Name='StorageType' Value='
    Premium_LRS' />..."
```

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine2 -
    CustomProperties "...<Property Name='StorageType' Value='
    StandardSSD_LRS' />..."
```

> **Nota:**
>
> Las actualizaciones no se aplican de forma inmediata.

3. Obtenga la lista de propiedades que se especificaron para actualizarse y la versión de configuración. Por ejemplo:

```
Get-ProvVMConfiguration -ProvisioningSchemeName AzureCatalog -
    VMName machine1
```

Compruebe el valor de la propiedad `Version` y las propiedades que se actualizarán (en este caso, `StorageType`).

4. Compruebe la versión de la configuración. Por ejemplo:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

Compruebe el valor de la propiedad `ProvVMConfigurationVersion`. La actualización aún no se ha aplicado. La máquina virtual aún tiene la configuración anterior.

5. Solicite una actualización programada. Por ejemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    StartsNow -DurationInMinutes -1
```

Para obtener más información sobre las actualizaciones programadas, consulte Actualizar las máquinas aprovisionadas al estado actual del esquema de aprovisionamiento.

> **Nota:**
>
> También se aplica cualquier actualización pendiente de esquemas de aprovisionamiento.

6. Reinicie la VM. Por ejemplo:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

7. Compruebe la versión de la configuración. Por ejemplo:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

Compruebe el valor de la propiedad `ProvVMConfigurationVersion`. Ahora la actualización sí se aplica. La máquina virtual ya tiene la nueva configuración.

8. Para aplicar más actualizaciones de configuración en la máquina virtual, apáguela y repita los pasos.

Conservar las propiedades actualizadas en una máquina virtual después de actualizar el catálogo de máquinas

Haga lo siguiente para mantener las propiedades actualizadas en una máquina virtual:

1. Apague la máquina virtual en la que quiera aplicar las actualizaciones.

2. Actualice el catálogo de máquinas. Por ejemplo, si quiere cambiar el tamaño de la máquina virtual (`ServiceOffering`) y el tipo de almacenamiento (`StorageType`), ejecute lo siguiente:

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -
    ServiceOffering Standard_E4_v3 -CustomProperties "...<Property
    Name='StorageType' Value='StandardSSD_LRS' />..."
```

3. Obtener los detalles de configuración del catálogo de máquinas. Por ejemplo:

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
```

   Ahora el valor de `ProvisioningSchemeVersion` se incrementa en uno. También se actualizan el tamaño y el tipo de almacenamiento de la máquina virtual.

4. Actualice las propiedades de la máquina virtual. Por ejemplo, proporcione un perfil de máquina a la máquina virtual.

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
    MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
    machineprofile.folder<resource-group>.resourcegroup<template-
    spec>.templatespec<template-spec-version>.templatespecversion"
```

   > **Nota:**
   >
   > La entrada del perfil de máquina tiene especificados una etiqueta y un tamaño de máquina virtual diferentes (`ServiceOffering`).

5. Obtenga la lista de propiedades que tendrá la máquina virtual después de combinar las actualizaciones de configuración de la máquina virtual con las actualizaciones del catálogo de máquinas. Por ejemplo:

```
Get-ProvVMConfigurationResultantSet -ProvisioningSchemeName
    AzureCatalog -VMName machine1
```

   > **Nota:**
   >
   > Cualquier actualización de la máquina virtual supeditará las actualizaciones realizadas en el catálogo de máquinas.

6. Solicite una actualización programada para la máquina virtual. Por ejemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    VMName machine1 -StartsNow -DurationInMinutes -1
```

7. Reinicie la VM. Por ejemplo:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```


La máquina virtual mantiene su tamaño de máquina virtual actualizado tal y como se deriva del perfil de máquina. Los valores de etiqueta especificados en el perfil de máquina también se aplican a la máquina virtual. Sin embargo, el tipo de almacenamiento se deriva del esquema de aprovisionamiento más reciente.

8. Obtenga la versión de configuración de la máquina virtual. Por ejemplo:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

Ahora, `ProvisioningSchemeVersion` y `ProvVMConfigurationVersion` muestra la versión más reciente.

Revertir las actualizaciones de configuración aplicadas a una máquina virtual

1. Después de aplicar las actualizaciones a una máquina virtual, apáguela.
2. Ejecute el siguiente comando para quitar las actualizaciones que se aplican en la máquina virtual. Por ejemplo:

```
Set-ProvVM -RevertToProvSchemeConfiguration -
    ProvisioningSchemeName AzureCatalog -VMName machine1
```

3. Solicite una actualización programada para la máquina virtual. Por ejemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    VMName machine1 -StartsNow -DurationInMinutes -1
```

4. Reinicie la VM. Por ejemplo:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
```

5. Compruebe la versión de configuración de la máquina virtual. Por ejemplo:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
```

Ahora, el valor de `ProvVMConfigurationVersion` es la versión de configuración del catálogo de máquinas.

Cambiar el cifrado del disco

Puede cambiar el cifrado del disco en los entornos de virtualización de Azure y hacer lo siguiente:

- Crear un catálogo de máquinas MCS con un conjunto de cifrado de disco (DES) distinto del DES de la imagen maestra mediante el comando `New-ProvScheme`. Por ejemplo:

```
$customProperties = @"
```



```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
<Property xsi:type="DiskEncryptionSetId" Name="Zones" Value="/
    subscriptions/XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX/resourceGroups/
    testrsg/providers/Microsoft.Compute/diskEncryptionSets/test-
    diskEncryptionSet"/>
</CustomProperties>
"@
New-ProvScheme -CleanOnBoot `
-ProvisioningSchemeName $provisioningSchemeName `
-HostingUnitName $hostingUnitName `
-IdentityPoolName $identityPoolName `
-InitialBatchSizeHint $numberOfVms `
-masterImagePath $masterImagePath `
-NetworkMapping $networkMapping `
-CustomProperties $customProperties
```

- Cambiar el tipo de cifrado del disco de una clave DES a otra clave DES de un catálogo de máquinas de MCS existente y de las máquinas virtuales existentes mediante los comandos `Set-ProvScheme` y `Set-ProvVMUpdateTimeWindow`. Después de reiniciar las máquinas virtuales, puede ver la clave DES actualizada. Por ejemplo:

```
$customProperties = '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="/subscriptions/456c683e2ed7/resourceGroups/testrg/
    providers/Microsoft.Compute/diskEncryptionSets/
    diskEncryptionSet1" />
</CustomProperties>'
Set-ProvScheme -ProvisioningSchemeName azure-catalog -
    CustomProperties $customProperties
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
    -VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

- Actualizar una máquina virtual y un catálogo de máquinas de MCS que antes no estuvieran habilitados para CMEK para que tengan cifrado (DES) con clave de cifrado administrada por el cliente (CMEK), cifrado de disco en el host o el doble cifrado mediante los comandos `Set-ProvScheme` y `Set-ProvVMUpdateTimeWindow`. Para obtener información sobre los diferentes tipos de cifrado, consulte Cifrado del lado del servidor de Azure, Cifrado de discos de Azure en el host y Cifrado doble en disco administrado.

- Actualizar máquinas virtuales y un catálogo de máquinas de MCS existentes para que no estén cifrados y que anteriormente estuvieran cifrados mediante los comandos `Set-ProvScheme` y `Set-ProvVMUpdateTimeWindow`. Por ejemplo:

```
$customProperties = '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
```



```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="" />
</CustomProperties>'
Set-ProvScheme -ProvisioningSchemeName azure-catalog -
    CustomProperties $customProperties
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
    -VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

- Habilitar el cifrado de discos con un dispositivo de punto final privado (un catálogo de máquinas MCS que use una conexión de host habilitada con `ProxyHypervisorTrafficThroughConnector`). Para obtener información sobre cómo habilitar el cifrado de disco con dispositivos de punto final privados, consulte Habilitar el cifrado de disco con dispositivos de punto final privados.

Habilitar el cifrado de disco con dispositivos de punto final privados

Según la limitación de Azure, actualmente no se puede usar el cifrado del lado del servidor con claves administradas por el cliente para dispositivos de punto final privados. Sin embargo, puede actualizar máquinas virtuales y un catálogo de máquinas de MCS con dispositivos de punto final privados para cifrarlos con la clave DES.

Actualizar un catálogo de máquinas existente con dispositivos de punto final privados Estos son los pasos detallados para actualizar un catálogo de máquinas existente con dispositivos de punto final privados:

1. Cree un catálogo sin cifrado de disco mediante `ProxyHypervisorTrafficThroughConnector`.
2. Ejecute `Set-ProvScheme` para actualizar el catálogo con `DiskEncryptionSetId`.

   > **Nota:**
   >
   > `DiskEcryptionSetId` se puede configurar mediante `CustomProperties` o `MachineProfile`. Cuando se define tanto en `CustomProperties` como en `MachineProfile`, se aplican las propiedades definidas en `CustomProperties`.

   Ejemplo al usar `CustomProperties`:

```
$customProperties = '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="/subscriptions/456c683e2ed7/resourceGroups/testrg/
    providers/Microsoft.Compute/diskEncryptionSets/
    diskEncryptionSet1"/>
</CustomProperties>'
Set-ProvScheme -ProvisioningSchemeName azure-catalog -
    CustomProperties $customProperties
```


Ejemplo al usar MachineProfile: Use una máquina virtual que tenga habilitado el cifrado de disco o una especificación de plantilla con parámetros de cifrado de disco:

```
Set-ProvScheme -ProvisioningSchemeName azure-catalog -
    MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.
    folder\testrg.resourcegroup\new-template.vm"
```

Como alternativa, puede actualizar el perfil de una máquina mediante la interfaz de Configuración completa.

3. Ejecute `Set-ProvVMUpdateTimeWindow` para actualizar las máquinas virtuales del catálogo existentes. Por ejemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -
    VMName azu01, azu02 -StartsNow -DurationInMinutes -1
```

4. Después de reiniciar las máquinas virtuales, puede ver el cifrado de disco actualizado en los discos de las máquinas virtuales en Azure Portal.
5. Ejecute `Set-ProvScheme` para anular el cifrado de disco antes de agregar nuevas máquinas virtuales de catálogo.

   > **Nota:**
   >
   > Este paso es obligatorio porque está actualizando un catálogo de dispositivos de punto final privados. Si no sigue este paso, aparecerán errores al intentar agregar nuevas máquinas virtuales al catálogo.

   Por ejemplo:

```
$customProperties = '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="" />
</CustomProperties>'
Set-ProvScheme -ProvisioningSchemeName azure-catalog -
    CustomProperties $customProperties
```

6. Agregue nuevas VM al catálogo.

Actualizar máquinas virtuales de catálogo individuales Los pasos detallados para actualizar las máquinas virtuales de catálogo individuales son los siguientes:

1. Cree un catálogo sin cifrado de disco mediante `ProxyHypervisorTrafficThroughConnector` .
2. Ejecute `Set-ProvVM` para actualizar la máquina virtual del catálogo con `DiskEncryptionSetId` .

> **Nota:**
>
> `DiskEcryptionSetId` se puede configurar mediante `CustomProperties` o `MachineProfile`.

Ejemplo al usar `CustomProperties`:

```
$customProperties = '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="/subscriptions/456c683e2ed7/resourceGroups/testrg/
    providers/Microsoft.Compute/diskEncryptionSets/
    diskEncryptionSet1" />
</CustomProperties>'
Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01 -
    CustomProperties $customProperties
```

Ejemplo al usar MachineProfile:

```
Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01 -
    MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.
    folder\testrg.resourcegroup\new-template.vm"
```

3. Ejecute `Set-ProvVMUpdateTimeWindow` para actualizar las máquinas virtuales del catálogo existentes. Por ejemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -
    VMName azu01 -StartsNow -DurationInMinutes -1
```

4. Después de reiniciar las máquinas virtuales, puede ver el cifrado de disco actualizado en los discos de las máquinas virtuales en Azure Portal.
5. Agregue nuevas VM al catálogo.

Obtener información de las máquinas virtuales de Azure, instantáneas, el disco del sistema operativo y la definición de imagen de la galería

Puede mostrar información de una máquina virtual de Azure, incluidos el disco y el tipo del sistema operativo, la instantánea y la definición de imágenes de galería. Esta información se muestra para los recursos de la imagen maestra cuando se asigna un catálogo de máquinas. Utilice esta funcionalidad para ver y seleccionar una imagen de Linux o Windows. Se agregó una propiedad de PowerShell, `TemplateIsWindowsTemplate`, al parámetro `AdditionDatafield`. Este campo contiene información específica de Azure: el tipo de máquina virtual, el disco del sistema operativo, la información de la imagen de la galería y la información sobre el tipo de SO. Al establecer `TemplateIsWindowsTemplate` en **True**, significa que el tipo de sistema operativo es Windows;

al establecer `TemplateIsWindowsTemplate` en **False**, significa que el tipo de sistema operativo es Linux.

> **Sugerencia:**
>
> La información que muestra la propiedad `TemplateIsWindowsTemplate` de PowerShell se deriva de la API de Azure. A veces, es posible que este campo esté vacío. Por ejemplo, una instantánea de un disco de datos no contiene el campo `TemplateIsWindowsTemplate` porque el tipo de sistema operativo no se puede obtener de una instantánea.

Por ejemplo, establezca el parámetro `AdditionData` de la máquina virtual de Azure en **True** para el tipo de sistema operativo Windows mediante PowerShell:

```
PS C:\Users\username> (get-item XDHyp:\HostingUnits\mynetwork\image.
    folder\username-dev-testing-rg.resourcegroup\username-dev-tsvda.vm).
    AdditionalData
Key Value
ServiceOfferingDescription Standard_B2ms
HardDiskSizeGB 127
ResourceGroupName FENGHUAJ-DEV-TESTING-RG
ServiceOfferingMemory 8192
ServiceOfferingCores 2
TemplateIsWindowsTemplate True
ServiceOfferingWithTemporaryDiskSizeInMb 16384
SupportedMachineGenerations Gen1,Gen2
```

Identificar los recursos creados por MCS

A continuación, se muestran las etiquetas que MCS agrega a los recursos. Las etiquetas de la tabla se representan como “clave”: “valor”.

Resource name	Etiqueta
Disco de ID	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
Imagen	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
NIC	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
Disco de SO	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”

Resource name	Etiqueta
	“CitrixResource”: “Internal”
PrepVM	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
Instantánea publicada	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
Resource group	“CitrixResource”: “Internal” CitrixSchemaVersion: 2.0
Cuenta de almacenamiento	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
VM en catálogo	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”
Disco WBC	“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal”

> **Nota:**
>
> Una máquina virtual no está visible en el inventario de Citrix si se agrega una etiqueta **CitrixResource** para identificarla como un recurso creado por MCS. Puede quitar la etiqueta o cambiarle el nombre para que sea visible.

Quitar etiquetas

Al crear un catálogo o una máquina virtual, se crean etiquetas en estos recursos:

- Resource group
- Máquina virtual
- Disco de SO
- Disco de identidad
- Interfaz de red

- Cuenta de almacenamiento

Puede quitar máquinas virtuales y catálogos de máquinas de la base de datos de Citrix y quitar etiquetas. Puede usar:

- `Remove-ProvVM` con el parámetro `ForgetVM` para quitar máquinas virtuales y etiquetas de una sola máquina virtual o una lista de máquinas virtuales de un catálogo de máquinas.
- `Remove-ProvScheme` con el parámetro `ForgetVM` para quitar un catálogo de máquinas de la base de datos de Citrix y etiquetas de todo un catálogo de máquinas.

Esta función solo se puede aplicar a máquinas virtuales persistentes.

Para hacerlo:

1. Abra una ventana de **PowerShell**.
2. Ejecute **asnp citrix*** para cargar los módulos de PowerShell específicos de Citrix.
3. Ejecute `Remove-ProvVM` para eliminar máquinas virtuales de la base de datos de Citrix y etiquetas de máquinas virtuales.
   Por ejemplo:

```
Remove-ProvVM -ProvisioningSchemeName “ ProvisioningSchemeName ” -
    VMName “ vmname ” -ForgetVM
```

4. Ejecute `Remove-ProvScheme` para eliminar el catálogo de máquinas de la base de datos de Citrix y etiquetas de catálogos de máquinas. Por ejemplo:

```
Remove-ProvScheme -ProvisioningSchemeName “ ProvisioningSchemeName
    ” -ForgetVM
```

> **Nota:**
>
> Después de usar el parámetro `ForgetVM` en `Remove-ProvScheme`, MCS elimina todas las instantáneas, incluida la instantánea del disco base, si el esquema de aprovisionamiento está presente en su propio grupo de recursos (BYORG) o en el grupo de recursos administrado por Citrix.

Más información

- Crear y administrar conexiones y recursos
- Conexión con Microsoft Azure
- Crear catálogos de máquinas
- Crear un catálogo de Microsoft Azure
- Administrar catálogos de máquinas

Administrar un catálogo de Microsoft System Center Virtual Machine Manager

August 17, 2024

Administrar catálogos de máquinas describe los asistentes con los que se administra un catálogo de máquinas. La siguiente información incluye detalles específicos de los entornos de virtualización de Microsoft System Center Virtual Machine Manager (VMM).

> **Nota:**
>
> Antes de administrar un catálogo de VMM, debe terminar de crear un catálogo de VMM. Consulte Crear un catálogo de Microsoft System Center Virtual Machine Manager.

Identificar los recursos creados por MCS

A continuación, se muestran las etiquetas que MCS agrega a los recursos. Las etiquetas de la tabla se representan como "clave": "valor".

Resource name	Etiqueta
Máquina virtual de preparación	Cadena de etiqueta: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" Entrada de propiedad personalizada: "XdConfig:"XdProvisioned=True"
VM en catálogo	Cadena de etiqueta: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" Entrada de propiedad personalizada: "XdConfig:"XdProvisioned=True"

Más información

- Crear y administrar conexiones y recursos
- Conexión con Microsoft System Center Virtual Machine Manager
- Crear catálogos de máquinas
- Crear un catálogo de Microsoft System Center Virtual Machine Manager
- Administrar catálogos de máquinas

Administrar un catálogo de VMware

August 17, 2024

Administrar catálogos de máquinas describe los asistentes con los que se administra un catálogo de máquinas. La siguiente información incluye detalles específicos de los entornos de virtualización de VMware.

> **Nota:**
>
> Antes de administrar un catálogo de VMware, debe terminar de crear un catálogo de VMware. Consulte Crear un catálogo de VMware.

Actualizar el ID de carpeta de un catálogo de máquinas

Para actualizar el ID de carpeta de un catálogo de máquinas de MCS, especifique `FolderId` en las propiedades personalizadas del comando `Set-ProvScheme`. Las máquinas virtuales creadas después de actualizar el ID de carpeta se crean bajo este nuevo ID de carpeta. Si esta propiedad no se especifica en `CustomProperties`, las máquinas virtuales se crean en la carpeta en la que se encuentra la imagen maestra.

Siga estos pasos para actualizar el ID de carpeta de un catálogo de máquinas.

1. Abra un explorador web e introduzca la URL de **vSphere Web Client**.
2. Introduzca las credenciales y haga clic en **Login**.
3. Cree una carpeta de ubicación de máquinas virtuales en **vSphere Web Client**.
4. Abra una ventana de PowerShell.
5. Ejecute **asnp citrix*** para cargar los módulos de PowerShell específicos de Citrix.
6. Especifique `FolderID` en el campo `CustomProperties` de `Set-ProvScheme`. En este ejemplo, el valor del ID de la carpeta es`group-v2406`.

```
Set-ProvScheme -ProvisioningSchemeUid "50bb319c-2e83-4a37-9ea1-94
    f630687372" -CustomProperties "<CustomProperties xmlns=""http
    ://schemas.citrix.com/2014/xd/machinecreation"" xmlns:xsi=""
    http://www.w3.org/2001/XMLSchema-instance""><Property xsi:type=
    ""StringProperty"" Name=""FolderId"" Value=""group-v2406"" /></
    CustomProperties>"
```

7. Agregue una VM al catálogo de máquinas mediante Studio.
8. Compruebe la nueva VM en vSphere Web Client. La nueva máquina virtual se crea en la nueva carpeta.

Buscar el ID de carpeta en vSphere

Acceda al explorador de objetos administrados (MOB) en cualquier sistema de servidor ESXi o de vCenter para buscar el ID de la carpeta de las máquinas virtuales.

MOB es una aplicación web de servidor que está integrada en todos los sistemas ESX/ESXi y vCenter Server. Esta utilidad vSphere le permite ver información detallada sobre objetos como máquinas virtuales, almacenes de datos y grupos de recursos.

1. Abra un explorador web e introduzca `http://x.x.x.x/mob`, donde x.x.x.x es la dirección IP del host de vCenter Server o ESX/ESXi. Por ejemplo, https://10.60.4.70/mob.
2. En la página de **inicio** de MOB, haga clic en el valor del **contenido** de la propiedad.
3. Haga clic en el valor de **rootFolder**.
4. Haga clic en el valor de **childEntity**.
5. Haga clic en el valor de **vmFolder**.
6. Puede encontrar el ID de la carpeta en el valor de **childEntity**.

Migración del almacenamiento de máquinas virtuales

Puede mover el almacenamiento en disco de las máquinas virtuales existentes de un almacenamiento antiguo a uno nuevo. Durante la migración, MCS conserva las capacidades de la máquina virtual, como la administración de energía, el restablecimiento del disco del sistema operativo, etc. También puede agregar nuevas máquinas virtuales al catálogo de máquinas mediante el nuevo almacenamiento en disco. Para hacer esto, use el comando de PowerShell `Move-ProvVMDisk`.

Actualmente, solo puede migrar máquinas virtuales persistentes de clonación completa.

El nuevo almacenamiento debe cumplir las siguientes condiciones:

- Debe estar dentro del mismo clúster del antiguo almacenamiento.
- El host en el que se ejecuta la máquina virtual debe tener acceso a los almacenes de datos antiguos y nuevos.

Puede realizar las siguientes tareas:

- Migre el almacenamiento en disco
- Retirar el almacenamiento anterior

Migre el almacenamiento en disco

Para migrar el almacenamiento en disco:

1. Agregue un nuevo almacenamiento a una unidad de alojamiento existente. Cambie el antiguo almacenamiento a **Reemplazado**. Puede hacerlo mediante Web Studio o los comandos de PowerShell.

   - Si usa Web Studio, consulte Modificar la opción de almacenamiento.
   - Si usa los comandos de PowerShell:
     - Ejecute `Add-Hyphostingunitstorage` para agregar el nuevo almacenamiento a la unidad de alojamiento existente.
     - Ejecute `Set-Hyphostingunitstorage` con **Reemplazado** como true para inhabilitar la creación de nuevas máquinas virtuales en el antiguo almacenamiento.

2. Apague las máquinas virtuales y active el **modo de mantenimiento**.

3. Mueva el almacenamiento en disco de las máquinas virtuales al nuevo almacenamiento y actualice la información de almacenamiento. Por ejemplo:

```
Move-ProvVMDisk -ProvisioningSchemeName "myFullCloneProvScheme" -
    VMName ("VMware-TestVM01", "VMware-TestVM02") -DiskType OS,
    Identity -DestinationStorageId datastore1,datastore1
```

4. Obtenga el identificador de la tarea de la migración. Por ejemplo:

```
,(Get-ProvVM -ProvisioningSchemeName xxxxx) | Move-ProvVMDisk -
    ProvisioningSchemeName xxxxx -DiskType OS,Identity -
    DestinationStorageId datastore1,datastore1
```

5. Compruebe el estado de la migración.

   - `(Get-ProvTask -TaskID xxxxxxxxx).DiskMovedVirtualMachines`: Proporciona la lista de máquinas virtuales que migraron correctamente los discos, incluidas las máquinas virtuales que ya migraron al nuevo almacenamiento.
   - `(Get-ProvTask -TaskID xxxxxxxxx).DiskMoveFailedVirtualMachines` : proporciona la lista de máquinas virtuales con una migración fallida.
   - `(Get-ProvTask -TaskID xxxxxxxxx).NotStartedVirtualMachines`: proporciona la lista de máquinas virtuales cuya migración aún no comenzó.
   - `Get-ProvVM -ProvisioningSchemeName xxxxx -VMName "VMware-TestVM01`: proporciona las propiedades de las máquinas virtuales actualizadas después de la migración. Compruebe las propiedades como `StorageId`, `AssignedImage`, `BootedImage`, `IdentityDiskId`, `IdentityDiskStorage` y `LastBootTime`.

Después de migrar los discos de las máquinas virtuales creadas por MCS con instantáneas, es posible que aparezca la advertencia **Se requiere consolidación en VSphere Client**. Para consolidar y evitar la pérdida de datos:

1. Realice una copia de seguridad de VMware VM. Por ejemplo, transfiera todos los archivos de máquina virtual a otra carpeta de un almacén de datos.

2. Cuando aparezca la advertencia, haga clic en **Consolidar** y, a continuación, en **Aceptar** para confirmar la consolidación.

Retirar el almacenamiento anterior

Para dejar de usar el antiguo almacenamiento después de la migración de discos de las máquinas virtuales:

1. Obtenga la información sobre los discos base y el número de máquinas en cada almacenamiento en disco de la unidad de alojamiento. Por ejemplo:

```
$result=Get-ProvSchemeResourceInStorage -ProvisioningSchemeName
    xxxxx
$result
$result.ProvResourceInStorage | Format-List -Property *
```

   Tras una correcta migración, MCS elimina automáticamente el disco base obsoleto y no hay máquinas en el antiguo almacenamiento. Por lo tanto, después de ejecutar el comando, asegúrese de que no haya máquinas ni discos base en el antiguo almacenamiento.

2. Ejecute `Remove-Hyphostingunitstorage` para eliminar por completo el antiguo almacenamiento de la unidad de alojamiento. También puede usar Web Studio para quitar el almacenamiento antiguo.

Identificar los recursos creados por MCS

A continuación, se muestran las etiquetas que MCS agrega a los recursos. Las etiquetas de la tabla se representan como "clave": "valor".

Resource name	Etiqueta
Máquina virtual de preparación	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "XdConfig:"XdProvisioned=True"
VM en catálogo	"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" "XdConfig:"XdProvisioned=True"

Más información

- Crear y administrar conexiones y recursos

- Conexión con VMware
- Crear catálogos de máquinas
- Crear un catálogo de VMware
- Administrar catálogos de máquinas

Administración de energía

August 17, 2024

Con Citrix Virtual Apps and Desktops, puede administrar la energía de las VM aprovisionadas por MCS en varios hipervisores y servicios de nube compatibles. La operación de administración de energía le proporciona:

- Una experiencia de usuario óptima
- Administración de costes y ahorro de energía

Las acciones de energía disponibles son:

- Iniciar
- Apagar
- Reiniciar
- Suspender
- Reanudar
- Forzar reinicio
- Forzar apagado

> **Nota:**
>
> - En el caso de una VM no persistente, el ciclo de energía (apagado/inicio y reinicio) hace que se restablezca el disco del sistema operativo.
> - Las capacidades y los comportamientos de la acción de energía varían según los hipervisores o los servicios de nube.

En este artículo se describen las principales funciones de administración de energía asociadas a determinados hipervisores compatibles.

- Administrar la energía de las VM de AWS
- Administrar la energía de las VM de Azure

Administrar la energía de las VM de AWS

August 17, 2024

Para obtener información sobre los permisos necesarios, consulte Permisos de AWS requeridos.

Hibernación de instancias

El proceso de hibernación almacena el estado en memoria de la instancia, junto con sus direcciones IP privadas y elásticas, lo que le permite continuar exactamente donde lo dejó.

Cuando se indica a una instancia que hiberne, esta escribe el estado en memoria en un archivo del volumen raíz de EBS y, a continuación, se apaga sola. Un volumen de Amazon EBS es un dispositivo de almacenamiento duradero a nivel de bloques que usted puede conectar a sus instancias. Después de conectar un volumen a una instancia, puede usarlo como si fuera un disco duro físico. Cifre el volumen de EBS raíz de la instancia. El cifrado garantiza la protección adecuada de los datos confidenciales cuando se copian de la memoria al volumen de EBS. Para obtener información sobre el cifrado de EBS, consulte Cifrado de Amazon EBS.

Estas son las limitaciones de la hibernación de instancias admitida:

- Se admite una memoria de instancia (RAM) de solo 150 GB
- No se admite el modo de arranque UEFI
- El SSD de uso general y el SSD de E/S por segundo aprovisionado solo se admiten como tipos de volumen de EBS.

Crear máquinas virtuales compatibles con la hibernación

Para crear máquinas virtuales compatibles con la hibernación:

1. Cree una conexión de host. Consulte Conexión con AWS.
2. Inicie una instancia con la raíz de EBS cifrada y la propiedad **Stop-Hibernate** habilitada. Para obtener más información sobre cómo iniciar la instancia, cifrar el volumen de EBS raíz y habilitar la hibernación, consulte https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html/. Utilice esta instancia como imagen maestra para crear una AMI.
3. Prepare la imagen maestra:
    a) Instale un VDA en la imagen maestra. 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. Para obtener más información sobre cómo instalar un VDA, consulte Instalar VDA.

b) Una 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.

4. Cree una AMI a partir de esa instancia. Para obtener información sobre cómo crear una AMI a partir de una instancia, consulte Crear una AMI a partir de una instancia de Amazon EC2.

5. Cree un catálogo de máquinas mediante el comando `New-ProvScheme`. Defina la propiedad personalizada `AwsCaptureInstanceProperties` en **True**. Para obtener información sobre cómo habilitar propiedades de las instancias de AWS en la interfaz de Configuración completa, consulte **Aplicar propiedades de instancias de AWS y etiquetar recursos operativos en la interfaz de Configuración completa**.

```
New-ProvScheme  -AdminAddress "xxx" -CleanOnBoot
-CustomProperties "AwsCaptureInstanceProperties,true;"
-HostingUnitName "xxx" -IdentityPoolName $catalog_name -
   InitialBatchSizeHint 1
-MasterImageVM "xyz.template" -NetworkMapping @{
 "0"="XDHyp:\HostingUnits\MyConn\us-east-2a.availabilityzone
    \10.0.0.0``/24 (vpc-0f1771e45671aedcd).network" }

-ProvisioningSchemeName $catalog_name
-RunAsynchronously -Scope @() -SecurityGroup @("xxx") -
   ServiceOffering "xxx"
```

Para obtener información sobre la creación de catálogos de máquinas mediante los comandos de PowerShell, consulte https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/.

Las máquinas virtuales que se pueden hibernar se crean si:

- Selecciona una AMI creada a partir de una imagen maestra que tenga habilitada la propiedad **Stop-Hibernate**.
- La máquina virtual principal está unida a un dominio y tiene el VDA instalado.
- Selecciona el tamaño de máquina virtual correcto (oferta de servicios) que pueda gestionar la hibernación.

El comando **New-ProvScheme** falla y muestra el mensaje de error correspondiente si:

- La máquina virtual principal está habilitada para la hibernación, pero la oferta de servicios no puede gestionar la hibernación.
- Si la máquina virtual principal no está unida a un dominio y no tiene ningún VDA instalado.

Estado de hibernación de las ofertas de servicios y AMI

Para obtener el estado de hibernación de las ofertas de servicios y las AMI (plantillas), ejecute estos comandos:

- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\WIN2016-ADDC-2021.09.10.145334-a1968709-10c4-47d5-9642-21e743159a7b (ami-0e6c5b33a52d2a6b6).template'`
- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\R6i Sixteen Extra Large Instance.serviceoffering'`

Actualizar la oferta de servicios de un esquema de aprovisionamiento compatible con la hibernación existente

1. Ejecute el comando `Set-ProvScheme`. Por ejemplo,

```
Set-ProvScheme -ProvisioningSchemeName <String> -ServiceOffering <String>
```

El sistema muestra un mensaje de excepción si la oferta de servicios no es compatible.

Cree un catálogo de máquinas compatible con hibernación

Al crear catálogos de máquinas, puede utilizar un perfil de máquina que admita la hibernación.

1. En el asistente para la creación de catálogos, siga las instrucciones hasta seleccionar el perfil de la máquina.
2. En la página **Plantilla de máquina**, haga clic en **Seleccione un perfil de máquina** y seleccione un perfil de máquina.
3. En la página **Máquina virtual**, haga clic en el icono **Modificar** y seleccione una máquina virtual.

   > **Nota:**
   >
   > Si el perfil de la máquina está habilitado para hibernación, el sistema muestra solo las VM que se pueden hibernar.

4. Siga las instrucciones que aparecen en pantalla para completar todos los parámetros. La página **Resumen** muestra el estado de hibernación del catálogo.

   > **Nota:**
   >
   > En Modificar el catálogo de máquinas, al cambiar el perfil de máquina a uno con hibernación habilitada, se le pide que reconfigure las VM en consecuencia.

Actualizar el catálogo de máquinas que admite la hibernación

Si intenta actualizar un catálogo de máquinas existente con un catálogo de máquinas que no admite la hibernación, la actualización fallará y aparecerá el mensaje de error correspondiente.

Administración de energía de máquinas virtuales en hibernación

Puede realizar estas operaciones de administración de energía en las máquinas virtuales hibernadas:

1. Suspender la VM del estado de ejecución.
2. Reanudar la máquina virtual desde el estado suspendido.
3. Reiniciar la máquina virtual desde el estado suspendido.

Administrar la energía de las VM de Azure

August 17, 2024

Para obtener información sobre los permisos necesarios, consulte Permisos de Azure requeridos.

Aprovisionamiento a demanda de Azure

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.

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

Al crear un catálogo con MCS, Azure Portal muestra los grupos de seguridad de red, las interfaces de red, las imágenes base y los discos de identidad de los grupos de recursos.

Azure Portal no muestra ninguna máquina virtual hasta que Citrix Virtual Apps and Desktops inicie una acción de encendido en ella. Existen dos tipos de máquinas con estas diferencias:

- Para una máquina agrupada, el disco del sistema operativo y la caché de reescritura solo existen cuando existe la máquina virtual. Al apagar una máquina agrupada en la consola, la VM no se ve en Azure Portal. Si apaga máquinas de forma rutinaria (por ejemplo, fuera del horario laboral), hay un ahorro significativo en los costes de almacenamiento.
- Para una máquina dedicada, el disco del sistema operativo se crea la primera vez que se encienda la máquina virtual. La VM de Azure Portal permanece almacenada hasta que se elimina la identidad de la máquina. Al apagar una máquina dedicada en la consola, la VM sigue viéndose en Azure Portal.

> **Nota:**
>
> La compatibilidad con los catálogos de Azure creados antes de existir la función de aprovisionamiento bajo demanda (catálogos "antiguos") ha quedado obsoleta. Por lo tanto, cree de nuevo las máquinas virtuales del catálogo antiguo de Azure. Después, los catálogos se aprovisionan bajo demanda, lo que ahorra costes de almacenamiento.

Conservar una máquina virtual aprovisionada durante los ciclos de apagado y encendido

Elija si quiere conservar una máquina virtual aprovisionada al apagar y encender. Utilice el parámetro `New-ProvScheme CustomProperties` de PowerShell. Este parámetro admite una propiedad adicional, `PersistVm`, que sirve para determinar si una máquina virtual aprovisionada persiste durante los ciclos de energía. Establezca la propiedad `PersistVm` en **true** para conservar una máquina virtual cuando se apague, o bien establezca la propiedad en **false** para asegurarse de que la máquina virtual no se conserve al apagarse.

> **Nota:**
>
> La propiedad `PersistVm` solo se aplica a los esquemas de aprovisionamiento con las propiedades `CleanOnBoot` y `UseWriteBackCache` habilitadas. Si no se especifica la propiedad `PersistVm` para máquinas virtuales no persistentes, se eliminan del entorno de Azure al apagarse.

En el ejemplo siguiente, el parámetro `New-ProvScheme CustomProperties` establece la propiedad `PersistVm` en **true**:

```
<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="StorageType" Value="Standard_LRS" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true" />
<Property xsi:type="StringProperty" Name="PersistVm" Value="true" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="demo-resourcegroup" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="Windows_Client" />
</CustomProperties>
```

En el siguiente ejemplo, el parámetro `New-ProvScheme CustomProperties` conserva la caché de reescritura estableciendo `PersistVM` en **true**:


```
New-ProvScheme
-AzureAdJoinType "None"
-CleanOnBoot
-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=`"StorageType`" Value=`"Standard_LRS`" /><
   Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"
   false`" /><Property xsi:type=`"StringProperty`" Name=`"
   PersistOsDisk`" Value=`"true`" /><Property xsi:type=`"
   StringProperty`" Name=`"PersistVm`" Value=`"true`" /><Property xsi:
   type=`"StringProperty`" Name=`"ResourceGroups`" Value=`"demo-
   resourcegroup`" /><Property xsi:type=`"StringProperty`" Name=`"
   LicenseType`" Value=`"Windows_Client`" /></CustomProperties>"
-HostingUnitName "demo"
-IdentityPoolName "NonPersistent-MCSIO-PersistVM"
-MasterImageVM "XDHyp:\HostingUnits\demo\image.folder\scale-test.
   resourcegroup\demo-snapshot.snapshot"
-NetworkMapping @ {
"0"="XDHyp:\HostingUnits\demo\virtualprivatecloud.folder\East US.
   region\virtualprivatecloud.folder\ji-test.resourcegroup\jitest-vnet
   .virtualprivatecloud\default.network" }

-ProvisioningSchemeName "NonPersistent-MCSIO-PersistVM"
 -ServiceOffering "XDHyp:\HostingUnits\demo\serviceoffering.folder\
   Standard_B2ms.serviceoffering" -UseWriteBackCache
 -WriteBackCacheDiskSize 127
 -WriteBackCacheMemorySize 256
```

> **Sugerencia:**
>
> La propiedad `PersistVm` determina si se debe conservar una máquina virtual aprovisionada. La propiedad `PersistOsdisk` determina si se debe conservar el disco del sistema operativo. Para conservar una máquina virtual aprovisionada, conserve primero el disco del sistema operativo. No elimine el disco del SO sin eliminar antes la máquina virtual. Puede utilizar la propiedad `PersistOsdisk` sin especificar el parámetro `PersistVm`.

Personalizar el comportamiento de encendido en caso de error en el cambio del tipo de almacenamiento

Al encenderse, el tipo de almacenamiento de un disco administrado puede no cambiar al tipo deseado debido a un error de Azure. En estos casos, la máquina virtual permanecería apagada y se le enviaría un mensaje de error. Sin embargo, puede optar por encender la máquina virtual incluso cuando no se pueda restaurar el almacenamiento al tipo configurado o mantener la máquina virtual apagada.

- Si configura la propiedad personalizada `FailSafeStorageType` como **verdadera** (configuración predeterminada) o no la especifica en los comandos `New-ProvScheme` y

`Set-ProvScheme`:

  - Al encenderla, la máquina virtual se enciende con un tipo de almacenamiento incorrecto.
  - Al apagarla, la máquina virtual permanece apagada con un tipo de almacenamiento incorrecto.

- Si configura la propiedad personalizada `FailSafeStorageType` como **falsa** en los comandos `New-ProvScheme` o `Set-ProvScheme`:

  - Al encenderla, la máquina virtual permanece apagada con un tipo de almacenamiento incorrecto.
  - Al apagarla, la máquina virtual permanece apagada con un tipo de almacenamiento incorrecto.

Para crear de un catálogo de máquinas:

1. Abra una ventana de PowerShell.
2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
3. Cree un grupo de identidades si aún no se ha creado.
4. Agregue la propiedad personalizada en `New-ProvScheme`. Por ejemplo:

```
1  New-ProvScheme -HostingUnitName "Azure-Resources-1" -
       IdentityPoolName "name" -InitialBatchSizeHint 1
2  -MasterImageVM "XDHyp:\HostingUnits\Azure-Resources-1\image.folder
       \abc.resourcegroup\def.snapshot"
3  -NetworkMapping @{
4   "0"="XDHyp:\HostingUnits\Azure-Resources-1\ght.folder\abc.
        resourcegroup\abc-vnet.virtualprivatecloud\default.network" }
5
6  -ProvisioningSchemeName "name"
7  -ServiceOffering "XDHyp:\HostingUnits\Azure-Resources-1\
       serviceoffering.folder\Standard_DS2_v2.serviceoffering"
8  -CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix
       .com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org
       /2001/XMLSchema-instance`">
9  <Property xsi:type=`"StringProperty`" Name=`"StorageType`" Value=`
       "Premium_LRS`" />
10 <Property xsi:type=`"StringProperty`" Name=`"StorageTypeAtShutdown
       `" Value=`"Standard_LRS`" />
11 <Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
        Value=`"true`" />
12 </CustomProperties>"
```

5. Cree el catálogo de máquinas Para obtener información sobre cómo crear un catálogo con el SDK de PowerShell remoto, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Para actualizar un catálogo de máquinas e incluir la propiedad personalizada `FailSafeStorageType`. Esta actualización no afecta a las máquinas virtuales existentes.

1. Actualice la propiedad personalizada en el comando `Set-ProvScheme`. Por ejemplo:

```
Set-ProvScheme -ProvisioningSchemeName <String> -CustomProperties "
<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
    machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
    instance`">
<Property xsi:type=`"StringProperty`" Name=`"StorageType`" Value=`"
    Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"IdentityDiskStorageType
    `" Value=`"Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
    Value=`"false`" />
</CustomProperties>"
```

Para aplicar el cambio realizado en Set-ProvScheme a las máquinas virtuales existentes, ejecute el comando `Set-ProvVMUpdateTimeWindow` mediante los parámetros `-StartsNow` y `-DurationInMinutes -1`.

1. Ejecute el comando `Set-ProvVMUpdateTimeWindow` mediante los parámetros `-StartsNow` y `-DurationInMinutes -1`. Por ejemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
    VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
```

2. Reinicie las máquinas virtuales.

Crear máquinas virtuales con capacidad de hibernación

En entornos de Azure, puede crear un catálogo de máquinas de MCS que admita la hibernación. Con esta función, puede suspender una máquina virtual y, a continuación, conectarse de nuevo al estado anterior de la misma cuando un usuario vuelva a iniciar sesión.

La capacidad de hibernación se aplica a lo siguiente:

- SO de sesión única
- Máquinas virtuales persistentes y no persistentes
- Escritorios VDI estáticos y aleatorios (agrupados)

Puede reanudar la misma sesión después de hibernar una máquina virtual, independientemente de si el escritorio VDI es estático o aleatorio.

En esta sección, consulte lo siguiente:

- Requisitos previos
- Limitaciones

- Crear y administrar un catálogo de máquinas con capacidad de hibernación
- Crear un catálogo de máquinas para VM con capacidad de hibernación existentes
- Habilitar la hibernación en VM aprovisionadas por MCS existentes
- Comprobar la propiedad de hibernación
- Administración de energía de VM (manual y automatizada)

Requisitos previos para usar la hibernación

Para usar la hibernación, complete las siguientes tareas:

- Instale Azure VM Agent en la imagen maestra para Windows y Linux. El archivo de paginación de la imagen de Windows puede estar en el disco temporal. MCS establece la ubicación del archivo de paginación en la unidad C: del disco base cuando la hibernación está habilitada en el catálogo de máquinas.
- MCS establece automáticamente la propiedad de hibernación para los recursos generados. No es necesario configurar propiedades de los recursos maestros para admitir la hibernación.
- Use un tamaño de máquina virtual en su suscripción compatible con la hibernación.
- Cree un perfil de máquina con capacidad de hibernación (VM o especificación de plantilla) para que las máquinas virtuales hereden la capacidad de hibernación. Para crear la máquina virtual, consulte Getting started with hibernation.

  > **Nota:**
  >
  > Según Microsoft, puede implementar máquinas virtuales con hibernación habilitada desde un disco de sistema operativo. Actualmente, esta función se admite en determinadas regiones y pronto estará disponible en todas ellas. Para obtener más información, consulte Implementar máquinas virtuales con hibernación habilitada desde un disco de sistema operativo.

  Para crear la especificación de plantilla, haga lo siguiente:

  1. Abra Azure Portal. Elija una máquina virtual cuya configuración quiera usar en la plantilla. Seleccione **Export template** en el panel izquierdo.
  2. Desactive la casilla de verificación **Include parameters**. Copie el contexto y guárdelo como archivo JSON, por ejemplo, `VMExportTemplate.json`.
  3. Asegúrese de que el parámetro `hibernationEnabled` tiene el valor **`true`** en la plantilla. Si el valor del parámetro no es **`true`**, compruebe la configuración de máquina virtual que utilizó. Puede especificar un tamaño de máquina virtual compatible en el archivo de plantilla. Sin embargo, también puede especificar el tamaño de la máquina al crear el catálogo.

4. Agregue la plantilla del recurso de interfaz de red al archivo JSON `VMExportTemplate.json`. Como resultado, tiene un archivo de plantilla de Azure Resource Manager con dos recursos.
5. Seleccione **Azure Portal > Template specs > Import template > Choose local template file** para importar este archivo de plantilla como una especificación de plantilla de Azure Resource Manager.
6. Una vez creada la especificación de plantilla de Azure Resource Manager, puede usarla como perfil de máquina.

> **Nota:**
>
> La sincronización con Citrix Studio puede tardar unos minutos.

Para obtener más información, consulte el documento de Microsoft Prerequisites to use hibernation.

Limitaciones

- Solo se admiten los catálogos de máquinas con sistema operativo de sesión única (persistentes y no persistentes).
- Los discos de SO efímeros y las funciones de E/S de MCS no admiten la hibernación de Azure.
- La hibernación puede fallar durante las actualizaciones automáticas de Windows.

Para obtener más información, consulte el documento de Microsoft.

Crear y administrar un catálogo de máquinas con capacidad de hibernación

Para crear máquinas virtuales con capacidad de hibernación, puede crear y administrar un catálogo de máquinas con capacidad de hibernación mediante:

- Web Studio o
- Comandos de PowerShell

Crear un catálogo mediante Web Studio

1. Seleccione **Crear catálogo de máquinas**. Se abrirá el asistente para la creación de catálogos.
2. En la página **Tipo de máquina**, seleccione el tipo de máquina con **SO de sesión única** para este catálogo.
3. En la página **Administración de máquinas**, seleccione la configuración de la siguiente manera:
    a) Selecciones **Máquinas con administración de energía (por ejemplo, máquinas virtuales o PC blade)**.

b) Seleccione **Citrix Machine Creation Services (MCS)**.

4. En la página **Experiencia de escritorio**, seleccione la experiencia de escritorio aleatoria o estática según sea necesario.
5. En la página **Imagen**, seleccione una imagen maestra. Seleccione la casilla **Usar un perfil de máquina** y seleccione un perfil de máquina que admita la hibernación. Haga clic en el texto de ayuda para saber si un perfil de máquina admite la hibernación.
6. En la página **Tipos de licencia y almacenamiento**, seleccione el almacenamiento y la licencia que se usarán en este catálogo.
7. En la página **Máquinas virtuales**, seleccione el número de máquinas virtuales, el tamaño de las máquinas virtuales y la zona de disponibilidad.

   > **Nota:**
   >
   > Solo se muestran los tamaños de máquina que admiten hibernación para que seleccione.

8. En la página **NIC**, agregue las tarjetas de interfaz de red que quiere que usen las máquinas virtuales.
9. En la página **Parámetros del disco**, seleccione el tipo de almacenamiento y el tamaño del disco de caché de reescritura.
10. En la página **Grupo de recursos**, seleccione el grupo de recursos para aprovisionar las máquinas virtuales.
11. En la página **Identidades de máquinas**, seleccione **Crear nuevas cuentas de Active Directory**. A continuación, especifique un esquema de nomenclatura de las cuentas.
12. En la página **Credenciales de dominio**, haga clic en **Introducir credenciales**. Introduzca las credenciales de su dominio para la creación de cuentas en el dominio de Active Directory de destino.
13. En la página **Resumen**, introduzca un nombre para el catálogo de máquinas y, a continuación, haga clic en **Finalizar**.

Cuando termine de crear el catálogo de máquinas de MCS, búsquelo en la lista de catálogos y, a continuación, haga clic en la ficha **Propiedades de plantilla**. El valor del parámetro **Hibernación** debe ser **Admitido**.

Si quiere modificar un catálogo de máquinas, tenga en cuenta las siguientes restricciones:

- Si el catálogo de máquinas actual admite la hibernación, no podrá:
  - Cambiar el tamaño de máquina virtual a uno no compatible con hibernación.
  - Cambiar el perfil de máquina a uno no compatible con hibernación.
- Si el catálogo de máquinas actual no admite la hibernación, no podrá:

- En la actualidad, cambiar el perfil de máquina a uno con capacidad de hibernación mediante Web Studio. Sin embargo, puede hacerlo mediante los comandos de PowerShell. Consulte Habilitar la hibernación en VM aprovisionadas por MCS existentes.

Crear un catálogo de máquinas para administrar VM con capacidad de hibernación existentes
Si ya tiene máquinas virtuales con capacidad de hibernación y quiere suspenderlas y reanudarlas, cree un catálogo de máquinas para importar esas máquinas virtuales para la administración de energía.

> **Nota:**
>
> Puede crear un catálogo de máquinas que contenga máquinas virtuales compatibles y no compatibles con hibernación. Sin embargo, si quiere usar funcionalidad relacionada con la hibernación, debe crear el catálogo de máquinas solo con VM compatibles con la hibernación.

Para crear un catálogo con las VM con capacidad de hibernación existentes mediante Web Studio, siga las instrucciones que aparecen en pantalla y preste atención a los siguientes parámetros clave:

1. En la página **Administración de máquinas**, seleccione **Máquinas con administración de energía** y, a continuación, seleccione **Otro servicio o tecnología** como forma de implementar las máquinas.
2. En la página **Máquinas virtuales**, agregue o importe solo máquinas virtuales con capacidad de hibernación.

Crear un catálogo de máquinas mediante comandos de PowerShell Una vez que cumpla con todos los requisitos para usar la hibernación, puede crear un catálogo de máquinas compatible con hibernación mediante el comando `New-ProvScheme`. Para obtener información sobre cómo crear un catálogo con Remote PowerShell SDK, consulte New-ProvScheme.

Al crear el catálogo, puede comprobar si un tamaño de máquina virtual y un perfil de máquina admiten la hibernación o no con los siguientes comandos de PowerShell:

- Para el tamaño de VM, ejecute el siguiente comando y compruebe si la propiedad `supportsHibernation` tiene el valor **True**. Por ejemplo,

```
Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -LiteralPath @
    ("XDHyp:\HostingUnits\ <VirtualNetwork> \serviceoffering.
    folder") | select Name, AdditionalData | ConvertTo-Json
```

- Para el perfil de máquina, ejecute el siguiente comando y compruebe si la propiedad `supportsHibernation` tiene el valor **True**. Por ejemplo,


```
Get-ChildItem -AdminAddress "MyDDC.MyDomain.local" -LiteralPath @
    ("XDHyp:\HostingUnits\ <VirtualNetwork> \machineprofile.folder
    \abc.resourcegroup")|select Name, AdditionalData|ConvertTo-
    Json
```

Si quiere modificar un catálogo de máquinas, tenga en cuenta las siguientes restricciones:

- Si el catálogo de máquinas actual admite la hibernación, no podrá:
  - Cambiar el tamaño de máquina virtual a uno no compatible con hibernación
  - Cambiar el perfil de máquina a uno no compatible con hibernación
- Si el catálogo de máquinas actual no admite la hibernación, no podrá:
  - En la actualidad, cambiar el perfil de máquina a uno con capacidad de hibernación mediante Web Studio. Sin embargo, puede hacerlo mediante los comandos de PowerShell. Consulte Habilitar la hibernación en VM aprovisionadas por MCS existentes.

Para obtener información sobre cómo modificar el tamaño de máquina virtual y el perfil de máquina de un catálogo mediante el SDK de PowerShell remoto, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Set-ProvScheme/.

Habilitar la hibernación en VM aprovisionadas por MCS existentes

Puede habilitar la hibernación de Azure en:

- VM aprovisionadas por MCS con Windows de un catálogo de máquinas creado sin un disco temporal.
- VM aprovisionadas por MCS con Linux de un catálogo de máquinas creado con y sin un disco temporal.

> **Nota:**
>
> - Las máquinas virtuales aprovisionadas por MCS existentes deben tener instalado un agente de VM de Azure.
> - Actualmente, solo puede usar el comando de PowerShell para habilitar esta función.

Para hacerlo:

1. Abra una ventana de **PowerShell**.
2. Ejecute `asnp citrix*` para cargar módulos de PowerShell específicos de Citrix.
3. Compruebe la configuración de las máquinas. Por ejemplo:

```
Get-ProvScheme | select ProvisioningSchemeName,
    ProvisioningSchemeVersion
```


4. Habilite la hibernación en este catálogo de máquinas mediante el comando `Set-ProvScheme`. Por ejemplo:

```
Set-ProvScheme -provisioningSchemeName xxxx
-machineprofile <path-to-machineprofile-with-hibernation-enabled>
-serviceoffering "XDHyp:\HostingUnits\msc-dev\serviceoffering.
   folder\Standard_D4as_v5.serviceoffering"
```

5. Solicite la actualización de las máquinas virtuales existentes de un catálogo de máquinas.

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeUid xxxx -VMName <
   String[]
```

6. Reinicie las máquinas virtuales para desencadenar las actualizaciones en las máquinas virtuales existentes. Por ejemplo:

```
New-BrokerHostingPowerAction -machinename "<name>" -Action Restart
```

Comprobar la propiedad de hibernación

Puede comprobar la propiedad de hibernación de un catálogo de máquinas, una máquina virtual y una máquina de broker mediante los comandos de PowerShell:

- Para comprobar la propiedad de hibernación de un esquema de aprovisionamiento, ejecute los siguientes comandos de PowerShell. El valor del parámetro `HibernationEnabled` debe ser `True`.

```
(Get-ProvScheme -provisioningSchemeName <YourSchemeName>).
   VMMetadata -join "" |  ConvertFrom-Json | Select
   HibernationEnabled
```

- Para comprobar la propiedad de hibernación de una VM de aprovisionamiento, ejecute los siguientes comandos de PowerShell. El valor del parámetro `SupportsHibernation` debe ser `True`.

```
(Get-ProvVM -VMName <YourVMName>).CustomVmData | ConvertFrom-Json
    | Select SupportsHibernation
```

- Para comprobar la capacidad de hibernación de una máquina de broker, ejecute los siguientes comandos de PowerShell. Las acciones de energía **Suspender** y **Reanudar** indican la capacidad de hibernación.

```
(Get-BrokerMachine -MachineName <YourMachineName>).
   SupportedPowerActions
```


Administración de energía de VM con capacidad de hibernación

Puede realizar estas operaciones de administración de energía en las máquinas virtuales con capacidad de hibernación:

- **Suspender** la VM desde el estado de ejecución
- **Reanudar** la VM desde el estado suspendido
- **Forzar el apagado** de la VM desde un estado suspendido
- **Forzar el reinicio** de la VM desde el estado suspendido

Consulte los siguientes apartados para obtener más información:

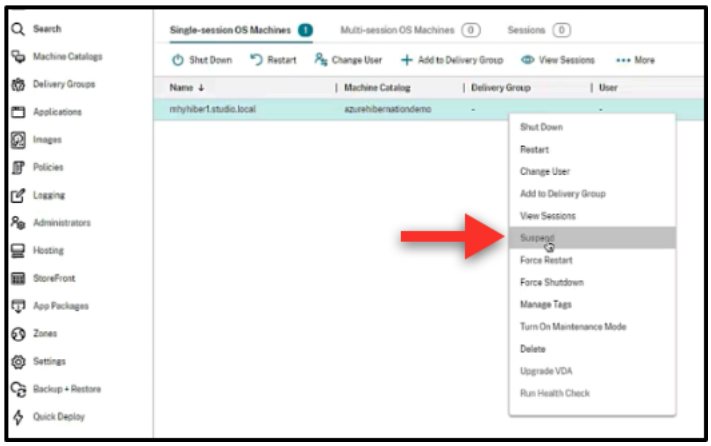
- Suspender
- Reanudar

Suspender Puede suspender una máquina virtual de una de las siguientes maneras:

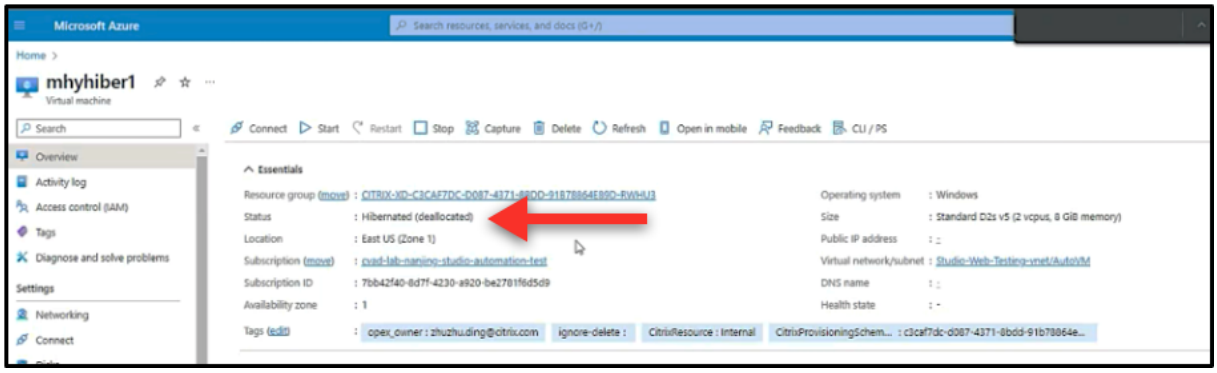
- **Manualmente** con Web Studio
- **Automáticamente** mediante la directiva de tiempo de espera: Para obtener más información, consulte Otros parámetros.

Para suspender manualmente una VM:

1. Haga clic con el botón secundario en la máquina virtual y seleccione **Suspender**. Haga clic en **Sí** para confirmar la acción. El **Estado de energía** cambia de **Suspendiendo** a **Suspendido**.

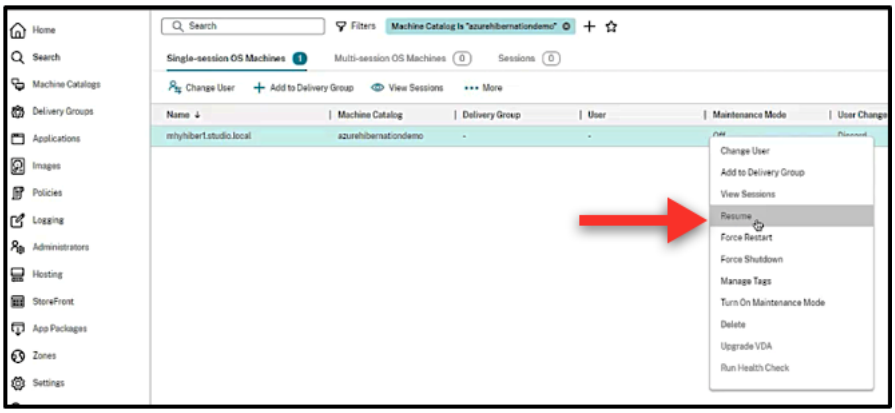


Puede comprobar el estado de la máquina virtual en Azure Portal.

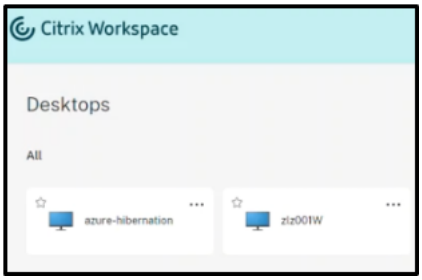


Reanudar Puede reanudar una máquina virtual hibernada de una de las siguientes formas:

- **Manualmente**:
  - Los administradores pueden reanudar la máquina virtual mediante Web Studio.

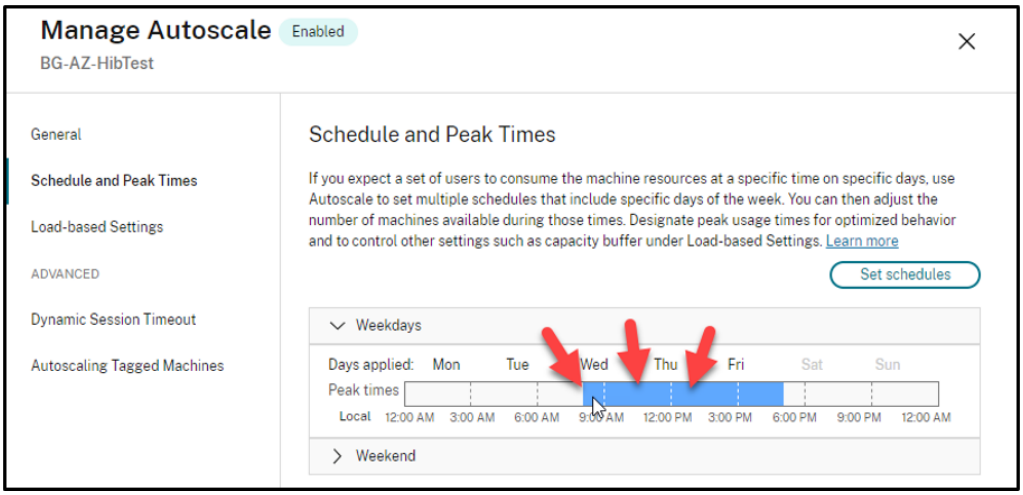


  - Los usuarios finales pueden iniciar la máquina virtual mediante el menú de Citrix Workspace una vez que hacen clic en el icono del escritorio.

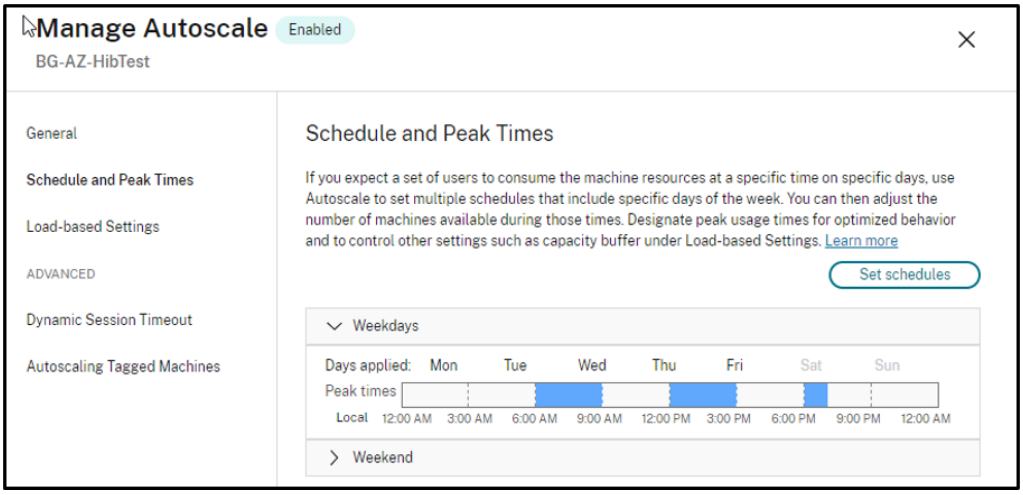


- **Automáticamente**:
  - Autoscale puede encender automáticamente las máquinas hibernadas si configura correctamente las horas punta. Puede establecer las horas punta en intervalos de 30 minutos haciendo clic en el horario. Cada marco azul representa una franja horaria marcada como hora punta. Las horas punta pueden tener franjas horarias consecutivas y no consecutivas.

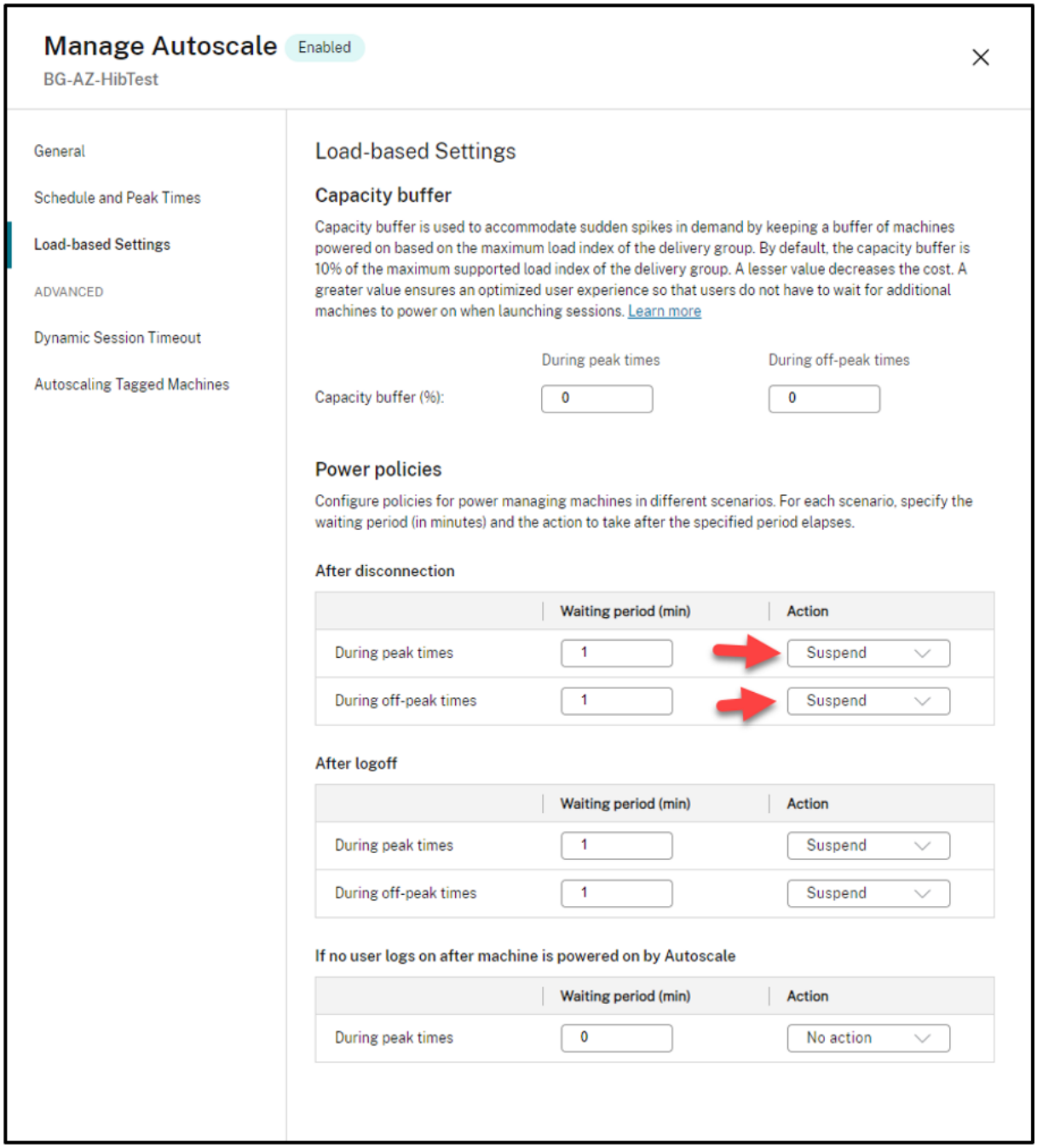
* Franjas horarias consecutivas



* Franjas horarias no consecutivas



> **Nota:**
>
> En **Administrar Autoscale > Parámetros por carga**, si la **Acción** está configurada como **Suspender**, asegúrese de que todas las VM de ese grupo de entrega tengan capacidad de hibernación. De lo contrario, las máquinas virtuales que no se pueden hibernar seguirán funcionando.



Recibir mensajes de advertencia en caso de error de hibernación

Puede recibir mensajes de advertencia mediante un comando de PowerShell `Get-ProvOperationEvent` en caso de que se produzca un error de hibernación en las máquinas virtuales aprovisionadas por MCS y existentes con capacidad de hibernación. Para obtener información sobre el comando de PowerShell, consulte la documentación del SDK, Get-ProvOperationEvent.

Para hacerlo:

1. Abra una ventana de PowerShell.
2. Ejecute `asnp citrix*` para cargar módulos de PowerShell específicos de Citrix.
3. Ejecute `Get-ProvOperationEvent` para recibir el mensaje de advertencia en caso de que haya un error de hibernación.

```
Get-ProvOperationEvent -filter {
  OperationName -eq "Suspend"  }
```

Resultado:

```
EventAdditionalData : Error code = OperationNotAllowed and Error message = The Hibernate-Deallocate Operation cannot be performed on a VM that has extension 'AzureHibernateExtension' in failed state. For more information, see https://aka.ms/hibernate-resume/errors. Error details from the extension : Enabling
                  hibernate failed. Response from the powercfg command. Exit Code: 1. Error message:
                  Hibernation failed with the following error: The request is not supported.

                  The following items are preventing hibernation on this system.
                    The current Device Guard configuration has disabled hibernation.
                    An internal system component has disabled hibernation.
                         Hypervisor
                  Status: 409
                  ErrorCode: OperationNotAllowed

                  Content:
                  {

                    "error": {

                      "code": "OperationNotAllowed",
                      "message": "The Hibernate-Deallocate Operation cannot be performed on a VM that has extension ' AzureHibernateExtension' in failed state. For more information, see https://aka.ms/hibernate-resume/errors. Error details from the extension : Enabling hibernate failed. Response from the
                  powercfg command. Exit Code: 1. Error message:\nHibernation failed with the following error: The request is not supported.\r\r\n\r\nThe following items are preventing hibernation on this system.\r\n\tThe current Device Guard configuration has disabled hibernation.\r\n\tAn internal system
```



```
                    component has disabled hibernation.\r\n\t\
                       tHypervisor"
                    }

                }

EventCategory       : Warning
EventDateTime       : 1/11/2024 4:18:31 AM
EventId             : 0
EventMessage        : Failed to suspend machine my-resource-group/
   my-vm.
EventSeverity       : Important
EventSource         : AzureRmPlugin
EventState          : New
LinkedObjectType    : ProvisioningScheme
LinkedObjectUid     : 589cb600-6e65-479f-9d47-9715c4732366
OperationName       : Suspend
OperationTargetName : my-resource-group/my-vm
OperationTargetType : VirtualMachine
OperationType       : PowerManagement
Recommendation      :
```

Solución de problemas de hibernación Aparece el siguiente mensaje de error si intenta habilitar las funciones de hibernación y de inicio seguro de máquina virtual; sin embargo, la configuración del sistema operativo invitado no es correcta.

Código de error	Mensaje de error
OperationNotAllowed	The Hibernate-Deallocate Operation cannot be performed on a VM that has extension 'AzureHibernateExtension'in failed state. Para obtener más información, consulte https://aka.ms/hibernate-resume/errors/. Error details from the extension : Enabling hibernate failed. Response from the powercfg command. Exit Code: 1. Error message: Hibernation failed with the following error: The request is not supported. The following items are preventing hibernation on this system. **The current Device Guard configuration has disabled hibernation. An internal system component has disabled hibernation**.

Para resolver el problema, asegúrese de que la virtualización esté habilitada en la máquina virtual invitada. Por ejemplo, confirme que Hyper-V está habilitado en un entorno Windows. Según la lim-

itación de Microsoft Windows, la hibernación solo se admite con la virtualización anidada cuando el inicio seguro está habilitado en la máquina virtual.

Para obtener más información sobre los mensajes de advertencia, consulte el documento de Microsoft Troubleshooting VM hibernation.

> **Nota:**
>
> Los mensajes de error relacionados con un error al reanudar una máquina virtual estarán disponibles en una versión futura.

Más información

Para obtener más información sobre la hibernación de Citrix Azure, consulte el artículo de Citrix Tech Zone.

Directivas de seguridad

August 17, 2024

En este artículo se describen las funciones de seguridad de varios servicios de nube compatibles. Las funciones de seguridad incluyen:

- Grupos de seguridad
- Arranque seguro
- Prestaciones de cifrado

Grupos de seguridad

August 17, 2024

Un grupo de seguridad es un grupo de reglas de seguridad para filtrar el tráfico de red entre los recursos de una red virtual. Las reglas de seguridad permiten o deniegan el tráfico de red entrante o saliente hacia o desde varios tipos de recursos. Cada regla especifica las siguientes propiedades:

- Nombre: Un nombre único dentro del grupo de seguridad de red
- Prioridad: Las reglas se procesan por orden de prioridad, procesándose los números más bajos antes que los más altos, ya que los números más bajos tienen una prioridad más alta

- Origen o destino: Cualquier dirección IP individual, bloque de enrutamiento entre dominios sin clases (CIDR - por ejemplo, 10.0.0.0/24), etiqueta de servicio o grupo de seguridad de aplicaciones
- Protocolo: Los protocolos en función de los cuales se agregan reglas para cada grupo de seguridad
- Dirección: Si la regla se aplica al tráfico entrante o saliente
- Intervalo de puertos: Puede especificar un puerto individual o un rango de puertos
- Acción: Permitir o denegar

Para obtener más información sobre los hipervisores compatibles, consulte lo siguiente:

- Grupos de seguridad en AWS
- Grupos de seguridad en Microsoft Azure
- Grupos de seguridad en Google Cloud Platform

Grupos de seguridad en AWS

Los grupos de seguridad actúan como firewalls virtuales que controlan el tráfico de las instancias en su nube VPC. Debe agregar reglas a los grupos de seguridad que permitan que las instancias en la subred pública se comuniquen con instancias en la subred privada. También puede asociar estos grupos de seguridad a cada instancia ubicada en la nube VPC. Las reglas de entrada controlan el tráfico entrante a la instancia y las reglas de salida controlan el tráfico saliente de la instancia.

Para obtener más información sobre la configuración de red durante la preparación de la imagen, consulte Configuración de red durante la preparación imágenes.

Al iniciar una instancia, puede especificar uno o más grupos de seguridad. Para configurar grupos de seguridad, consulte Configurar grupos de seguridad.

Grupos de seguridad en Microsoft Azure

Citrix Virtual Apps and Desktops admite grupos de seguridad de red en Azure. Se presupone que los grupos de seguridad de red estén asociados a subredes. Para obtener más información, consulte Grupos de seguridad de red.

Para obtener más información sobre el grupo de seguridad de red creado durante la preparación de la imagen, consulte Crear un catálogo de máquinas con una imagen de Azure Resource Manager.

Grupos de seguridad en Google Cloud Platform

Durante la preparación de un catálogo de máquinas, se prepara una imagen de máquina para que sirva como disco del sistema de la imagen maestra del catálogo. Cuando se produce este proceso,

el disco se conecta temporalmente a una máquina virtual. Esta máquina virtual debe ejecutarse en un entorno aislado que impida todo el tráfico de red entrante y saliente. Esto se logra mediante un par de reglas de firewall "deny-all"(denegar todo). Para obtener más información, consulte Reglas de firewall.

Arranque seguro

August 17, 2024

El arranque seguro está diseñado para garantizar que solo se utilice software de confianza para arrancar el sistema. El firmware tiene una base de datos de certificados de confianza y verifica que la imagen que carga esté firmada por uno de tales certificados. Si esa imagen carga otras imágenes, entonces esa imagen también debe verificarse de la misma manera. vTPM es una instancia de software virtualizada de un módulo TPM físico tradicional. vTPM habilita la atestación midiendo toda la cadena de arranque de la máquina virtual (UEFI, SO, sistema y controladores).

Consulte lo siguiente para obtener más información sobre los servicios compatibles en la nube:

- Arranque seguro en Google Cloud Platform
- Arranque seguro en Microsoft Azure
- Arranque seguro en VMware

Arranque seguro en Google Cloud Platform

Puede aprovisionar máquinas virtuales blindadas en GCP. Una máquina virtual blindada está reforzada mediante un conjunto de controles de seguridad que proporcionan integridad verificable de sus instancias de Compute Engine, con prestaciones avanzadas de seguridad de plataforma como el arranque seguro, un módulo de plataforma virtual segura, firmware UEFI y supervisión de la integridad.

Para obtener más información sobre el uso de PowerShell para crear un catálogo con máquinas virtuales blindadas, consulte Uso de PowerShell para crear un catálogo con máquinas virtuales blindadas.

> **Nota:**
>
> Si instala Windows 11 en la imagen maestra, debe habilitar vTPM durante el proceso de creación de la imagen maestra. Además, debe habilitar vTPM en el origen del perfil de máquina (plantilla de instancia o máquina virtual). Para obtener información sobre la creación de máquinas virtuales de Windows 11 en el nodo de arrendatario único, consulte Crear máquinas virtuales de Windows 11 en el nodo de arrendatario único.

Arranque seguro en Microsoft Azure

En los entornos de Azure, puede crear catálogos de máquinas habilitados con inicio seguro. Azure ofrece el inicio seguro como una forma integrada de mejorar la seguridad de las máquinas virtuales de 2.ª generación. Inicio seguro protege contra técnicas de ataque avanzadas y persistentes. En la base del inicio seguro está el arranque seguro de la máquina virtual. El inicio seguro también utiliza el vTPM para realizar la atestación remota por parte de la nube. Se utiliza para comprobar el estado de la plataforma y para tomar decisiones basadas en la confianza. Puede habilitar el arranque seguro y el vTPM de forma individual. Para obtener más información sobre cómo crear un catálogo de máquinas con inicio seguro, consulte Catálogos de máquinas con inicio seguro.

Arranque seguro en VMware

MCS permite crear catálogos de máquinas con una plantilla de VMware con un vTPM conectado como origen para la entrada del perfil de la máquina. Si Windows 11 está instalado en la imagen maestra, es necesario tener habilitado vTPM para la imagen maestra. Por lo tanto, la plantilla de VMware, que es el origen del perfil de la máquina, debe tener el vTPM conectado. Para obtener más información, consulte Crear un catálogo de máquinas mediante un perfil de máquina.

Prestaciones de cifrado

August 17, 2024

Las prestaciones de cifrado protegen el contenido de las máquinas virtuales de los ataques de invitados malintencionados en un host de máquina virtual compartido y de los ataques lanzados por el software de control del hipervisor que administra todas las máquinas virtuales del host.

Consulte lo siguiente para obtener más información sobre los servicios compatibles en la nube:

- Prestaciones de cifrado en AWS
- Prestaciones de cifrado en Google Cloud Platform
- Prestaciones de cifrado en Microsoft Azure

Prestaciones de cifrado en AWS

En esta sección se describen las prestaciones de cifrado en los entornos de virtualización de AWS.

Cifrado automático

Puede activar el cifrado automático de los nuevos volúmenes de Amazon EBS y de las copias de instantáneas creadas en su cuenta. Para obtener más información, consulte Cifrado automático.

Prestaciones de cifrado en Google Cloud Platform

En esta sección se describen las prestaciones de cifrado de los entornos de virtualización de Google Cloud Platform (GCP).

Si necesita más control sobre las operaciones con claves del que permiten las claves de cifrado gestionadas por Google, puede utilizar claves de cifrado gestionadas por el cliente. Cuando se utiliza una clave de cifrado administrada por el cliente, Cloud Storage cifra un objeto con la clave en el momento en que se almacena en un depósito y lo descifra automáticamente cuando el objeto se entrega a los solicitantes. Para obtener más información, consulte Claves de cifrado administradas por el cliente.

Puede utilizar claves de cifrado administradas por el cliente (CMEK) para catálogos de MCS. Para obtener más información, consulte Uso de claves de cifrado administradas por el cliente (CMEK).

Prestaciones de cifrado en Microsoft Azure

En esta sección se describen las prestaciones de cifrado en los entornos de virtualización de Azure.

Cifrado del lado del servidor de Azure

La mayoría de los discos administrados de Azure se cifran mediante el cifrado de Azure Storage, que utiliza el cifrado del lado del servidor (SSE) para proteger sus datos y para ayudarle a satisfacer sus exigencias en materia de seguridad y cumplimiento. Citrix Virtual Apps and Desktops admite claves de cifrado administradas por el cliente para los discos administrados por Azure a través de Azure Key Vault. Para obtener más información, consulte Cifrado del lado del servidor de Azure.

Cifrado de discos de Azure en el host

Puede crear un catálogo de máquinas de MCS con capacidad de cifrado en el host.

Este método de cifrado no cifra los datos a través del almacenamiento de Azure. El servidor que aloja la máquina virtual cifra los datos y, a continuación, los datos cifrados fluyen a través del servidor de almacenamiento de Azure. Por lo tanto, este método de cifrado cifra los datos de extremo a extremo.

Para obtener más información sobre cómo crear un catálogo de máquinas de MCS con capacidad de cifrado en el host, consulte Cifrado de discos de Azure en el host.

Cifrado doble de Azure

El cifrado doble es el cifrado del lado de la plataforma (predeterminado) y el cifrado administrado por el cliente (CMEK). Por lo tanto, si usted es un cliente altamente confidencial al que le preocupa el riesgo asociado a cualquier algoritmo de cifrado, implementación o claves comprometidas, puede optar por este doble cifrado. Los discos de datos y del SO persistentes, las instantáneas y las imágenes se cifran en REST con doble cifrado. Para obtener más información, consulte Cifrado doble en discos administrados.

Máquinas virtuales confidenciales de Azure

Las máquinas virtuales de computación confidencial de Azure garantizan que su escritorio virtual esté cifrado en memoria y protegido mientras se usa.

Puede usar MCS para crear un catálogo con máquinas virtuales confidenciales de Azure. Para crear dicho catálogo, debe usar el flujo de trabajo del perfil de máquina. Puede usar una máquina virtual o una especificación de plantilla de Azure Resource Manager como entrada para un perfil de máquina.

Para obtener más información, consulte Máquinas virtuales confidenciales de Azure.

Crear grupos de entrega

August 17, 2024

> **Nota:**
>
> Puede administrar la implementación de Citrix Virtual Apps and Desktops mediante dos consolas de administración: Web Studio (basada en la web) y Citrix Studio (basada en Windows). Este artículo se refiere únicamente a Web Studio. Para obtener información sobre Citrix Studio, consulte el artículo equivalente en Citrix Virtual Apps and Desktops 7 2212 o versiones anteriores.

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, además de las aplicaciones y los 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 ha creado un sitio y un catálogo de máquinas, sin un grupo de entrega, Web Studio le guiará hasta el punto de partida para crear uno.
2. Si ya creó un grupo de entrega y quiere crear otro, siga estos pasos:
    a) Seleccione **Grupos de entrega**. Seleccione **Crear grupo de entrega** en el panel de acciones.
    b) Para organizar grupos de entrega mediante carpetas, cree carpetas en la carpeta **Delivery Groups** predeterminada. Para obtener más información, consulte Crear una carpeta.
    c) Seleccione la carpeta en la que quiere crear el grupo y, a continuación, haga clic en **Crear grupo de entrega**. Se abre el asistente de creación de grupos.
3. El asistente se inicia con la página **Introducción**, que se puede eliminar de futuros inicios de este asistente.
4. El asistente le guiará a través de las páginas que se describen en la sección siguiente. 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:

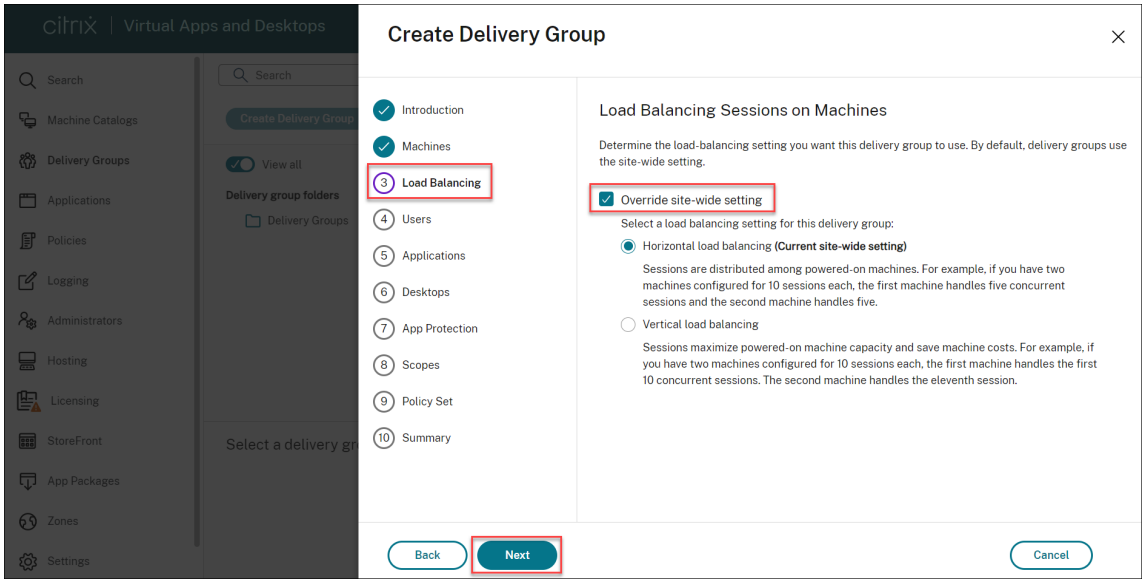
- Al menos una máquina debe permanecer sin uso en el catálogo de máquinas seleccionado.
- Se puede especificar un mismo catálogo en más de un grupo de entrega. Una máquina se puede utilizar en un solo grupo de entrega.
- Un grupo de entrega puede usar más de un catálogo de máquinas. Sin embargo, esos catálogos deben contener los mismos tipos de máquina (SO multisesión, SO de sesión única 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. Actualice catálogos 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 es compatible con la versión más antigua de VDA. Este es el *nivel funcional* del grupo. Por ejemplo: si una de las máquinas tiene la versión 7.1 de VDA y otras máquinas tienen la versión actual, todas las máquinas del grupo podrán usar 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.

- Cada máquina de un catálogo de acceso con Remote PC se asocia automáticamente a un grupo de entrega. Cuando se crea un sitio de acceso con Remote PC, se crea automáticamente un catálogo de máquinas llamado "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 de acceso con Remote PC
  - Comprobación relacionada con AppDisk

Paso 2. Equilibrio de carga

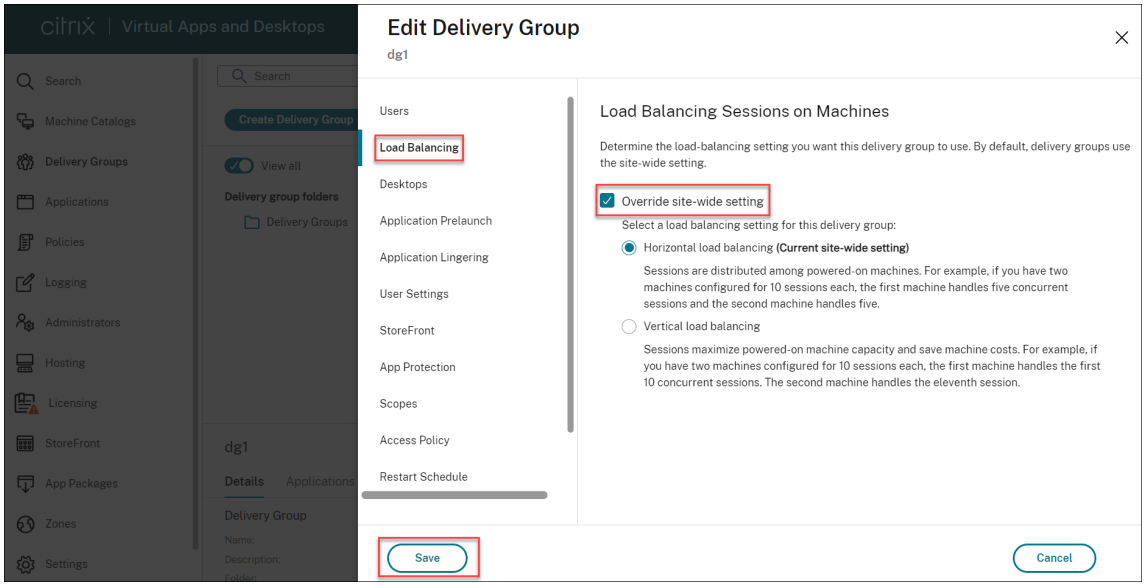
Para configurar los parámetros de equilibrio de carga al crear un grupo de entrega:

1. Inicie sesión en Web Studio.
2. En el panel de navegación de la izquierda, haga clic en **Grupos de entrega**.
3. En la página **Grupos de entrega**, haga clic en **Crear grupo de entrega**.
4. En el asistente de **Crear grupo de entrega**, haga clic en **Siguiente**. Se abre el asistente de **Máquina**.
5. En el asistente de **Máquinas**, seleccione un catálogo de máquinas y haga clic en **Siguiente**. Se abre el asistente de **Equilibrio de carga**.
6. En el asistente de **Equilibrio de carga**, seleccione la casilla de verificación **Supeditar la configuración al nivel del sitio**.
7. Seleccione la opción **Equilibrio de carga horizontal** o **Equilibrio de carga vertical** según sea necesario y haga clic en **Siguiente**.

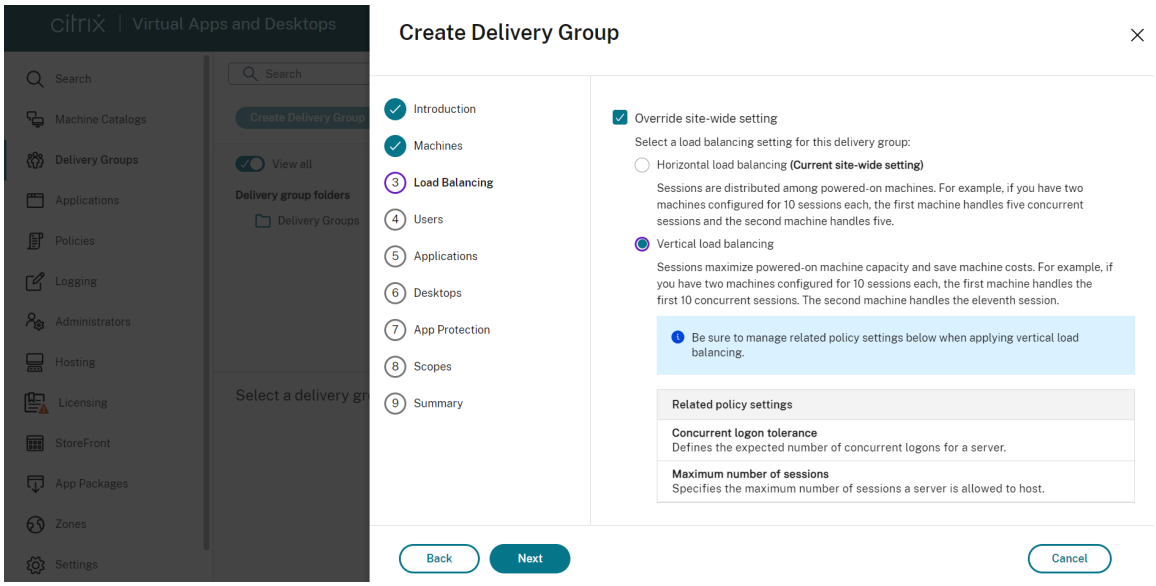


Para configurar los parámetros de equilibrio de carga al modificar un grupo de entrega existente:

1. Inicie sesión en Web Studio.
2. En el panel izquierdo, haga clic en **Grupos de entrega**.
3. Seleccione un **grupo de entrega** de la lista y haga clic en **Modificar**. Se abre el asistente de **Modificar grupo de entrega**.
4. En la página **Modificar grupo de entrega**, haga clic en **Equilibrio de carga**.
5. Selecciona la casilla **Supeditar la configuración al nivel del sitio**.
6. Seleccione la opción **Equilibrio de carga horizontal** o **Equilibrio de carga vertical** según sea necesario y haga clic en **Guardar**.



> **Nota:**
>
> Cuando se aplique el parámetro Equilibrio de carga vertical, asegúrese de que las directivas **Tolerancia de inicios de sesión simultáneos** y **Número máximo de sesiones** estén configuradas correctamente.



Para obtener más información sobre el equilibrio de carga a nivel de sitio y de grupo de entrega, consulte Equilibrar la carga de las máquinas

Paso 3. Tipo de entrega

Esta página solo aparece si ha seleccionado un catálogo que contiene máquinas estáticas (asignadas) con SO de sesión única.

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 sesión única o SO multisesión, se entiende que el tipo de entrega serán aplicaciones y escritorios, por lo que podrá entregar aplicaciones, escritorios o ambos.

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 Web Studio. Las reglas predeterminadas de la directiva que rigen los derechos a las aplicaciones incluyen 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 concreto, sin restringir el acceso a 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 sesión única, 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 multisesión, 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 Anon*XYZ*, 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:

- De forma predeterminada, las nuevas aplicaciones que agregue se colocan en una carpeta denominada Aplicaciones. 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 va a agregar. 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 Web Studio; de lo contrario, los usuarios ven nombres duplicados en la aplicación Citrix Workspace.

- Puede agregar aplicaciones empaquetadas a los grupos de entrega estáticos de sesión única y a los de acceso con Remote PC. Los paquetes se montan automáticamente cada vez que los usuarios inician sesión en sus escritorios o equipos remotos.

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**.
- **Manualmente:** Se trata de aplicaciones que se encuentran en un VDA del grupo de entrega o en otro lugar de la red. Al seleccionar este origen, se abre una nueva página en la que se especifica una aplicación para agregarla de las siguientes maneras:
  - Especifique la ruta al archivo ejecutable, el directorio de trabajo, los argumentos opcionales de línea de comandos y los nombres simplificados de los administradores y los usuarios.
  - Seleccione una aplicación de un VDA del grupo de entrega. Para ello, haga clic en **Examinar**, introduzca las credenciales de acceso al VDA, espere a que se conecte al VDA y, a continuación, seleccione una aplicación del VDA. Los campos de la página se rellenan automáticamente con las propiedades de la aplicación seleccionada.
- **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 aplicaciones detectadas. Agregue las aplicaciones y haga clic en **Aceptar**.
- **Paquetes de aplicaciones:** Aplicaciones en paquetes de aplicaciones en formato App-V, MSIX o de conexión de aplicaciones MSIX. Al seleccionar este origen, se abre una nueva página en la que puede seleccionar el tipo de origen y, a continuación, las aplicaciones que quiere agregar de la pantalla resultante.

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 estáticas de sesión única y especificó "Escritorios" en la página **Tipo de entrega**, esta página se llamará **Asignaciones de usuario - Escritorio**.

- Si eligió un catálogo que contiene máquinas estáticas de sesión única y especificó "Aplicaciones"en la página **Tipo de entrega**, esta página se llamará **Asignaciones de usuario - Máquinas de aplicación**.

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.)
- Utilice los botones de opción para iniciar un escritorio o asignar una máquina al iniciar el escritorio. 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 estáticas de sesión única, 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 estáticas de sesión única). Al inhabilitar un escritorio, se detiene la entrega del escritorio. Al inhabilitar una regla de asignación de escritorios, se 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 -MaxPerEntitlementInst
    2
  ```

- Para obtener ayuda, use el cmdlet Get-Help. Por ejemplo, `Get-Help Set-BrokerEntitlementPolic -Parameter MaxPerEntitlementInstances`.

Paso 7: Configuración de la caché de host local

Este parámetro solo está visible para los grupos de entrega que contienen máquinas agrupadas de sesión única con administración de energía.

De forma predeterminada, esas máquinas no están disponibles en el modo de caché de host local (LHC) debido a los riesgos de exposición de los datos. Para cambiar el comportamiento predeterminado y hacer que estén disponibles para las conexiones de nuevos usuarios en el modo LHC, seleccione **Mantener los recursos disponibles**.

Como alternativa, puede cambiar el comportamiento predeterminado mediante comandos de PowerShell. Para obtener más información, consulte Compatibilidad con aplicaciones y escritorios.

> **Importante:**
>
> Habilitar el acceso a máquinas agrupadas de sesión única con administración de energía puede provocar que los datos y los cambios de las sesiones de usuario anteriores estén presentes en las sesiones posteriores.

Paso 8. Resumen

Escriba un nombre para el grupo de entrega. También puede especificar una descripción (opcional), que aparece en Web Studio y en la aplicación Citrix Workspace.

Revise la información de resumen y, a continuación, haga clic en **Finalizar**.

Administrar grupos de entrega

August 17, 2024

> **Nota:**
>
> Puede administrar la implementación de Citrix Virtual Apps and Desktops mediante dos consolas de administración: Web Studio (basada en la web) y Citrix Studio (basada en Windows). Este artículo se refiere únicamente a Web Studio. Para obtener información sobre Citrix Studio, consulte el artículo equivalente en Citrix Virtual Apps and Desktops 7 2212 o versiones anteriores.

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:

- Las aplicaciones contienen 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

- Ver detalles del grupo
- Cambiar el método de entrega
- Cambiar direcciones de StoreFront
- Cambiar el nivel funcional
- Administrar grupos de entrega de acceso con Remote PC
- Organizar grupos de entrega mediante carpetas
- Administrar App Protection

Ver detalles del grupo

1. Use la función de búsqueda para localizar un grupo de entrega específico. Para obtener instrucciones, consulte Buscar instancias.
2. En los resultados de la búsqueda, seleccione un grupo según sea necesario.
3. Consulte la siguiente tabla para ver las descripciones de las columnas del grupo.
4. Haga clic en una ficha del panel de detalles inferior para obtener más información sobre este grupo.

Columna	Descripción
Grupo de entrega	El nombre del grupo y el tipo de sesión. Los tipos de sesión incluyen sistemas operativos de sesión única y sistemas operativos multisesión.
Entregando	El tipo de recursos que entrega este grupo. Los valores posibles incluyen Aplicaciones, Escritorios y Aplicaciones y escritorios. Aparece "Asignación de máquina estática"si el grupo de entrega está formado por máquinas dedicadas.

Columna	Descripción
Sesión en uso	La cantidad de máquinas que están configuradas y la cantidad de máquinas que están en estado desconectado.
Recuento asignado	La cantidad de máquinas del catálogo asignadas a un grupo de entrega.
Carpeta	La ubicación del grupo en el árbol de **grupos de entrega**. Muestra el nombre de la carpeta en la que se encuentra el grupo (incluida la barra invertida al final) o − si el grupo está en el nivel raíz.

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 la izquierda.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar** en la barra de 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 **Guardar** para aplicar los cambios y cerrar la ventana.

Cambiar direcciones de StoreFront

1. Seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar** en la barra de acciones.
3. En la página **StoreFront**, seleccione o agregue direcciones URL de StoreFront. La aplicación Citrix Workspace, que se instala en cada máquina del grupo de entrega, utiliza estas direcciones URL.
4. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta. También puede hacer clic en **Guardar** para aplicar los cambios y cerrar la ventana.

También puede seleccionar **StoreFront** en el panel de la izquierda para especificar las direcciones del servidor de StoreFront.

Cambiar el nivel funcional

Cambie el nivel funcional del grupo de entrega después de actualizar la versión de los VDA de sus máquinas y los catálogos de máquinas que contienen las máquinas utilizadas en el grupo de entrega.

Antes de comenzar:

- 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 utilizando versiones anteriores de VDA, las funciones más recientes del producto no están disponibles. Para obtener más información, consulte la documentación de la actualización de versiones.

Para actualizar la versión de un grupo de entrega:

1. Seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo de entrega y haga clic en **Actualizar grupo de entrega** en la barra de acciones. La acción **Cambiar el nivel funcional** solo aparece si se detectan los VDA actualizados.

La pantalla le indica qué máquinas, si las hay, no se pueden cambiar al nivel funcional y por qué. A continuación, puede cancelar la acción del cambio, resolver los problemas de la máquina y realizar el cambio de nuevo.

Una vez finalizado el cambio, puede revertir las máquinas a sus estados anteriores. Seleccione el grupo de entrega y, a continuación, seleccione **Deshacer cambio de nivel funcional** en la barra de acciones.

Administrar grupos de entrega de acceso con Remote PC

Si una máquina del catálogo de acceso con Remote PC no está asignada, 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 prioritario. La prioridad determina el grupo de entrega asignado de la máquina cuando 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 mayor prioridad. 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. Las cuentas de máquinas o las 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 la izquierda.
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**.

Organizar grupos de entrega mediante carpetas

Puede crear carpetas para organizar grupos de entrega y simplificar el acceso a estos.

Roles obligatorios De forma predeterminada, debe tener uno de estos roles integrado para crear y administrar carpetas de grupos de entrega: administrador de la nube, administrador total o administrador de grupos de entrega. Si es necesario, puede personalizar roles para crear y administrar carpetas de grupos de entrega. Para obtener más información, consulte Permisos requeridos.

Crear una carpeta de grupos de entrega Antes de empezar, planifique cómo organizar los grupos de entrega. Se deben tener en cuenta las siguientes cuestiones:

- Puede anidar carpetas en hasta cinco niveles (excluyendo la carpeta raíz predeterminada).
- Una carpeta puede contener grupos de entrega y subcarpetas.
- Todos los nodos (como los nodos **Catálogos de máquinas**, **Aplicaciones** y **Grupos de entrega**) comparten un árbol de carpetas en el back-end. Para evitar conflictos de nombres con otros nodos al cambiar el nombre de las carpetas o moverlas, le recomendamos que asigne nombres diferentes a las carpetas de primer nivel de los distintos nodos.

Para crear una carpeta de grupos de entrega, siga estos pasos:

1. Seleccione **Grupos de entrega** en el panel de la izquierda.
2. En la jerarquía de carpetas, seleccione una carpeta y, a continuación, seleccione **Crear carpeta** en la barra de **acciones**.
3. Introduzca un nombre para la nueva carpeta y, a continuación, haga clic en **Listo**.

> **Sugerencia:**
>
> Si crea una carpeta en una ubicación no deseada, puede arrastrarla a la ubicación correcta.

Mover un grupo de entrega

Puede mover un grupo de entrega de una carpeta a otra. Estos son los pasos detallados:

1. Seleccione **Grupos de entrega** en el panel de la izquierda.
2. Puede ver grupos por carpeta. También puede activar **Ver todo** por encima de la jerarquía de carpetas para ver todos los grupos a la vez.
3. Haga clic con el botón secundario en un grupo y, a continuación, seleccione **Mover grupos de entrega**.
4. Seleccione la carpeta a la que quiere mover el grupo y, a continuación, haga clic en **Listo**.

> **Sugerencia:**
>
> Puede arrastrar un grupo a una carpeta.

Administrar carpetas de grupos de entrega

Puede eliminar, cambiar el nombre y mover las carpetas de grupos de entrega.

Tenga en cuenta que solo puede eliminar una carpeta si ni sus subcarpetas contienen grupos de entrega.

Para administrar una carpeta, siga estos pasos:

1. Seleccione **Grupos de entrega** en el panel de la izquierda.
2. En la jerarquía de carpetas, seleccione una carpeta y, a continuación, seleccione una acción en la barra de **acciones**:
   - Para cambiar el nombre de la carpeta, seleccione **Cambiar nombre de carpeta**.
   - Para eliminar la carpeta, seleccione **Eliminar carpeta**.
   - Para mover la carpeta, seleccione **Mover carpeta**.
3. Siga las instrucciones que aparecen en pantalla para completar los pasos restantes.

Permisos requeridos En esta tabla, se enumeran los permisos necesarios para realizar acciones en carpetas de grupos de entrega.

Acción	Permisos requeridos
Crear carpetas de grupos de entrega	Crear carpeta de grupos de entrega
Eliminar carpetas de grupos de entrega	Quitar carpeta de grupos de entrega
Mover carpetas de grupos de entrega	Mover carpeta de grupos de entrega
Cambiar el nombre de carpetas de grupos de entrega	Modificar carpeta de grupos de entrega
Mover grupos de entrega a carpetas	Modificar carpeta de grupos de entrega y modificar propiedades de grupo de entrega

Administrar App Protection

Esta información es complementaria a la protección de aplicaciones. Tenga en cuenta estos detalles:

- Debe tener derechos de App Protection válidos. Para adquirir la funcionalidad App Protection, contacte con su representante de ventas de Citrix.
- App Protection requiere confianza en XML. Para habilitar la confianza en XML, vaya a **Parámetros > Habilitar confianza en XML**.
- En cuanto a la protección contra la captura de pantalla:
  - En Windows y macOS, solo la ventana del contenido protegido está en blanco. App Protection está activa cuando una ventana protegida no está minimizada.
  - En Linux, toda la captura aparece vacía. App Protection está activa tanto si una ventana protegida está minimizada como si no.

Para elegir un método de App Protection para un grupo de entrega, siga estos pasos:

1. Seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo y, a continuación, seleccione **Modificar** en la barra de acciones.
3. En la página **App Protection**, aparecen las siguientes opciones:

Opciones	Descripción
No se aplica	Seleccione esta opción para no aplicar el parámetro.

Opciones	Descripción
Aplicar a este grupo de entrega	Seleccione las opciones **Protección contra el registro de tecleo** o **Protección contra las capturas de pantalla**. Pase el cursor sobre cada uno de estos parámetros para leer los detalles de la información sobre herramientas.
Aplicar contextualmente	Para aplicar este parámetro, configure la directiva de acceso en la página de **parámetros de la directiva de acceso**. a) Haga clic en **Directiva de acceso** en el panel izquierdo y, a continuación, en **Agregar**. b) En la página **Agregar directiva**, haga lo siguiente • i. Introduzca un **nombre de directiva** y configure los parámetros según sea necesario. • ii. En los campos **Filtro** y **Valor**, introduzca los detalles y haga clic en **Listo**. La nueva directiva aparece en la página **App Protection**. Habilite los parámetros necesarios para esta directiva. • iii. Haga clic en **Guardar**.

4. En la página **Grupo de entrega**, seleccione el **grupo de entrega** y haga clic en la ficha **Detalles** en la parte inferior. Se muestran los nuevos parámetros de **App Protection** aplicados.

Usuarios

En esta sección, se tratan los siguientes temas:

- Cambiar los parámetros del usuario
- Agregar o quitar usuarios
- Administrar asignaciones de usuarios:

Cambiar los parámetros 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 la izquierda.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar** en la barra de 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 **Guardar** 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. **Nota:** Al cambiar la zona horaria de un grupo de entrega, es posible que se reinicien las máquinas de ese grupo de entrega. Para evitarlo, asegúrese de cambiar los parámetros de la zona horaria fuera del horario de producción.
Habilitar Secure ICA	Oculta todas las comunicaciones que tienen lugar desde y hacia las máquinas del grupo de entrega mediante 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 más métodos de cifrado como el cifrado TLS cuando se trabaje en redes públicas. Asimismo, SecureICA no comprueba la integridad de los datos.

Agregar o quitar 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 la izquierda.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar** en la barra de 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 **Guardar** 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 dos encabezados de columna, separados por una coma. Asegúrese de que el primer encabezado sea `Machine Account` y el segundo encabezado sea `User Names`. (Puede incluir encabezados adicionales, pero no son compatibles). Las líneas siguientes del archivo contienen datos separados por comas. Las entradas `Machine Account` pueden ser SID de equipo, nombres de dominio completo (FQDN) o pares de dominio y nombre de equipo.

Para importar o exportar la información de usuarios:

1. Seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar** en la barra de 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 **Guardar** para aplicar los cambios y cerrar la ventana.

Administrar asignaciones de usuarios

Administre las asignaciones de usuarios para las máquinas de un grupo de entrega. Cuando se configuran las reglas de asignación de escritorios para el grupo de entrega, las máquinas se asignan aleatoriamente a los usuarios al iniciar el escritorio por primera vez y permanecen asignadas a los usuarios a menos que se modifiquen sus asignaciones de usuario. Si quiere asignar manualmente una máquina no asignada a usuarios específicos o cambiar la asignación de usuario existente para una máquina, siga los pasos que se describen en este tema para hacer cambios. Con estos pasos, también puede modificar los nombres que aparecen en la aplicación Citrix Workspace para las máquinas asignadas a los usuarios.

Estos son los pasos detallados:

1. En la consola, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo y, a continuación, seleccione **Modificar** en la barra de acciones.
3. En el panel izquierdo, seleccione **Asignación de máquinas**. Aparecen los siguientes detalles de cada máquina del grupo:
    - **Nombre de la máquina:** Muestra el nombre de una máquina.
    - **Nombre simplificado:** Muestra el nombre simplificado de la máquina en la aplicación Citrix Workspace.

- **Usuarios:** Muestra los usuarios asignados a esta máquina. Si se configuran las reglas de asignación de escritorios, las máquinas se asignan aleatoriamente a los usuarios al iniciar el escritorio por primera vez y permanecen asignadas a ellos a menos que se modifiquen sus asignaciones de usuario.

4. Busque una máquina y, a continuación, asígnele usuarios o cambie su asignación de usuario:
   - Haga clic en **Examinar** para buscar usuarios.
   - En la columna **Usuarios**, introduzca una lista de nombres de usuario separados por punto y coma.
   - Haga clic en **Importar desde un archivo CSV** para importar los detalles de la configuración mediante un archivo CSV.
5. (Opcional) Si la máquina está asignada a usuarios, modifique su nombre simplificado según sea necesario.

   > **Nota:**
   >
   > El campo Nombre simplificado solo se habilita cuando la máquina está asignada a usuarios:
   >
   > - Si la máquina está asignada a un usuario en función de una regla de asignación de escritorios, este campo muestra el nombre simplificado configurado en esa regla.
   > - Si la máquina se asigna manualmente a los usuarios y el campo se deja en blanco, se usa el nombre publicado del grupo de entrega (si se especifica) como nombre simplificado de la máquina. Se usa el nombre del grupo de entrega si no se especifica el nombre publicado. Tenga en cuenta que solo puede especificar los nombres publicados para los grupos de entrega a través de PowerShell.

6. Seleccione **Aplicar** para aplicar los cambios y deje la ventana abierta. También puede seleccionar **Aceptar** para aplicar los cambios y cerrar la ventana.

Máquinas

- Cambio de asignaciones de máquinas a usuarios
- Habilitar la caché de host local para los VDA agrupados de sesión única con administración de energía
- 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
- Cargar máquinas administradas
- Máquinas con energía administrada

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 la izquierda.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar** en la barra de 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 **Guardar** para aplicar los cambios y cerrar la ventana.

Habilitar la caché de host local para los VDA agrupados de sesión única con administración de energía

De forma predeterminada, las máquinas agrupadas de sesión única con administración de energía no están disponibles en el modo de caché de host local. Puede anular el comportamiento predeterminado por grupo de entrega. Estos son los pasos detallados:

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.

   En la lista de grupos, los grupos que contienen máquinas agrupadas de sesión única aprovisionadas por MCS o Citrix Provisioning muestran un icono de advertencia.

2. Seleccione el grupo que quiera y después seleccione **Modificar** en la barra de acciones.
3. En la página **Caché del host local**, seleccione **Mantener los recursos disponibles**.
4. Seleccione **Aplicar** para aplicar los cambios que haya hecho y deje la ventana abierta. También puede seleccionar **Aceptar** para aplicar los cambios y cerrar la ventana.

Como alternativa, puede anular el comportamiento predeterminado mediante comandos de PowerShell. Para obtener más información, consulte Compatibilidad con aplicaciones y escritorios.

> **Importante:**
>
> Habilitar el acceso a máquinas agrupadas de sesión única con administración de energía puede

> provocar que los datos y los cambios de las sesiones de usuario anteriores estén presentes en las sesiones posteriores.

Cambio de la cantidad máxima de máquinas por usuario en un grupo de entrega

1. Seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar** en la barra de 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 **Guardar** 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 la izquierda.
2. Seleccione un grupo y, a continuación, seleccione **Ver máquinas** en la barra de acciones.
3. Seleccione una máquina y, a continuación, seleccione **Actualizar máquinas** en la barra de acciones.

Para elegir otra imagen, seleccione **Imagen** 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 reciben

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 la izquierda.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar** en la barra de 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 **Guardar** 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 la izquierda.
2. Seleccione un grupo y, a continuación, seleccione **Ver máquinas** en la barra de acciones.
3. Compruebe que la máquina esté apagada.
4. Seleccione la máquina y, a continuación, haga clic en **Quitar del grupo de entrega** en la barra de 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 los recursos 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.

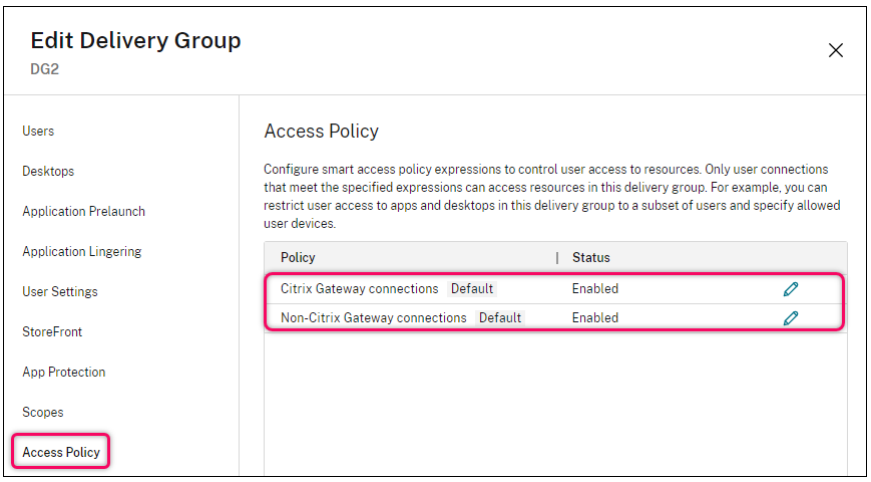
- **Restringir el acceso de los usuarios a través de expresiones de directiva de Smart Access:** Puede configurar reglas de directiva de acceso para controlar el acceso de los usuarios a un grupo de entrega específico. Por ejemplo:
  - Restringir el acceso a un subconjunto de usuarios y especificar los dispositivos de usuario permitidos.
  - Restringir el acceso a los usuarios conectados a través de Workspace (en lugar de StoreFront).
  - Restringir el acceso a los usuarios conectados a través de una URL específica de Workspace.

En esta sección se explica cómo restringir el acceso de los usuarios a los grupos de entrega mediante reglas de directiva de acceso:

- Acerca de las reglas de directiva de acceso
- Agregar reglas de directiva de acceso
- Administrar reglas de directiva de acceso mediante Web Studio
- Agregar y ajustar reglas de directiva con PowerShell

Acerca de las reglas de directiva de acceso Puede configurar varias reglas de directiva de acceso para un grupo de entrega. Las aplicaciones y los escritorios de un grupo de entrega aparecen en StoreFront o Workspace de un usuario cuando la conexión del usuario coincide con cualquier regla de directiva de acceso que haya definido para el grupo de entrega, independientemente del orden.

Cada regla se puede habilitar o inhabilitar de forma individual. Una regla inhabilitada se ignora cuando se evalúa la directiva de acceso.



En Web Studio, la lista Directiva de acceso incluye las siguientes reglas de directiva de SmartAccess predeterminadas. Puede agregar más si es necesario.

- **Conexiones de Citrix Gateway.** Esta directiva solo permite que las conexiones de usuario realizadas a través de Citrix Gateway accedan a los recursos del grupo de entrega. Las conexiones

de usuario realizadas a través de Workspace cuando las funciones Postura del dispositivo o Ubicación de red están habilitadas también se consideran conexiones a través de Citrix Gateway.

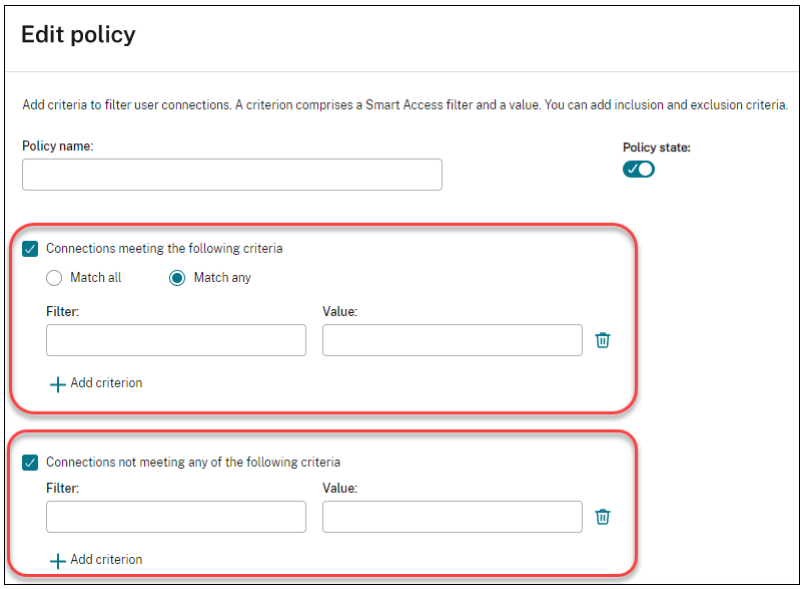
- **Conexiones que no son de Citrix Gateway.** Esta directiva solo permite que las conexiones de usuario no realizadas a través de Citrix Gateway accedan a los recursos del grupo de entrega.

> **Nota:**
>
> - Para evitar que las reglas predeterminadas anulen una recién configurada, debe inhabilitar las reglas predeterminadas o ajustarlas para excluir los filtros usados en la nueva directiva.
> - Las directivas predeterminadas no se pueden eliminar, pero se pueden inhabilitar. Para inhabilitar una directiva, haga clic en el icono **Modificar** y, a continuación, cambie el **estado de la directiva** a **Inhabilitada**.
> - La lista de directivas también muestra las reglas agregadas mediante los comandos de PowerShell. Esas directivas se pueden eliminar, pero no se pueden modificar en Web Studio.

Agregar reglas de directiva de acceso mediante Web Studio Una regla de directiva de acceso comprende un conjunto de filtros. Para obtener más información sobre los filtros, consulte este artículo. Al agregar una regla de directiva de acceso, agrega varios filtros de condición a la regla según sea necesario.

Para agregar una directiva para un grupo de entrega mediante Web Studio, siga estos pasos:

1. En la consola, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar** en la barra de acciones.
3. En la página **Directiva de acceso**, haga clic en **Agregar**. Aparecerá la página **Agregar directiva**.



4. En el campo **Nombre de la directiva**, escriba un nombre descriptivo para la directiva. El nombre debe ser único en la implementación.

5. Para definir los criterios para las conexiones de usuario permitidas, siga estos pasos:

   a) Seleccione **Conexiones que cumplen estos criterios**.

   b) Haga clic en **Agregar criterio**.

   c) En el campo **Filtro**, escriba el nombre del filtro que quiere usar. En el campo **Valor**, escriba el valor deseado para el filtro. Por ejemplo, para permitir que solo los usuarios conectados a través de Workspace (en lugar de StoreFront) accedan a los recursos de este grupo de entrega, introduzca `Citrix-Via-Workspace` para **Filtro** y `True` para **Valor**.

   d) Para agregar otros criterios, repita los pasos b-c.

   e) Seleccione la relación entre los criterios:

      - **Hacer coincidir cualquiera**. Permite acceder solo cuando la conexión de usuario entrante cumple con alguno de los criterios de filtro configurados.
      - **Hacer coincidir todo**. Permite acceder solo cuando la conexión de usuario entrante cumple con todos los criterios de filtro configurados.

6. Para definir los criterios para las conexiones de usuario prohibidas, siga estos pasos:

   a) Seleccione **Conexiones que no cumplen ninguno de estos criterios**.

   b) Haga clic en **Agregar criterio**.

   c) En el campo **Filtro**, escriba el nombre del filtro que quiere usar. En el campo **Valor**, escriba el valor deseado para el filtro. Por ejemplo, para prohibir que los usuarios conectados a través de la URL `example.cloud.com` de Workspace accedan a los recursos de este grupo de entrega. introduzca `Citrix.Workspace.UsingDomain` para **Filtro** y `example.cloud.com` para **Valor**.

   d) Para agregar otros criterios, repita los pasos b-c.

   > **Nota:**
   >
   > Las conexiones de usuario que cumplan cualquiera de los criterios configurados no podrán acceder a los recursos de este grupo de entrega.

7. Haga clic en **Listo**.

   La nueva directiva aparece en la lista de directivas.

8. Revise y ajuste las reglas de directiva predeterminadas para evitar superposiciones involuntarias con las conexiones cubiertas por esta nueva directiva. Para ajustar las directivas existentes, utilice los siguientes métodos:

   - Inhabilite las reglas de directiva predeterminadas.

- Configure las reglas de directiva predeterminadas para excluir los filtros de SmartAccess que agregó a los criterios de inclusión de la nueva directiva. Para obtener más información, consulte Administrar reglas de directiva mediante Web Studio y Agregar y administrar reglas de directiva de acceso mediante PowerShell.

> **Importante:**
>
> Como se explica en Acerca de las reglas de directiva de acceso, cuando la conexión de un usuario coincide con una o más reglas de directiva de un grupo de entrega, el usuario obtiene acceso a sus recursos. Por lo tanto, después de crear una regla, debe revisar y ajustar cuidadosamente las reglas existentes para evitar cualquier superposición involuntaria con las conexiones cubiertas por la nueva regla.

Administrar reglas de directiva de acceso mediante Web Studio Puede usar los criterios de inclusión y exclusión para ajustar las directivas predeterminadas. Por ejemplo, para restringir el acceso a un subconjunto de esas conexiones, siga estos pasos:

1. Modifique una directiva predeterminada.
2. Seleccione **Conexiones que cumplen uno de estos criterios**.
3. Agregue, modifique o quite las expresiones de directiva de SmartAccess para los supuestos de acceso de usuario permitidos.

Para obtener más información, consulte la documentación de Citrix Gateway.

Agregar y administrar reglas de directiva de acceso mediante PowerShell Puede usar los siguientes cmdlets de PowerShell para agregar y administrar reglas de directiva de acceso para los grupos de entrega:

- New-BrokerAccessPolicyRule
- Get-BrokerAccessPolicyRule
- Set-BrokerAccessPolicyRule
- Rename-BrokerAccessPolicyRule
- Remove-BrokerAccessPolicyRule

Para obtener más información, consulte los artículos correspondientes en la documentación para desarrolladores de Citrix.

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 la izquierda.
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 la barra de acciones.

   Para activar el modo de mantenimiento en una máquina, seleccione **Ver máquinas** en la barra de acciones. Seleccione una máquina y, a continuación, seleccione **Activar modo de mantenimiento** en la barra de 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 la barra de 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:

- El modo de mantenimiento está activado, tal y 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**. 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 la izquierda.
2. Seleccione un grupo y, a continuación, seleccione **Ver máquinas** en la barra de acciones.
3. Seleccione la máquina y, a continuación, haga clic en una de las siguientes entradas en la barra de acciones:

    - **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 forzosas, 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

> **Nota:**
>
> - Cuando se aplica una programación de reinicios a un grupo de entrega con Autoscale habilitado, sus máquinas simplemente se apagan para que Autoscale las encienda.
> - Cuando se aplican programaciones de reinicios a máquinas aleatorias de sesión única, esas máquinas se apagan en lugar de reiniciarse para ahorrar costes. Le recomendamos que utilice Autoscale para encender las máquinas.
> - Al cambiar la zona horaria de un grupo de entrega, es posible que se reinicien las máquinas de ese grupo de entrega. Para evitarlo, asegúrese de cambiar los parámetros de la zona horaria fuera del horario de producción.

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 que tienen la etiqueta.

Por ejemplo: Supongamos que todas las máquinas se encuentran en un solo grupo de entrega. 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.

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 solo una sola vez.
- Por tanto, cuanto más difieran las programaciones en la hora de inicio y la duración, más probabilidades hay de 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 más rápidamente que el reinicio 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 la izquierda.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar** en la barra de 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.

Agregar (aplicar) etiquetas Si configura una programación de reinicios que usa una restricción por etiquetas, compruebe que esa etiqueta se haya agregado 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 la izquierda.
2. Seleccione el grupo de entrega que contiene las máquinas controladas por 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 la barra de 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 la izquierda.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar** en la barra de acciones.
3. En la página **Programación de reinicios**, haga clic en **Agregar**.
4. En la página **Agregar programación de reinicios**:
   - Para habilitar la programación, seleccione **Sí**. Para inhabilitar la programación, seleccione **No**.
   - Escriba un nombre y una descripción para la programación.
   - En **Restringir a la etiqueta**, aplique una restricción de etiqueta.

- En **Incluir máquinas en modo de mantenimiento**, elija si quiere incluir en esta programación las máquinas que estén en modo de mantenimiento. Para usar PowerShell en su lugar, consulte Reinicios programados para máquinas en modo de mantenimiento.
- En **Frecuencia de reinicio**, seleccione la frecuencia con que se produce el reinicio: diariamente, semanalmente, mensualmente o una única vez. Si selecciona **Semanalmente** o **Mensualmente**, puede especificar uno o varios días específicos.
- Para **Se repite cada**, especifique la frecuencia con la que quiere que se realice la programación.
- Para **Fecha de inicio**, especifique una fecha de inicio para la primera instancia de la programación.
- En **Empezar el reinicio a**, especifique, en el formato de 24 horas, la hora del día en que comenzará el reinicio.
- En **Duración del reinicio**:
  - Si no quiere utilizar el reinicio natural, seleccione **Reiniciar todas las máquinas a la vez** o **Reiniciar todas las máquinas en un plazo determinado**.
  - Si quiere utilizar el reinicio natural, seleccione **Reiniciar todas las máquinas después de la purga de sesiones**.

    Al poner en marcha un programa de reinicio que esté configurado para usar el reinicio natural:

    * Todas las máquinas inactivas pertenecientes al grupo de entrega se reinician inmediatamente
    * Las máquinas pertenecientes a un grupo de entrega con una o más sesiones activas se reiniciarán cuando se cierren todas las sesiones.

    > **Nota:**
    >
    > Puede usar esta opción para máquinas con administración de energía y también para máquinas sin administración de energía.

- 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 aparece 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 una cuenta atrás para reiniciarse, incluya la variable **%m%**. A menos que haya optado por reiniciar todas las máquinas a la vez, el mensaje de notificación aparece en cada máquina en el momento correspondiente antes de que empiece el reinicio.

5. Haga clic en **Listo** para aplicar los cambios y cerrar la ventana **Agregar programación de reinicios**.
6. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta. También puede hacer clic en **Guardar** para aplicar los cambios y cerrar la ventana.

Reiniciar después de la purga Hay otro valor de duración de reinicio disponible al utilizar PowerShell para crear una programación de reinicio de máquinas (`New-BrokerRebootSchedulev2` o `Set-BrokerRebootSchedulev2`).

Al habilitar la función de reinicio después de la purga con el parámetro `-UseNaturalReboot <Boolean>`, todas las máquinas se reinician después de purgar todas las sesiones. Cuando llega el momento del reinicio, las máquinas se ponen en estado de purga y se reinician una vez cerradas todas las sesiones.

Esta funcionalidad se admite para grupos de entrega que contienen máquinas de sesión única o multisesión. Puede usar esta opción para máquinas con administración de energía y también para máquinas sin administración de energía.

En un entorno local, esta función solo está disponible al utilizar PowerShell. La función no está disponible en Web Studio.

Modificar, quitar, habilitar o inhabilitar una programación de reinicios

1. Seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar** en la barra de 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 en 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 (a las 2:00). La interrupción dura seis horas (hasta las 08:00). La programación de reinicios comienza cuando se restaura la conexión entre el Delivery Controller y la base de datos del sitio. Ahora, los reinicios de VDA se dan cinco horas después de la programación original, lo que provoca 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 este parámetro se omite o su valor es cero, 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 Web Studio.

Reinicios programados para máquinas en modo de mantenimiento

> **Nota:**
>
> Esta función solo está disponible en PowerShell. La opción `IgnoreMaintenanceMode` está disponible en Citrix Virtual Apps and Desktops 7 2006 y versiones posteriores.

Para indicar si una programación de reinicio afecta a las máquinas que están en modo de mantenimiento, utilice la opción `IgnoreMaintenanceMode` con los cmdlets `BrokerRebootScheduleV2`.

Por ejemplo: el cmdlet siguiente crea una programación que reinicia las máquinas que están en el modo de mantenimiento (además de las máquinas que no se hallan en el modo de mantenimiento).

```
New-Brokerrebootschedulev2 rebootSchedule1 -DesktopGroupName <myDesktopGroup
> -IgnoreMaintenanceMode $true
```

El cmdlet siguiente modifica programaciones de reinicio existentes.

```
Set-Brokerrebootschedulev2 rebootSchedule1 -IgnoreMaintenanceMode
$true
```

Para obtener más información, consulte la ayuda de los cmdlets. Esta función solo está disponible en PowerShell.

Máquinas con carga administrada en grupos 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 una sesión.

  Puede supervisar el índice de carga en el SDK, en Director (Supervisión) y en la búsqueda de Web 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.

Máquinas con energía administrada en grupos 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 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 extra 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.

  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 la izquierda.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en la barra de 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 **Guardar** 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:

- Establezca `PeakDisconnectAction` en “Nada”
- Establezca `OffPeakDisconnectAction` en “Apagar”
- Establezca `OffPeakDisconnectTimeout` en “10”

Para obtener más información sobre las acciones de desconexión en la directiva de energía, consulte 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.

Si quiere 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 `LegacyPeakTransitionDisconnectedBehaviour` del Registro en `1`, el equivalente de *true* que habilita el comportamiento anterior. De forma predeterminada, el valor es `0` o *false*, y 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:

- Tener una sesión desconectada.
- No tener ninguna acción de energía pendiente.
- Pertenecer a un grupo de entrega de VDI (sesión única) que pasa a otro período de tiempo.
- Tener 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.

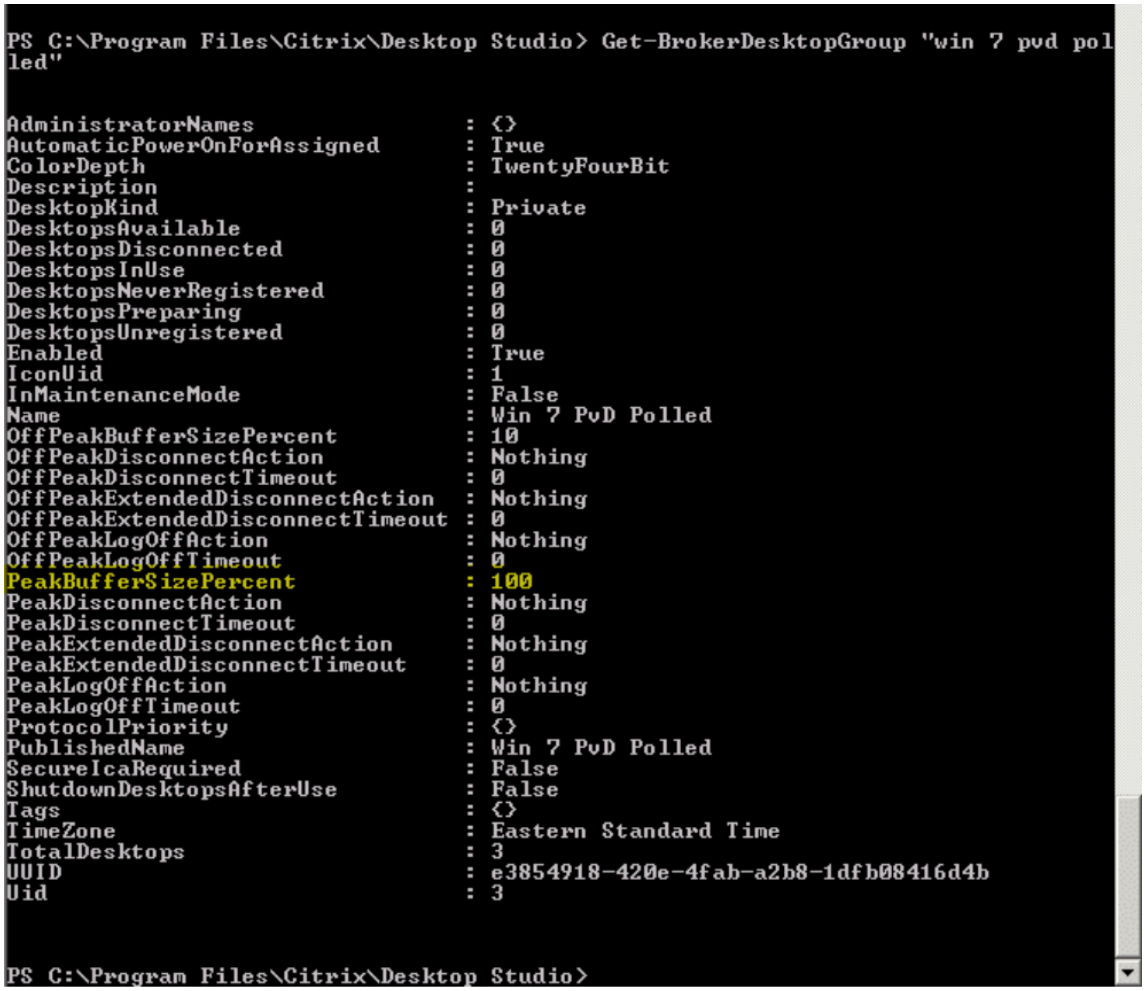
   ```
   asnp Citrix*

   # 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"
   ```



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
- Reconexión de sesiones de control al desconectarse de la máquina en modo de mantenimiento
- Configurar la itinerancia de sesiones

Cerrar sesión o desconectar una sesión

1. Seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo de entrega y, a continuación, seleccione **Ver máquinas** en la barra de acciones.
3. En el panel central, seleccione la máquina, seleccione **Ver sesiones** en la barra de 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 una sesión, seleccione **Cerrar sesión** en la barra de 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 la barra de 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 detallada, consulte Máquinas con energía administrada.

Enviar un mensaje a un grupo de entrega

1. Seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo de entrega y, a continuación, seleccione **Ver máquinas** en la barra de acciones.
3. En el panel central, seleccione una máquina a la que quiera enviar un mensaje.
4. En la barra de acciones, seleccione **Ver sesiones**.
5. En el panel central, seleccione todas las sesiones y, a continuación, seleccione **Enviar mensaje** en la barra de 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 tener activo 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.

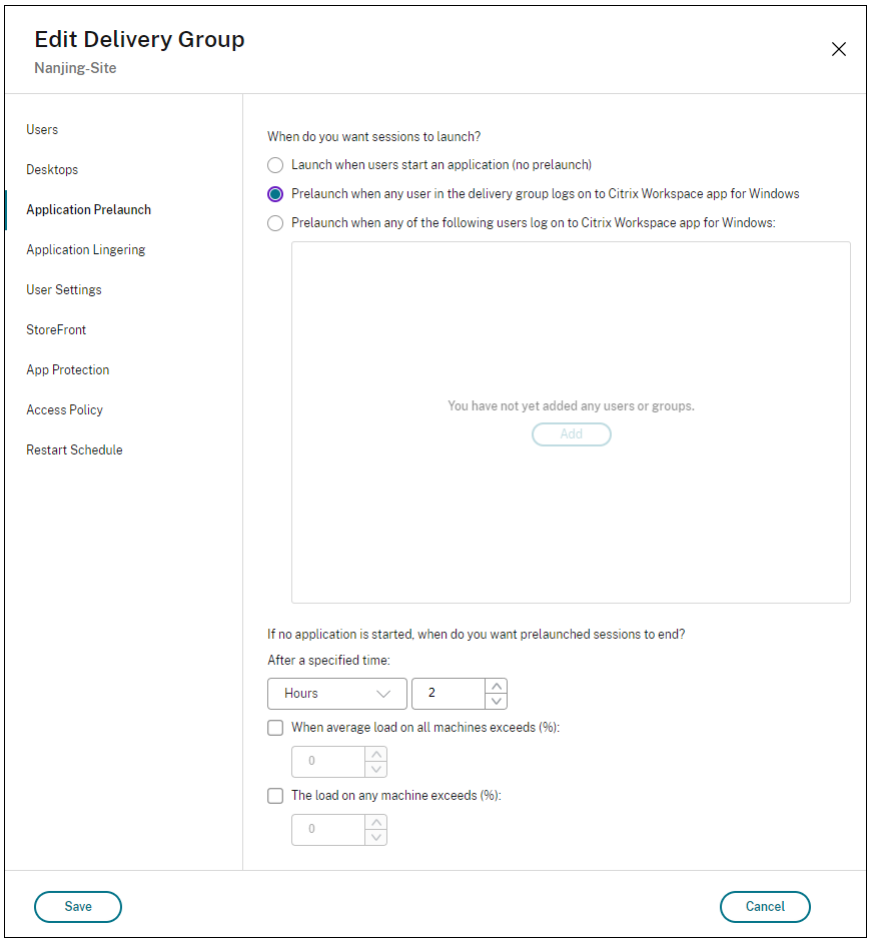
  Puede configurar dos umbrales: el porcentaje medio de carga para todos los servidores del grupo de entrega y el porcentaje máximo de carga para un servidor único del grupo de entrega. Cuando se supera un umbral, se finalizan aquellas sesiones que hayan tenido el estado de preinicio o persistente durante 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 un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en la barra de acciones.
2. 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.



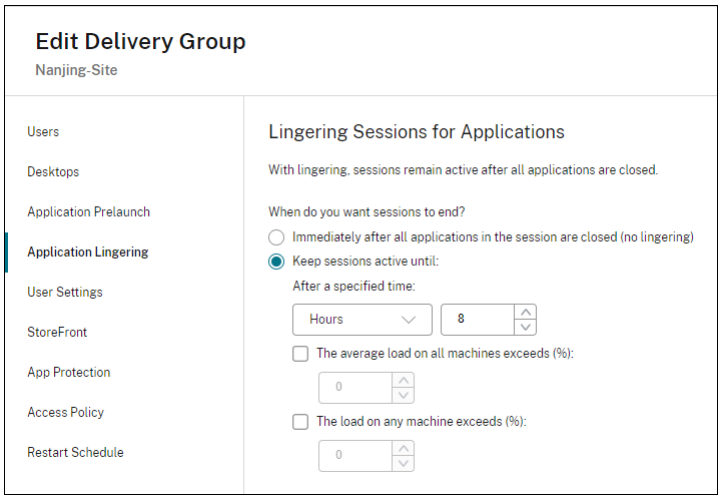
3. Una sesión preiniciada se reemplaza por una sesión habitual cuando el usuario inicia una aplicación. Si el usuario no inicia una aplicación (es decir, la sesión preiniciada no se llega a utilizar), la siguiente configuración afecta a la cantidad de tiempo que esta sesión permanece activa.

   - 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 (entre el 1 y el 99%).
   - Cuando la carga de una máquina del grupo de entrega supera un porcentaje especificado (entre el 1 y el 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 la izquierda.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en la barra de 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: entre el 1 y el 99%.
   - Cuando la carga de una máquina del grupo de entrega supera un porcentaje especificado: entre el 1 y el 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.

Reconexión de sesiones de control al desconectarse de la máquina en modo de mantenimiento

> **NOTA:**
>
> Esta función solo está disponible en PowerShell.

Puede controlar si las sesiones que están desconectadas en máquinas en modo de mantenimiento pueden volver a conectarse a máquinas del grupo de entrega.

Antes de la versión 2106, no se permitía la reconexión de sesiones de escritorio agrupadas de sesión única que se habían desconectado de las máquinas en modo de mantenimiento. A partir de la versión 2106, puede configurar un grupo de entrega para permitir o prohibir las reconexiones (independientemente del tipo de sesión) después de la desconexión de una máquina en modo de mantenimiento.

Al crear o modificar un grupo de entrega (`New-BrokerDesktopGroup`, `Set-BrokerDesktopGroup`), utilice el parámetro `-AllowReconnectInMaintenanceMode` <**boolean**> para permitir o prohibir las reconexiones de máquinas desconectadas de una máquina en modo de mantenimiento.

- Al establecerse en true, las sesiones pueden volver a conectarse a las máquinas del grupo.
- Al establecerse en false, las sesiones no pueden volver a conectarse a las máquinas del grupo.

Valores predeterminados:

- Sesión única: Inhabilitada
- Multisesión: Habilitada

Configurar la itinerancia de sesiones

De forma predeterminada, la itinerancia de sesiones está habilitada para grupos de entrega. 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 simultáneamente en ambos dispositivos. Puede ver las aplicaciones en varios dispositivos. Las aplicaciones se mueven, independientemente del dispositivo o de si las sesiones actuales existen. A menudo, las impresoras y otros recursos asignados a la aplicación también se mueven. Como alternativa, puede usar PowerShell. Para obtener más información, consulte Itinerancia de sesiones.

Configurar la itinerancia de sesiones para aplicaciones Para configurar la itinerancia de sesiones para aplicaciones, siga estos pasos:

1. En la consola, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo de entrega y, a continuación, seleccione **Modificar grupo de entrega** en la barra de acciones.

3. En la página **Usuarios**, marque la casilla **Las sesiones se mueven con los usuarios mientras se mueven entre dispositivos** para habilitar la itinerancia de sesiones.

    - Al habilitarse, cuando el usuario inicia una sesión de aplicación y, más tarde, cambia de dispositivo, se usa la misma sesión, y esta están disponible en ambos dispositivos. Al inhabilitarse, la sesión ya no se mueve entre dispositivos.

4. Seleccione **Aceptar** para aplicar los cambios y cerrar la ventana.

Configurar la itinerancia de sesiones para escritorios Para configurar la itinerancia de sesiones para un escritorio, siga estos pasos:

1. En la consola, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo y, a continuación, seleccione **Modificar** en la barra de acciones.
3. En la página **Escritorios**, seleccione el escritorio y seleccione **Modificar**.
4. Marque la casilla **Itinerancia de sesiones** para habilitar la itinerancia de sesiones.

- Al habilitarse, si el usuario inicia un escritorio y, más tarde, cambia de dispositivo, se usa la misma sesión, y las aplicaciones están disponible en ambos dispositivos. Al inhabilitarse, la sesión ya no se mueve entre dispositivos.

Seleccione **Aceptar** para aplicar los cambios y cerrar la ventana.

Aplicaciones

Ver y agregar aplicaciones a un grupo de entrega.

1. En la consola, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo. Si este grupo contiene aplicaciones, la opción **Ver aplicaciones** se muestra en la barra de acciones.
3. Seleccione **Ver aplicaciones**. Se le dirigirá al nodo **Aplicaciones**, donde se muestran todas las aplicaciones disponibles en este grupo.
4. Para agregar más aplicaciones a este grupo, vaya al nodo **Grupos de entrega**, seleccione el grupo y seleccione **Agregar aplicaciones** en la barra de acciones.

Solucionar problemas

- Los VDA no registrados en un Delivery Controller no se tienen en cuenta cuando se inicien sesiones con intermediario. Esto provoca una infrautilización 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 pueden 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 funciones 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

August 17, 2024

> **Nota:**
>
> Puede administrar la implementación de Citrix Virtual Apps and Desktops mediante dos consolas de administración: Web Studio (basada en la web) y Citrix Studio (basada en Windows). Este artículo se refiere únicamente a Web Studio. Para obtener información sobre Citrix Studio, consulte el artículo equivalente en Citrix Virtual Apps and Desktops 7 2212 o versiones anteriores.

Introducción

Los grupos de aplicaciones permiten administrar colecciones de aplicaciones. Cree grupos de aplicaciones para las aplicaciones compartidas entre diferentes grupos de entrega. O bien las aplicaciones utilizadas por un subconjunto de usuarios dentro de grupos de entrega. Los grupos de aplicaciones son optativos: ofrecen una alternativa para no tener que agregar las mismas aplicaciones a varios grupos de entrega. Asocie grupos de entrega a más de un grupo de aplicaciones y asocie un grupo de aplicaciones a más de un grupo de entrega.

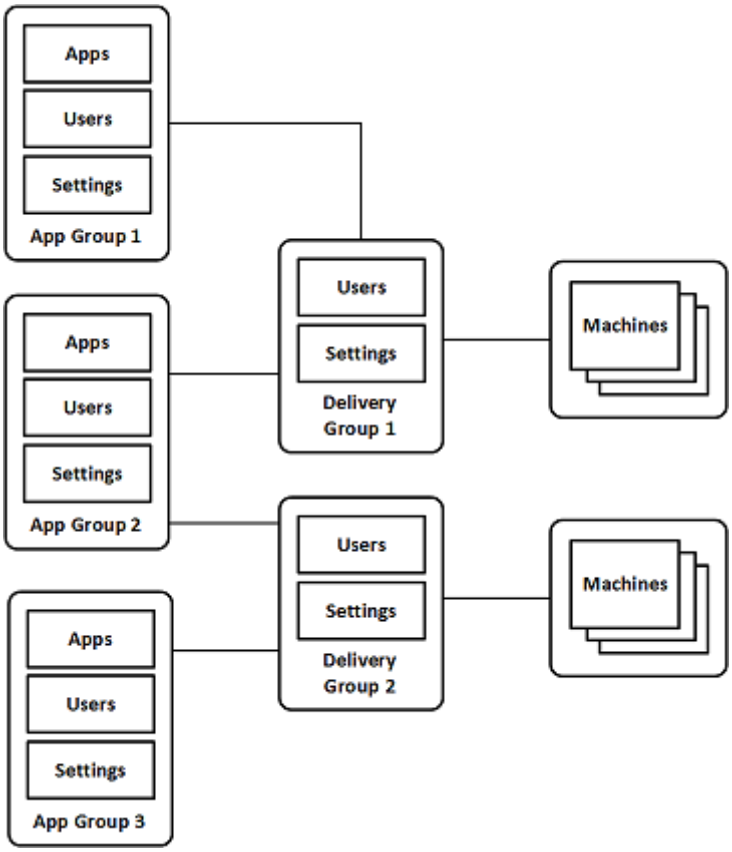
El uso de grupos de aplicaciones puede proporcionar ventajas para la administración de aplicaciones y para el control de los recursos frente a la opción de grupos de entrega:

- 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 resultar beneficiosa.
- 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 de etiqueta, 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 por etiquetas 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 por etiquetas 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:



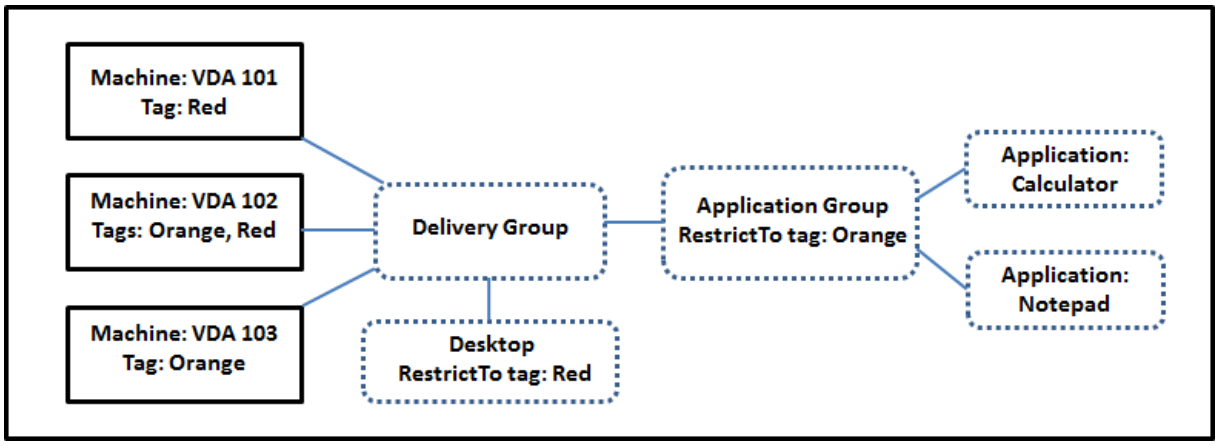
En esta configuración, las aplicaciones se agregan a los grupos de aplicaciones no a los grupos de entrega. Los grupos de entrega especifican qué máquinas se utilizan. (Aunque no se muestra, las máquinas se encuentran en catálogos de máquinas.)

El grupo de aplicaciones 1 está asociado al grupo de entrega 1. Acceda a las aplicaciones del grupo de aplicaciones 1 con los usuarios especificados en el grupo de aplicaciones 1. Estos grupos solo aparecen mientras estén también en la lista de usuarios del grupo de entrega 1. Esta configuración cumple la recomendación de que la lista de usuarios de un grupo de aplicaciones sea 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 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 asigna 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. Acceda a las aplicaciones del grupo de aplicaciones 2 con los usuarios especificados en el grupo de aplicaciones 2. Sin embargo, también deben aparecer en las listas de usuarios del grupo de entrega 1 y del grupo de entrega 2.

Ejemplo 2:

En esta sencilla distribución, se usan restricciones de 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 grupo de aplicaciones se creó con la restricción de etiqueta "Orange". Cada una de sus aplicaciones solo se inicia en máquinas de ese grupo de entrega que tengan la etiqueta "Orange", 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 actualizar la versión de los grupos de entrega a la actual. Este proceso 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 detallada, consulte Administración delegada.

En este artículo se refiere a "asociar"una aplicación a varios grupos de aplicaciones. Se diferencia esa acción de agregar instancias de esa aplicación desde un origen disponible. Del mismo modo, los grupos de entrega se asocian a grupos de aplicaciones, en lugar de agregarse como componentes 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 más aplicaciones 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:**

  Una configuración con un conjunto de aplicaciones que no funcionan bien con otras aplicaciones instaladas en las mismas máquinas. Como dos versiones diferentes del mismo paquete de software o dos versiones diferentes del mismo explorador web. Usted prefiere no permitir que un usuario inicie ambas versiones en una misma sesión.

  Cree 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. El usuario sigue pudiendo ejecutar otras aplicaciones al mismo tiempo, pero no en la misma sesión. Si el usuario inicia una de las aplicaciones de diferente versión 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 sesiones existentes en la máquina a medida que sea necesario al compartir sesiones.

Solo se pueden ofrecer las sesiones preiniciadas a los grupos de aplicaciones que tienen permitido compartir sesiones (las sesiones que usan la función 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 puede configurarlas 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.

De forma predeterminada, se pueden compartir sesiones entre grupos de aplicaciones cuando se crea un grupo de aplicaciones. No puede cambiar este parámetro al crear 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. Inicie sesión en Web Studio.
2. Seleccione **Aplicaciones** en el panel de la izquierda y, a continuación, seleccione la ficha **Grupos de aplicaciones**.
3. Para organizar grupos de aplicaciones mediante carpetas, cree carpetas en la carpeta raíz **Application Groups**.
4. Seleccione la carpeta en la que quiere crear el grupo y, a continuación, haga clic en **Crear grupo de entrega**. El asistente de creación de grupos se inicia con una página de **introducción**. Puede quitar la página para futuras versiones de este asistente.
5. Siga las instrucciones del asistente para configurar los parámetros en las páginas que se describen a continuación. Cuando haya terminado con cada página, seleccione **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 de manera estática.

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 de creación de grupos 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 usan 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 de etiqueta, elija **Restringir inicios a máquinas con la etiqueta** y, a continuación, seleccione la etiqueta en el menú desplegable.

Paso 2. Usuarios

Especifique usuarios de aplicaciones en el grupo de aplicaciones. Permita todos los usuarios y los grupos de usuarios de los grupos de entrega seleccionados en la página anterior, o bien seleccione un grupo específico de usuarios y grupos de usuarios de los grupos de entrega. Si restringe el uso a unos cuantos usuarios especificados, entonces solo los usuarios especificados en el grupo de entrega y el grupo de aplicaciones pueden acceder a las aplicaciones de este grupo. 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 **Aplicaciones**. 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 va a agregar. 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 Web Studio. De lo contrario, los usuarios ven 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 el menú 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 Implementar y entregar aplicaciones de 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 del menú 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 (optativa).

Revise la información de resumen y, a continuación, haga clic en **Finalizar**.

Administrar grupos de aplicaciones

August 17, 2024

> **Nota:**
>
> Puede administrar la implementación de Citrix Virtual Apps and Desktops mediante dos consolas de administración: Web Studio (basada en la web) y Citrix Studio (basada en Windows). Este artículo se refiere únicamente a Web Studio. Para obtener información sobre Citrix Studio, consulte el artículo equivalente en Citrix Virtual Apps and Desktops 7 2212 o versiones anteriores.

Introducción

En este artículo, se describe cómo administrar grupos de aplicaciones después de crearlos.

Consulte 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 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. Si las aplicaciones se agregaron explícitamente a grupos de entrega asociados al grupo de aplicaciones, inhabilitar el grupo de aplicaciones no afecta a esas aplicaciones agregadas a esos grupos de entrega.

Un grupo de aplicaciones está habilitado cuando se crea. No puede cambiar esta configuración al crear el grupo.

1. Seleccione **Aplicaciones** en el panel de la izquierda y, a continuación, seleccione la ficha **Grupos de aplicaciones**.
2. Seleccione un grupo de aplicaciones y, a continuación, seleccione **Modificar grupo de aplicaciones** en la barra de acciones.
3. En la página **Parámetros**, marque o desmarque la casilla **Habilitar grupo de aplicaciones**.
4. Haga clic en **Aplicar** para mantener la ventana abierta o en **Guardar** 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 esta configuración al crear el grupo. Para obtener más información, consulte Compartir sesiones con grupos de aplicaciones.

1. Seleccione **Aplicaciones** en el panel de la izquierda y, a continuación, seleccione la ficha **Grupos de aplicaciones**.
2. Seleccione un grupo de aplicaciones y, a continuación, seleccione **Modificar grupo de aplicaciones** en la barra de 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 mantener la ventana abierta o en **Guardar** 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, esta opción 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. Cuando hay disponibles varias sesiones desconectadas adecuadas, se elige una de ellas para reconectarse de forma aleatoria pero determinante. Cuando 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.

Use 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 con el uso compartido de sesiones inhabilitado.

Ejemplos de cmdlets de PowerShell

Para inhabilitar el uso compartido de sesiones, utilice 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 sesión 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 la tiene en `False`, lo que resulta en un comportamiento inesperado.

Cambiar el nombre de un grupo de aplicaciones

1. Seleccione **Aplicaciones** en el panel de la izquierda y, a continuación, seleccione la ficha **Grupos de aplicaciones**.
2. Seleccione un grupo de aplicaciones y, a continuación, seleccione **Cambiar nombre del grupo de aplicaciones** en la barra de 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 la izquierda y, a continuación, seleccione la ficha **Grupos de aplicaciones**.

2. Seleccione un grupo de aplicaciones y, a continuación, seleccione **Modificar grupo de aplicaciones** en la barra de 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). Una vez seleccionados, 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, marque la casilla de 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 **Guardar** para aplicar los cambios y cerrar la ventana.

Agregar, modificar o quitar una restricción por etiquetas 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 la izquierda y, a continuación, seleccione la ficha **Grupos de aplicaciones**.
2. Seleccione un grupo de aplicaciones y, a continuación, seleccione **Modificar grupo de aplicaciones** en la barra de acciones.
3. Seleccione la página **Grupos de entrega**.
4. Para agregar una restricción de etiqueta, 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 o quite la restricción de etiqueta por completo; para ello, desmarque **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 **Guardar** 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 la izquierda y, a continuación, seleccione la ficha **Grupos de aplicaciones**.
2. Seleccione un grupo de aplicaciones y, a continuación, seleccione **Modificar grupo de aplicaciones** en la barra de 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 **Guardar** para aplicar los cambios y cerrar la ventana.

Agregar, cambiar o quitar un icono de aplicación en un grupo de aplicaciones

Lleve a cabo los siguientes pasos para agregar, cambiar o quitar un icono de aplicación.

1. Seleccione **Aplicaciones** en el panel de la izquierda.
2. En la ficha **Aplicaciones**, seleccione una aplicación y, a continuación, seleccione **Propiedades**.

   Para realizar cambios al nivel del grupo de aplicaciones, vaya a la ficha **Grupos de aplicaciones**, seleccione una aplicación de un grupo y, a continuación, seleccione **Propiedades**.
3. Seleccione la página **Entrega** y, a continuación, seleccione **Cambiar**. Aparecerá la ventana **Seleccionar icono**.
4. En la ventana **Seleccionar icono**, realice una de las siguientes acciones:

   - Para agregar un icono, seleccione **Agregar** y, a continuación, vaya al icono.
   - Para quitar un icono, selecciónelo y, a continuación, seleccione **Quitar**.
   - Para cambiar un icono, seleccione el icono de la aplicación.

   > **Importante:**
   >
   > - No se pueden agregar iconos cuyo tamaño sea superior a 200 KB.
   > - Solo se pueden agregar archivos .icon.
   > - No se pueden quitar iconos integrados.
   > - No se puede quitar el icono de una aplicación que está en uso.

5. Seleccione **Guardar** 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 la izquierda y, a continuación, seleccione la ficha **Grupos de aplicaciones**.

2. Seleccione un grupo de aplicaciones y, a continuación, seleccione **Modificar grupo de aplicaciones** en la barra de 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 **Guardar** 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 la izquierda y, a continuación, seleccione la ficha **Grupos de aplicaciones**.
2. Seleccione un grupo de aplicaciones y, a continuación, seleccione **Modificar grupo de aplicaciones** en la barra de acciones.
3. Seleccione la página **Ámbitos**. Marque o deje sin marcar la casilla de verificación situada junto a los ámbitos que desea cambiar.
4. Seleccione **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta, o bien seleccione **Guardar** para aplicar los cambios y cerrar la ventana.

Eliminar un grupo de aplicaciones

La aplicación debe estar asociada a, al menos, un grupo de entrega o un grupo de aplicaciones. Si eliminar un grupo de aplicaciones provoca que una o varias aplicaciones dejen de pertenecer a un grupo, se le advertirá de 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 la izquierda y, a continuación, seleccione la ficha **Grupos de aplicaciones**.
2. Seleccione un grupo de aplicaciones y, a continuación, seleccione **Eliminar grupo** en la barra de acciones.
3. Confirme la eliminación cuando se le solicite.

Organizar grupos de aplicaciones mediante carpetas

Puede crear carpetas para organizar grupos de aplicaciones y acceder a ellos fácilmente.

Roles obligatorios

De forma predeterminada, cree y administre carpetas para grupos de aplicaciones si tiene uno de estos roles integrados:

- Administrador de Cloud
- Administrador total
- Administrador de grupos de aplicaciones

Puede delegar acciones de administración a otros usuarios mediante la creación de roles personalizados. En esta tabla se enumeran los permisos necesarios para cada acción.

Acción	Permisos requeridos
Crear carpetas de grupos de aplicaciones	Crear carpeta de grupo de aplicaciones
Eliminar carpetas de grupos de aplicaciones	Quitar carpeta de grupo de aplicaciones
Mover carpetas de grupos de aplicaciones	Mover carpeta de grupo de aplicaciones
Cambiar el nombre de carpetas de grupos de aplicaciones	Modificar carpeta de grupo de aplicaciones
Mover grupos de aplicaciones a carpetas	Modificar carpeta de grupo de aplicaciones, Modificar propiedades del grupo de aplicaciones

Para obtener más información, consulte Crear y administrar roles.

Crear y administrar carpetas

Puede utilizar la barra Acciones o el menú contextual para crear y administrar carpetas de grupos de aplicaciones. Además, puede arrastrar un grupo de aplicaciones o una carpeta a la ubicación que quiera en el árbol de carpetas.

Información útil:

- Puede anidar carpetas en hasta cinco niveles (excluyendo la carpeta raíz predeterminada).
- Una carpeta puede contener grupos de aplicaciones y subcarpetas. Solo puede eliminar una carpeta si ni dicha carpeta ni sus subcarpetas contienen grupos de aplicaciones.
- Todos los nodos (como catálogos de máquinas, grupos de entrega, aplicaciones y grupos de aplicaciones) comparten un árbol de carpetas en el back-end. Para evitar conflictos de nombres con otras carpetas de recursos al cambiar el nombre de las carpetas o al moverlas, le recomendamos que asigne nombres diferentes a las carpetas de primer nivel de los distintos árboles de carpetas.

Acceso con Remote PC

August 17, 2024

> **Nota:**
>
> Puede administrar la implementación de Citrix Virtual Apps and Desktops mediante dos consolas de administración: Web Studio (basada en la web) y Citrix Studio (basada en Windows). Este artículo se refiere únicamente a Web Studio. Para obtener información sobre Citrix Studio, consulte el artículo equivalente en Citrix Virtual Apps and Desktops 7 2212 o versiones anteriores.

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. De forma predeterminada, asignamos automáticamente varios usuarios a la siguiente máquina sin asignar. Para restringir la asignación automática a un solo usuario, inicie sesión en Web Studio, vaya a **Parámetros** y desactive el parámetro **Habilitar la asignación automática de varios usuarios para el acceso con Remote PC**.

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 DaaS (antes, 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. Las opciones disponibles son las siguientes:
  - 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.

> **Nota:**
>
> Al diseñar el acceso con Remote PC, debe tener en cuenta la cantidad de monitores físicos que estén conectados a la GPU en el PC remoto y configurados o en funcionamiento actualmente. Aunque el monitor no se use en la sesión de Citrix, pero la GPU lo detecta, la presencia del monitor se cuenta para el límite máximo de monitores que puede admitir la GPU.

Consideraciones acerca del catálogo de máquinas

El tipo de catálogo de máquinas requerido depende del caso de uso:

- Catálogo de máquinas de acceso con Remote PC
  - PC Windows dedicados
  - PC multiusuario Windows dedicados Este caso de uso es aplicable a los equipos de oficina físicos a los que diferentes usuarios pueden acceder de forma remota en distintos turnos.
  - PC Windows agrupados. Este caso de uso es aplicable a los PC físicos a los que pueden acceder varios usuarios aleatorios, como los laboratorios informáticos.
- Catálogo de máquinas con SO de sesión única
  - Estático: PC Linux dedicados
  - Aleatorio: PC 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 asignación automática de usuarios no está disponible para máquinas Linux.
- Si los usuarios ya han iniciado sesión en sus equipos localmente, los intentos de iniciarlos desde StoreFront fallan.
- Las opciones de ahorro de energía no están disponibles para las máquinas Linux.

Requisitos técnicos y consideraciones

En esta sección, se incluyen los requisitos técnicos y consideraciones para PC físicos.

- Las siguientes opciones no son compatibles:

  - 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.
  - Máquinas de arranque dual.

- 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 y Windows 11.
- 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 **Suspender** 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 (VDAWorkstationCoreSetup.exe).
    - También puede utilizar el instalador completo de VDA de SO de sesión única (VDAWorkstationSetup.exe) con la opción `/remotepc/physicalmachine`, que ofrece el mismo resultado que usar el instalador básico de VDA.

        > **Nota:**
        >
        > Para la instalación de Remote PC, utilice el argumento `/physicalmachine` con `/remotepc`, para que el VDA se comporte de la manera prevista en determinados casos de usuario.

    - 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 Management 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 usa 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 (presionando 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: RpcaMode
- 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: RpcaTimeout
- 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.

Registros de administración de sesiones

Acceso con Remote PC incluye ahora funcionalidades de registro que registran cuando alguien intenta acceder a un PC con una sesión ICA activa. Esto le permite supervisar su entorno en busca de actividades no deseadas o imprevistas y auditar dichos eventos si necesita investigar cualquier incidente.

Los eventos se registran con el Visor de eventos de Windows y se encuentran en **Aplicaciones y servicios > Citrix > HostCore > ICA Service > Admin**.

Hay tres eventos distintos que se registran cuando se utiliza Acceso con Remote PC.

Evento Ctrl+Alt+Supr

Este evento aparece cuando el usuario local pulsa Ctrl+Alt+Supr en el teclado de la consola con una sesión remota activa.

Detalles del evento

- Nombre del registro: Application and Services
- ID de evento: 43, 44, 45
- Origen: ICA Service

ID de evento 43 Este ID de evento aparece cuando el valor de Registro SasNotification no existe o es 0.

- Mensaje:

```
1          Ctrl+Alt+Del has been pressed on the endpoint.
2          The session management behavior is set to automatically
               disconnect the remote session.
```

ID de evento 44 Este identificador de evento aparece cuando el valor de Registro SasNotification es 1 y el valor de registro RpcaMode es 1 o no existe.

- Mensaje:

```
1          Ctrl+Alt+Del has been pressed on the endpoint.
2          The session management behavior is set to notify the
               remote user. The user preference is set to remote user
               .
```


ID de evento 45 Este ID de evento aparece cuando el valor de Registro SasNotification es 1 y el valor de registro RpcaMode es 2.

- Mensaje:

```
Ctrl+Alt+Del has been pressed on the endpoint.
The session management behavior is set to notify the
    remote user.
The user preference is set to local user.
```

Evento de desconexión de sesión remota

Este evento aparece cuando la sesión remota se ha desconectado por varios motivos.

Detalles del evento

- Nombre del registro: Application and Services
- ID de evento: 46, 47, 48
- Origen: ICA Service

ID de evento 46 Este identificador de evento aparece cuando la sesión remota se ha desconectado y cuando el valor de Registro SasNotification no existe o es 0.

- Mensaje:

```
The remote session for <remoteUserName> has been
    disconnected.
```

ID de evento 47 Este identificador de evento aparece cuando el usuario remoto acepta desconectar la sesión y cuando el valor de Registro SasNotification es 1 y el valor de Registro RpcaMode es 1, 2 o no existe.

- Mensaje:

```
The remote session for <remoteUserName> has been
    disconnected because the user accepted the request to
    disconnect the session.
```

ID de evento 48 Este identificador de evento aparece cuando el usuario remoto no rechaza la solicitud de desconexión dentro del período de tiempo de espera específico y cuando el valor de Registro SasNotification es 1 y el valor de Registro RpcaMode es 2.

- Mensaje:

```
The remote session for <remoteUserName> has been
    disconnected because the user did not decline the
    disconnection request within the configured timeout
    period (<timeout period>).
```

Evento Ctrl+Alt+Supr pulsado dos veces Este evento aparece cuando se pulsa Ctrl+Alt+Supr dos veces en un plazo de 10 segundos.

Detalles del evento

- Nombre del registro: Application and Services
- ID de evento: 49
- Origen: ICA Service

ID de evento 49 Este identificador de evento aparece cuando se pulsa Ctrl+Alt+Supr dos veces en un plazo de 10 segundos.

- Mensaje:

```
The remote session for <remoteUserName> has been forcibly
    disconnected.
```

Wake on LAN

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 reduce los costes de energía. También permite el acceso remoto cuando una máquina se ha apagado inadvertidamente.

Con la función Wake on LAN, los Magic Packets se envían directamente desde el VDA a la subred en la que reside el equipo cuando se lo indica el Delivery Controller. Esto permite que la función no requiera dependencias de componentes de infraestructura adicionales ni soluciones de terceros para la entrega de Magic Packets.

La función Wake on LAN difiere de la función Wake on LAN que se basa en una versión de SCCM antigua. Para obtener información sobre Wake on LAN basada en SCCM, consulte Función Wake on LAN integrada en SCCM.

Requisitos del sistema

A continuación, se indican los requisitos del sistema para usar la función Wake on LAN:

- Plano de control:
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2009 o una versión posterior
- PC físicos:
  - Versión 2009 de VDA o una posterior
  - Windows 10 o Windows 11. Para obtener información detallada sobre la compatibilidad, consulte los requisitos del sistema de VDA.
  - Wake on LAN habilitado en BIOS/UEFI
  - Wake on LAN habilitado en las propiedades del adaptador de red dentro de la configuración de Windows

Configurar Wake on LAN

Si utiliza Citrix Virtual Apps and Desktops localmente, la configuración de Wake on LAN integrada solo se admite con PowerShell.

Para configurar Wake on LAN:

1. Cree el catálogo de máquinas de acceso con Remote PC si aún no tiene uno.
2. Cree la conexión de host Wake on LAN si aún no tiene una.

   > **Nota:**
   >
   > Para utilizar la función Wake on LAN, si tiene una conexión de host del tipo "Microsoft Configuration Manager Wake on LAN", cree otra conexión de host.

3. Obtenga el identificador único de la conexión de host Wake on LAN.
4. Asocie la conexión de host Wake on LAN a un catálogo de máquinas.

Para crear la conexión de host Wake on LAN:

```
# Load Citrix SnapIns
Add-PSSnapIn -Name "*citrix*"

# Provide the name of the Wake on LAN host connection
[string]$connectionName = "Remote PC Access Wake on LAN"

# Create the hypervisor connection
$hypHc = New-Item -Path xdhyp:\Connections `
                  -Name $connectionName `
```



```
                -HypervisorAddress "N/A" `
                -UserName "woluser" `
                -Password "wolpwd" `
                -ConnectionType Custom `
                -PluginId VdaWOLMachineManagerFactory `
                -CustomProperties "<CustomProperties></CustomProperties
                   >" `
                -Persist

$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
   $hypHc.HypervisorConnectionUid

# Wait for the connection to be ready before trying to use it
while (-not $bhc.IsReady)
{

    Start-Sleep -s 5
    $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
       $hypHc.HypervisorConnectionUid
 }
```

Cuando la conexión de host esté lista, ejecute los siguientes comandos para obtener el identificador único de la conexión de host:

```
$bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"
$hypUid = $bhc.Uid
```

Después de obtener el identificador único de la conexión, ejecute los siguientes comandos para asociar la conexión al catálogo de máquinas de acceso con Remote PC:

```
Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog -
   RemotePCHypervisorConnectionUid $hypUid
```

Consideraciones sobre el diseño

Cuando planee usar Wake on LAN con acceso con Remote PC, tenga en cuenta lo siguiente:

- Varios catálogos de máquinas pueden utilizar la misma conexión de host Wake on LAN.
- Para que un equipo reactive otro equipo, ambos deben estar en la misma subred y utilizar la misma conexión de host Wake on LAN. No importa si los equipos están en los mismos catálogos de máquinas o en catálogos diferentes.
- Las conexiones de host se asignan a zonas específicas. Si la implementación contiene más de una zona, debe disponer de una conexión de host Wake on LAN en cada zona. Lo mismo es aplicable a los catálogos de máquinas.
- Los Magic Packets se transmiten mediante la dirección de difusión global 255.255.255.255. Asegúrese de que la dirección no esté bloqueada.

- Debe haber al menos un equipo encendido en la subred por cada conexión Wake on LAN para poder activar máquinas en esa subred.

Consideraciones operativas

A continuación, se incluyen consideraciones para uso de la función Wake on LAN:

- El VDA debe registrarse al menos una vez antes de que el PC pueda activarse mediante la función Wake on LAN integrada.
- Wake on LAN solo se puede utilizar para activar PC. No admite otras acciones de energía, como reinicio o apagado.
- Después de crear la conexión Wake on LAN, es visible en Web Studio. Sin embargo, no se admite la modificación de sus propiedades en Web Studio si se usa Citrix Virtual Apps and Desktops en el entorno local.
- Los Magic Packets se envían de una de dos maneras:
  1. Cuando un usuario intenta iniciar una sesión en su PC y el VDA no está registrado
  2. Cuando un administrador envía manualmente un comando de encendido desde Web Studio o PowerShell
- Dado que el Delivery Controller no conoce el estado de energía de un equipo, Web Studio muestra **No compatible** con el estado de alimentación. El Delivery Controller utiliza el estado del registro del VDA para determinar si un equipo está encendido o apagado.

Wake on LAN: integrada en SCCM

La función Wake on LAN integrada en SCCM es una alternativa a Wake on LAN para el acceso con Remote PC que solo está disponible con instancias de Citrix Virtual Apps and Desktops locales.

Requisitos del sistema

A continuación, se indican los requisitos del sistema para uso de la función Wake on LAN integrada en SCCM:

- Citrix Virtual Apps and Desktops 1912 o versiones posteriores
- PC físicos:
  - VDA versión 1912 o posterior.
  - Windows 10. Para obtener información detallada sobre la compatibilidad, consulte los requisitos del sistema de VDA.
  - Wake on LAN habilitado en BIOS/UEFI

  - Wake on LAN habilitado en las propiedades del adaptador de red dentro de la configuración de Windows

- System Center Configuration Manager (SCCM) 2012 R2 o una versión posterior

Configurar Wake on LAN integrada en SCCM

Complete los siguientes requisitos previos:

1. 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 forzar uno manualmente, si es necesario.
2. 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.
3. 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.
4. Configure la función Wake on LAN en los ajustes de BIOS/UEFI de cada equipo.
5. Implemente el VDA en los equipos físicos si aún no lo ha hecho.

Después de cumplir los requisitos previos, siga estos pasos para permitir que el Delivery Controller se comunique con SCCM:

1. Cree una conexión de host para SCCM. Para obtener más información, consulte Conexiones y recursos.
   - Seleccione **Microsoft Configuration Manager Wake on LAN** como tipo de conexión.
   - Las credenciales introducidas deben conceder acceso a las colecciones del ámbito y al rol de **operador de herramientas remotas**.
2. Seleccione la conexión en Web Studio y, a continuación, seleccione **Modificar conexión** y haga clic en **Avanzadas**.
3. Seleccione la opción adecuada para gestionar Wake on LAN:
   - Si utiliza el proxy de reactivación, seleccione la primera opción: **Proxy de reactivación de Microsoft System Center Configuration Manager**.
   - Si utiliza Magic Packets, seleccione la segunda opción: **Paquetes de Wake on LAN transmitidos por el Delivery Controller**.
     - Seleccione el método de transmisión adecuado: **Difusiones dirigidas a subred** o **Unidifusión**.

Después de crear la conexión de host, asóciela a un catálogo de acceso con Remote PC:

- Si va a crear un nuevo catálogo de acceso con Remote PC, en la página **Sistema operativo** del asistente de creación de catálogos, seleccione **Acceso con Remote PC** como tipo de catálogo y elija la conexión adecuada en la lista desplegable.
- Para agregar Wake on LAN a un catálogo existente de acceso con Remote PC:
  1. Vaya al nodo **Catálogos de máquinas** en Web Studio, seleccione el catálogo correspondiente y, a continuación, seleccione **Modificar catálogo de máquinas**.
  2. Seleccione la ficha **Administración de energía** y elija **Sí** para habilitar la administración de energía para el catálogo de máquinas.
  3. Seleccione la conexión adecuada en la lista desplegable y haga clic en **Aceptar**.

Solucionar 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.

Publicar contenido

August 17, 2024

> **Nota:**
>
> Puede administrar la implementación de Citrix Virtual Apps and Desktops mediante dos consolas de administración: Web Studio (basada en la web) y Citrix Studio (basada en Windows). Este artículo se refiere únicamente a Web Studio. Para obtener información sobre Citrix Studio, consulte el artículo equivalente en Citrix Virtual Apps and Desktops 7 2212 o versiones anteriores.

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 si deben utilizarse aplicaciones locales o publicadas para abrir el contenido.

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 Web Studio para publicar contenido. No obstante, puede usar Web 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.)

```
New-BrokerApplication –ApplicationType PublishedContent -
    CommandLineExecutable location -Name app-name -DesktopGroup delivery
    -group-name
```

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 Citrix DaaS (antes, Citrix Virtual Apps and Desktops Service), descargue e instale el SDK de PowerShell remoto de Citrix Virtual Apps and Desktops.
- 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 con SO multisesión 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 Citrix DaaS, introduzca sus credenciales de Citrix Cloud para autenticarse. 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.

```
$citrixUrl = "https://www.citrix.com/"
$appName = "Citrix Home Page"

New-BrokerApplication –ApplicationType PublishedContent –
    CommandLineExecutable $citrixURL –Name $appName –DesktopGroup $dg.
    Uid
```

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-xd7/.
- 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.

```
$rtfUNC = "\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedRTF.rtf"
$rtfAppName = "PublishedRTF"

New-BrokerApplication –ApplicationType PublishedContent
 –CommandLineExecutable $rtfUNC -Name $rtfAppName
-DesktopGroup $dg.Uid

$docxUNC = "\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.docx
    "
$docxAppName = "PublishedDOCX"

New-BrokerApplication –ApplicationType PublishedContent
 –CommandLineExecutable $docxUNC -Name $docxAppName
-DesktopGroup $dg.Uid
```


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.

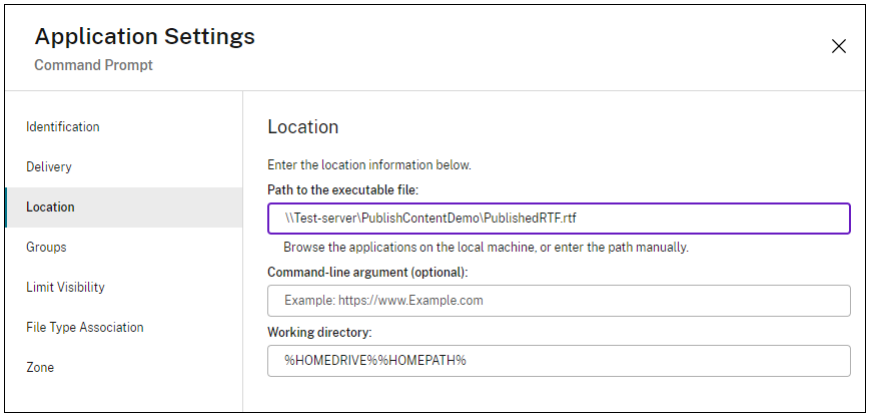
Ver y modificar aplicaciones PublishedContent

Puede administrar el contenido publicado con los mismos métodos que se utilizan para otros tipos de aplicación.

Para ver y modificar aplicaciones de `PublishedContent`, siga estos pasos:

1. Inicie sesión en Web Studio y seleccione **Aplicaciones** en el panel de la izquierda.
2. En la ficha **Aplicaciones**, seleccione una aplicación de PublishedContent y, a continuación, seleccione **Propiedades**.

   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**.
3. Para cambiar el recurso, modifique el campo **Ruta del archivo ejecutable** en dicha página.

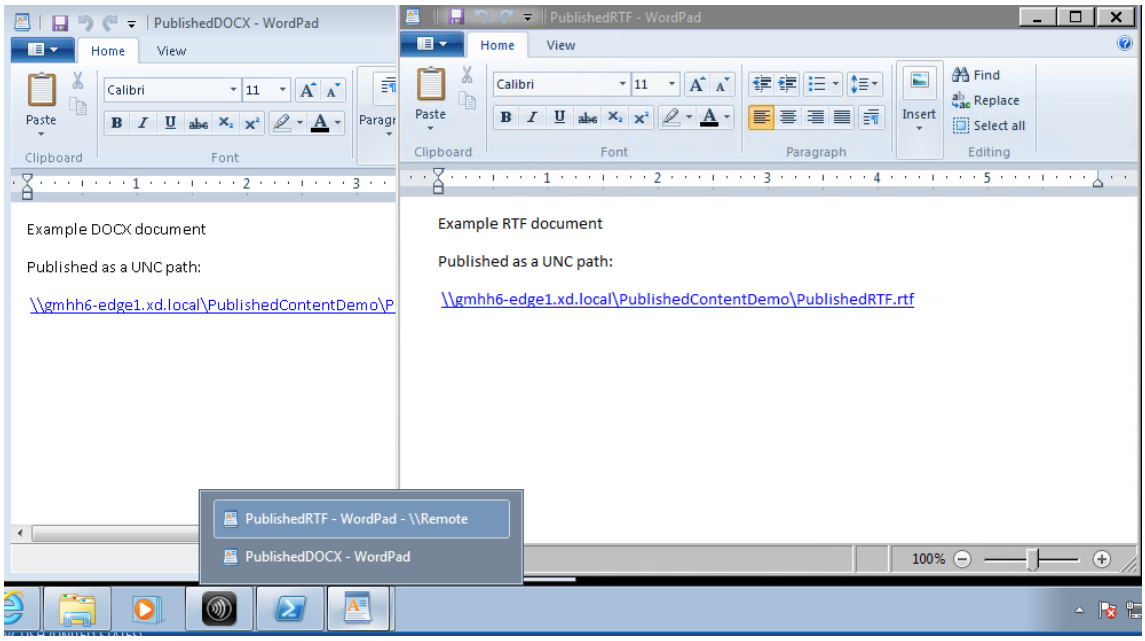


4. Para usar una aplicación publicada para abrir una aplicación de `PublishedContent` (en lugar de una aplicación local), siga estos pasos:

   En este ejemplo, la aplicación publicada de WordPad se modifica para crear una asociación de tipos de archivo para archivos RTF.

   a) Active el modo de mantenimiento del grupo de entrega.
   b) Modifique la propiedad **Asociación de tipos de archivo**.
   c) Desactive el modo de mantenimiento cuando haya terminado.

d) 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. **PublishedDOCX** 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

August 17, 2024

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.

Compatibilidad:

- En las implementaciones de Citrix Virtual Apps and Desktops y Citrix DaaS (antes, Citrix Virtual Apps and Desktops Service), se admite VDI de servidor con Windows Server 2022, Windows Server 2019 y Windows Server 2016.
- Todas las implementaciones de VDI de servidor admiten la tecnología de capa de personalización del usuario.
- Para que VDI de servidor funcione con los dispositivos TWAIN (por ejemplo, escáneres), debe instalarse la función Experiencia de escritorio de servidor Windows.
- Las siguientes funciones no se pueden usar con VDI de servidor:
  - Aplicaciones alojadas
  - Acceso a aplicaciones locales
  - Conexiones de escritorio directas (sin broker)
  - Acceso con Remote PC

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\Terminal Server

     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 supedita 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 DaaS:

```
- VDAWorkstationSetup.exe /quiet /servervdi
```

Otras opciones:

- Utilice `/controllers` para especificar Delivery Controllers o Cloud Connectors.
- Use `/enable_hdx_ports` para abrir puertos en el firewall, a menos que el firewall deba configurarse manualmente.
- Use `/mastermcsimage` (o `/masterimage`) si va a instalar VDA en una imagen y piensa usar MCS para crear máquinas virtuales de servidor a partir de esa imagen.
- 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 realizar búsquedas en Studio, el catálogo de VDI de servidor aparece en la ficha **Máquinas con SO de sesión única**, aunque el VDA se haya instalado en una máquina de multisesión.

4. Cree un grupo de entrega y seleccione el catálogo de VDI de servidor que ha creado.

Si no especificó Delivery Controllers o Cloud Connectors durante la instalación del VDA, recuerde especificarlos después. Para obtener información detallada, consulte Registro de VDA.

Capa de personalización de usuarios

August 17, 2024

> **Nota:**
>
> Puede administrar la implementación de Citrix Virtual Apps and Desktops mediante dos consolas de administración: Web Studio (basada en la web) y Citrix Studio (basada en Windows). Este artículo se refiere únicamente a Web Studio. Para obtener información sobre Citrix Studio, consulte el artículo equivalente en Citrix Virtual Apps and Desktops 7 2212 o versiones anteriores.

La función de capa de personalización de usuarios de Citrix Virtual Apps and Desktops amplía las prestaciones de los catálogos de máquinas no persistentes para conservar en todas las sesiones los

datos de los usuarios y las aplicaciones instaladas localmente. Con la tecnología subyacente de Citrix App Layering, la capa de personalización de usuarios funciona con Citrix Provisioning y Machine Creation Services (MCS) en catálogos de máquinas no persistentes.

Los componentes de la capa de personalización de usuarios se instalan con Virtual Delivery Agent dentro de la imagen maestra. Un archivo VHD almacena localmente las aplicaciones instaladas por el usuario. El VHD montado en la imagen hace las veces de disco duro virtual del usuario.

> **Importante:**
>
> Puede implementar capas de personalización de usuarios en Citrix Virtual Apps and Desktops o capas de usuarios de App Layering habilitadas en una plantilla de imagen, pero no puede hacer las dos cosas. No instale la función de capa de personalización de usuarios en una capa de App Layering.

Esta función reemplaza los discos Personal vDisks (PvD), al tiempo que proporciona a los usuarios una experiencia persistente para los espacios de trabajo en un entorno de escritorios no persistentes (agrupados).

Para implementar la función de capa de personalización de usuarios, instálela y configúrela con los pasos detallados en el artículo.

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, la aplicación pasa a su capa de usuarios. Si el usuario agrega o modifica a un usuario o grupo locales, los cambios no se conservan más allá de la sesión.

> **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 o una posterior
- Citrix Provisioning, versión 1909 o una posterior
- Recurso compartido de archivos (SMB) de Windows o Azure Files con autenticación de AD local habilitada

Puede implementar la función Capa de personalización de usuarios en las siguientes versiones de Windows cuando el sistema operativo se implementa como SO de sesión única. La compatibilidad está limitada a un solo usuario en una sola sesión.

- Windows 11 Enterprise x64
- Windows 10 Enterprise x64, versión 1607 o una posterior
- Windows Server 2019 (compatible con Azure Files)
- Windows Server 2022 (compatible con Azure Files)

Para Citrix Virtual Apps and Desktops 7, se admite el uso de Azure Files con capas de personalización de usuarios en Windows Server 2022, Windows Server 2019 y clientes Windows 10.

> **Nota:**
>
> Si usa un SO de servidor, solo se admite la VDI de servidor. Para obtener información detallada sobre las implementaciones, consulte el artículo VDI de servidor.
>
> La capa de personalización de usuarios admite solo un usuario a la vez por máquina y, a contin-

> uación, la máquina tiene que reiniciar para restablecer los discos. No se puede utilizar la capa de personalización de usuarios con sistemas operativos de servidor multisesión: esa capa solo se puede utilizar con sistemas de servidor de sesión única. La capa de personalización de usuarios solo se admite en escritorios no persistentes.

Desinstale la función de capa de personalización de usuario, si está instalada. Reinicie la imagen maestra antes de instalar la versión más reciente.

Configurar el recurso compartido de archivos

La función de capa de personalización de usuarios requiere almacenamiento de Windows Server Message Block (SMB). Para crear un recurso compartido de archivos de Windows, siga los pasos habituales para el sistema operativo Windows en el que se encuentra.

Para obtener más información sobre el uso de Azure Files con catálogos basados en Azure, consulte Configurar el almacenamiento de Azure Files para capas de personalización de usuarios.

Recomendaciones

Siga las recomendaciones que se indican en esta sección para implementar correctamente la capa de personalización de usuarios.

Microsoft System Center Configuration Manager (SCCM)

Si utiliza SCCM con la funcionalidad de capa de personalización de usuarios, siga las instrucciones de Microsoft para preparar la imagen en un entorno VDI. Consulte este artículo de Microsoft TechNet para obtener más información.

Tamaño de capa de usuarios

Una capa de usuarios es un disco aprovisionado ligero que se expande a medida que se utiliza espacio en el disco. El tamaño predeterminado de la capa de usuarios es de 10 GB, el mínimo que recomendamos.

> **Nota:**
>
> Durante la instalación, si el valor se establece en cero (0), el tamaño predeterminado de la capa de usuarios se establece en 10 GB.

Si quiere cambiar el tamaño de la capa de usuarios, puede introducir un valor diferente para la directiva **Tamaño de capa de usuarios**. Consulte el **Paso 5: Crear directivas personalizadas de grupo de entrega**, en **Opcional: haga clic en Seleccionar junto a Tamaño de capa de usuarios en GB.**

Herramientas para invalidar el tamaño de capa de usuarios (opcional)

Puede pasar por alto el tamaño de capa de usuarios definiendo, con una herramienta de Windows, una cuota para el recurso compartido de archivos en la capa de usuarios.

Utilice una de las siguientes herramientas de configuración de cuotas de Microsoft para establecer una cuota fija en el directorio de capa de usuarios denominado **Usuarios**:

- Administrador de recursos del servidor de archivos (FSRM)
- Administrador de cuotas

> **Nota:**
>
> Aumentar la cuota afecta a las nuevas capas de usuarios y expande las existentes. Disminuir la cuota solo afecta a las nuevas capas de usuarios. Las capas de usuarios existentes nunca disminuyen de tamaño.

Implementar una capa de personalización de usuarios

Al implementar la función de personalización de usuarios, defina las directivas en Web Studio. A continuación, asigne las directivas al grupo de entrega vinculado al catálogo de máquinas, donde se implementa la función.

Si deja la imagen maestra sin configuración de capa de personalización de usuarios, los servicios permanecen inactivos y no interfieren con las actividades de creación.

Si establece las directivas en la imagen maestra, los servicios intentarán ejecutar y montar una capa de usuarios en la imagen maestra. La imagen maestra presenta comportamientos inesperados e inestabilidad.

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.

> **Nota:**
>
> Iniciar sesión por primera vez después de actualizar la versión de Windows 10 en la imagen tarda más de lo habitual. La capa del usuario debe actualizarse para la nueva versión de Windows 10, lo que prolonga el inicio de sesión.

Paso 1: Verifique la disponibilidad de un entorno Citrix Virtual Apps and Desktops

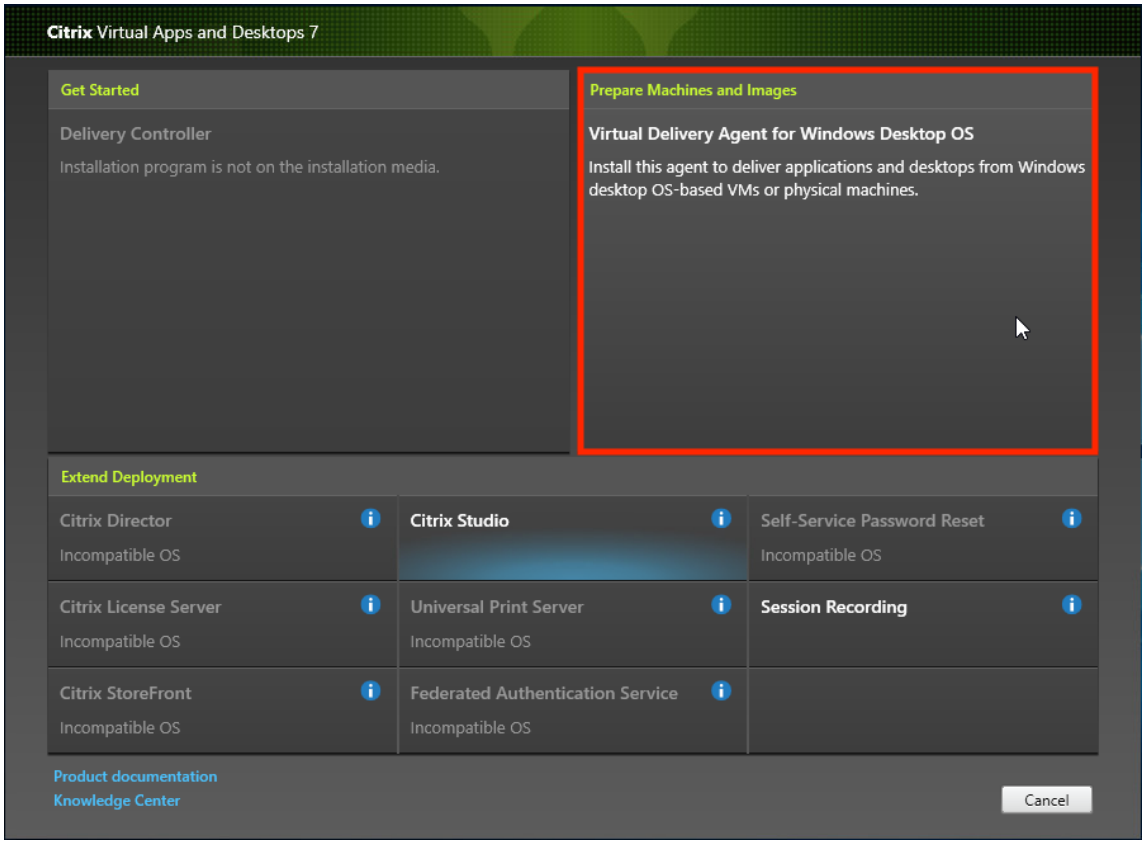
Asegúrese de que su entorno Citrix Virtual Apps and Desktops esté disponible para su uso con esta nueva función. Para obtener información detallada sobre la configuración, consulte Instalar y configurar Citrix Virtual Apps and Desktops.

Paso 2: Prepare la imagen maestra

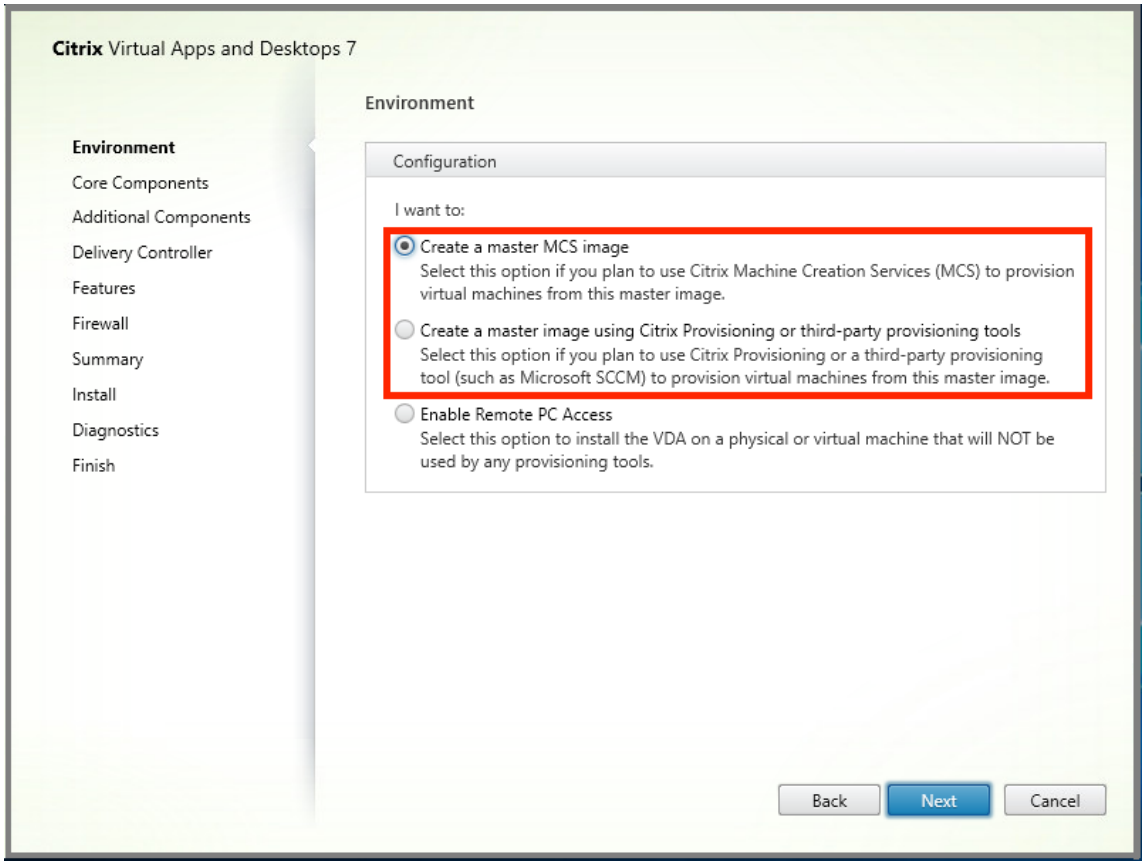
Para preparar la imagen maestra:

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. Si va a implementar VDI de servidor, siga los pasos descritos en el artículo VDI de servidor. Debe incluir el componente opcional, la **Capa de personalización de usuarios**. Para obtener información detallada, consulte Opciones de línea de comandos para instalar un VDA.
3. Si utiliza Windows 10, instale Virtual Delivery Agent (VDA) 1912 o una versión posterior. 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, la **Capa de personalización de usuarios de Citrix**, de la siguiente manera:

    a) Haga clic en el icono **Virtual Delivery Agent para SO de escritorio Windows**:

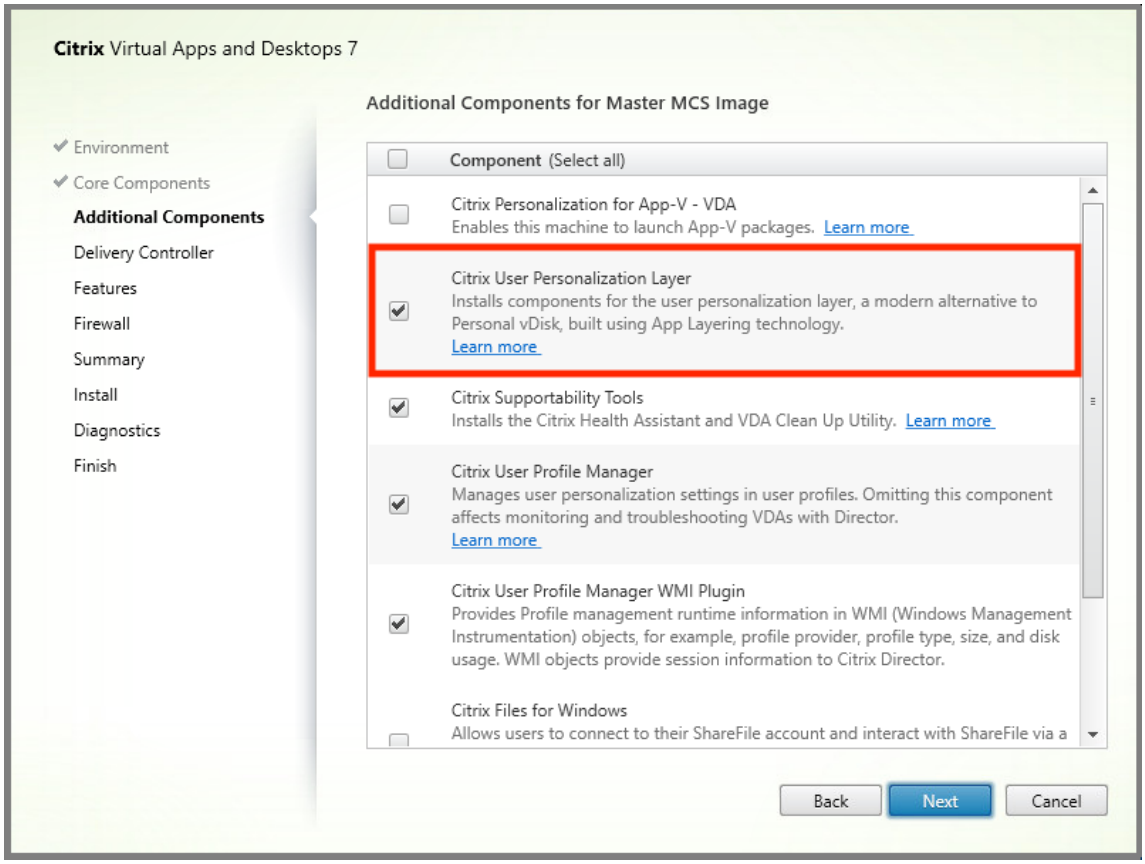


a) **Entorno:** Seleccione **Crear una imagen maestra de MCS** o **Crear una imagen maestra mediante Citrix Provisioning o herramientas de aprovisionamiento de terceros**.



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.

4. 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 Web Studio.

> **Nota:**
>
> Si simplemente quiere actualizar la versión de la capa de personalización de usuarios (UPL), puede hacerlo con una versión más reciente de UPL y el paquete independiente. No necesita actualizar la versión del VDA.

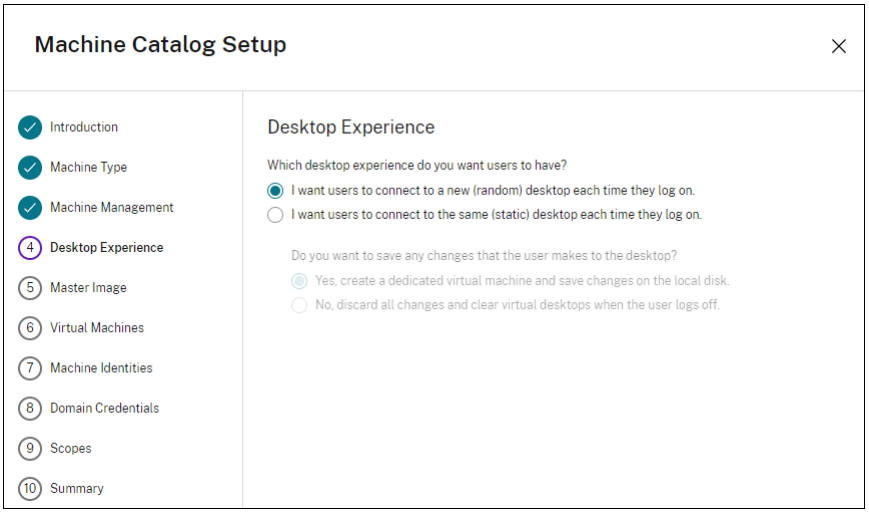
Paso 3: Cree un catálogo de máquinas

En Web Studio, siga los pasos para crear un catálogo de máquinas. Utilice las siguientes opciones durante la creación del catálogo:

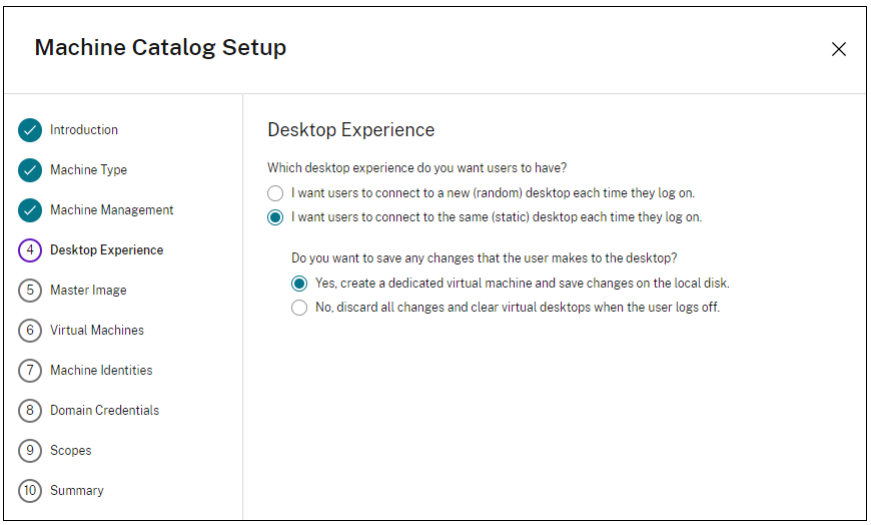
1. Seleccione **Sistema operativo** y establezca el valor en **SO de sesión única**.

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** 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.

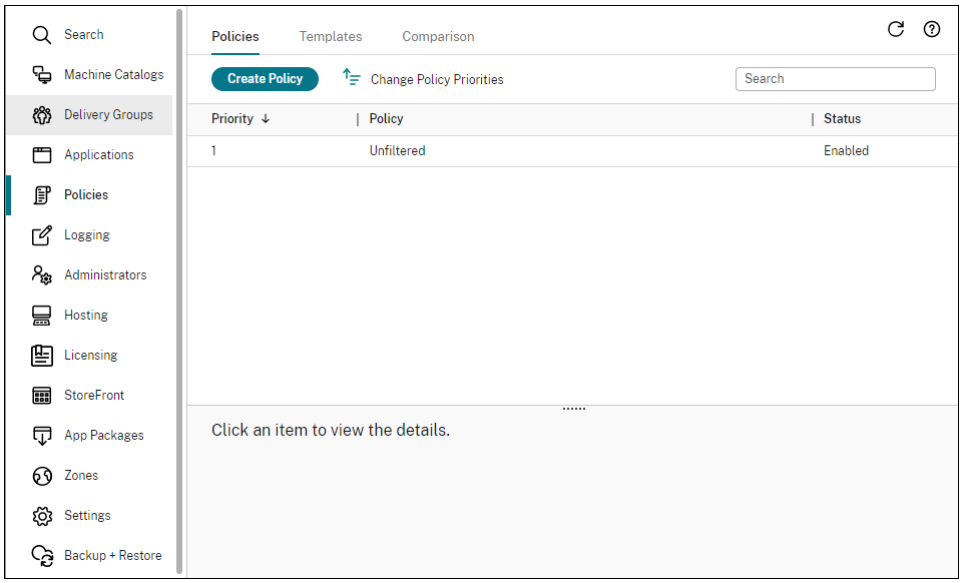
Paso 5: Cree directivas personalizadas de grupo de entrega

Para habilitar el montaje de capas de usuarios dentro de Virtual Delivery Agents, use 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.

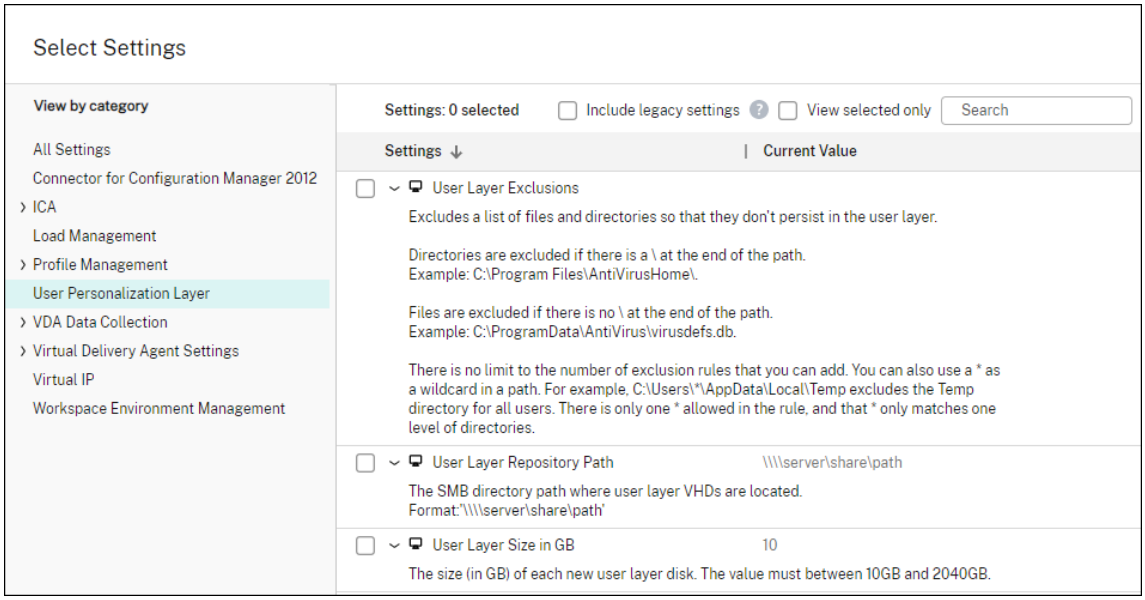
Para definir los parámetros como directivas de Citrix personalizadas en Web Studio y asignarlos al grupo de entrega.

1. Inicie sesión en Web Studio y seleccione **Directivas** en el panel de la izquierda:

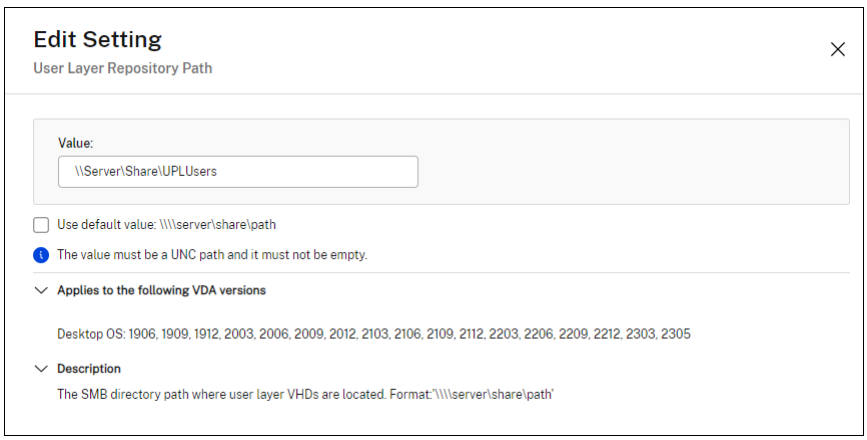


2. Seleccione **Crear directiva** en la barra de acciones. Aparecerá la ventana Crear directiva.
3. Escriba `user layer` en el campo de búsqueda. En la lista de directivas disponibles, aparecen las tres directivas siguientes:
    - Exclusiones de capas de usuarios
    - Ruta del repositorio de capas de usuarios
    - Tamaño de capa de usuarios en GB

> **Nota:**
>
> Aumentar el tamaño afecta a las nuevas capas de usuarios y expande las existentes. Disminuir el tamaño solo afecta a las nuevas capas de usuarios. Las capas de usuarios existentes nunca disminuyen de tamaño.



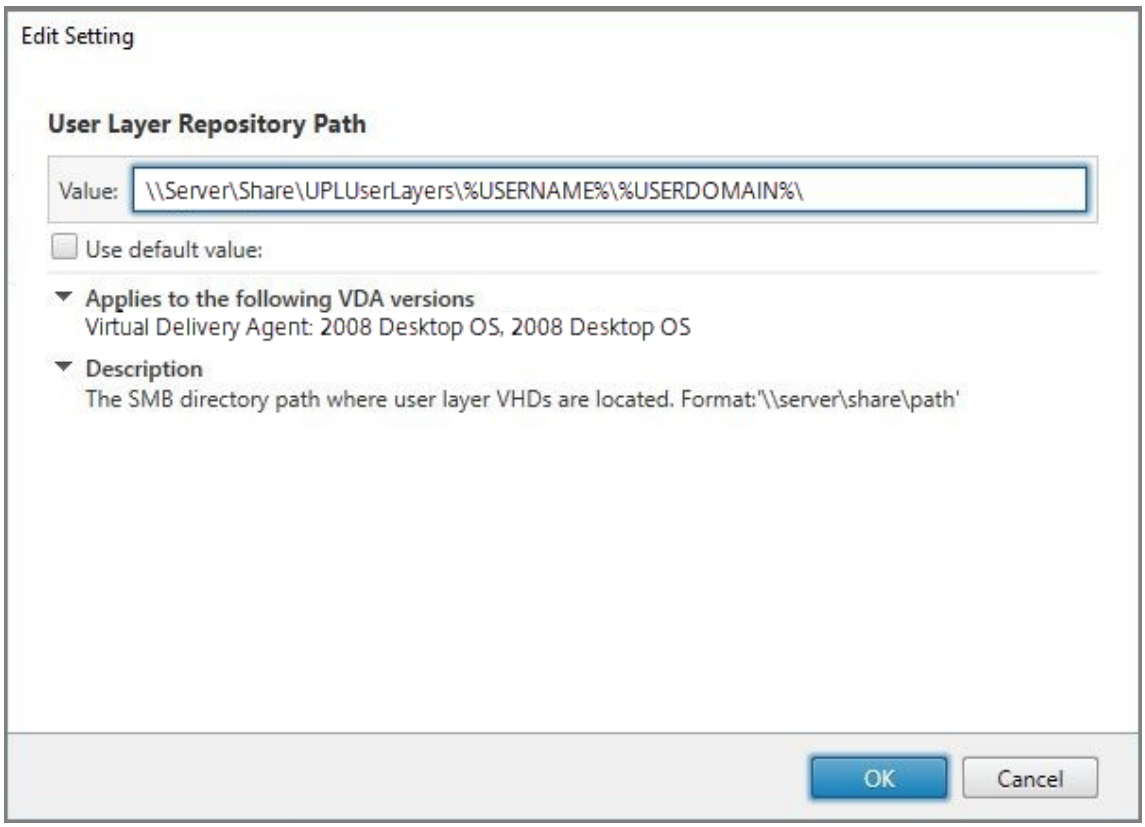
4. Marque la casilla situada junto a **Ruta del repositorio de capas de usuarios** y haga clic en **Modificar**. Se muestra la ventana **Modificar parámetro** .
5. Introduzca una ruta en el campo **Valor** y haga clic en **Guardar**:
   - **Formato de ruta:** `\\server-name-or-address\share-name\folder`
   - **Ejemplo de ruta:** `\\Server\Share\UPLUsers`
   - **Ejemplo de ruta resultante:** Para un usuario llamado **Alex** en **CoolCompanyDomain**, la ruta sería: `\\Server\Share\UPLUsers\Users\CoolCompanyDomain_Alex\A_OK`



Puede personalizar la ruta mediante las variables %USERNAME% y %USERDOMAIN%, las variables de entorno de la máquina y los atributos de Active Directory (AD). Cuando se expanden, estas variables dan como resultado rutas explícitas.

Ejemplo de variables de entorno:

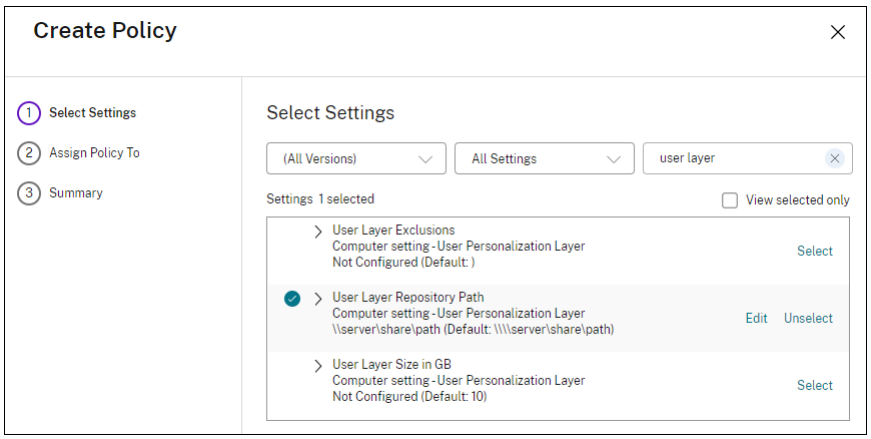
- **Formato de ruta:** `\\Server-name-or-address\share-name\folder-with-environment-variables`
- **Ejemplo de ruta:** `\\Server\Share\UPLUserLayers\%USERNAME%\%USERDOMAIN%`
- **Ejemplo de ruta resultante:** Para un usuario llamado **Alex** en **CoolCompanyDomain**, la ruta sería: `\\Server\Share\UPLUserLayers\Alex\CoolCompanyDomain\A_OK`



Ejemplo de atributos de AD personalizados:

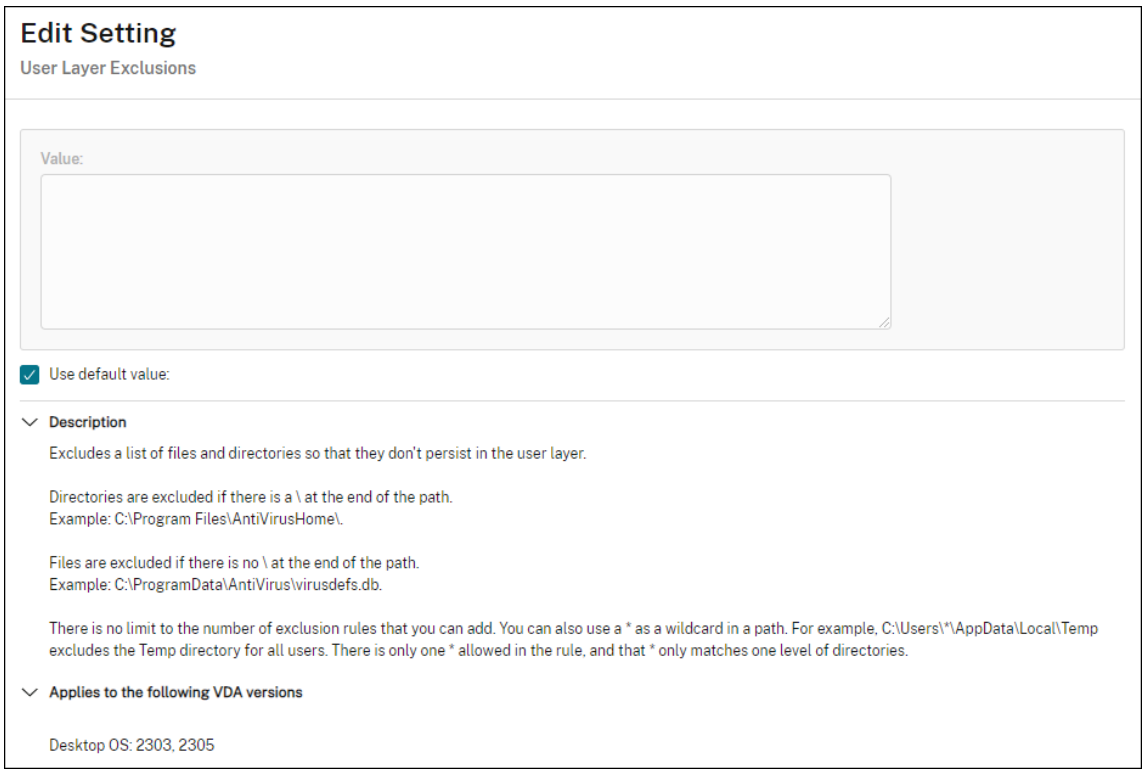
- Formato de ruta: `\\Server-name-or-address\share-name\AD-attribute`
- Ejemplo de ruta: `\\Server\share\\#sAMAccountName#`
- Ejemplo de rutas resultantes: `\\Server\share\JohnSmith` (si #sAMAccountName# se resuelve en JohnSmith para el usuario actual)

6. Opcional: Marque la casilla situada junto a **Tamaño de las capas de usuarios en GB** y haga clic en **Modificar**:

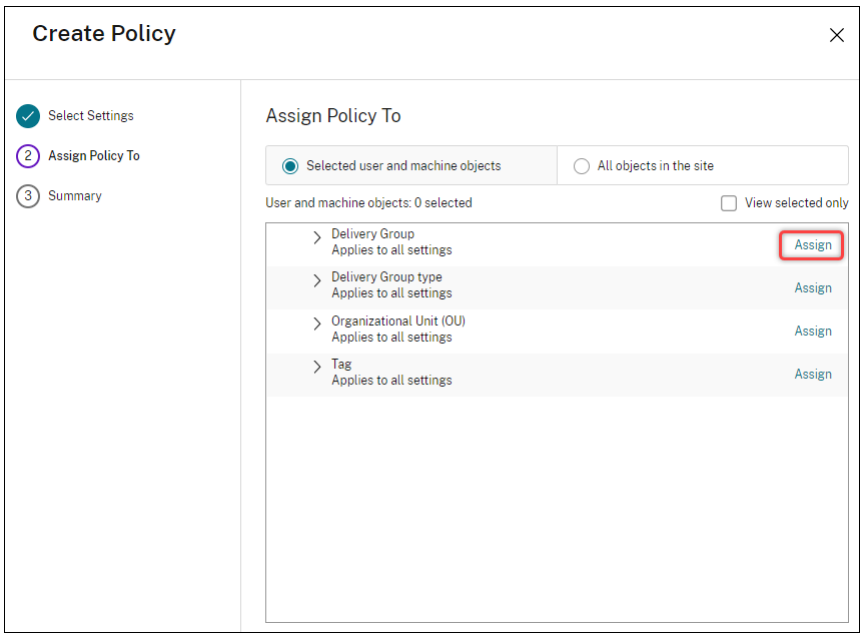


Aparecerá la ventana Modificar parámetros.

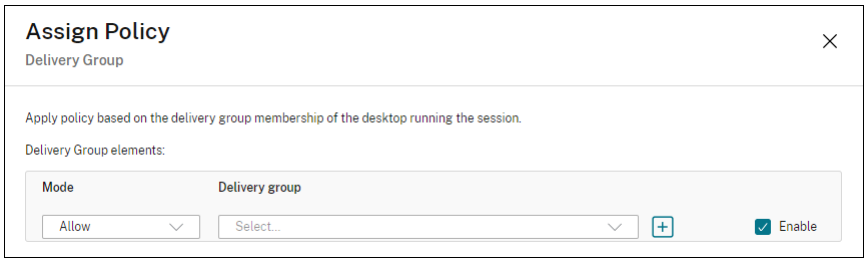
7. Opcional: Cambie el valor predeterminado de **10 GB** al tamaño máximo que puede tener cada capa de usuario. Haga clic en **Guardar**.
8. Opcional: Marque la casilla situada junto a **Exclusiones de capas de usuarios** y haga clic en **Modificar**.



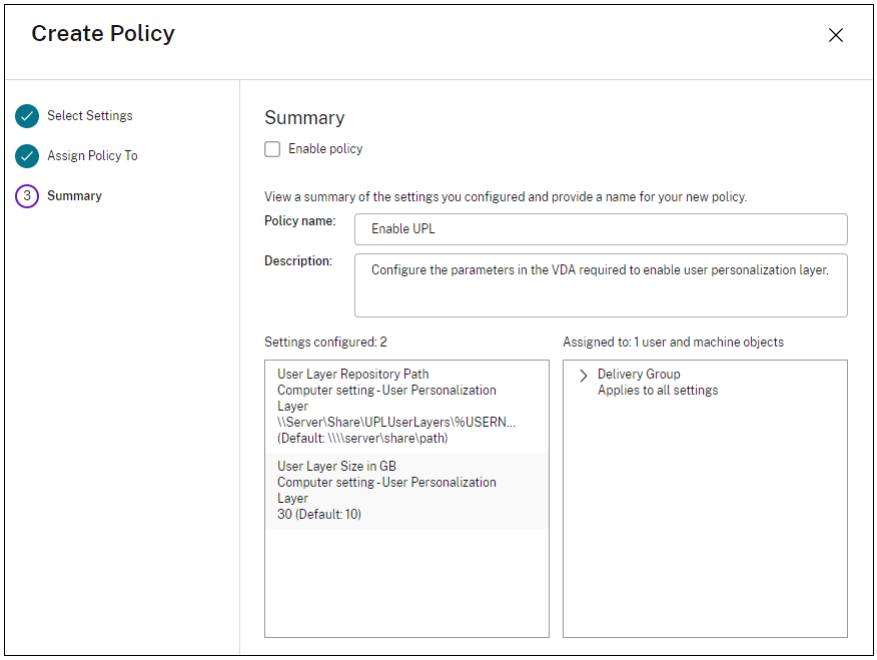
9. Opcional: Especifique los archivos y carpetas que quiera excluir y, a continuación, haga clic en **Guardar**. Para obtener más información, consulte la documentación de Citrix App Layering.
10. Haga clic en **Siguiente** para configurar los usuarios y las máquinas a los que quiera asignar. Haga clic en el enlace **Asignar grupo de entrega** resaltado en esta imagen:



11. En el menú **Grupo de entrega**, seleccione el grupo de entrega creado en la sección anterior. Haga clic en **Aceptar**.



12. 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 la capa de usuarios

Como administrador de dominios, puede especificar más de una ubicación de almacenamiento para las capas de usuarios. Cree una subcarpeta `\Users` para cada ubicación de almacenamiento (incluida la ubicación predeterminada). Proteja cada ubicación mediante la siguiente configuración.

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 carpeta/ejecutar archivo; Mostrar lista de carpetas/leer datos; Leer atributos	Solo carpeta seleccionada
Sistema	Control total	Carpeta, subcarpetas y archivos seleccionados
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**

  ```
  We were unable to attach your user layer because it is in use.
  Any changes you make to application settings or data will not be
  saved. Be sure to save any work to a shared network location.
  ```

- **Capa de usuarios no disponible**

  ```
  We were unable to attach your user layer. Any changes you make to
   application settings or data will not be saved. Be sure to save
  any work to a shared network location.
  ```

- **El sistema no se restablece después de que el usuario haya cerrado la sesión**

  ```
  This system was not shut down properly. Please 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
```

Recuperación de espacio de capa de usuarios/UPL

Puede usar la función de **recuperación de espacio de capa de usuarios/UPL** para comprimir automáticamente los archivos VHDX cada vez que el usuario cierre sesión.
Para obtener más información, consulte Recuperación de espacio de capa de usuarios/UPL

Limitaciones

Tenga en cuenta las siguientes limitaciones al instalar y usar la funcionalidad de capa de personalización de usuarios.

- *No* intente implementar el software de la capa de personalización del usuario en una capa dentro de App Layering. Implemente capas de personalización de usuarios en Citrix Virtual Apps and Desktops o habilite capas de usuarios en una plantilla de imagen de App Layering, pero no realice ambos procesos. Cualquiera de los dos produce las capas de usuarios que necesita.

- *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 usada al crear el catálogo de máquinas.
- *No* use controladores de tiempo de arranque, ni ninguna otra personalización de primera fase de arranque.
- *No* migre datos de PvD a la función de la capa de personalización de usuarios.
- *No* migre capas de usuarios existentes del producto App Layering completo a la función de 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.
- Cuando un usuario cierra la sesión y vuelve a iniciarla, la nueva sesión se ejecuta en otra máquina del grupo. En un entorno VDI, Microsoft Software Center muestra una aplicación como **Instalada** en la primera máquina, pero la muestra como **No disponible** en la segunda máquina.

  Para averiguar el verdadero estado de la aplicación, indique al usuario que seleccione la aplicación en el Centro de software y haga clic en **Instalar**. A continuación, SCCM actualiza el estado al valor verdadero.
- 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 el Centro de software.
- En Directivas de grupo (Configuración de equipo), los parámetros de capa de usuarios supeditan los parámetros aplicables a la imagen maestra. Por consiguiente, los cambios que realice 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:

  ```
  gpudate /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.

- Una cuenta de usuario de dominio no debe ser el último usuario que haya iniciado sesión en una imagen maestra. De lo contrario, las máquinas aprovisionadas desde esa imagen podrían tener problemas.
- Los certificados personalizados no persisten cuando la capa UPL está habilitada en un entorno de Azure AD puro por un problema subyacente en Windows que se ejecuta en Azure. Si Microsoft corrige este problema en una mejora futura, actualizaremos este artículo.

Eliminar componentes

August 17, 2024

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 Apps and 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`, 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 Web Studio.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components webstudio
```

Eliminar VDA mediante la línea de comandos

Desde el directorio `\x64\XenDesktop Setup`, ejecute el comando `XenDesktopVdaSetup.exe`.

- Para quitar uno o varios componentes, use las opciones `/remove` y `/components`. Por ejemplo: para quitar el VDA y la aplicación Citrix Workspace, use `/remove /components vda,plugin`.
- La opción `/removeall` quita solo el VDA. No elimina la aplicación Citrix Workspace.

Para obtener información detallada acerca de parámetros y comandos, consulte Instalación desde la línea de comandos.

De forma predeterminada, la máquina se reinicia automáticamente después de la eliminación.

Para quitar agentes VDA mediante un script en Active Directory, consulte Instalar o quitar agentes VDA mediante scripts.

Actualización y migración

August 17, 2024

Introducción

Las actualizaciones cambian la implementación de la **Versión actual (Current Release)** de Citrix Virtual Apps and Desktops 7, 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.

Información general sobre la actualización

1. Revise el artículo Actualizar la versión de una implementación antes de comenzar la actualización. Esta es la fuente de información principal para prepararse y aprender a implementar una actualización.
2. Asegúrese de que las fechas actuales de Customer Success Services sean válidas y no hayan caducado. Para obtener más información, consulte el artículo Licencias de renovación de Customer Success Services.
3. Complete las instrucciones de preparación.
4. Ejecute los instaladores para actualizar los componentes principales.
5. Actualice las bases de datos del sistema y el sitio.
6. Actualice los VDA en imágenes (o directamente en máquinas).
7. Actualice otros componentes.

Cada paso de preparación y actualización se detalla en Actualizar la versión de una implementación.

Versiones que puede actualizar

Puede actualizar a Citrix Virtual Apps and Desktops 2402 LTSR desde:

- Virtual Apps and Desktops 2203 LTSR con o sin CU, hasta CU4 incluida
- Virtual Apps and Desktops 1912 LTSR con o sin CU, hasta CU8 incluida
- Versiones CR compatibles actualmente de Citrix Virtual Apps and Desktops

En [Citrix Upgrade Guide](/en-us/upgrade.html) puede encontrar también una lista de las versiones de Citrix Virtual Apps and Desktops (y XenApp y XenDesktop) desde las que se puede actualizar.

> Nota:
>
> - Antes de iniciar el proceso de actualización de versión, Citrix recomienda que los clientes la prueben en un entorno controlado y verifiquen que satisface sus requisitos específicos. Además, recomendamos revisar toda la documentación relevante del producto, incluida la lista de productos obsoletos y los problemas conocidos, para garantizar una transición sin problemas. Este enfoque ayuda a mitigar las posibles interrupciones en los sistemas de producción y mejora la experiencia general con la actualización de versión.
> - Citrix Virtual Apps and Desktops 1912 LTSR llegará pronto a su fase de fin de vida.
>
> Para obtener más información sobre las versiones compatibles, consulte Tabla de productos.

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?**

  Para obtener una ilustración y una descripción de la secuencia de actualización recomendada, 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 de versión.

- **¿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](/en-us/upgrade).

- **¿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](https://www.citrix.com/support/product-lifecycle/milestones/citrix-virtual-apps-and-desktops.html).

- **¿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 usando 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.

For details, see [Servicing Options](https://www.citrix.com/support/citrix-customer-success-services/citrix-virtual-apps-and-desktops-servicing-options.html).

- **¿Necesito actualizar mis licencias?**

  Compruebe 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?**

  En el artículo Requisitos del sistema de la versión a la que está actualizando, se indican los sistemas operativos compatibles.

  Si la implementación actual utiliza sistemas operativos que ya no son compatibles, consulte Sistemas operativos anteriores.

- **¿Qué versiones de VMware vSphere (vCenter + ESXi) son compatibles?**

  En CTX131239, se indican los hosts y versiones compatibles, además de enlaces a problemas conocidos.

- **¿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 para Windows

Más información

[Long Term Service Release (LTSR)](https://www.citrix.com/support/citrix-customer-success-services/citrix-virtual-apps-and-desktops-servicing-options.html)

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 2203 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.

Migrar

Migrar a la nube

Puede usar la herramienta de configuración automatizada de Citrix Virtual Apps and Desktops para migrar la implementación local a la nube. Para obtener más información, consulte Migrar a la nube.

Migración antigua

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.

No hay herramientas ni scripts compatibles para migrar versiones de XenApp y XenDesktop, ni para migrar versiones anteriores de Citrix Virtual Apps and Desktops. La *actualización* es compatible con las versiones de Citrix Virtual Apps and Desktops descritas en esta documentación de producto.

Para obtener información sobre el contenido de migración anterior de XenApp 6.x, consulte lo siguiente. No se admiten ni mantienen los scripts ni los artículos.

- Los scripts de migración en código abierto para las versiones de XenApp 6.x están disponibles en https://github.com/citrix/xa65migrationtool. Citrix no admite ni mantiene estos scripts de migración
- Cambios en 7.x
- Actualizar un servidor de trabajo XenApp 6.5 a un nuevo VDA
- Migrar XenApp 6.x

Actualizar la versión de una implementación

August 17, 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.

Antes de actualizar a cualquiera de las versiones de Citrix Virtual Apps and Desktops, compruebe que las fechas actuales de Customer Success Services sean válidas y no hayan caducado. Para obtener más información, consulte el artículo Licencias de renovación de Customer Success Services.

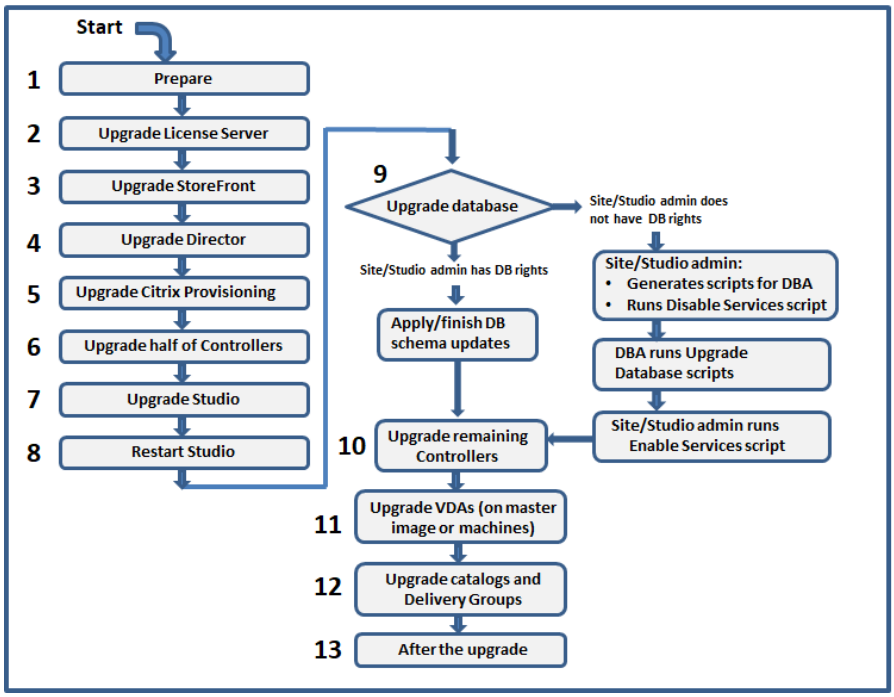
Para iniciar una actualización, ejecute el instalador desde la nueva versión para actualizar los componentes principales, los VDA y otros componentes previamente instalados. A continuación, actualice las bases de datos y el sitio.

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.

Licencias de derechos híbridos

Las licencias de Derechos híbridos son licencias de suscripción temporales que se proporcionan, además de la suscripción de servicio de la nube, cuando un cliente pasa o cambia de una licencia perpetua a una suscripción de servicio de la nube. También puede adquirir un complemento de Derechos híbridos con sus suscripciones de DaaS.

Si tiene una licencia de Derechos híbridos con un atributo SaaS, al actualizar Citrix Virtual Apps and Desktops a la versión LTSR 2203 o una posterior, podrá acceder a prestaciones no disponibles con Citrix Virtual Apps and Desktops LTSR 1912. Estas prestaciones incluyen el aprovisionamiento y el alojamiento de cargas de trabajo en nubes públicas, como Microsoft Azure, AWS EC2 y Google Cloud. Antes de implementar el nuevo archivo de licencias, actualice el Servidor de licencias a la versión más reciente.

Si tiene acceso a una licencia de Derechos híbridos sin ningún atributo SaaS, siga estos pasos para acceder a la nueva licencia de Derechos híbridos con el atributo SaaS:

> **Nota:**
>
> - Recibirá un correo electrónico con un nuevo código de licencia. Para obtener más información, consulte Usar un código de acceso de licencias.
> - Las licencias existentes se rescinden. Las licencias rescindidas deben eliminarse de los servidores de licencias y, a continuación, debe instalarse una nueva licencia. Para obtener más información, consulte Eliminar archivos de licencias.

1. Vaya al portal Administrar licencias de citrix.com y descargue el nuevo archivo de licencia de derechos híbridos con derechos de aprovisionamiento en la nube habilitados (atributo SaaS). Para obtener más información, consulte Descargar licencias. La siguiente imagen muestra el archivo de licencia de derechos híbridos con el atributo SaaS en la sección Increments.

2. Instale el archivo de licencia de derechos híbridos en el servidor de licencias. Para obtener más información, consulte Instalar licencias.
3. Si hay un cambio en las ediciones o el modelo de licencia, ejecute el comando de broker para establecer la edición y el modelo y, a continuación, inicie la actualización. Para obtener más información sobre los comandos de Broker, consulte la sección SDK de Broker PowerShell.

Para obtener más información sobre la compatibilidad con nube pública en las versiones Current Release y Long Term Service Release (LTSR) de Citrix Virtual Apps and Desktops, consulte CTX270373.

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:

- Quitar discos PvD, AppDisks y hosts no admitidos
- VDA que tienen componentes PvD o AppDisk
- 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 la versión de Web Studio (porque estaba en la misma máquina que otro componente), ejecute el instalador en la máquina que contiene Studio.

> **Nota:**
>
> Tras actualizar Web Studio, es posible que la información de la versión no se actualice inmediatamente. Es posible que se le pida que actualice la versión de Web Studio aunque ya esté actualizado. Para solucionar el problema, vaya al servidor de Web Studio, abra Administrador de Internet Information Services (IIS), vaya a Start Page > Sites > Default Web Site y seleccione **Restart** en el panel Manage Website.

Paso 8: Reinicie Studio

Reinicie la versión de Web 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 pro-

ducto 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**.

> **Nota:**
>
> Para que la **actualización de versión de los Delivery Controllers restantes** esté disponible, cree al menos un catálogo de máquinas y un grupo de entrega para el sitio.

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 Actualización de agentes VDA a la versión 1912 o 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.

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

Al actualizar la implementación, pueden actualizarse 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	2203
7.15 RTM or 7.15 CU releases	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 RTM	Config	Site, Config	Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU1		Site	Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU2			Site, Config	Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU3				Site; Monitor; Config	Site; Monitor; Config	Site; Monitor; Config; Logging
1912 CU4					Site, Config	Site; Monitor; Config; Logging
1912 CU5						Site; Monitor; Config; Logging
2112						Site; Monitor; Config

Definición de términos:

- Sitio: Almacén de datos del sitio. La actualización de DbSchema se realiza en el almacén de datos del sitio.

- Supervisar: 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 2203 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 2203 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**.
- 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 (2203 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.
2. Instale el nuevo VDA.

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

> **Nota:**
>
> *¿Puedo usar Personal vDisk con escritorios Windows 7 en XenApp y XenDesktop 7.15 LTSR?*
>
> Citrix excluyó Personal vDisk (PvD) de XenApp y XenDesktop 7.6 LTSR, que se anunció en enero de 2016. Además, Citrix anunció la retirada de la tecnología PvD y recomienda que los clientes comiencen a utilizar Citrix App Layering en el futuro. Citrix App Layering (a partir de la versión 4.4) es un componente compatible de XenApp y XenDesktop 7.15 LTSR. Sin embargo, para ayudar a los clientes con implementaciones de PvD existentes en Windows 7 a migrar a la tecnología Citrix App Layering, Citrix ha decidido ofrecer asistencia por tiempo limitado a implementaciones de PvD para escritorios Windows 7 a través de las versiones LTSR Cumulative Update (CU) de XenApp y XenDesktop 7.15 hasta el 14 de enero de 2020. El componente PvD se quitará de las versiones LTSR CU y dejará de desarrollarse a partir del 14 de enero de 2020. Además, el uso de PvD para Windows 7 después del 14 de enero de 2020 hará que los sitios LTSR no cumplan con la normativa vigente. Por último, PvD para Windows 10 sigue excluido de la versión 7.15 LTSR. Por lo tanto, los clientes no deben usarlo con sus sitios de LTSR 7.15.

Quitar discos PvD, AppDisks y hosts no admitidos

Las tecnologías y los tipos de hosts que se indican a continuación no se admiten en las implementaciones de la versión Current Release de Citrix Virtual Apps and Desktops 7:

- **Personal vDisk (PvD)** para almacenar datos junto a las VM de los usuarios en catálogos. Ahora la entidad de la capa de personalización de usuarios controla la persistencia del usuario.
- **AppDisks** para administrar aplicaciones utilizadas en grupos de entrega.
- **Tipos de host:** Azure Classic, CloudPlatform (el producto original de Citrix).
  - Para obtener información sobre los tipos de host admitidos en esta versión, consulte Requisitos del sistema.
  - Para obtener información sobre formas alternativas de seguir utilizando ARM y AWS, consulte CTX270373.

Si la implementación actual utiliza discos PvD o AppDisks, o bien tiene conexiones con tipos de hosts no admitidos (por ejemplo, Microsoft Azure Classic), puede actualizar la versión a la 2006 (o a una versión posterior compatible) solamente tras haber quitado los elementos que utilizan esas tecnologías. Si su implementación actual utiliza conexiones de host de nube pública (por ejemplo, AWS), asegúrese de que cuenta con una licencia de derechos híbridos antes de proceder a la actualización. Cuando el instalador detecta una o más de las tecnologías o conexiones de host no compatibles sin licencia de derechos híbridos, la actualización se pone en pausa o se detiene y se muestra un mensaje explicativo. Los registros del instalador contienen información detallada.

Para ayudar a garantizar una actualización correcta, revise y siga las instrucciones correspondientes para quitar los elementos no compatibles.

- Quitar PvD
- Quitar AppDisks
- Quitar elementos de hosts no admitidos

Aunque no haya utilizado discos PvD o AppDisks en la implementación, es posible que los MSI relacionados se hayan incluido en una instalación o una actualización de VDA anteriores. Antes de poder actualizar la versión de VDA a la versión 2006 (o a una versión posterior compatible), debe quitar ese software, aunque no lo haya utilizado nunca. Al utilizar la interfaz gráfica, dicha eliminación se puede hacer en su nombre, o bien puede incluir opciones de eliminación al usar la interfaz de línea de comandos. Para obtener más información, consulte Actualizar la versión de VDA que tienen componentes PvD o AppDisks.

Quitar PvD

La actualización de la versión de una implementación no se puede realizar correctamente hasta que no haya quitado todas las máquinas configuradas para usar PvD. Esto afecta a los catálogos y a los grupos de entrega.

Para quitar PvD de grupos y catálogos:

1. Desde Studio, si un grupo de entrega contiene máquinas de un catálogo que utiliza PvD, quite esas máquinas del grupo.
2. Desde Studio, elimine todos los catálogos que contengan máquinas que usan PvD.

Actualización de versiones de VDA: La actualización de la versión de la implementación no detecta si los VDA tienen instalados los componentes AppDisk ni PvD. Sin embargo, los instaladores de VDA sí los detectan. Para obtener más información, consulte VDA que tienen componentes PvD o AppDisk.

Si piensa utilizar App Layering en lugar de PvD, consulte Migrar Personal vDisk a App Layering para obtener información sobre cómo mover datos.

Quitar AppDisks

La actualización de la versión de una implementación no puede continuar hasta que haya quitado AppDisks de todos los grupos de entrega que los utilicen y, a continuación, haya quitado los propios AppDisks.

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo y, a continuación, haga clic en **Administrar AppDisks** en el panel Acción.
3. Haga clic en la acción que quita el AppDisk del grupo.
4. Repita los pasos 2 y 3 para cada grupo de entrega que use AppDisks.
5. Seleccione **AppDisks** en el panel de navegación de Studio.

6. Seleccione un AppDisk y haga clic en la acción que elimina el AppDisk.
7. Repita los pasos 5 y 6 para cada AppDisk.

Actualización de versiones de VDA: La actualización de la versión de la implementación no detecta si los VDA tienen instalados los componentes AppDisk ni PvD. Sin embargo, los instaladores de VDA sí los detectan. Para obtener más información, consulte VDA que tienen componentes PvD o AppDisk.

Quitar elementos de hosts no admitidos

La actualización de la versión de una implementación a la versión 2006 (o una versión posterior compatible) no puede continuar si el sitio tiene conexiones con tipos de hosts no admitidos, como Citrix CloudPlatform o Microsoft Azure Classic. Realice las tareas siguientes antes de intentar llevar a cabo una actualización.

Desde Studio:

- Elimine todas las conexiones a hosts no admitidos.
- Si un grupo de entrega contiene máquinas de un catálogo creado con una imagen maestra de un host no compatible, quite esas máquinas del grupo.
- Elimine todos los catálogos que se crearon mediante una imagen maestra de un host no compatible.

VDA que tienen componentes de PvD o AppDisk

Si los componentes que habilitan las tecnologías PvD y AppDisk están instalados en un VDA, la versión de dicho VDA no se puede actualizar hasta que se hayan quitado esos componentes.

> **Nota:**
>
> Al actualizar la versión a la 1912, tuvo que desinstalar el VDA actual e instalar el nuevo VDA. En esta versión, se le preguntará si quiere que Citrix quite el componente y, a continuación, continuar con la actualización.

Es posible que los componentes AppDisk y PvD se hayan instalado en versiones anteriores de VDA, aunque nunca haya utilizado esas tecnologías:

- Interfaz gráfica: En los instaladores de VDA, la página **Componentes adicionales** contenía la opción **Citrix AppDisk / Personal vDisk**. 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 que la ofreciera), ese componente se instalaba.
- Interfaz de línea de comandos: Al especificar la opción `/baseimage`, se instalaba el componente.

Qué se debe hacer Si el instalador de VDA no detecta los componentes AppDisk o PvD en el VDA instalado actualmente, la actualización de la versión continúa como de costumbre.

Si el instalador detecta los componentes AppDisk o PvD en el VDA instalado actualmente:

- Interfaz gráfica: La actualización de la versión queda en pausa. Un mensaje le pregunta si quiere que los componentes no admitidos se quiten automáticamente. Si hace clic en **Aceptar**, los componentes se quitan automáticamente y la actualización continúa.
- Interfaz de línea de comandos: Para evitar errores de comando, incluya las siguientes opciones en el comando:
  - `/remove_appdisk_ack`
  - `/remove_pvd_ack`

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 2016. Ahora quiere actualizar ese VDA a la versión actual, pero Windows Server 2016 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:

- Versión actual (Current Release) de Citrix Virtual Apps and Desktops
  - 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.
- Para las versiones LTSR, consulte las listas de componentes de su versión LTSR y CU. (Seleccione su versión LTSR en la página principal de la documentación del producto Citrix Virtual Apps and Desktops.)

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.

Sistema operativo	Componente o función	Última versión válida	Instalar o actualizar no es posible a partir de la versión
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

Sistema operativo	Componente o función	Última versión válida	Instalar o actualizar no es posible a partir de la versión
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 Server 2016	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 (esto incluye actualizaciones de versión internas de su SO). Por ejemplo: de Windows 10, versión 1903, a Windows 10, versión 1909). De lo contrario, el software Citrix no será compatible. Luego, instale el nuevo componente.
- Para actualizar la versión del sistema operativo de una máquina VDA sin tener que crear la imagen de nuevo, primero debe instalar una versión del VDA compatible con la versión del sistema operativo a la que lo actualizará, o bien actualizar la versión del VDA después de actualizar la del sistema operativo. De lo contrario, el software Citrix no será compatible. Puede actualizar a las siguientes versiones mínimas del sistema operativo al realizar una actualización en contexto sin desinstalar el VDA:
  - Windows 11 con la actualización acumulativa 2023-07 para Windows 11 (KB5028185) o posterior instalada (compilación 22621.1992 o posterior).
  - Windows 10 con la actualización dinámica 2023-07 para Windows 10 (KB5028311) instalada.
- Si la versión de Windows a la que piensa actualizar no se ajusta a la directriz mencionada anteriormente, debe desinstalar el VDA antes de actualizar el sistema operativo y, a continuación, instalar una versión de VDA compatible una vez finalizada la actualización del sistema operativo.

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.
3. Agregue los nuevos Controllers al sitio.

4. Quite los Controllers que se ejecutan en sistemas operativos no válidos para la versión actual. Siga las recomendaciones para eliminar Controllers en Delivery Controllers.

Preparar

Antes de comenzar una actualización, revise la siguiente información y complete las tareas necesarias.

> **Nota:**
>
> Aunque la actualización de versión de los VDA se produce más adelante en la secuencia de actualización, es recomendable elegir un instalador y revisar el procedimiento antes de iniciar la actualización para que sepa a qué atenerse.

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.

Durante el proceso de actualización de un VDA a la versión actual, la máquina se reinicia. (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 LocalDB 2019. Para obtener información detallada sobre cómo reemplazar SQL Server Express LocalDB con la 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. La fecha debe ser 2021.11.15 o posterior.

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.
- Desde el directorio `XenDesktop Setup` en los medios de instalación, ejecute el comando `.\LicServVerify.exe -h <license-server-fqdn> -p 27000 -v`. La pantalla 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 version, si ha hecho modificaciones en los archivos de `C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data`, como *default.ica* y *usernamepassword.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
- Si desea agregar conexiones de host de nube pública (por ejemplo, AWS), debe tener una licencia de derechos híbridos. De lo contrario, la prueba preliminar del sitio se pone en pausa o se detiene y aparece un mensaje explicativo.

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 para la base de datos del sitio (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 LocalDB de SQL Server Express. ¿Por qué no? Porque es posible que tenga componentes que no dependan 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 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 admitida es SQL Server Express LocalDB 2019. Si instaló originalmente un Delivery Controller anterior a la versión 1912 y no ha reemplazado SQL Server Express LocalDB con la 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 2019.
- 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\NETWORKSERVICE"cmd
   ```

   Opcionalmente, puede utilizar `whoami` para confirmar que el símbolo del sistema se está ejecutando como la cuenta Servicio de red.

   ```
   whoami
   ```

   ```
   nt authority\networkservice
   ```
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.*
   ```

   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 2019. 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\150\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`.

Compatibilidad de proxy con el agente de actualización de VDA

July 4, 2024

Se ha agregado la compatibilidad de proxy para el agente de actualización de VDA en 2311 VDA.

El agente de actualización de VDA de 2311 VDA (es decir, la versión 7.40) puede reconocer y enviar tráfico a través del proxy.

El agente de actualización de VDA (VUA) admite el proxy en forma de Nombre de host:Puerto (IP:Puerto) y archivo PAC.

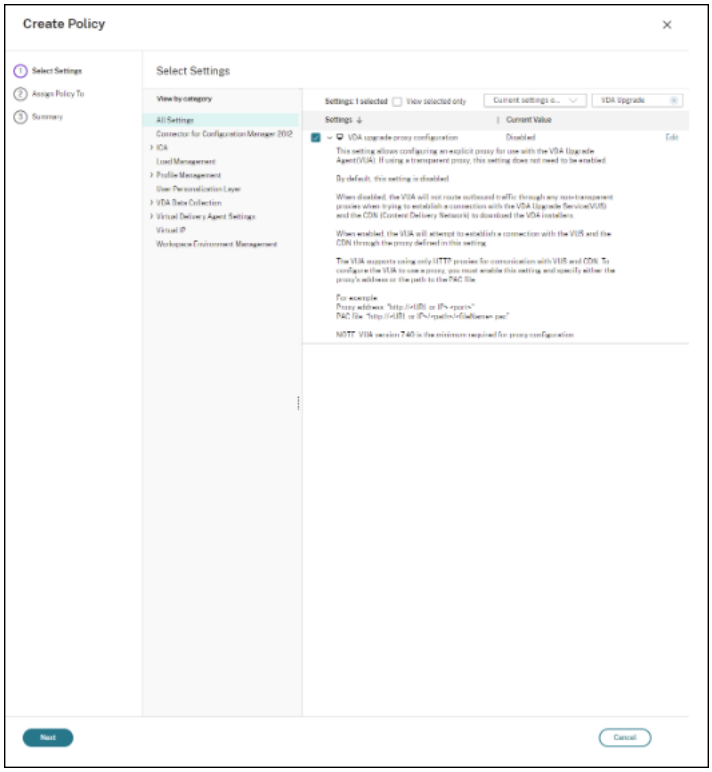
Solo se admiten proxies HTTP.
No se admite el descifrado y la inspección de paquetes.

No se admite la autenticación de proxy.
No se admite SOCKS5.

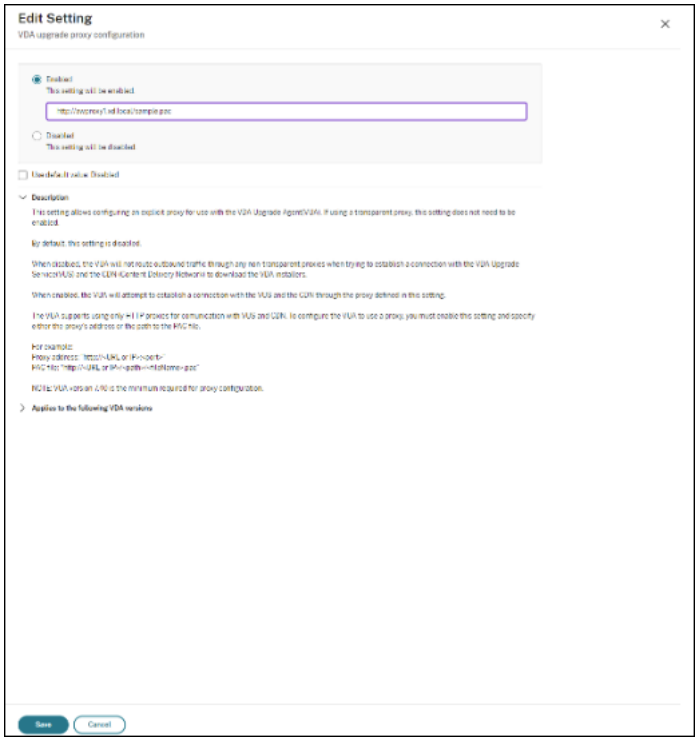
Configuración del proxy del agente de actualización de VDA

El proxy del agente de actualización de VDA se puede configurar de dos maneras:

1. **Configuración de la directiva del agente de actualización de VDA** mediante la **Directiva de Webstudio**.
2. Seleccione **Configuración del proxy de actualización del VDA** en la página **Parámetros** de la página **Crear directiva**.



3. Habilite el parámetro. De forma predeterminada, este parámetro está inhabilitado.



4. Configuración del agente de actualización de VDA mediante la clave de registro.

   La clave de registro se establece en Meta-Installer durante la instalación del VDA.

Registro:

Clave: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent`

tipo de valor: cadena

Nombre del valor: ProxySettings

Información del valor: dirección del proxy o ruta al archivo pac.

Por ejemplo:

a) Dirección proxy: `http://<URL or IP>:<port>`
b) Archivo PAC: `http://<URL or IP>/<path/<filename>.pac`

Hacer copia de seguridad o migrar la configuración

July 4, 2024

Esta función le ayuda a realizar una copia de seguridad de sus configuraciones de DaaS. Las copias de seguridad facilitan el proceso de migración de las configuraciones de un sitio en la nube a otro. También facilita la recuperación inmediata de un sitio en caso de emergencia.
Puede usar los siguientes métodos para realizar copias de seguridad:

1. Copia de seguridad + Restauración
    a) Integrado con WebStudio.
2. Herramienta de configuración automatizada (ACT)
    a) Herramienta basada en PowerShell. Instale la herramienta para usarla.

Las copias de seguridad se pueden usar para:

1. Restauración
2. Migración

Citrix recomienda las siguientes herramientas para los casos descritos.

Backup

Entorno	Caso de uso	Herramienta recomendada	Consideraciones especiales	Enlace
DaaS	Copias de seguridad programadas y bajo demanda	Copia de seguridad + Restauración	Citrix conserva la copia de seguridad y el usuario puede descargarla si fuera necesario	Copia de seguridad y restauración en Studio
Local	Copias de seguridad bajo demanda	ACT	El usuario conserva la copia de seguridad	Copia de seguridad y restauración mediante la herramienta de configuración automatizada

Migración

Entorno	Caso de uso	Herramienta recomendada	Consideraciones especiales	Enlace
De local a la nube	Migrar un sitio local a DaaS	ACT		Migrar la configuración local a la nube
	Consolidar varios sitios locales en un sitio de DaaS	ACT	Fusión de sitios	Combinar varios sitios locales en un único sitio en la nube
De local a local	Migrar un sitio local a otro sitio local	ACT		Guía POC: herramienta de configuración automatizada para migrar un sitio local a otro sitio local

Entorno	Caso de uso	Herramienta recomendada	Consideraciones especiales	Enlace
	Consolide varios sitios locales en otro sitio local	ACT	Fusión de sitios	Guía POC: herramienta de configuración automatizada para migrar un sitio local a otro sitio local Combinar varios sitios locales en un único sitio en la nube
De una nube a otra nube	Migrar un sitio de DaaS a otro sitio de DaaS	ACT		Migrar de una nube a otra nube
Consolida varios sitios de DaaS en un solo sitio de DaaS	ACT	Fusión de sitios		Migrar de una nube a otra nube Migrar varios sitios locales a un solo sitio en la nube

Protección

August 17, 2024

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/.

Autenticación FIDO2 y WebAuthn

August 17, 2024

Autorización local y autenticación virtual mediante FIDO2 y WebAuthn

Los usuarios pueden autenticarse en aplicaciones que usen FIDO2 o WebAuthn en su sesión virtual mediante claves de seguridad de FIDO2 y dispositivos biométricos integrados con TPM 2.0 y Windows Hello.

Para obtener más información acerca de FIDO2, consulte FIDO2: WebAuthn & CTAP.

Para obtener información sobre el uso de esta función, consulte Redirección FIDO2.

> **NOTA**
>
> Tenga en cuenta que esta función no admite el inicio de sesión virtual mediante WebAuthn o FIDO2. Esta función solo permite usar estos métodos de autenticación en aplicaciones dentro de la sesión virtual.
>
> Esta función no está disponible en casos de doble salto.

Tabla de compatibilidad

Sistema operativo del host de la sesión	Autenticación de aplicaciones web	Autenticación de aplicaciones UWP
Windows Server 2016	Compatible mediante la redirección de USB	No compatible
Windows Server 2019	Compatible	No compatible
Windows Server 2022	Compatible	Compatible
Windows 10	Compatible	Compatible
Windows 11	Compatible	Compatible

Para obtener información adicional, consulta los requisitos que aparecen a continuación.

Autenticación de aplicaciones web

Requisitos

Estos son los requisitos para usar la autenticación FIDO2 y WebAuthn con aplicaciones web:

Plano de control de Citrix

- Citrix Virtual Apps and Desktops 2009 o una versión posterior

Host de la sesión

- Sistema operativo
  - Windows 10 1809 o una versión posterior
  - Windows Server 2019 o una versión posterior
- VDA
  - Windows: Versión 2009 o una versión posterior

Dispositivo cliente

- Sistema operativo
  - Windows 10 1809 o una versión posterior
  - Linux: Consulte los requisitos del sistema de la aplicación Workspace para Linux.
- Aplicación Workspace
  - Windows: Versión 2009.1 o una posterior
  - Linux: 2303 o una versión posterior

Requisitos del explorador web

- Solo exploradores web de 64 bits

Métodos de autenticación admitidos

- Clave de seguridad FIDO2
- Windows Hello
  - TPM 2.0
  - Biometría integrada
    - Reconocimiento facial

        - Escáner de huellas dactilares
    - WebAuthn

Autenticación de aplicaciones UWP

Con la publicación de Citrix Virtual Apps and Desktops 2112, Citrix permite la autenticación WebAuthn y FIDO2 en aplicaciones UWP.

Las aplicaciones como Microsoft Teams, Microsoft Outlook para Office 365 y OneDrive usan una aplicación UWP para la autenticación como enlace a Azure Active Directory. Citrix ahora admite el uso de FIDO2 para autenticar esas aplicaciones.

Requisitos

Estos son los requisitos para usar la autenticación FIDO2 y WebAuthn con aplicaciones UWP:

Plano de control de Citrix

- Citrix Virtual Apps and Desktops 2112 o una versión posterior

Host de la sesión

- Sistema operativo
    - Windows 10 1809 o una versión posterior
    - Windows Server 2022 o una versión posterior
- VDA
    - Windows: Versión 2112 o una versión posterior

Dispositivo cliente

- Sistema operativo
    - Windows 10 1809 o una versión posterior
    - Linux: Consulte los requisitos del sistema de la aplicación Workspace para Linux.
- Aplicación Workspace
    - Windows: Versión 2009.1 o una posterior
    - Linux: 2303 o una versión posterior

Métodos de autenticación admitidos

- Clave de seguridad FIDO2
- Windows Hello
  - TPM 2.0
  - Biometría integrada
    - Reconocimiento facial
    - Escáner de huellas dactilares
  - WebAuthn

> **Nota:**
>
> En casos en que la redirección FIDO2 no está disponible porque la función no es compatible con el cliente, el VDA o el sistema operativo, las claves FIDO2 basadas en USB se pueden redirigir mediante la redirección de USB.
> También es posible utilizar la redirección de USB para redirigir las claves FIDO2 basadas en USB en casos en que la redirección de FIDO2 esté disponible. En este caso concreto, debe inhabilitar la redirección de FIDO2 y configurar las reglas de redirección de USB adecuadas.
> Consulte la documentación sobre Reglas de los dispositivos de redirección de USB para obtener detalles sobre cómo configurar claves FIDO2 usando reglas de redirección de USB.

Configuración avanzada para aplicaciones basadas en msedgewebview2.exe

> **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 usa el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Para las empresas que tienen aplicaciones web basadas en msedgewebview2.exe, es necesario agregar valores de registro adicionales en el VDA para que la redirección de FIDO2 funcione dentro de las sesiones de HDX -

Agregue la ruta completa del archivo msedgewebview2.exe en el valor de registro AllowedProcesses:

- Clave: HKLM\SOFTWARE\Citrix\WebAuthnAllowedProcesses
- Nombre del valor: AllowedProcesses
- Tipo de valor: REG_MULTISZ
- Información del valor: <add full path of the msedgewebview2.exe here >

Para las aplicaciones de 64 bits, es necesario establecer los siguientes valores:

- Clave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook\msedgewebvi
- Clave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- Nombre del valor: FilePathName
- Tipo de valor: REG_SZ
- Datos de valor: C:\Program Files\Citrix\HDX\bin\CtxWebAuthnHook.dll
- Clave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHook
- Nombre del valor: Indicador
- Tipo de valor: DWORD
- Datos de valor: 00000002

Para aplicaciones de 32 bits, es necesario establecer los siguientes valores:

- Clave: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHoc
- Clave: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHoc
- Nombre del valor: FilePathName
- Tipo de valor: REG_SZ
- Datos de valor: C:\Program Files\Citrix\HDX\bin\CtxWebAuthnHook.dll
- Clave: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\CtxHook\AppInit_DLLs\CtxWebAuthnHoc
- Nombre del valor: Indicador
- Tipo de valor: DWORD
- Datos de valor: 00000002

Reinicie el VDA después de configurar los valores de Registro para que la redirección de FIDO2 se habilite para las aplicaciones basadas en msedgewebview2.exe.

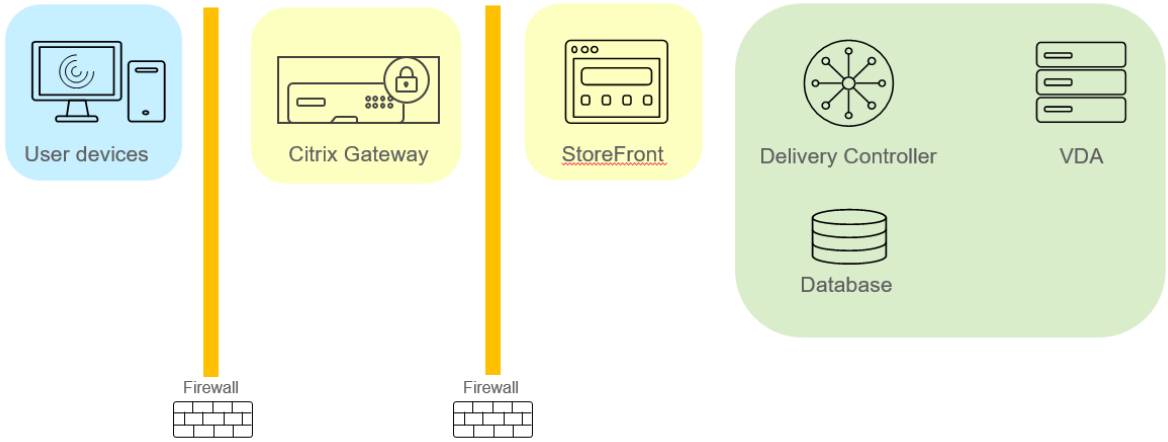
Integrar Citrix Virtual Apps and Desktops con Citrix Gateway

August 17, 2024

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.

Recomendaciones y consideraciones de seguridad

August 17, 2024

> **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 Provisioning 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 Controllers 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 actualmente. Si se ha habilitado, inhabilítelo.

- 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 Config Synchronizer Service necesita que la cuenta NETWORK SERVICE pertenezca al grupo de administradores locales del Delivery Controller. Esto permite que la caché de host local funcione correctamente.

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 suminis-

trar 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 usa 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:

```
HKEY\_LOCAL\_MACHINE\Software\Citrix|DesktopServer
Name: AllowMultipleRemotePCAssignments
Type: REG_DWORD
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 sea 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 este parámetro solo cuando haya protegido las comunicaciones entre los Delivery Controllers y StoreFront mediante claves de seguridad u otro mecanismo, como firewalls o IPsec.

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 -TrustRequestsSentToTheXmlServ $true`.
- Para inhabilitar la confianza en XML, ejecute `Set-BrokerSite -TrustRequestsSentToTheXmlSer $false`.

Tarjetas inteligentes

August 17, 2024

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. Es posible que la inscripción con tarjeta inteligente funcione cuando la tarjeta inteligente rápida está inhabilitada, 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 podrían 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, es posible 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. Es posible que el controlador del dispositivo también se describa como un minicontrolador, 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. Cuando la latencia es alta, la mejora del rendimiento puede ser significativa (por ejemplo, 15 segundos para un inicio de sesión rápido en Windows con tarjeta inteligente en lugar de más de 1 minuto con la redirección de tarjeta inteligente basada en PC/SC).

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:

```
HKLM\SOFTWARE\Citrix\SmartCard
CryptographicRedirectionDisable (DWORD)
```

En el lado del cliente, para habilitar la tarjeta inteligente rápida, incluya el parámetro ICA SmartCardCryptographicRedirection en el archivo *default.ica* del sitio de StoreFront asociado:

```
[WFClient]
SmartCardCryptographicRedirection=On
```

Además, en el lado del cliente, se puede forzar la activación o la desactivación de la tarjeta inteligente rápida (por ejemplo, para fines de diagnóstico) con estos parámetros del Registro:

- HKLM\SOFTWARE[\WOW6432Node]\Citrix\ICA Client\SmartCard\ForceEnableCryptographicRedirection (como un valor DWORD que no sea cero)

O bien,

- HKLM\SOFTWARE[\WOW6432Node]\Citrix\ICA Client\SmartCard\ForceDisableCryptographicRedirection (como un valor DWORD que no sea cero)

El subárbol del Registro de 32 bits debe especificarse (mediante `WOW6432Node`) si la máquina cliente es de 64 bits.

Limitaciones:

- Solo la aplicación Citrix Workspace para Windows admite tarjetas inteligentes rápidas. Si configura tarjetas inteligentes rápidas en el archivo default.ica, las aplicaciones Citrix Workspace 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.

A partir de la versión 2203 de VDA y de la versión 2202 de la aplicación Citrix Workspace para Windows, la tarjeta inteligente rápida es compatible con Cryptography Next Generation (CNG). Además, las tarjetas inteligentes de criptografía de curva elíptica (Elliptic Curve Cryptography o ECC) son compatibles con estas curvas: P-256, P-384, P-521 bits, tanto para ECDSA como para ECDH.

A partir de la versión 2203 de VDA, la tarjeta inteligente rápida permite almacenar en la caché el PIN de la tarjeta inteligente entre las aplicaciones de la misma sesión de inicio del usuario. Por ejemplo: si el **almacenamiento en caché de PIN de sesión** está habilitado y el usuario final ha proporcionado previamente el PIN de la tarjeta inteligente a Outlook, cuando se usa Word para firmar un documento, Word usa el PIN de la tarjeta inteligente ya almacenado en la caché (enviado a Outlook). El **almacenamiento en caché de PIN de sesión** mejora la experiencia de usuario porque reduce las veces que el usuario tiene que introducir el PIN de su tarjeta inteligente. Además, si quiere, si la tarjeta inteligente se usa para iniciar sesión en el VDA, el PIN de inicio de sesión de la tarjeta inteligente de Windows se puede guardar en la **caché de PIN de sesión**. Esto puede mejorar aún más la experiencia de usuario.

El **almacenamiento en caché de PIN de sesión** está inhabilitado de forma predeterminada Se puede habilitar y controlar con estos parámetros del Registro en el VDA:

En HKLM\SOFTWARE\Citrix\SmartCard:

- `EnablePinSessionCache` como DWORD (valor que no sea cero para habilitarlo)
- `EnableLogonPinSessionCache` como DWORD (valor que no sea cero para habilitarlo)
- `PinSessionCacheEntryStaleTimeout` como DWORD (segundos antes de que una entrada se vuelva obsoleta; el valor predeterminado es 1 hora)

Tipos de lectores de tarjetas inteligentes

Es posible integrar el lector de tarjetas inteligentes en el dispositivo del usuario, o bien conectarse 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 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. Es posible que los lectores de tarjetas inteligentes de clase 2 estén integrados en un teclado que contenga a su vez un teclado numérico seguro. Para lectores de tarjetas inteligentes de clase 2, contacte con su representante de Citrix. Es posible que se necesite 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 se incluyen 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 predeterminada.

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 otras solicitudes 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 se descargan 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 usan 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).

Seguimiento del recuento de inserciones del lector de tarjetas inteligentes

Con la función de control remoto de tarjetas inteligentes, puede hacer un seguimiento del número de veces que se ha insertado o retirado una tarjeta inteligente de un lector mediante la función SCardGetStatusChange. La función actualiza una matriz de estructuras de datos SCARD_READERSTATE, una por cada lector que supervise. El byte alto (16 bits) del campo dwEventState de cada SCARD_READERSTATE contiene el recuento del lector. Para obtener más información, consulte los artículos de Microsoft SCardGetStatusChangeA function y SCARD_READERSTATEA structure.

El parámetro para **notificación del recuento de inserciones del lector** está inhabilitado de forma predeterminada. Para habilitarlo, agregue la siguiente clave del Registro:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard

Nombre: EnableReaderInsertCountReporting

Tipo: DWORD

Valor: Un valor distinto de cero

Cuando la sesión se desconecta, el recuento se vuelve a poner a cero.

La **notificación del recuento de inserciones del lector** es compatible con middleware de tarjetas inteligentes de terceros.

Implementaciones de tarjeta inteligente

August 17, 2024

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 dispos-

itivos 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 autentiquen 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.

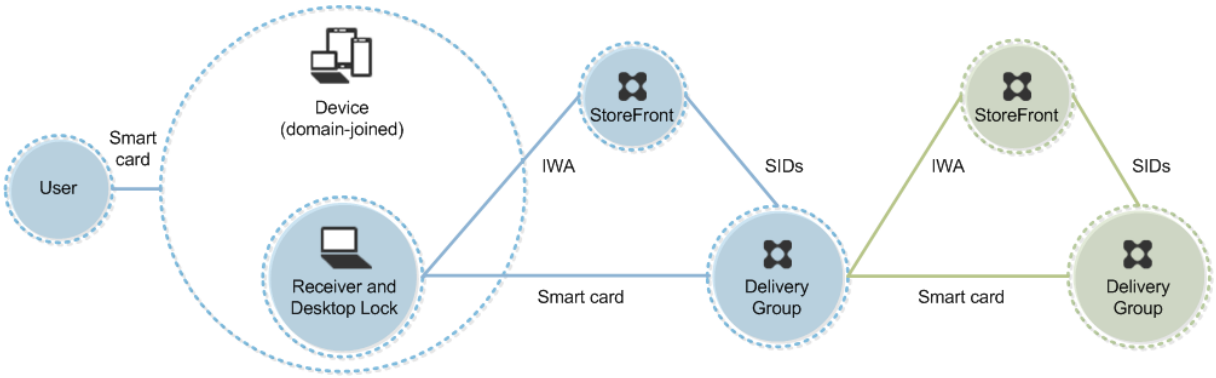
Configuración de directiva	Comportamiento del escritorio
Ninguna acción	Ninguna acción.
Bloquear estación de trabajo	La sesión de escritorio se desconecta y el escritorio virtual queda bloqueado.
Forzar cierre de sesión	El usuario se ve forzado a cerrar la sesión. Si se pierde la conexión de red y esta 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.

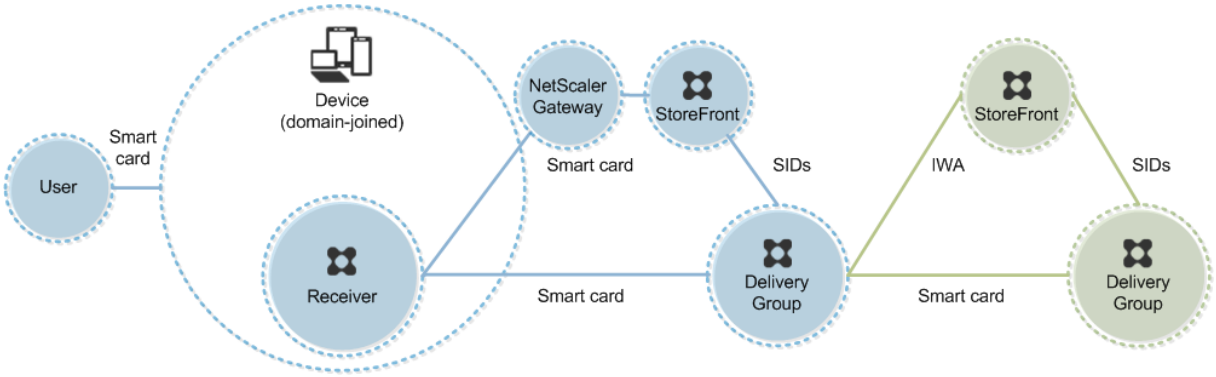


El usuario inicia sesión en un dispositivo mediante una tarjeta inteligente y un PIN. Receiver autentica al usuario en un servidor de StoreFront mediante la autenticación integrada de Windows (IWA). StoreFront pasa los identificadores de seguridad del usuario (SID) a Citrix Virtual Apps o Citrix Virtual 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.



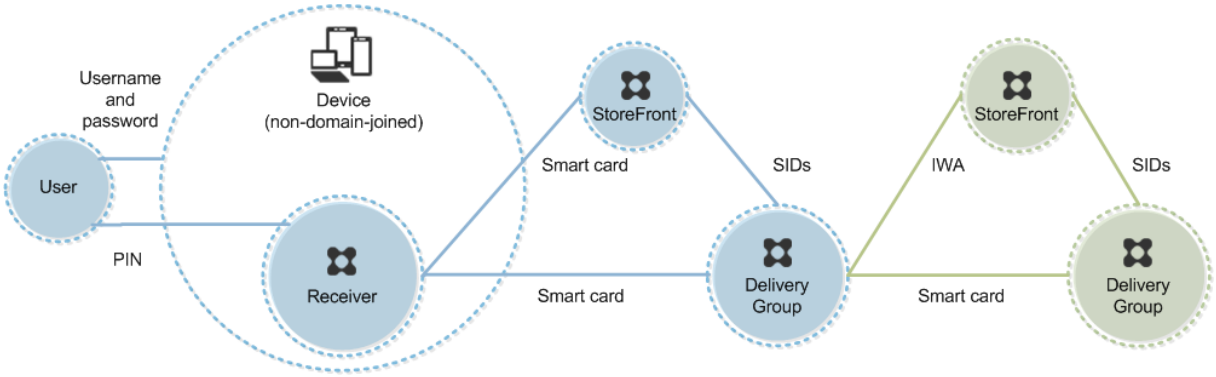
El usuario inicia sesión en un dispositivo con una tarjeta inteligente y un PIN. A continuación, inicia otra sesión en Citrix Gateway o Access Gateway. Este segundo inicio de sesión puede realizarse con la tarjeta inteligente y el PIN, o con un nombre de usuario y una contraseña, porque Receiver permite 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

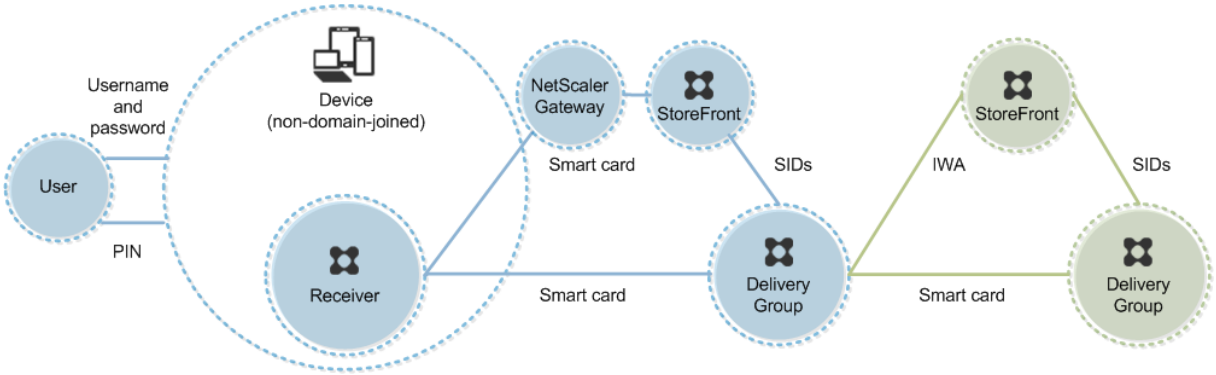
sesión son optativas. Como la autenticación bimodal es posible en esta implementación, Receiver pide al usuario una tarjeta inteligente y un PIN, o un nombre de usuario y una contraseña. A continuación, Receiver se autentica en StoreFront.

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.

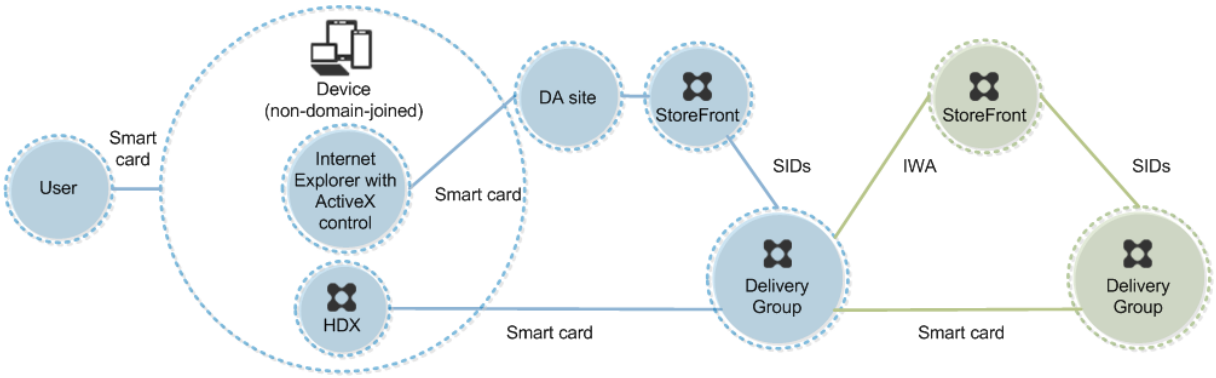
Esta implementación se puede ampliar a una configuración de doble salto con la incorporación de un segundo servidor de StoreFront y un servidor que aloja aplicaciones. Un Receiver desde el escritorio virtual se autentica en el segundo servidor de StoreFront. Con esta segunda conexión se puede usar

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.



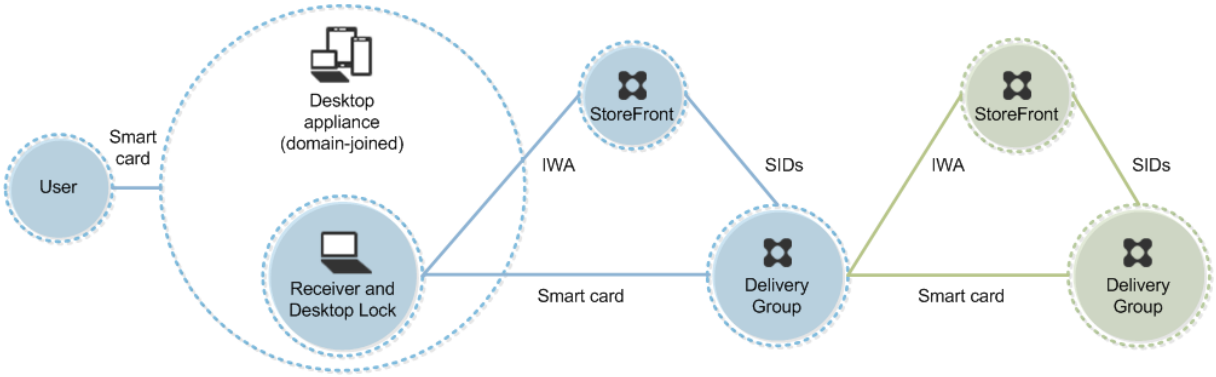
El usuario inicia una sesión en un dispositivo mediante una tarjeta inteligente. Si Desktop Lock se está ejecutando en el dispositivo, el dispositivo está configurado para iniciar el sitio de Desktop Appliance a través de Internet Explorer ejecutado en modo quiosco (pantalla completa). Un control ActiveX 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

August 17, 2024

Autenticación 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 Professional.

La autenticación PassThrough con tarjeta inteligente en aplicaciones alojadas se admite en servidores que ejecutan 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: Desactive DisableCtrlAltDel
- Implementaciones de tarjetas inteligentes unidas a dominio, desde NetScaler a StoreFront: Active UseLocalUserAndPassword

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)

August 17, 2024

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 usa 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.

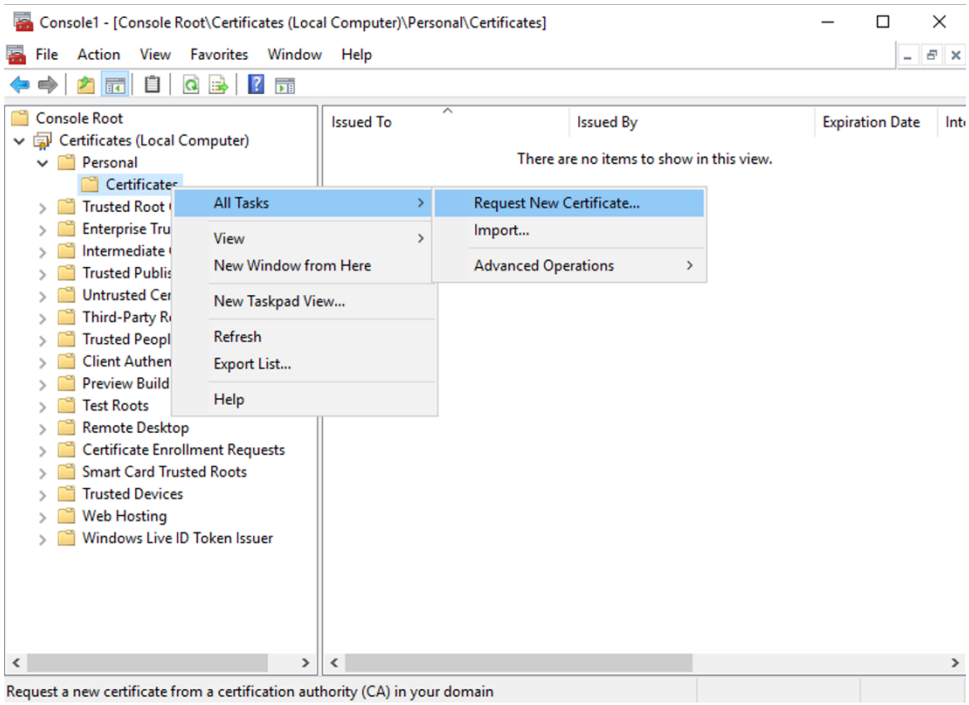
Aunque hay varios tipos diferentes de entidades de certificación y métodos para solicitar certificados de ellas, en este artículo se describe la entidad emisora de certificados de Microsoft. La entidad de

certificación de Microsoft debe tener una plantilla de certificado publicada con el propósito Autenticación de servidor.

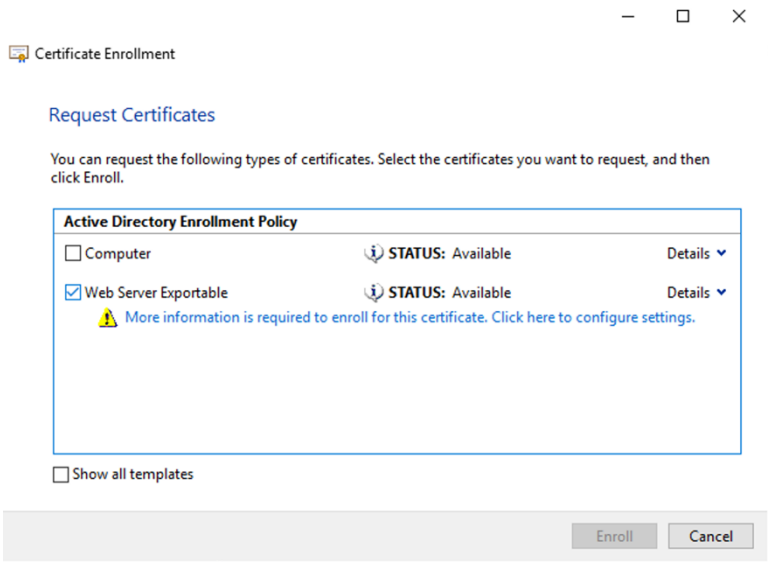
Si la entidad de certificación de Microsoft está integrada en un dominio de Active Directory o en el bosque de confianza al que están unidos los Delivery Controllers, se puede adquirir un certificado desde el asistente para inscripción de certificados del complemento MMC Certificados.

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**.



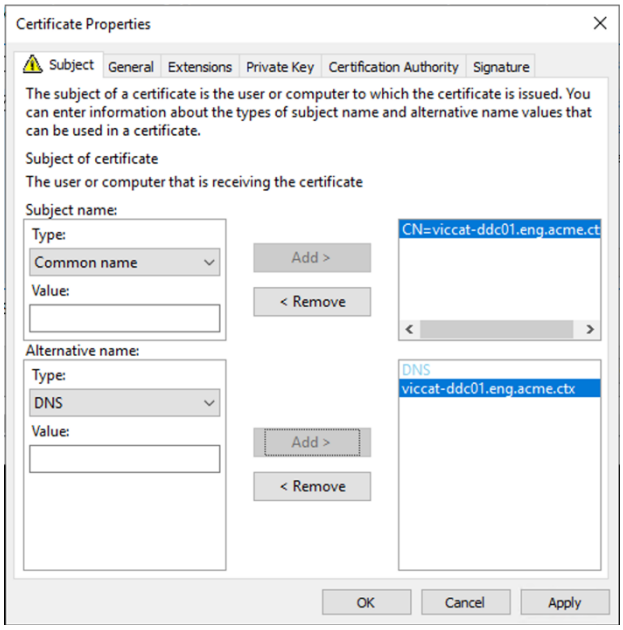
3. Haga clic en **Siguiente** para comenzar y en **Siguiente** para confirmar que va a adquirir el certificado de inscripción en Active Directory.
4. Seleccione la plantilla para Certificado de autenticación de servidor. Si la plantilla se ha configurado para proporcionar automáticamente los valores 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:


```
New-PSDrive -Name HKCR -PSProvider Registry -Root
    HKEY_CLASSES_ROOT

$Service_Guid = Get-ChildItem HKCR:\Installer\Products -Recurse -
    Ea 0 | Where-Object {
  $key = $_; $_.GetValueNames() | ForEach-Object {
  $key.GetValue($_)  }
  | Where-Object {
  $_ -like 'Citrix Broker Service'  }
   }
  | Select-Object Name

$Service_Guid.Name -match "[A-Z0-9]*$"

$Guid = $Matches[0]

[GUID]$Formatted_Guid = $Guid

Remove-PSDrive -Name HKCR

Write-Host "Broker Service Application GUID: $($Formatted_Guid)" -
    ForegroundColor Yellow
```

3. Ejecute los siguientes comandos en la misma ventana de PowerShell para obtener la huella digital del certificado que instaló anteriormente:

```
$HostName = ([System.Net.Dns]::GetHostByName(($env:computerName)))
    .Hostname

$Thumbprint = (Get-ChildItem -Path Cert:\LocalMachine\My | Where-
    Object {
 $_.Subject -match ("CN=" + $HostName) }
 ).Thumbprint -join ';'

Write-Host -Object "Certificate Thumbprint for $($HostName): $(
    $Thumbprint)" -Foreground Yellow
```

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:

```
$IPV4_Address = Test-Connection -ComputerName $HostName -Count 1
    | Select-Object -ExpandProperty IPV4Address

$IPPort = "$($IPV4_Address):443"

$SSLxml = "http add sslcert ipport=$IPPort certhash=$Thumbprint
    appid={
 $Formatted_Guid }
 "

$SSLxml | netsh

```



```
. netsh http show sslcert
```

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.

La lista ordenada de los conjuntos de cifrado debe incluir el conjunto de cifrado `TLS_ECDHE_RSA_WITH_AES_25` o `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` (o ambos), 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.

`TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` o `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` deben preceder a cualquier conjunto 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 \<http-port> -WISSLPORT \<https-port>
```

donde <http-port> es el número de puerto para el tráfico HTTP y <https-port> 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:

```
Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding
    XML_HTTPS |
Unregister-ConfigRegisteredServiceInstance
Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |
Register-ConfigServiceInstance
```

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, TLS 1.2 y TLS 1.3. 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 1.3. Si elige SSL 3.0 como la versión mínima, se permitirán conexiones con todas las versiones admitidas. Si especifica TLS 1.3 como la versión mínima, solo se permiten conexiones con TLS 1.3.

DTLS 1.0 corresponde a TLS 1.1, mientras que DTLS 1.3 corresponde a TLS 1.3.

- **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:

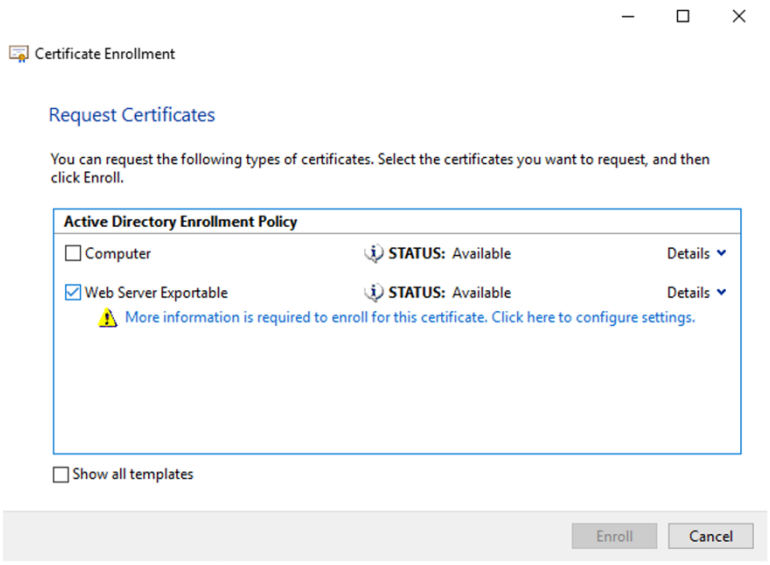
Conjunto de cifrado TLS/DTLS	**ALL**	**COM**	**GOV**	**ALL**	**COM**	**GOV**
Modo FIPS	No	No	No	Sí	Sí	Sí
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	X		X	X		X
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	X		X	X		X
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	X			X	X	

> **Nota:**
>
> El VDA no admite los 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 y TLS_DHE_RSA_WITH_AES_128_CBC_SHA). Si Windows los selecciona, Receiver no podrá utilizarlos.
>
> 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

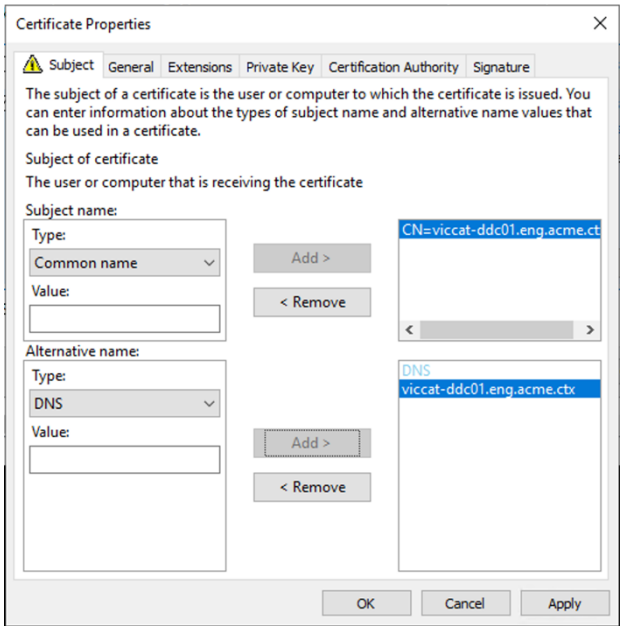
1. En el VDA, abra la consola de MMC y agregue el complemento Certificados. Cuando se le solicite, seleccione Cuenta de equipo.
2. Expanda **Personal > Certificados** y, a continuación, utilice el comando de menú contextual **Todas las tareas > Solicitar un nuevo certificado**.
3. Haga clic en **Siguiente** 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

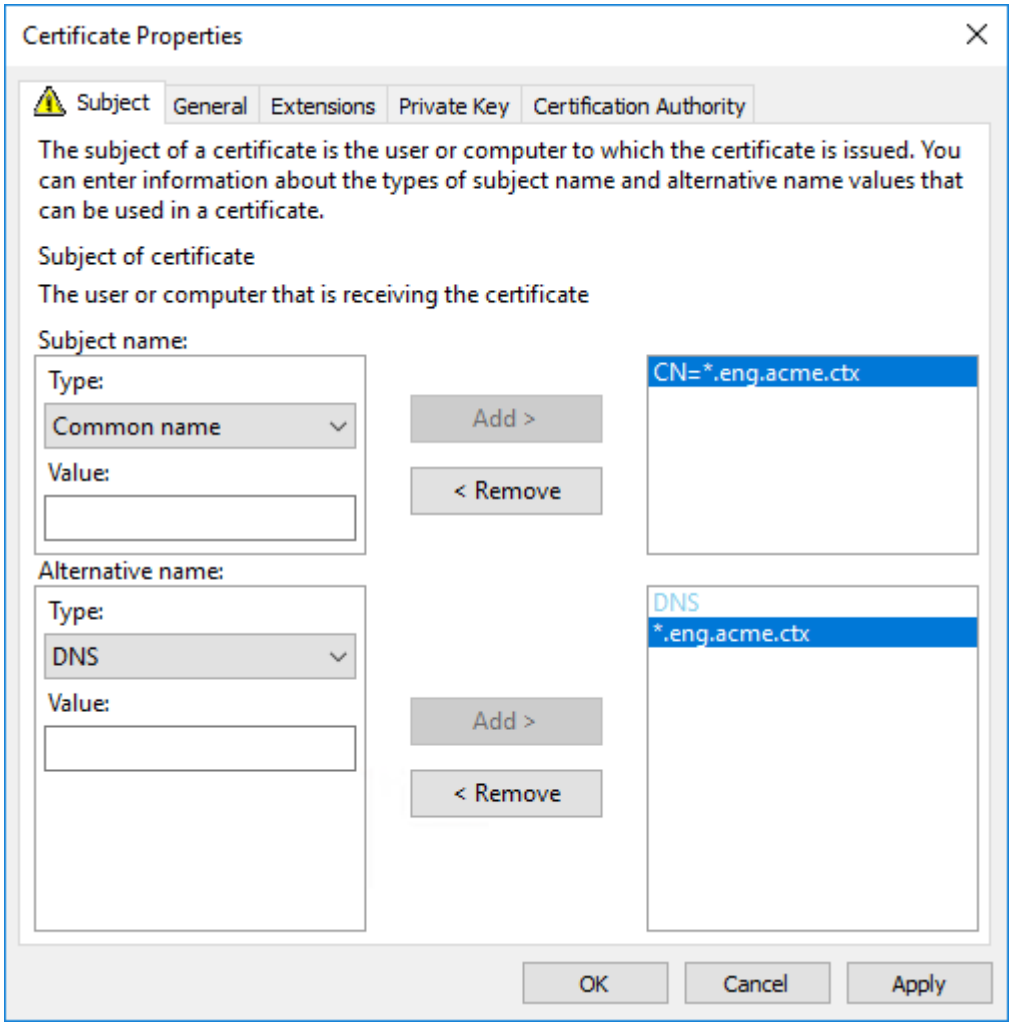


> **Nota:**
>
> Use la función de inscripción automática de certificados de Servicios de certificados de Active Directory para automatizar la emisión y la implementación de certificados en los VDA. Esto se describe en https://support.citrix.com/article/CTX205473.

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

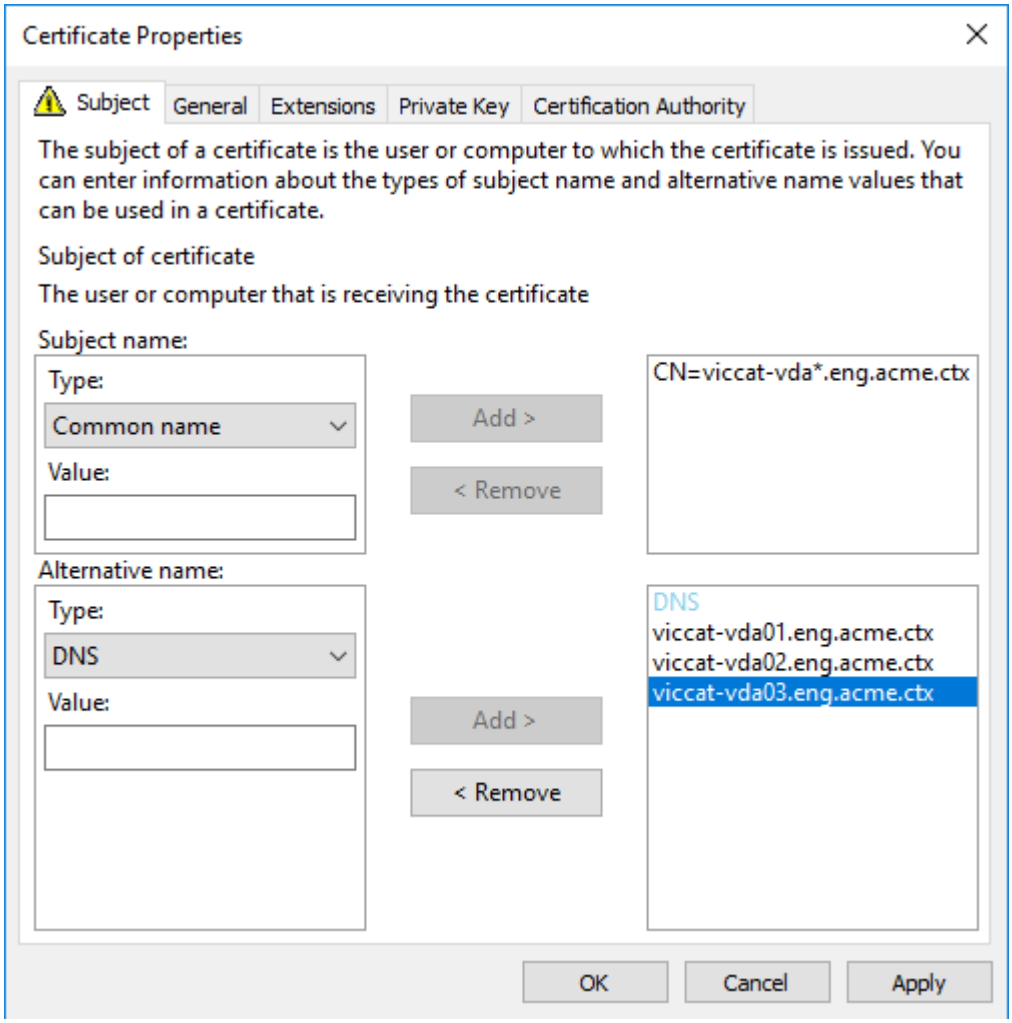
Nombre alternativo: Seleccione el tipo **DNS** y agregue el dominio *.primary.domain de los VDA



Puede usar certificados SAN para permitir que un solo certificado cubra diversos VDA específicos:

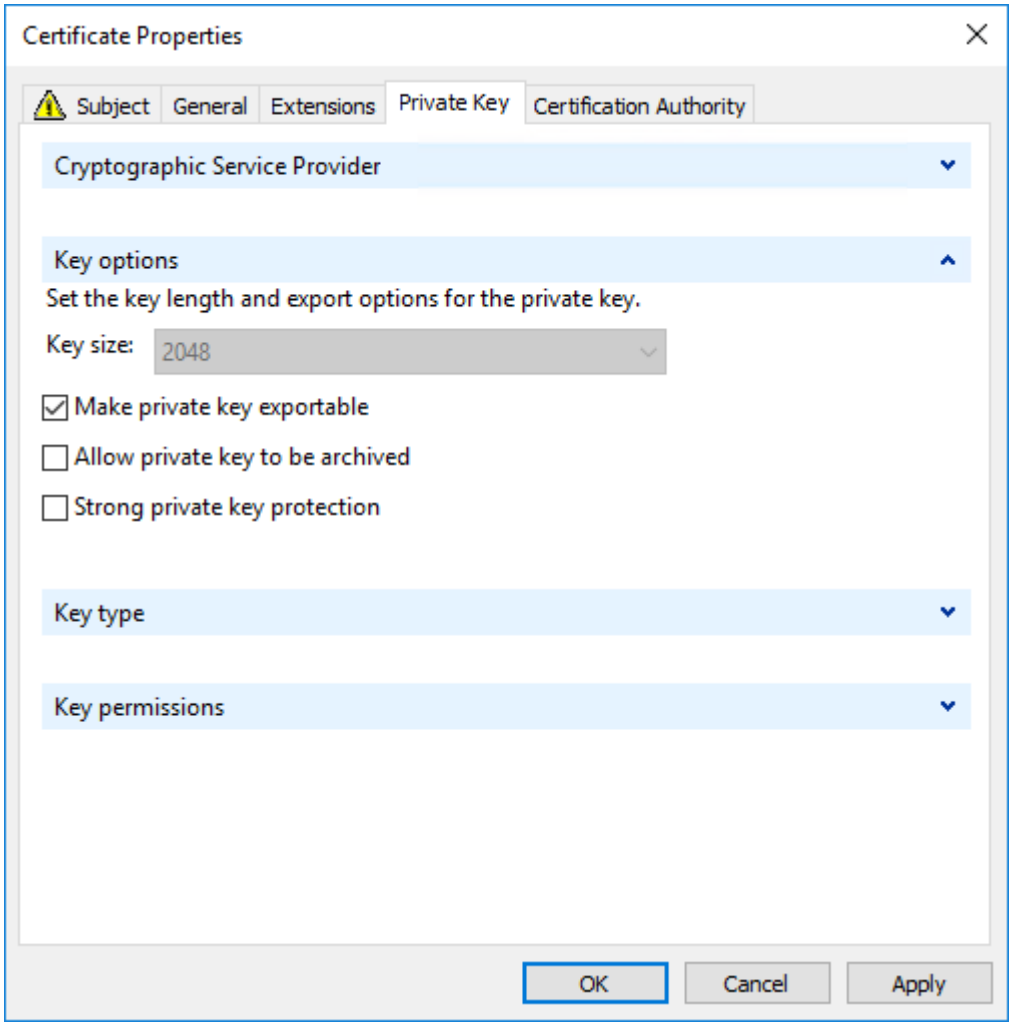
Nombre del sujeto: Seleccione el tipo **Nombre común** e introduzca una cadena que ayude a identificar el uso del certificado

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 Framehawk.

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_1.3”.
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.

```
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.

```
Enable-VdaSSL -Enable
-CertificateThumbPrint "12345678987654321"
-SSLPort 400 -SSLMinVersion "TLS_1.3"
-SSLCipherSuite "All"
```

El siguiente script inhabilita la escucha de TLS en el VDA.

```
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 1.3. 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:**
>
> Es necesario un paso adicional si el VDA está en Windows 10 Anniversary Edition o en una versión posterior compatible. Esto afecta a las conexiones desde Citrix Receiver para Windows (desde la versión 4.6 hasta la versión 4.9), 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. Eso afecta a todas las versiones de Citrix Receiver.

En el VDA (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:

```
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:**
>
> 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.

Se necesita una configuración adicional si:

- la versión de Citrix Receiver admite el transporte adaptable HDX y DTLS: Receiver para Windows (4.7, 4.8, 4.9), Receiver para Mac (12.5, 12.6, 12.7), Receiver para iOS (7.2, 7.3.x) o Receiver para Linux (13.7)

y también se da una de estas condiciones:

- 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 que fallen las conexiones desde Citrix Receiver, realice una de estas acciones:

- actualice Citrix Receiver a: Receiver para Windows 4.10 o una versión posterior, Receiver para Mac 12.8 o una versión posterior o Receiver para iOS 7.5 o una versión posterior;
- 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:**
>
> La actualización correspondiente de Receiver para Linux aún no está disponible. Receiver para Android (versión 3.12.3) no admite el transporte adaptable HDX ni DTLS a través de Citrix Gateway y, por lo tanto, no se ve afectado.
>
> 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

August 17, 2024

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 usa el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

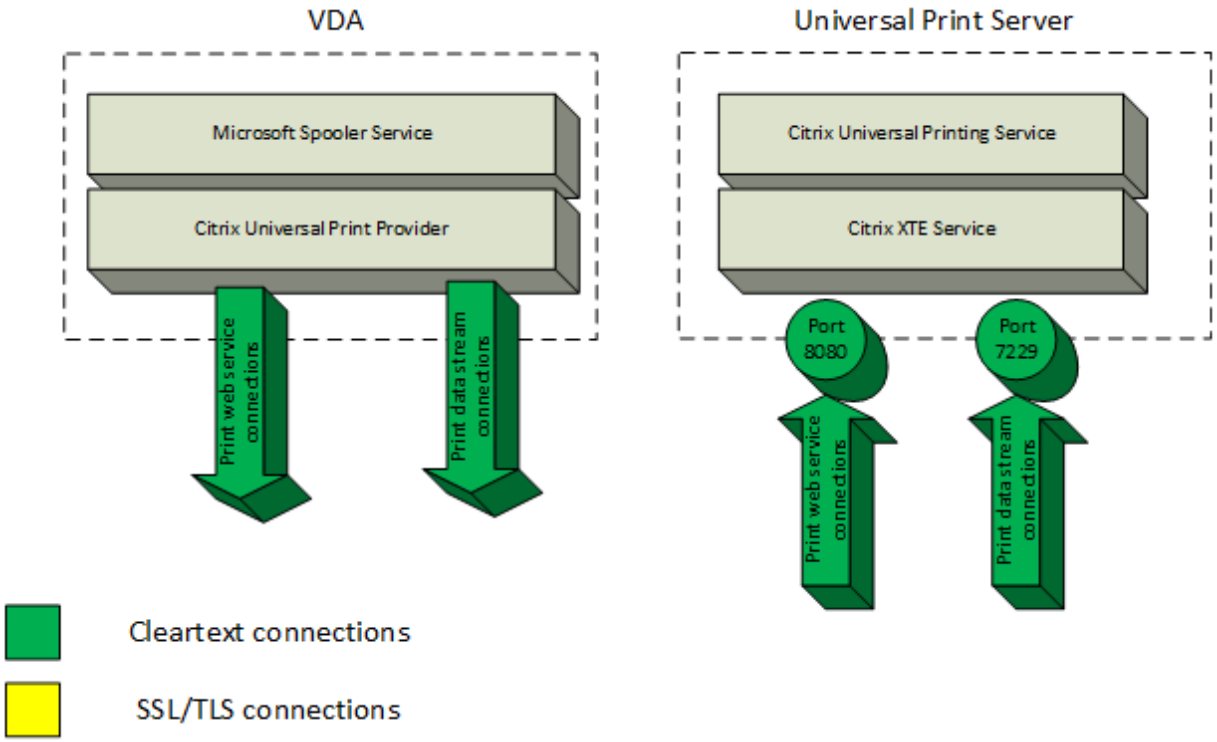
Tipos de conexiones de impresión entre el VDA y el Universal Print Server

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)

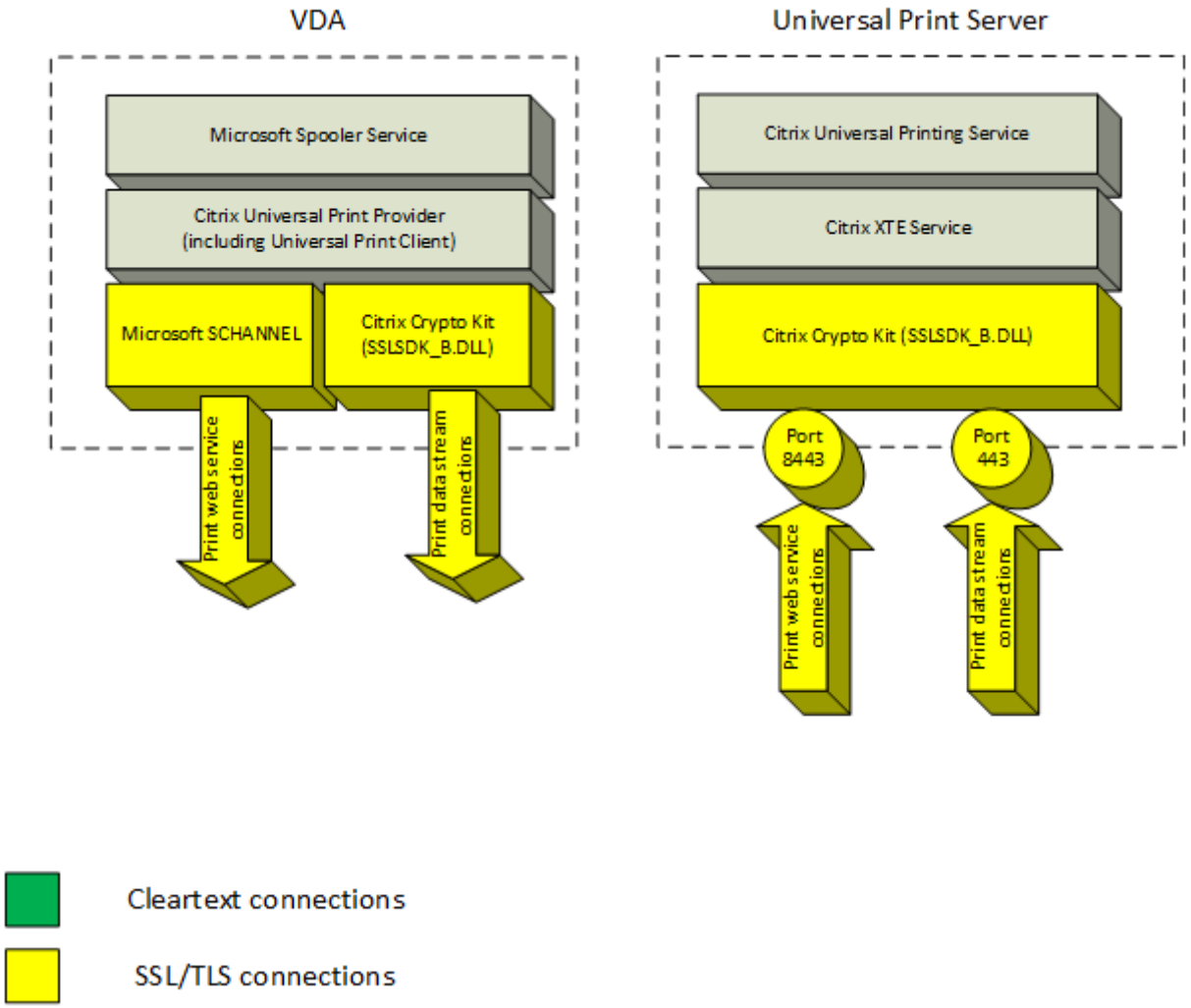
En el artículo Introducción a los servicios y requisitos de puerto de red para Windows de asistencia de Microsoft, se describen los puertos que utiliza el administrador de trabajos de impresión de Microsoft Windows, el servicio Print Spooler. La configuración de SSL/TLS de este documento no se aplica 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, vaya a **Configuración del equipo > Plantillas administrativas > Red > Opciones de configuración SSL > Orden de conjuntos de cifrado SSL**. Seleccione el siguiente orden cuando TLS 1.3 esté configurado:

TLS_AES_256_GCM_SHA384
TLS_AES_128_GCM_SHA256

Seleccione el siguiente orden cuando TLS 1.2 esté configurado:

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 EnableUpsSsl.ps1.

- Qué versiones del protocolo TLS se deben permitir.

Universal Print Server presenta compatibilidad con las versiones de protocolo TLS 1.3 y 1.2. Especifique la versión mínima permitida.

La versión predeterminada del protocolo TLS es 1.2.

> **Nota:**
>
> La versión 2311 de Citrix Virtual Apps and Desktops ya no es compatible con TLS 1.1 ni 1.0.

- 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		X
TLS_ECDHE_RSA_AES256_CBC_SHA384	X		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

```
Enable-UpsSSL.ps1 -Enable [-HTTPPort <port>] [-CGPPort <port>] [-
    HTTPSPort <port>] [-CGPSSLPort <port>] [-SSLMinVersion <version>] [-
    SSLCipherSuite <name>] [-CertificateThumbprint <thumbprint>] [-
    FIPSMode <Boolean>] [-ComplianceMode <mode>]
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
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_1.2”y “TLS_1.3”. Predeterminado: TLS_1.2.

Parámetro	Descripción
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 Web 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 Web Studio, **inhabilite** la configuración de directiva **Modo FIPS de SSL** de Citrix. 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.

> **Nota:**
>
> El modo FIPS no es compatible cuando la versión del protocolo SSL está configurada en TLS 1.3.

Configurar la versión del protocolo SSL/TLS

La versión predeterminada del protocolo SSL/TLS es TLS 1.2. TLS 1.2 y TLS 1.3 son las versiones de protocolo SSL/TLS recomendadas para 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 o TLS 1.3 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 en el cliente **TLS 1.2 o TLS 1.3** mediante los parámetros de 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 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.

Lista de canales virtuales permitidos

August 17, 2024

La lista de canales virtuales permitidos es una función que le permite controlar qué canales virtuales que no son de Citrix están permitidos en su entorno. De forma predeterminada, la funcionalidad de lista de canales virtuales permitidos está habilitada. Como resultado, solo se pueden abrir los canales virtuales de Citrix en las sesiones de Citrix 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.

Configuración

La lista de canales virtuales permitidos está habilitada de forma predeterminada. Puede configurar esta función mediante los siguientes parámetros de la directiva de Citrix:

- **Lista de canales virtuales permitidos**: Para habilitar o inhabilitar la función y agregar canales virtuales a la lista.
- **Limitación de los registros de la lista de canales virtuales permitidos**: Establece el período de limitación para el registro de eventos de la lista de canales virtuales permitidos.
- **Registros de la lista de canales virtuales permitidos**: Establece el nivel de registro de la lista de canales virtuales permitidos.

Agregar canales virtuales a la lista de permitidos

Para agregar un canal virtual a la lista de permitidos, necesita la siguiente información:

1. El nombre del canal virtual tal y como se define en el código, que puede tener hasta 7 caracteres. Por ejemplo, `CTXCVC1`.
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, puede agregarlos separando cada proceso con comas.

Para procesos individuales

Con los ejemplos anteriores, agregue la entrada siguiente a la lista:

```
CTXCVC1,C:\Program Files\Application\run.exe
```

Para varios procesos

Si hay varios procesos, agregue la entrada siguiente a la lista:

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application
\run2.exe
```

Uso de comodines

Se admite el uso de comodines (*). Puede usar caracteres comodín cuando los nombres de los directorios o ejecutables cambian en función de la versión de la aplicación o si el componente de terceros está instalado en los perfiles de los usuarios.

Puede usar caracteres comodín en los siguientes casos:

- Para reemplazar el nombre completo del directorio.
  Por ejemplo: `C:\Program Files\Application\*\run1.exe`
- Para reemplazar parte del nombre del directorio.
  Por ejemplo: `C:\Program Files\Application\v*\run1.exe`
- Para reemplazar el nombre del ejecutable.
  Por ejemplo: `C:\Program Files\Application\v1.2\*.exe`
- Para reemplazar parte del nombre del ejecutable.
  Por ejemplo: `C:\Program Files\Application\v1.2\run*.exe`

Se aplican las siguientes restricciones:

- El comodín solo se puede usar para reemplazar un único directorio. Por ejemplo: si el ejecutable se encuentra en `C:\Program Files\Application\v1.2\run1.exe`
  - Permitido: `C:\Program Files\Application\*\run1.exe`
  - No permitido: `C:\Program Files\*\run1.exe`
- Las entradas deben contener la extensión de archivo.
  - Permitido: `C:\Program Files\Application\v1.2\*.exe`
  - No permitido: `C:\Program Files\Application\v1.2\*`
- Todas las rutas deben ser locales.

> **Nota:**
>
> - No se permiten las rutas de red.
> - La compatibilidad con caracteres comodín está disponible a partir de Citrix Virtual Apps and Desktops 2206.
> - La compatibilidad con caracteres comodín está disponible en Citrix Virtual Apps and Desktops 2203 LTSR a partir de la CU2.

Uso de variables de entorno del sistema

Puede usar variables de entorno del sistema para simplificar la definición de los procesos de confianza en su lista de permitidos. Puede usar cualquiera de las variables listas para usar, como `%programfiles%`, `%programfiles(x86)%`, `%systemdrive%` y `%systemroot%`.

También puede usar variables de entorno personalizadas siempre que estén definidas a nivel del sistema.

En los siguientes ejemplos se muestran variables de entorno listas para usar:

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application\*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

En el siguiente ejemplo se muestra una variable de entorno del sistema personalizada:

- Nombre de variable personalizada: `app`
- Valor de variable personalizada: `%programfiles%\Application\`
- Entrada en la lista de permitidos: `CTXCVC1,%app%\run.exe`

> **Nota:**
>
> No se admiten variables de entorno de usuario.
>
> La compatibilidad con variables de entorno está disponible a partir de la versión 2209 de Citrix Virtual Apps and Desktops.

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 y el proceso que lo intentó abrir. Para obtener más información sobre los eventos disponibles, consulte Registros de eventos.
3. Cierre la sesión.
4. Agregue una entrada a la configuración de directiva Lista de canales virtuales permitidos para el canal virtual y el proceso identificados.
5. Reinicie la máquina.
6. Una vez registrado el VDA, ejecute la aplicación virtual o el escritorio virtual para comprobar que los canales virtuales personalizados se abren correctamente.

Consideraciones sobre canales virtuales Citrix

Todos los canales virtuales Citrix integrados son de confianza y se permite abrirlos sin ninguna configuración adicional. Sin embargo, las dos funcionalidades siguientes requieren entradas explícitas en la lista de permitidos debido a dependencias externas:

- Redirección multimedia
- HDX RealTime Optimization Pack para Skype for Business

Redirección multimedia

Si usa un reproductor multimedia distinto de Windows Media Player como reproductor multimedia del sistema, debe agregarlo a la lista de permitidos como proceso de confianza. 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:\Program Files (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 for Business

Esta información es necesaria para la entrada en la lista de permitidos:

- Nombre del canal virtual: `CTXRMEP`
- Proceso: Ruta al archivo ejecutable de Skype for Business en la máquina VDA, que puede variar según la versión de Skype for Business o si se ha usado una ruta de instalación personalizada.

Por ejemplo, `C:\Program Files\Microsoft Office\root\Office16\lync.exe`.

- Entrada en la lista de permitidos: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

Comunicación WebSocket entre el VDA y el Delivery Controller

August 17, 2024

En este artículo se describe cómo configurar una conexión WebSocket para la comunicación entre los VDA y los Delivery Controllers.

Información general

El protocolo WebSocket funciona a través del protocolo Citrix Brokering y facilita una comunicación estable entre los Delivery Controllers y los VDA.
El uso del protocolo WebSocket para la comunicación ofrece las siguientes ventajas:

- Solo requiere el puerto TLS 443 para la comunicación del VDA al Delivery Controller.
- Proporciona canales de comunicación fiables y sin interrupciones entre los VDA y los Delivery Controllers.

Funcionamiento

En la siguiente sección se describe el flujo de trabajo para la conexión WebSocket entre un Delivery Controller y un VDA:

1. Los administradores de Citrix Virtual Apps and Desktops inician el proceso aprovisionando los VDA mediante Machine Creation Services (MCS).
2. Durante el proceso de aprovisionamiento con MCS, MCS genera pares de claves públicas-privadas para cada VDA y registra las claves públicas en el servicio de confianza de FMA en el Delivery Controller. MCS guarda el par de claves pública-privada como un archivo en el disco de identidad de los VDA.
3. Cuando se inicia la máquina VDA, el agente de MCS instalado en la máquina VDA lee el par de claves del disco de identidad y escribe esta información en la ubicación del Registro del VDA.
4. El agente broker instalado en el VDA lee los pares de claves del registro y genera una solicitud WebSocket compatible con SSL dirigida al Delivery Controller con la clave de servicio firmada por la clave privada.

5. El Delivery Controller verifica el encabezado de autorización de la clave de servicio firmada con la clave pública del servicio de confianza de FMA.
6. Una vez finalizada la verificación, el sistema establece la conexión WebSocket entre el VDA y el Delivery Controller.

Compatibilidad con WebSocket para VDA unidos a AD

Antes de comenzar

1. Configure el sitio. Para obtener más información, consulte Crear un sitio.
2. Instale los certificados TLS en los Delivery Controllers. Para obtener más información, consulte Instalar certificados de servidor TLS en los Controllers.
3. Instale la CA raíz y la CA intermedia en el VDA para confiar en el Delivery Controller.

Procedimiento

Siga las instrucciones para configurar una conexión WebSocket:

1. Habilite la conexión WebSocket en el Delivery Controller. Ejecute el siguiente comando en cada Delivery Controller presente en su sitio:

   ```
   New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\WorkerProxy
   "-Name "WebSocket_Enabled"-PropertyType "DWord"-Value 1 -Force
   ```

   > **Nota:**
   >
   > Asegúrese de reiniciar los Delivery Controllers después de habilitar el WebSocket.

2. Cree un catálogo de máquinas para los VDA unidos a AD con aprovisionamiento de MCS. Para obtener más información, consulte Crear un catálogo de máquinas.
3. Cree un grupo de entrega y agréguele su VDA. Para obtener más información, consulte Crear grupos de entrega.
4. Habilite la conexión de WebSocket en el VDA. Ejecute el siguiente comando en el VDA:

   ```
   `New-ItemProperty "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
      Services\CitrixBrokerAgent\WebSocket" -Name "Enabled" -
      PropertyType "DWord" -Value 1 -Force`
   ```

   - Para comprobar si el VDA está conectado al servidor a través de WebSocket, compruebe el siguiente valor de clave de registro.

     Clave:


```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
   CitrixBrokerAgent\WebSocket
```

Nombre: Connected

Tipo: REG_DWORD

Valor: 1 o 0

1: VDA conectado al servidor mediante WebSocket.

0: el VDA no puede acceder al servidor a través de WebSocket o WebSocket no está habilitado.

- Para comprobar si WebSocket está habilitado, compruebe el siguiente valor de clave de Registro. El valor de `Enabled` debe ser 1.

  Clave:

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
     CitrixBrokerAgent\WebSocket
  ```

  Nombre: Enabled

  Tipo: REG_DWORD

  Valor: 1

Conectividad HDX

August 17, 2024

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.

En la oferta de HDX, puede conectarse a través de un protocolo de transporte exclusivo y patentado, utilizar el máximo de unidades de transmisión al establecer sesiones y optimizar la conectividad con Citrix SD-WAN.

Transporte adaptable

August 17, 2024

El transporte adaptable es un mecanismo de Citrix Virtual Apps and Desktops que permite establecer conexiones para las sesiones HDX mediante un protocolo de transporte preferido y, al mismo tiempo, proporciona una alternativa con TCP si la conectividad con el protocolo preferido no está disponible.

Se admiten los siguientes protocolos de transporte:

- Enlightened Data Transport (EDT)
- Protocolo de control de transferencias (TCP)

Configuración

El transporte adaptable está habilitado de forma predeterminada. Puede configurar el transporte adaptable para que funcione de los siguientes modos:

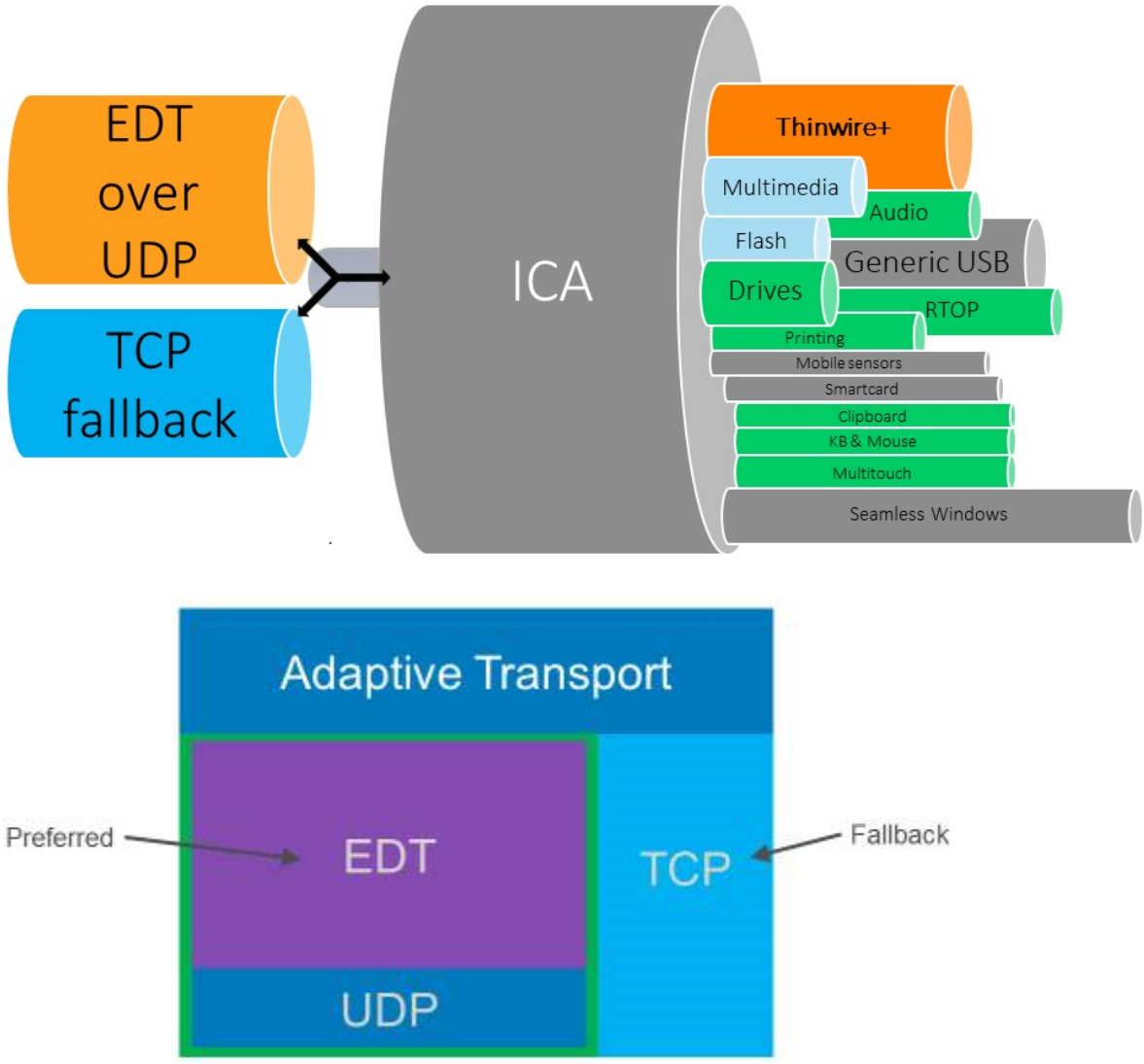
- **Preferido**: (Predeterminado) El cliente intenta conectarse con el protocolo preferido y recurre a TCP si la conectividad con el protocolo preferido no está disponible.
- **Modo de diagnóstico**: El cliente solo intenta conectarse mediante el protocolo preferido. Se inhabilita la posibilidad de recurrir a TCP.
- **Desactivado**: El cliente solo intenta conectarse mediante TCP.

Funcionamiento

Cuando el **transporte adaptable** está establecido en `Preferred`, el cliente intenta conectarse a la sesión con el protocolo preferido y TCP en paralelo. Esto permite optimizar el tiempo de conexión si no es posible conectarse con el protocolo preferido y el cliente debe recurrir a TCP. Si la conexión se establece mediante TCP, el cliente intenta conectarse con el protocolo preferido en segundo plano cada cinco minutos.

Cuando el **transporte adaptable** está establecido en `Diagnostic mode`, el cliente se conecta a la sesión solo con el protocolo preferido. Si el cliente no puede establecer una conexión mediante el protocolo preferido, no recurre al uso de TCP y la conexión falla.

Cuando el **transporte adaptable** está establecido en `Off`, el **transporte adaptable** está inhabilitado y el cliente se conecta a la sesión mediante TCP únicamente.



Requisitos del sistema

A continuación se detallan los requisitos para utilizar el transporte adaptable y EDT:

- Plano de control
  - Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service)
  - Citrix Virtual Apps and Desktops: Versión compatible actualmente
- Virtual Delivery Agent
  - Windows: Versión compatible actualmente (se recomienda 2402 o posterior)
  - Linux: Versión compatible actualmente (se recomienda 2402 o posterior)
- Aplicación Citrix Workspace

  - Windows: Versión compatible actualmente (se recomienda 2402 o posterior)
  - Linux: Versión compatible actualmente (se recomienda 2402 o posterior)
  - Mac: Versión compatible actualmente (se recomienda 2402 o posterior)
  - iOS: La versión más reciente disponible en el App Store de Apple
  - Android: La versión más reciente disponible en Google Play

- Citrix NetScaler Gateway
  - 14.1.12.30 o posterior (recomendado)
  - 13.1.17.42 o posterior (se recomienda 13.1-52.19 o posterior)

> **Nota:**
>
> Para obtener más información sobre Linux VDA, consulte la documentación de Linux Virtual Delivery Agent.

Requisitos de la red

Las siguientes secciones contienen los requisitos de red para usar EDT con transporte adaptable:

Hosts de sesión

Si los hosts de la sesión tienen un firewall como el Firewall de Windows Defender, debe permitir el siguiente tráfico entrante para las conexiones internas.

Descripción	Origen	Protocolo	Puerto
Conexión interna: Fiabilidad de la sesión habilitada	Cliente	UDP	2598
Conexión interna: Fiabilidad de la sesión inhabilitada			1494
Conexión interna: HDX Direct o VDA SSL			443

> **Nota:**
>
> El instalador del VDA agrega las reglas de entrada apropiadas al Firewall de Windows Defender. Si usa un firewall diferente, debe agregar las reglas anteriores.

Red interna

La siguiente tabla muestra las reglas de firewall necesarias para usar EDT en la red:

Descripción	Protocolo	Origen	Destino	Puerto de destino
Conexión interna directa: Fiabilidad de la sesión habilitada	UDP	Red del cliente	Red VDA	2598
Conexión interna directa: Fiabilidad de la sesión inhabilitada				1494
Conexión interna directa: HDX Direct o VDA SSL				443
NetScaler Gateway		SNIP de NetScaler		2598
NetScaler Gateway: VDA SSL				443

> **Nota:**
>
> Si usa Citrix Gateway Service, debe habilitar **Rendezvous** para usar EDT como protocolo de transporte. Consulte la documentación de Rendezvous para conocer los requisitos del sistema y la red.

Red del cliente

En la siguiente tabla se describen los requisitos de conectividad de los dispositivos cliente:

Descripción	Protocolo	Origen	Destino	Puerto de destino
Conexión interna: Fiabilidad de la sesión habilitada	UDP	IP de cliente	Red VDA	2598

Descripción	Protocolo	Origen	Destino	Puerto de destino
Conexión interna: Fiabilidad de la sesión inhabilitada				1494
Conexión interna: HDX Direct o SSL VDA				443
Conexión externa: NetScaler Gateway			Dirección IP pública de NetScaler Gateway	443
Conexión externa: Citrix Gateway Service			Citrix Gateway Service	443

> **Nota:**
>
> Si usa Citrix Gateway Service, los clientes deben poder acceder a https://*.*.nssvc.net. Si no puede autorizar todos los subdominios con https://*.*.nssvc.net, puede usar https://*.c.nssvc.net y https://*.g.nssvc.net en su lugar. Para obtener más información, consulte el artículo CTX270584 de Knowledge Center.

Enlightened Data Transport

August 17, 2024

Enlightened Data Transport (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** está habilitado, EDT es el protocolo preferido.

Qué debe saber

- **Fiabilidad de la sesión** debe estar habilitada para usar **detección de MTU** y EDT con NetScaler Gateway y Citrix Gateway Service.
- La fragmentación de paquetes puede degradar el rendimiento o, en algunos casos, incluso impedir que se abran las sesiones. Para evitar esto, debe ajustar la MTU de EDT a un valor adecuado para sus redes. Puede usar la detección de MTU de EDT o una solución manual que se describe en How to configure MSS when using EDT on networks with non-standard MTU.
- Para obtener más información sobre cómo habilitar el uso de EDT con NetScaler Gateway, consulte Configurar NetScaler Gateway para que sea compatible con Enlightened Data Transport.

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.

La detección de MTU está habilitada de forma predeterminada. Si necesita inhabilitarla, consulte Funciones HDX administradas a través del registro para obtener más información.

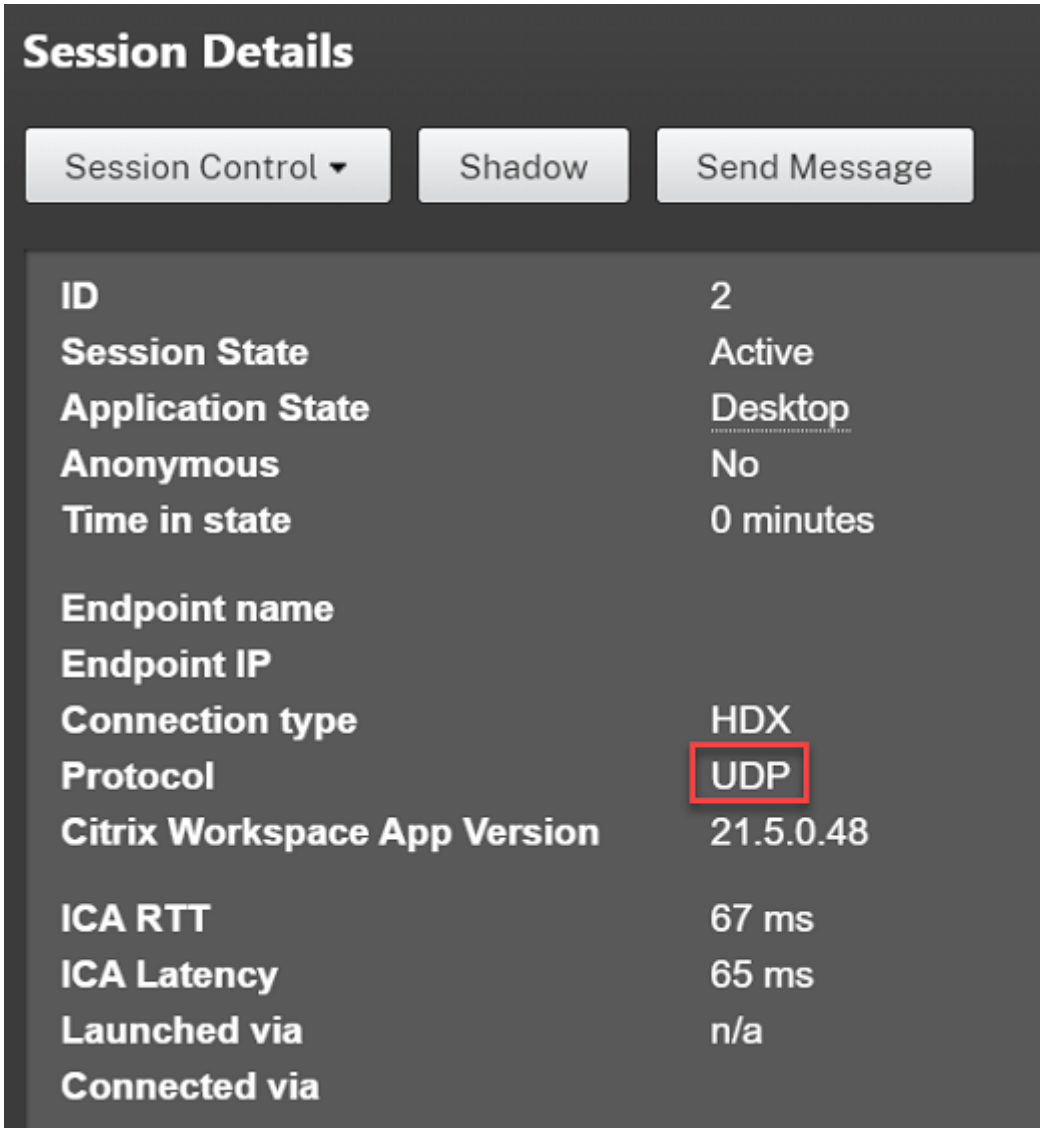
> **Nota:**
>
> - **Fiabilidad de la sesión** debe estar habilitada para que Detección de MTU funcione.
> - La detección MTU con ICA multisecuencia está disponible a partir de la versión 2209 de VDA.

Solución de problemas

August 17, 2024

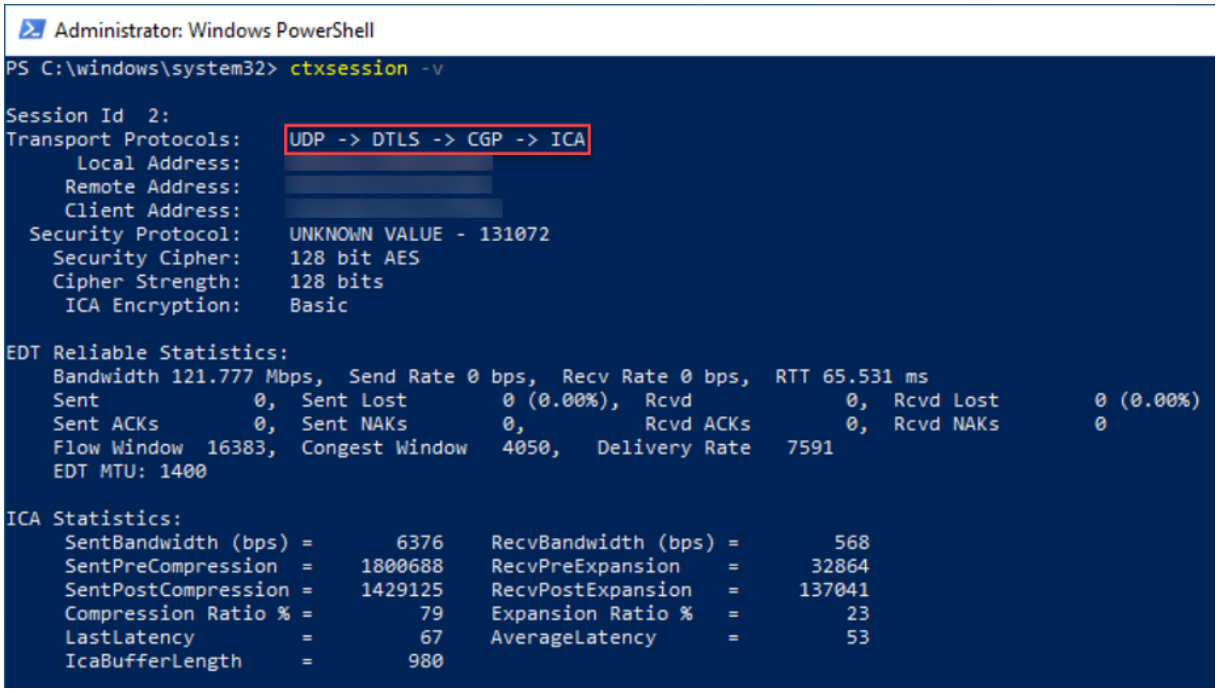
Para confirmar que EDT se usa como protocolo de transporte de la sesión, puede utilizar Director o la utilidad de la línea de comandos `CtxSession.exe` en el VDA.

En Director, busque la sesión y seleccione **Detalles**. Si el **Tipo de conexión** es HDX y el **Protocolo** es UDP, EDT se usa como protocolo de transporte de la sesión.



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)



Cuando las sesiones no se conectan con EDT

Para solucionar problemas relacionados con el **transporte adaptable** y **EDT**, sugerimos lo siguiente:

1. Revise las secciones Requisitos del sistema, Requisitos de red, Problemas conocidos y Qué debe saber.
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. 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.
6. Inicie una sesión directa internamente, omita NetScaler Gateway o Citrix Gateway Service y compruebe qué protocolo se usa. Si la sesión usa EDT, el VDA está listo para usar EDT para conexiones externas a través de NetScaler Gateway o Citrix Gateway Service.

7. Si EDT funciona para conexiones internas directas y no para sesiones que pasan por NetScaler Gateway o Citrix Gateway Service:

   - Compruebe que la **fiabilidad de la sesión** esté habilitada.
   - Si usa NetScaler Gateway, asegúrese de que su configuración cumpla con los requisitos descritos en Configurar NetScaler Gateway para que sea compatible con Enlightened Data Transport y HDX Insight.

8. Si usa Citrix Gateway Service, asegúrese de que Rendezvous esté habilitado y funcione.

9. 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 usan VPN, algunos puntos de acceso Wi-Fi y redes móviles, como 4G y 5G. Asegúrese de que tiene habilitada la detección de MTU o de que está configurando una MTU personalizada como se describe en How to configure MSS when using EDT on networks with non-standard MTU.

Problemas conocidos

- Las rutas de red asimétricas pueden provocar que la detección de MTU falle en las conexiones que no pasan por NetScaler Gateway o Citrix Gateway Service. Para solucionar este problema, actualice la versión del VDA a la 2103 o a una posterior. [CVADHELP-16654]
- Al usar NetScaler Gateway, 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. Hay disponible una corrección para este problema, a partir de la versión de firmware 13.1 compilación 17.42. Para obtener información detallada sobre cómo habilitar la corrección, consulte la documentación de NetScaler Gateway. [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.
  - Inhabilite la **detección de MTU** y use una MTU fija como se describe en How to configure MSS when using EDT on networks with non-standing MTU.
  - Inhabilitar el **transporte adaptable** para obligar a las sesiones a usar TCP. Si solo se ve afectado un subconjunto de usuarios, considere inhabilitarlo en el lado del cliente para que otros usuarios puedan seguir usando EDT.

HDX Direct (Technical Preview)

August 20, 2024

Al acceder a los recursos entregados por Citrix, HDX Direct permite que los dispositivos cliente internos y externos establezcan una conexión directa segura con el host de la sesión si es posible la comunicación directa.

> **Importante:**
>
> HDX Direct se encuentra actualmente en versión Technical Preview. Esta función se proporciona sin asistencia y aún no se recomienda su uso en entornos de producción. Para enviar comentarios o notificar problemas, use este formulario.

Requisitos del sistema

Estos son los requisitos para usar HDX Direct:

- Plano de control
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2402 o posterior
- Virtual Delivery Agent (VDA)
  - Windows: versión 2402 o posterior
- Aplicación Workspace
  - Windows: versión 2402 o posterior
- Nivel de acceso
  - Citrix Gateway Service y Citrix Workspace
  - Citrix Workspace con NetScaler Gateway
- Otros
  - El transporte adaptable debe estar habilitado para las conexiones directas externas

Requisitos de la red

Estos son los requisitos de la red para usar HDX Direct.

Hosts de sesión

Si los hosts de la sesión tienen un firewall como el Firewall de Windows Defender, debe permitir el siguiente tráfico entrante para las conexiones internas.

Descripción	Origen	Protocolo	Puerto
Conexión interna directa	Cliente	TCP	443
Conexión interna directa	Cliente	UDP	443

> Nota:
>
> El instalador del VDA agrega las reglas de entrada apropiadas al Firewall de Windows Defender. Si usa un firewall diferente, debe agregar las reglas anteriores.

Red del cliente

En la tabla siguiente se describe la red de clientes para usuarios internos y externos.

Usuarios internos

Descripción	Protocolo	Origen	Puerto de origen	Destino	Puerto de destino
Conexión interna directa	TCP	Red del cliente	1024–65535	Red VDA	443
Conexión interna directa	UDP	Red del cliente	1024–65535	Red VDA	443

Usuarios externos

Descripción	Protocolo	Origen	Puerto de origen	Destino	Puerto de destino
STUN (solo usuarios externos)	UDP	Red del cliente	1024–65535	Internet (ver nota más abajo)	3478, 19302

Descripción	Protocolo	Origen	Puerto de origen	Destino	Puerto de destino
Conexión de usuarios externos	UDP	Red del cliente	1024–65535	Dirección IP pública del centro de datos	1024–65535

Red de centros de datos

En la siguiente tabla se describe la red del centro de datos para usuarios internos y externos.

Usuarios internos

Descripción	Protocolo	Origen	Puerto de origen	Destino	Puerto de destino
Conexión interna directa	TCP	Red del cliente	1024–65535	Red VDA	443
Conexión interna directa	UDP	Red del cliente	1024–65535	Red VDA	443

Usuarios externos

Descripción	Protocolo	Origen	Puerto de origen	Destino	Puerto de destino
STUN (solo usuarios externos)	UDP	Red VDA	1024–65535	Internet (ver nota más abajo)	3478, 19302
Conexión de usuarios externos	UDP	DMZ/ Red interna	1024–65535	Red VDA	55000–55250
Conexión de usuarios externos	UDP	Red VDA	55000–55250	IP pública del cliente	1024–65535

> **Nota:**
>
> Tanto el VDA como la aplicación Workspace intentan enviar solicitudes STUN a los siguientes servidores en el mismo orden:
>
> - stunserver.stunprotocol.org:3478
> - employees.org:3478
> - stun.l.google.com:19302
>
> Si cambia el intervalo de puertos predeterminado para las conexiones de usuarios externos mediante la configuración de directiva de **intervalo de puertos de HDX Direct**, las reglas de firewall correspondientes deben coincidir con su intervalo de puertos personalizado.

Configuración

HDX Direct está inhabilitado de forma predeterminada. Puede configurar esta función mediante el parámetro **HDX Direct** de la directiva de Citrix.

- **HDX Direct**: para habilitar o inhabilitar una función.
- **Modo HDX Direct**: determina si **HDX Direct** está disponible solo para clientes internos o para clientes internos y externos.
- **Intervalo de puertos de HDX Direct**: define el intervalo de puertos que usa el VDA para las conexiones desde clientes externos.

Consideraciones

Estos son los aspectos a tener en cuenta al usar HDX Direct:

- HDX Direct para usuarios externos solo está disponible con EDT (UDP) como protocolo de transporte. Por lo tanto, el **transporte adaptable** debe estar habilitado.
- Si usa **HDX Insight**, tenga en cuenta que el uso de **HDX Direct** impide la recopilación de datos de HDX Insight, ya que la sesión ya no se redirigiría mediante proxy a través de NetScaler Gateway.
- Cuando use máquinas no persistentes para sus Virtual Apps and Desktops, Citrix recomienda habilitar **HDX Direct** en los hosts de sesión en lugar de en la imagen maestra o de plantilla para que cada máquina genere sus propios certificados.
- Actualmente, no es compatible el uso de sus propios certificados con HDX Direct.

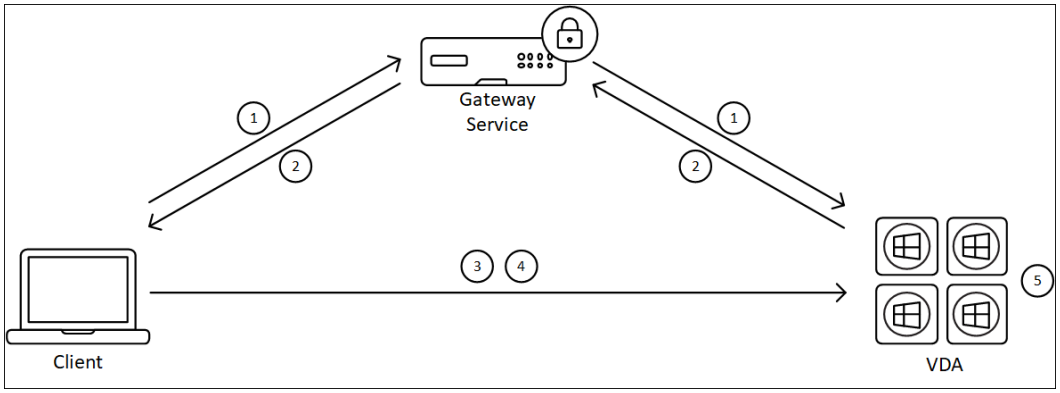
Funcionamiento

HDX Direct permite a los clientes establecer una conexión directa con el host de la sesión cuando hay una comunicación directa disponible. Cuando se realizan conexiones directas mediante HDX Direct,

se usan los certificados autofirmados para protegerlas con el cifrado a nivel de red (TLS/DTLS).

Usuarios internos

El diagrama siguiente muestra el proceso general de conexión de usuarios internos con HDX Direct.

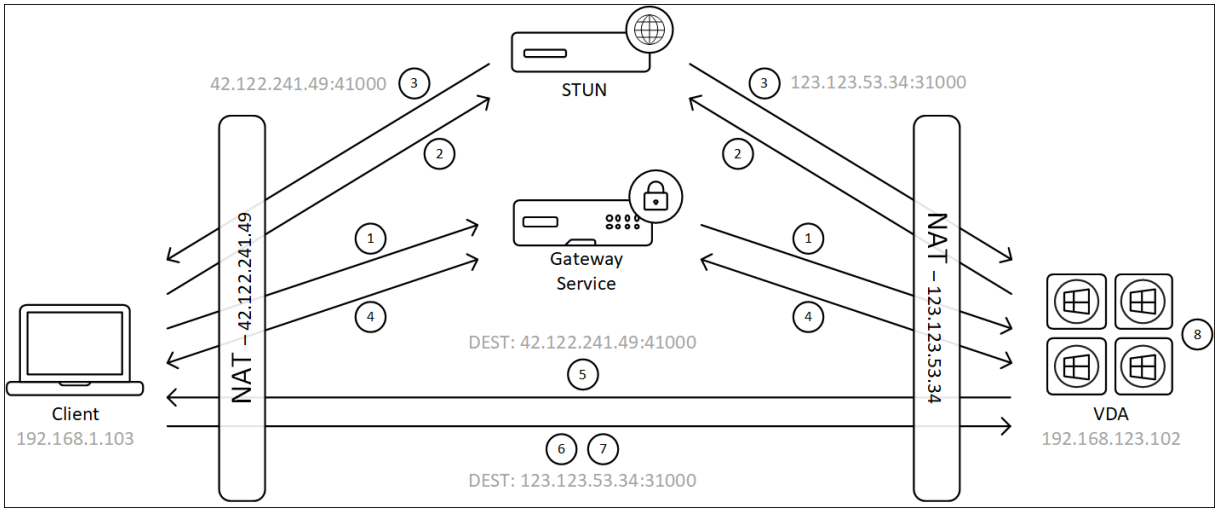


1. El cliente establece una sesión HDX a través del Gateway Service.
2. Una vez realizada la conexión, el VDA envía al cliente el nombre de dominio completo (FQDN) de la máquina VDA, una lista de sus direcciones IP y el certificado de la máquina VDA a través de la conexión HDX.
3. El cliente sondea las direcciones IP para ver si pueden comunicarse directamente con el VDA.
4. Si el cliente puede acceder al VDA directamente con cualquiera de las direcciones IP compartidas, establece una conexión directa con el VDA, protegida con (D)TLS, mediante un certificado que coincide con el intercambiado en el paso (2).
5. Una vez que la conexión directa se haya establecido correctamente, la sesión se transferirá a la nueva conexión, y se cancelará la conexión con Gateway Service.

> **Nota:**
>
> Tras establecer la conexión en el paso 2 anterior, la sesión está activa. Los pasos posteriores no provocan ninguna demora ni interfieren con la capacidad del usuario para usar la aplicación o el escritorio virtuales. Si se produce un error en alguno de los pasos posteriores, se mantiene la conexión a través de Gateway sin interrumpir la sesión del usuario.

Usuarios externos

El diagrama siguiente muestra el proceso general de conexión de usuarios externos con HDX Direct:



1. El cliente establece una sesión HDX a través del Gateway Service.
2. Tras establecerse la conexión, tanto el cliente como el VDA envían una solicitud STUN para detectar sus puertos y direcciones IP públicas.
3. El servidor STUN responde al cliente y al VDA con sus puertos y direcciones IP públicas correspondientes.
4. A través de la conexión HDX, el cliente y el VDA intercambian sus direcciones IP públicas y sus puertos UDP, y el VDA envía su certificado al cliente.
5. El VDA envía paquetes UDP a la dirección IP pública y al puerto UDP del cliente. El cliente envía paquetes UDP a la dirección IP pública y al puerto UDP del VDA.
6. Al recibir un mensaje del VDA, el cliente responde con una solicitud de conexión segura.
7. Durante el protocolo de enlace (handshake) DTLS, el cliente verifica que el certificado coincide con el certificado intercambiado en el paso (4). Tras la validación, el cliente envía su token de autorización. Ahora se ha establecido una conexión directa segura.
8. Una vez que la conexión directa se haya establecido correctamente, la sesión se transferirá a la nueva conexión, y se cancelará la conexión con Gateway Service.

> **Nota:**
>
> Tras establecer la conexión en el paso 2 anterior, la sesión está activa. Los pasos posteriores no provocan ninguna demora ni interfieren con la capacidad del usuario para usar la aplicación o el escritorio virtuales. Si se produce un error en alguno de los pasos posteriores, se mantiene la conexión a través de Gateway sin interrumpir la sesión del usuario.

Administración de certificados

Host de la sesión

Los dos servicios siguientes de la máquina VDA gestionan la creación y la administración de certificados, y ambos están configurados para ejecutarse automáticamente al iniciar la máquina:

- Citrix ClxMtp Service: Responsable de la generación y la rotación de certificados de CA.
- Citrix Certificate Manager Service: Responsable de la generación y la administración del certificado de CA raíz autofirmado y los certificados de la máquina.

Los siguientes pasos describen el proceso de administración de certificados:

1. Los servicios se inician al iniciar la máquina.
2. `Citrix ClxMtp Service` crea claves si aún no se creó ninguna.
3. Citrix Certificate Manager Service comprueba si **HDX Direct** está habilitado. De lo contrario, el servicio se detiene solo.
4. Si **HDX Direct** está habilitado, Citrix Certificate Manager Service comprueba si existe un certificado de CA raíz autofirmado. De lo contrario, se crea un certificado raíz autofirmado.
5. Una vez que haya un certificado de CA raíz disponible, Citrix Certificate Manager Service comprueba si existe un certificado de máquina autofirmado. De lo contrario, el servicio genera claves y crea un certificado mediante el FQDN de la máquina.
6. Si existe un certificado de máquina creado por Citrix Certificate Manager Service, y el nombre del asunto no coincide con el FQDN de la máquina, se genera un certificado nuevo.

> **Nota:**
>
> Citrix Certificate Manager Service genera certificados RSA que emplean claves de 2048 bits.

Dispositivo cliente

Para establecer correctamente una conexión segura de **HDX Direct**, el cliente debe confiar en los certificados utilizados para proteger la sesión. Para facilitar esto, el cliente recibe el certificado de CA para la sesión a través del archivo ICA (suministrado por Workspace), por lo que no es necesario distribuir los certificados de CA a los almacenes de certificados de los dispositivos cliente.

Compatibilidad con NAT

August 17, 2024

Para establecer una conexión directa entre un dispositivo de usuario externo y el host de la sesión, HDX Direct utiliza una técnica conocida como "hole punching"(perforación de agujeros) para NAT transversal y STUN a fin de facilitar el intercambio de la dirección IP pública y las asignaciones de puertos para el dispositivo cliente y el host de la sesión. Es algo parecido a cómo funcionan las soluciones VoIP, comunicaciones unificadas y P2P.

Siempre que los firewalls y otros componentes de red estén configurados para permitir el tráfico UDP para las solicitudes STUN y las sesiones HDX, se prevé que HDX Direct para los usuarios externos funcione. Sin embargo, hay algunos casos en los que los tipos de NAT de las redes de usuario y host de sesión dan lugar a una combinación incompatible, lo que provoca el error de HDX Direct.

Validaciones

Puede validar el tipo de NAT en el cliente y el host de la sesión mediante la utilidad de cliente STUN de STUNTMAN:

1. Descargue el paquete correspondiente a la plataforma de destino desde stunprotocol.org y extraiga el contenido.
2. Abra un el símbolo del sistema en un terminal y vaya al directorio donde se extrajo el contenido.
3. Ejecute este comando:
   ```
   .\stunclient.exe stunserver.stunprotocol.org --mode behavior
   ```
4. Tome nota del resultado.

Si las pruebas de enlace y comportamiento se realizan correctamente, tanto la **prueba de enlace** como la **prueba de comportamiento** informan de su correcta realización y se especifica un comportamiento de NAT:

Si las pruebas fallan, tanto la **prueba de enlace** como la **prueba de comportamiento** informan de la falla.

Consulte la siguiente tabla para determinar si se prevé que HDX Direct funcione para los usuarios externos conforme a los resultados de las pruebas del cliente y del host de sesión:

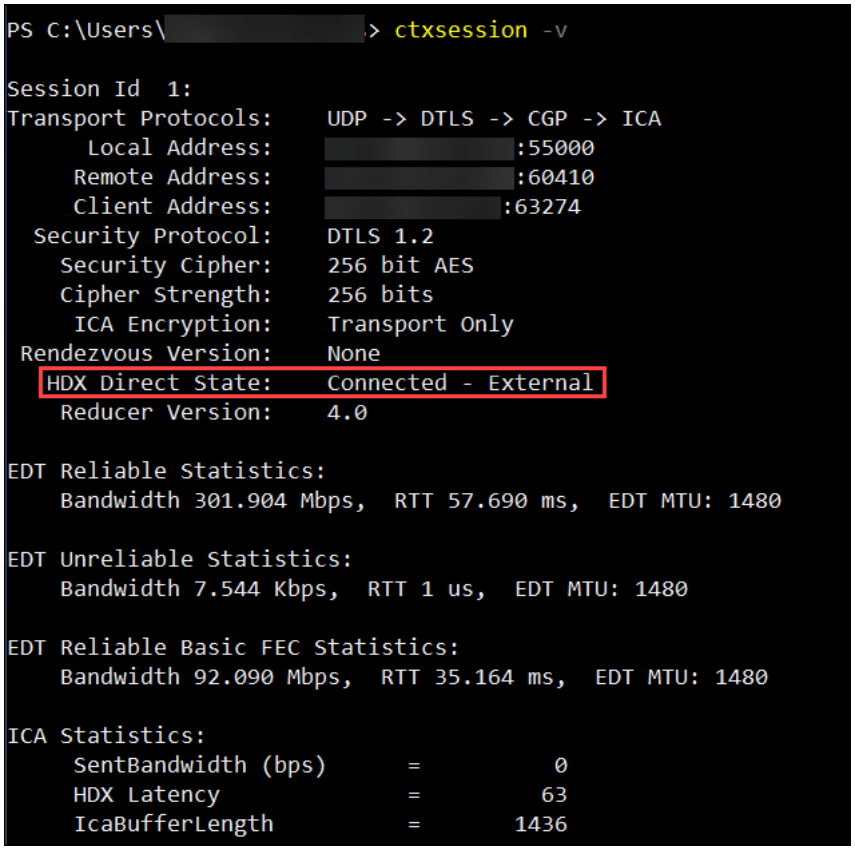
Dispositivo cliente	Host de la sesión	¿Se prevé que funcione?
Asignación independiente de los dispositivos de punto final	Asignación independiente de los dispositivos de punto final	Sí
Asignación independiente de los dispositivos de punto final	Asignación dependiente de los dispositivos de punto final	Sí
Asignación dependiente de los dispositivos de punto final	Asignación independiente de los dispositivos de punto final	Sí
Asignación dependiente de los dispositivos de punto final	Asignación dependiente de los dispositivos de punto final	No
Asignación dependiente de la dirección y el puerto	Cualquier tipo de NAT	No
Cualquier tipo de NAT	Asignación dependiente de la dirección y el puerto	No
error	Cualquier tipo de NAT	No
Cualquier tipo de NAT	error	No
error	error	No

Solución de problemas

August 17, 2024

Para confirmar que **HDX Direct** haya establecido correctamente una conexión directa, puede usar la utilidad `CtxSession.exe` en la máquina VDA.

Para usar la utilidad `CtxSession.exe`, inicie un símbolo del sistema o PowerShell dentro de la sesión y ejecute `ctxsession.exe -v`. Si la conexión **HDX Direct** se establece correctamente, el **estado de HDX Direct** es `Connected`.



También puede consultar los registros de eventos del host de la sesión para obtener información sobre si la conexión HDX Direct se estableció correctamente o no. Consulte la sección **Registros de eventos** para obtener más información.

> Nota:
>
> En función del entorno y la cantidad de direcciones IP disponibles para los hosts de sesión, la conexión HDX Direct puede tardar hasta 5 minutos en establecerse.

Cuando HDX Direct no puede establecer una conexión directa

Si HDX Direct no puede establecer una conexión directa, revise los pasos siguientes:

1. Asegúrese de que la versión del VDA y la versión de la aplicación Workspace en uso son compatibles con la función según los requisitos del sistema.
2. Confirme que tiene una directiva aplicada al VDA que habilita HDX Direct y que no hay otras directivas con mayor prioridad para inhabilitar la función.
3. Confirme que tiene una directiva aplicada al VDA que establece el modo HDX Direct deseado y que no hay otras directivas con mayor prioridad que sobrescriban la configuración.
4. Asegúrese de que el servicio Citrix ClxMtp se esté ejecutando en el host de la sesión.

5. Asegúrese de que Citrix Certificate Manager Service se esté ejecutando en el host de la sesión. Si no se está ejecutando, pruebe a iniciarlo manualmente. El servicio se detiene automáticamente si HDX Direct está inhabilitado.
6. Compruebe si el host de la sesión tiene su propio certificado de CA raíz autofirmado:

    a) Expedido para: `CA-<hostname>`(Por ejemplo, CA-FTLW11-001)
    b) Expedido para: `CA-<hostname>`(Por ejemplo, CA-FTLW11-001)
    c) Detalles del emisor: La organización es Citrix Systems, Inc.

7. Compruebe si el host de la sesión tiene su certificado de servidor autofirmado:

    a) Emitido para: `<host FQDN>`(Por ejemplo, FTLW11-001.ctxlab.net)
    b) Expedido para: `CA-<hostname>`(Por ejemplo, CA-FTLW11-001)
    c) Detalles del emisor: La organización es Citrix Systems, Inc.

8. Si faltan los certificados, contacte con el equipo de asistencia técnica de Citrix.
9. Si los certificados están presentes:

    a) Detenga Citrix Certificate Manager Service en el host de la sesión.
    b) Elimine tanto el certificado de CA raíz autofirmado como el certificado de servidor autofirmado.
    c) Inicie Citrix Certificate Manager Service en el host de la sesión. El servicio crea nuevos certificados una vez que se inicia.

10. Para usuarios internos:

    a) Asegúrese de que el firewall del host de la sesión no bloquee el tráfico entrante en UDP 443 o TCP 443, para HDX por EDT y HDX por TCP, respectivamente.
    b) Asegúrese de que su firewall de red no bloquee el tráfico en UDP 443 y TCP 443 entre la red de sus clientes y la red de los hosts de sesión.

11. Para usuarios externos:

    a) Compruebe el tipo de NAT para el cliente y el host de sesión y asegúrese de que se prevé que la combinación funcione. Para obtener más información, consulte la sección Compatibilidad con NAT.
    b) Si la prueba de NAT falla en el cliente o en el host de la sesión:
        i. Si hay un firewall ejecutándose en el sistema, asegúrese de que no esté bloqueando el tráfico saliente en UDP 3478.
        ii. Asegúrese de que los firewalls de red no bloqueen el tráfico saliente en UDP 3478.
        iii. Asegúrese de que los firewalls no bloqueen la respuesta del servidor STUN.
    c) Asegúrese de que los firewalls de red tengan configuradas las reglas adecuadas para permitir todo el tráfico necesario. Consulte la sección Requisitos de red para obtener más información.

d) Si cambia el rango de puertos predeterminado mediante la configuración de directiva de intervalo de puertos de HDX Direct, asegúrese de que las reglas de firewall estén configuradas para el intervalo de puertos personalizado.

Registros de eventos

Los siguientes eventos se registran en el registro de eventos de la máquina VDA:

Registro	ID	Origen	Nivel	Descripción
Registros de aplicaciones y servicios > Citrix-HostCore-HDX Direct/Operational	1	HDX Direct	Información	Se estableció la conexión HDX Direct para el usuario interno <username>.
Registros de aplicaciones y servicios > Citrix-HostCore-HDX Direct/Operational	2	HDX Direct	Información	Se estableció la conexión HDX Direct para el usuario externo <username>.
Registros de aplicaciones y servicios > Citrix-HostCore-HDX Direct/Operational	3	HDX Direct	Información	Error al realizar la conexión directa de HDX para el usuario <username>.

Problemas conocidos

Es posible que HDX Direct deje de funcionar después de realizar una actualización en contexto del VDA en una máquina que ya tiene **HDX Direct** habilitado.
Para resolver el problema, siga estos pasos:

1. Detenga Citrix Certificate Manager Service en el host de la sesión.
2. Elimine el certificado de CA raíz autofirmado y el certificado de servidor autofirmado.
3. Abra el registro.
4. Elimine la clave `HKLM\Software\Citrix\HDX-Direct`.

5. Vaya a `HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\icawd`.
6. Establezca el valor **SSLEnabled** en `0`.
7. Elimine el contenido del valor **SSLThumbprint**.
8. Inicie el **Citrix Certificate Manager Service**.

Secure HDX (Tech Preview)

August 17, 2024

Secure HDX es una solución de cifrado a nivel de aplicación (ALE) que impide que ningún elemento de la red en la ruta del tráfico pueda inspeccionar el tráfico HDX. Para ello, proporciona un verdadero cifrado de extremo a extremo (E2EE) a nivel de aplicación entre la aplicación Citrix Workspace (cliente) y el VDA (host de sesión) mediante el cifrado AES-256-GCM.

> **Importante:**
>
> Secure HDX se encuentra actualmente en Technical Preview. Esta función se proporciona sin asistencia y aún no se recomienda su uso en entornos de producción. Para enviar comentarios o notificar problemas, use este formulario.

Requisitos del sistema

La siguiente lista describe los requisitos del sistema para usar Secure HDX.

- Plano de control
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2402 o posterior
- Virtual Delivery Agent (VDA)
  - Windows: versión 2402 o posterior
- Aplicación Workspace
  - Windows: versión 2402 o posterior
- Nivel de acceso
  - Citrix Workspace
  - Citrix StoreFront 2402 o posterior

Configuración

Secure HDX está inhabilitado de forma predeterminada. Puede configurar esta función mediante el parámetro Secure HDX de la directiva de Citrix:

Secure HDX: define si se debe habilitar la función para todas las sesiones, solo para las conexiones directas, o si se inhabilita.

Consideraciones

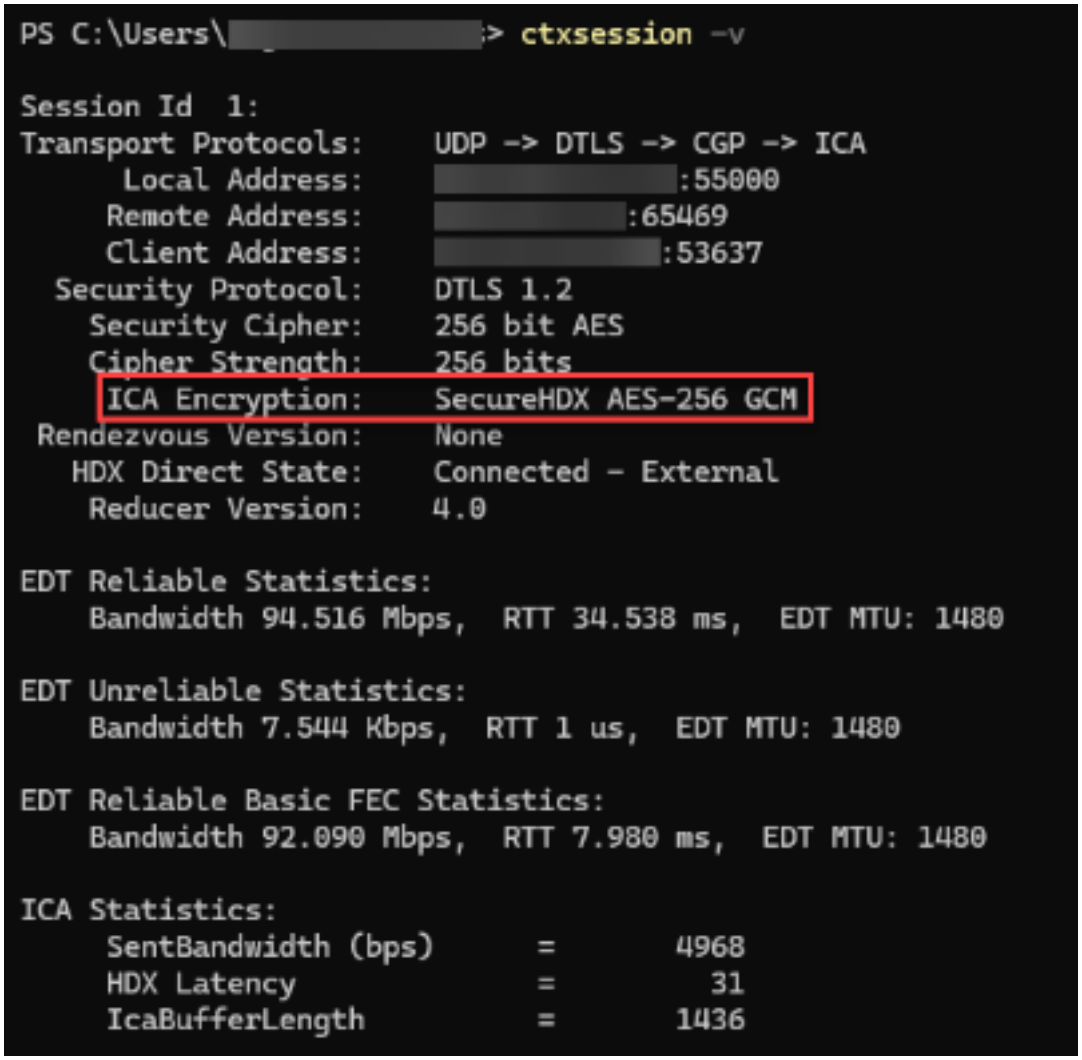
Estas son algunas consideraciones para usar Secure HDX:

- Si un usuario intenta conectarse a un host de sesión con Secure HDX habilitado usando un cliente que no admite esta función, se denegará la conexión.
- La continuidad del servicio no es compatible actualmente con Secure HDX. Si tiene habilitada la continuidad del servicio en su entorno de Citrix Cloud, no podrá conectarse a ningún host de sesión que tenga Secure HDX habilitado si se produce una interrupción del servicio de nube.
- Si usa HDX Insight, tenga en cuenta que el uso de Secure HDX impide la recopilación de datos de HDX Insight, ya que NetScaler no puede inspeccionar el tráfico HDX cifrado. Si debe usar HDX Insight, puede configurar Secure HDX para que solo se habilite para conexiones directas.
- Si utiliza SmartControl, tenga en cuenta que el uso de Secure HDX impide que funcione SmartControl, ya que el NetScaler no puede inspeccionar el tráfico HDX cifrado. Si debe usar SmartControl, puede configurar Secure HDX para que solo se habilite para conexiones directas.
- No se admite ICA multisecuencia cuando Secure HDX está habilitado.
- Si usa soluciones de terceros que dependen de la inspección del tráfico HDX, dejarán de funcionar si habilita Secure HDX, ya que el tráfico de HDX está cifrado.

Solución de problemas

Para confirmar que Secure HDX está activo, puede usar la utilidad `ctxsession.exe` en la máquina VDA.

Para usar la utilidad `CtxSession.exe`, abra un símbolo del sistema o PowerShell dentro de la sesión y ejecute `ctxsession.exe -v`. Si Secure HDX está en uso, el cifrado ICA muestra `SecureHDX AES-256 GCM`.



Cuando Secure HDX no se habilita en la sesión

- Asegúrese de que la versión del VDA en uso es compatible con la función según los requisitos del sistema.
- Confirme que tiene una directiva aplicada al VDA que habilita Secure HDX y que no hay otras directivas con mayor prioridad para inhabilitar la función.
- Si el dispositivo cliente se conecta a través de NetScaler Gateway o Gateway Service, asegúrese de que Secure HDX no esté configurado como "Solo conexiones directas".
- Si el host de sesión ya estaba en ejecución cuando configuró Secure HDX, reinicie la máquina para asegurarse de que los cambios surtan efecto.

Lista de canales virtuales permitidos

August 17, 2024

La lista de canales virtuales permitidos es una función que le permite controlar qué canales virtuales que no son de Citrix están permitidos en su entorno. De forma predeterminada, la funcionalidad de lista de canales virtuales permitidos está habilitada. Como resultado, solo se pueden abrir los canales virtuales de Citrix en las sesiones de Citrix 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.

Configuración

La lista de canales virtuales permitidos está habilitada de forma predeterminada. Puede configurar esta función mediante los siguientes parámetros de la directiva de Citrix:

- **Lista de canales virtuales permitidos**: Para habilitar o inhabilitar la función y agregar canales virtuales a la lista.
- **Limitación de los registros de la lista de canales virtuales permitidos**: Establece el período de limitación para el registro de eventos de la lista de canales virtuales permitidos.
- **Registros de la lista de canales virtuales permitidos**: Establece el nivel de registro de la lista de canales virtuales permitidos.

Agregar canales virtuales a la lista de permitidos

Para agregar un canal virtual a la lista de permitidos, necesita la siguiente información:

1. El nombre del canal virtual tal y como se define en el código, que puede tener hasta 7 caracteres. Por ejemplo, `CTXCVC1`.
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, puede agregarlos separando cada proceso con comas.

Para procesos individuales

Con los ejemplos anteriores, agregue la entrada siguiente a la lista:

```
CTXCVC1,C:\Program Files\Application\run.exe
```

Para varios procesos

Si hay varios procesos, agregue la entrada siguiente a la lista:

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application
\run2.exe
```

Uso de comodines

Se admite el uso de comodines (*). Puede usar caracteres comodín cuando los nombres de los directorios o ejecutables cambian en función de la versión de la aplicación o si el componente de terceros está instalado en los perfiles de los usuarios.

Puede usar caracteres comodín en los siguientes casos:

- Para reemplazar el nombre completo del directorio.
  Por ejemplo: `C:\Program Files\Application\*\run1.exe`
- Para reemplazar parte del nombre del directorio.
  Por ejemplo: `C:\Program Files\Application\v*\run1.exe`
- Para reemplazar el nombre del ejecutable.
  Por ejemplo: `C:\Program Files\Application\v1.2\*.exe`
- Para reemplazar parte del nombre del ejecutable.
  Por ejemplo: `C:\Program Files\Application\v1.2\run*.exe`

Se aplican las siguientes restricciones:

- El comodín solo se puede usar para reemplazar un único directorio. Por ejemplo: si el ejecutable se encuentra en `C:\Program Files\Application\v1.2\run1.exe`
  - Permitido: `C:\Program Files\Application\*\run1.exe`
  - No permitido: `C:\Program Files\*\run1.exe`
- Las entradas deben contener la extensión de archivo.
  - Permitido: `C:\Program Files\Application\v1.2\*.exe`
  - No permitido: `C:\Program Files\Application\v1.2\*`
- Todas las rutas deben ser locales.

> **Nota:**
>
> - No se permiten las rutas de red.
> - La compatibilidad con caracteres comodín está disponible a partir de Citrix Virtual Apps and Desktops 2206.
> - La compatibilidad con caracteres comodín está disponible en Citrix Virtual Apps and Desktops 2203 LTSR a partir de la CU2.

Uso de variables de entorno del sistema

Puede usar variables de entorno del sistema para simplificar la definición de los procesos de confianza en su lista de permitidos. Puede usar cualquiera de las variables listas para usar, como `%programfiles%`, `%programfiles(x86)%`, `%systemdrive%` y `%systemroot%`.

También puede usar variables de entorno personalizadas siempre que estén definidas a nivel del sistema.

En los siguientes ejemplos se muestran variables de entorno listas para usar:

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application\*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

En el siguiente ejemplo se muestra una variable de entorno del sistema personalizada:

- Nombre de variable personalizada: `app`
- Valor de variable personalizada: `%programfiles%\Application\`
- Entrada en la lista de permitidos: `CTXCVC1,%app%\run.exe`

> **Nota:**
>
> No se admiten variables de entorno de usuario.
>
> La compatibilidad con variables de entorno está disponible a partir de la versión 2209 de Citrix Virtual Apps and Desktops.

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 y el proceso que lo intentó abrir. Para obtener más información sobre los eventos disponibles, consulte Registros de eventos.
3. Cierre la sesión.
4. Agregue una entrada a la configuración de directiva Lista de canales virtuales permitidos para el canal virtual y el proceso identificados.
5. Reinicie la máquina.
6. Una vez registrado el VDA, ejecute la aplicación virtual o el escritorio virtual para comprobar que los canales virtuales personalizados se abren correctamente.

Consideraciones sobre canales virtuales Citrix

Todos los canales virtuales Citrix integrados son de confianza y se permite abrirlos sin ninguna configuración adicional. Sin embargo, las dos funcionalidades siguientes requieren entradas explícitas en la lista de permitidos debido a dependencias externas:

- Redirección multimedia
- HDX RealTime Optimization Pack para Skype for Business

Redirección multimedia

Si usa un reproductor multimedia distinto de Windows Media Player como reproductor multimedia del sistema, debe agregarlo a la lista de permitidos como proceso de confianza. 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:\Program Files (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 for Business

Esta información es necesaria para la entrada en la lista de permitidos:

- Nombre del canal virtual: `CTXRMEP`
- Proceso: Ruta al archivo ejecutable de Skype for Business en la máquina VDA, que puede variar según la versión de Skype for Business o si se ha usado una ruta de instalación personalizada.

Por ejemplo, `C:\Program Files\Microsoft Office\root\Office16\lync.exe`.

- Entrada en la lista de permitidos: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

Solución de problemas

August 17, 2024

Si su canal virtual personalizado no se abre, revise los pasos siguientes:

1. Asegúrese de usar la versión de VDA correcta.
2. Confirme que tiene una directiva aplicada al VDA con el canal virtual personalizado en la lista de canales virtuales permitidos y que no hay otras directivas con mayor prioridad que sobrescriban esta configuración.
3. Compruebe el registro de eventos del VDA y confirme que el nombre del canal virtual notificado coincide con el definido en la lista de permitidos.
    a) Si tiene varios procesos, asegúrese de que estén definidos correctamente como se describe en Agregar canales virtuales a la lista de permitidos.
    b) Si usa caracteres comodín en la ruta de proceso definida, asegúrese de cumplir las directrices sobre uso de comodines.
    c) Si usa variables de entorno en la ruta de proceso definida, asegúrese de cumplir las directrices sobre uso de variables de entorno del sistema.

Registros de eventos

Los siguientes eventos se registran en el registro de eventos de la máquina VDA.

VDA de sesión única

Los siguientes eventos se registran en el registro de eventos de la máquina VDA de sesión única:

Nombre de registro	ID	Origen	Nivel	Descripción
Sistema	2001	Picadd	Información	El proceso <processName> ha abierto el canal virtual personalizado <vcName>
Sistema	2002	Picadd	Advertencia	El proceso <processName> no puede abrir el canal virtual personalizado <vcName>
Sistema	2003	Picadd	Información	<username> abrió el canal virtual personalizado <vcName>
Sistema	2004	Picadd	Advertencia	<username> intentó abrir el canal virtual personalizado <vcName>
Sistema	2005	Picadd	Error	La ruta indicada en la directiva <pathInPolicy> no puede resolverse en la ruta del proceso
Sistema	2007	Picadd	Información	La ruta del proceso cargado es <processPath>

Nombre de registro	ID	Origen	Nivel	Descripción
Sistema	2008	Picadd	Error	No se encuentra la variable de entorno <varName> en la ruta de la directiva de canal virtual

VDA multisesión

Los siguientes eventos se registran en el registro de eventos de la máquina VDA multisesión:

Nombre de registro	ID	Origen	Nivel	Descripción
Sistema	13	Rpm	Información	El proceso <processName> ha abierto el canal virtual personalizado <vcName>
Sistema	14	Rpm	Advertencia	El proceso <processName> no puede abrir el canal virtual personalizado <vcName>
Sistema	15	Rpm	Información	<username> abrió el canal virtual personalizado <vcName>
Sistema	16	Rpm	Advertencia	<username> intentó abrir el canal virtual personalizado <vcName>

Nombre de registro	ID	Origen	Nivel	Descripción
Sistema	17	Rpm	Error	La ruta indicada en la directiva <pathInPolicy> no puede resolverse en la ruta del proceso
Sistema	18	Rpm	Información	La ruta del proceso cargado es <processPath>
Sistema	19	Rpm	Error	No se encuentra la variable de entorno <varName> en la ruta de la directiva de canal virtual

Canales virtuales de terceros conocidos

August 17, 2024

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
- ControlUp
- Cisco WebEx Teams
- Cisco WebEx Meetings Virtual Desktop Software
- deviceTrust
- Epic Warp Drive
- Epic Slingshot
- Imprivata OneSign
- Extensiones de cliente Midmark IQPath
- Extensiones de cliente Nuance PowerMic

- Nuance Dragon Medical Network Edition 360 vSync
- Zoom Meetings para VDI
- Ultima IA-Connect

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

August 17, 2024

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:

- Escaneo
- Dispositivo USB genérico
- Asignación de unidades del cliente
- Dispositivos móviles y de pantalla táctil
- Dispositivos en serie
- Teclados especiales
- 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

Escaneo

August 17, 2024

Un escáner es un dispositivo que analiza ópticamente imágenes, texto impreso, escritura a mano o un objeto y lo convierte en una imagen digital.

Si usa un escáner y su equipo funciona con Windows, es muy probable que use el controlador de escáner WIA. Este controlador es responsable de la comunicación entre el equipo y el escáner.

- **Adquisición de imágenes de Windows** (WIA) es el modelo de controlador y la interfaz de programación de aplicaciones (API) de Microsoft que permite al software comunicarse con el hardware de procesamiento de imágenes, como los escáneres.
- **TWAIN** (Windows y Mac) es otro protocolo de escaneo que conecta escáneres y aplicaciones mediante una interfaz estándar. TWAIN permite a las aplicaciones adquirir imágenes de dispositivos compatibles con TWAIN (escáneres, cámaras digitales, etc.).

Redirección TWAIN

August 17, 2024

Introducción

TWAIN es un protocolo de escaneo que sirve para vincular software de procesamiento de imágenes a escáneres o cámaras digitales.

Cómo funciona TWAIN

- Para escanear documentos, use cualquiera de las aplicaciones de 32 bits de su sesión de Citrix.

  > **Nota:**
  >
  > Para escanear los documentos, use un escáner compatible con TWAIN conectado de forma local.

- El módulo de escaneo de Citrix redirige la solicitud TWAIN al escáner del cliente.
- Una vez finalizado el escaneo, se notifica al host de la sesión.

Requisitos

Plano de control de Citrix

- Citrix Virtual Apps and Desktops 1912 o versiones posteriores
- Citrix DaaS

Host de la sesión

- Sistema operativo
  - Windows 10 1809 o una versión posterior
  - Windows 11
  - Windows Server 2022 o una versión posterior
- VDA
  - Versión 1912 o posterior
- Aplicación
  - Aplicación de 32 bits

Dispositivo cliente

- Sistema operativo
  - Windows 10 1809 o una versión posterior
  - Windows 11
- Aplicación Workspace
  - Windows: Versión 1912 o una posterior
- Escáner
  - Escáner compatible con TWAIN

Configuración

- Instale los controladores TWAIN en el dispositivo de punto final del cliente.
- Configure los dispositivos o las aplicaciones para seleccionar el protocolo de escaneo requerido si son compatibles tanto con TWAIN como con WIA.
- Conecte el escáner al dispositivo de punto final del cliente de forma local (a través de USB).
- Redirija los dispositivos TWAIN a la sesión mediante redirección USB si es necesario.

> **Nota:**
>
> Los dispositivos TWAIN no funcionan bien con la redirección USB, lo que provoca una baja calidad de escaneo.

Configuraciones de directivas

Configuraciones de directivas para definir la redirección TWAIN y mejorar la calidad de escaneo.

- **Redirección de dispositivos TWAIN del cliente:** Para habilitar o inhabilitar la redirección TWAIN.

  > **Nota:**
  >
  > De forma predeterminada, la redirección TWAIN está habilitada.

- **Nivel de compresión TWAIN:** Para establecer los niveles de compresión de las imágenes del cliente al host.

Para obtener más información, consulte Configuraciones de directiva de Dispositivos TWAIN.

Solución de problemas

Pruebe TWAIN con la aplicación de prueba pública Twacker, que se puede descargar desde esta URL.

Siga los pasos necesarios para validar TWAIN en una sesión de escritorio publicada:

1. Instale **Twacker** en el VDA.
2. Inicie **Twacker** (versión de 32 bits).
3. Haga clic en **File > Select Source** y seleccione su escáner de la lista.
4. Haga clic en **File > Acquire**.
5. Haga clic en el **botón Scan** para probar el escáner.

Si **Twacker** puede escanear correctamente, confirma lo siguiente acerca de la configuración de **Citrix Virtual Apps and Desktops**:

- Está configurado para redirección USB
- Es compatible con dispositivos TWAIN
- Cumple con todos los requisitos acerca de los dispositivos cliente locales

Si sigue teniendo problemas al escanear en una aplicación en particular, es probable que se trate de un problema de software.

Dispositivos WIA

August 17, 2024

Requisitos

- El escáner debe ser compatible con WIA.
- Instale los controladores WIA 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 servicio Adquisición de imágenes de Windows, no el controlador TWAIN local.
- 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.

Lista de aplicaciones permitidas de Adquisición de imágenes de Windows

Una lista de permitidos le permite controlar qué aplicaciones del VDA pueden acceder a la redirección del escáner de Adquisición de imágenes de Windows (WIA). El Editor del Registro utiliza la información de configuración de la lista de permitidos en cada VDA que contiene Adquisición de imágenes de Windows. De forma predeterminada, ninguna aplicación tiene acceso a Adquisición de imágenes de Windows.

Para ajustar Adquisición de imágenes de Windows para las aplicaciones del VDA, consulte la configuración de Lista de aplicaciones permitidas de Adquisición de imágenes de Windows en la lista de funciones administradas a través del Registro.

Para obtener información acerca de las configuraciones de directiva, consulte Configuraciones de directiva de dispositivos WIA.

Dispositivos USB genéricos

August 17, 2024

Introducción

La función de redirección de USB genérico permite redirigir los dispositivos USB de las máquinas cliente a las sesiones HDX. De esta forma, los usuarios finales pueden interactuar con una amplia selección de dispositivos USB genéricos en su sesión HDX. Esto resulta útil en situaciones en las que los usuarios necesitan usar dispositivos especiales no optimizados.

> **Nota:** Los dispositivos USB que no estén optimizados para compatibilidad con canales virtuales volverán al canal virtual USB genérico mediante redirección USB básica.

Cómo funciona

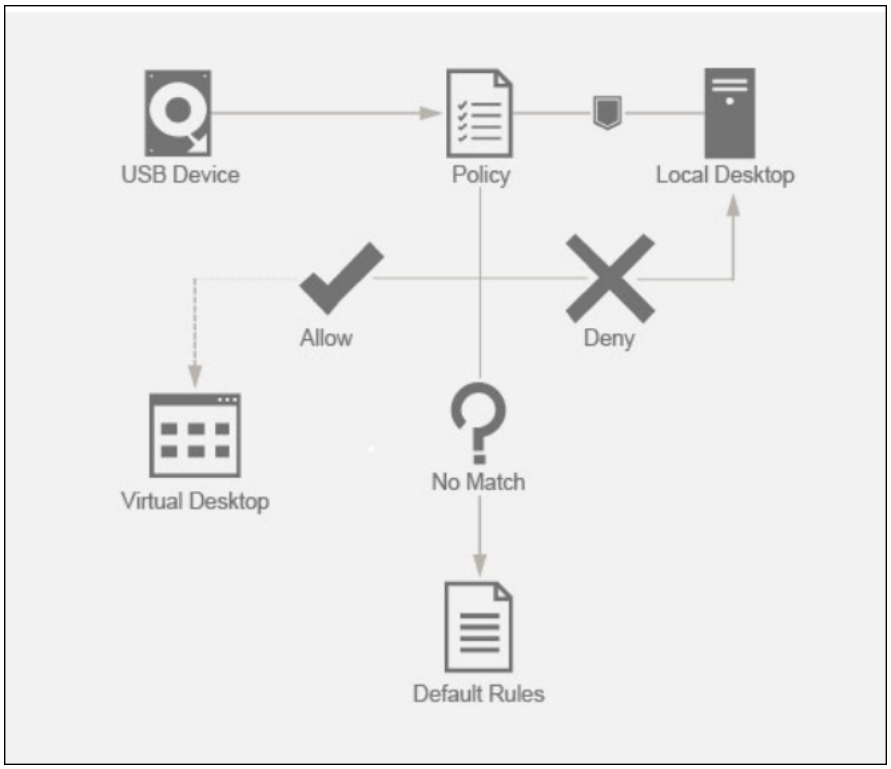
La redirección de USB genérico funciona a bajo nivel y redirige los mensajes de solicitudes y respuestas de USB entre las máquinas cliente y el escritorio virtual de XenDesktop.

Así se evita el requisito de tener controladores de dispositivo compatibles en la máquina cliente, y el controlador solo necesita ser compatible en el escritorio virtual. Las reglas de las directivas de redirección USB siguen un orden de prioridad determinado que permite respetar las directivas del lado del cliente y las reglas predeterminadas después de evaluar y aplicar las reglas de las directivas de DDC. Esto permite a los administradores de Citrix impedir la redirección de dispositivos no autorizados o falsificados dentro de una sesión.

Además, es posible auditar y marcar el registro de eventos de los dispositivos no autorizados que intentan acceder a la sesión remota, y los administradores pueden adoptar medidas adicionales para evitar la filtración de datos.

Cuando un usuario conecta un dispositivo USB, el host de la sesión lo coteja sucesivamente con cada regla de directiva hasta que encuentra una coincidencia. La primera coincidencia para cualquier dispositivo se considera definitiva.

- Si la primera coincidencia es una regla para Permitir, el dispositivo se redirige al escritorio virtual.
- Si la primera coincidencia es una regla para Denegar, el dispositivo no se redirige a la sesión y solo está disponible para uso en el dispositivo local del usuario. Si no hay coincidencias, se usan las reglas predeterminadas.



Configuración

August 17, 2024

La redirección USB está inhabilitada de forma predeterminada. Puede configurar la redirección USB genérica mediante los siguientes parámetros de la directiva de Citrix:

- **Redirección de dispositivos USB del cliente**: Para habilitar o inhabilitar la redirección USB

- **Reglas de redirección de dispositivos USB del cliente**: Para especificar una acción específica del dispositivo, es decir, permitir o denegar el acceso a un dispositivo en particular
- **Reglas de redirección de dispositivos USB del cliente (versión 2)**: Para especificar reglas para filtrar, dividir y conectar automáticamente dispositivos USB
- **Reglas de optimización de dispositivos USB del cliente**: Para inhabilitar la optimización o para cambiar el modo de optimización
- **Permitir que los dispositivos USB existentes se conecten automáticamente**: Para permitir o impedir la conexión automática de los dispositivos USB existentes que están conectados a un dispositivo de punto final cliente al comienzo de una sesión HDX
- **Permitir que los dispositivos USB recién llegados se conecten automáticamente**: Para permitir o impedir la conexión automática de los dispositivos USB que están conectados a un dispositivo de punto final cliente durante una sesión HDX

Consulte Configuraciones de directiva USB para obtener más información.

Cómo configurar la redirección USB

De forma predeterminada, la configuración de redirección USB está inhabilitada. Para usarla, la directiva de redirección USB y las reglas de redirección específicas deben estar habilitadas y configuradas en el DDC.

> **Nota:**
>
> Si usa algún componente anterior a la versión 2212 o la aplicación Workspace para Linux/Mac, consulte Configuración de la redirección USB antigua para obtener más información sobre cómo configurar la redirección USB.

Habilitar la redirección de USB genérico

1. Abra las **directivas de Citrix Web Studio** y haga clic en la ficha **Directivas** .
2. Haga clic en **Crear directiva** y expanda las **directivas ICA > Dispositivos USB**.
3. Modifique la **directiva Redirección de dispositivos USB del cliente**.
4. Seleccione **Permitida** y haga clic en **Guardar**.

Creación de reglas de directiva de redirección USB

Cuando el usuario intenta redirigir un dispositivo USB a un escritorio virtual, se coteja sucesivamente cada regla de directiva USB hasta que encuentra una coincidencia. La primera coincidencia para cualquier dispositivo se considera definitiva. Si la primera coincidencia es una regla para **Permitir**,

se autoriza la redirección del dispositivo al escritorio virtual. Si la primera coincidencia es una regla para **Denegar**, el dispositivo solamente está disponible en el escritorio local. Si no hay coincidencias, se usan las reglas predeterminadas.

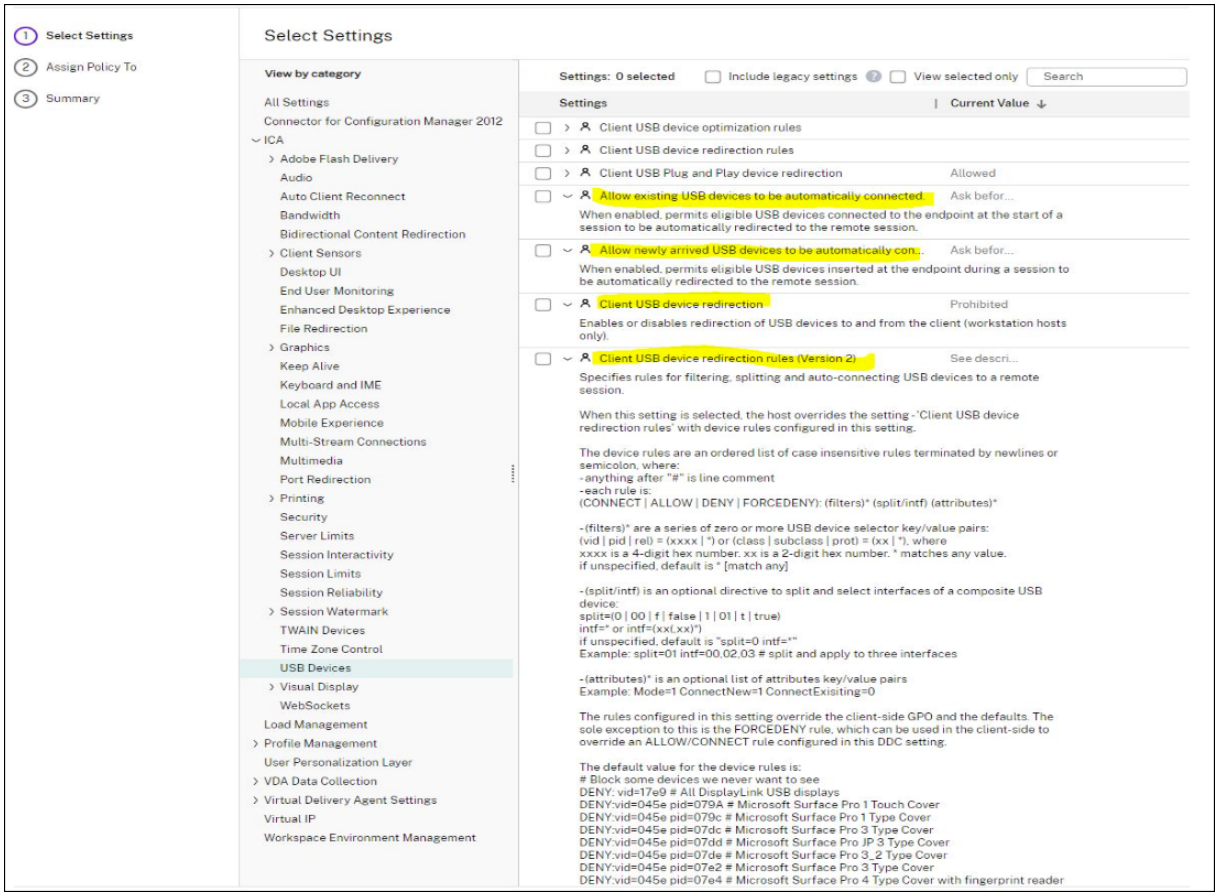
Reglas de dispositivo Al igual que los dispositivos USB normales, las reglas de dispositivo establecidas en la directiva o en la configuración de la aplicación Citrix Workspace del cliente en el dispositivo de punto final seleccionan los dispositivos para el reenvío. La aplicación Citrix Workspace usa estas reglas para decidir los dispositivos USB para los que permitir o impedir el reenvío a la sesión remota.

Cada regla consta de una palabra clave de acción (**Permitir, Conectar o Denegar**), dos puntos (:) y cero o más parámetros de filtro que coinciden con dispositivos reales en el subsistema USB de los dispositivos de punto final. Estos parámetros de filtro corresponden a los metadatos descriptores del dispositivo USB que usa cada dispositivo USB para identificarse.

Las reglas de dispositivo son texto no cifrado con cada regla en una sola línea y un comentario opcional precedido de un carácter #. Las reglas se cotejan de arriba a abajo (orden de prioridad descendente). Se aplica la primera regla que coincida con la interfaz del dispositivo o la interfaz secundaria. Se ignoran las reglas subsiguientes que seleccionen el mismo dispositivo o interfaz.

Ejemplo: ALLOW VID=1050 PID=0421 #Device1
Ejemplo: CONNECT VID=xxxx PID=yyyy Class=03 #Device2

Palabra clave	Descripción
CONNECT	Use esta palabra clave para permitir que los dispositivos se redirijan a través del canal virtual USB, así como para que se redirijan automáticamente durante el inicio de la sesión y al insertarlos.
ALLOW	Use esta palabra clave para permitir que los dispositivos se redirijan a través del canal virtual USB
DENY	Use esta palabra clave para impedir que los dispositivos se redirijan a través del canal virtual USB



Configuración de la directiva en el DDC:

1. Abra las **directivas de Citrix Web Studio** y haga clic en la ficha **Directivas** .
2. Haga clic en **Crear directiva** y expanda las **directivas ICA > Dispositivos USB**.
3. Modifique las **Reglas de redirección de dispositivos USB del cliente** (**versión 2**).
4. Establezca el valor conforme a los ejemplos proporcionados en la descripción de cada dispositivo USB que necesite redirigirse y haga clic en Guardar.

   Por ejemplo: Allow: VID=056A PID=00A4 #STU-430
   Deny: Class=08 subclass=05 # Almacenamiento masivo

   > **Nota:**
   >
   > Si un administrador de Citrix marca la casilla **Usar el valor predeterminado** y hace clic en **Guardar**, las reglas predeterminadas se encuentran en el siguiente registro del VDA.
   >
   > **Precaución:**
   >
   > Consulte la renuncia de responsabilidades al final de este artículo antes de usar el Editor del Registro.

   `HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

> **Nota:**
>
> Las directivas aún se pueden establecer en el dispositivo cliente mediante reglas de dispositivo de directivas de grupo, pero eso ya no es necesario en las versiones más recientes de CVAD y CWA.
>
> Para ver la configuración antigua de dispositivos USB, consulte Configuración de la redirección USB antigua.

Configurar redirección automática de dispositivos USB (opcional)

Los dispositivos USB se redirigen automáticamente cuando se habilita la compatibilidad con USB. Además, la configuración de preferencias de usuario de USB está definida para conectar automáticamente dispositivos USB. 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 aparezcan en la lista o se redirijan, utilice DeviceRules en el dispositivo de punto final del cliente o en la directiva de DDC.
Esta directiva se puede configurar en el DDC, en el cliente mediante un objeto de directiva de grupo, mediante las Preferencias de Citrix Workspace o en la ficha Conexiones, en CDViewer. Todos estos métodos se describen a continuación:

Configuración de la directiva en el DDC:

Hay dos directivas en el DDC que se pueden configurar para permitir la redirección automática de dispositivos USB:

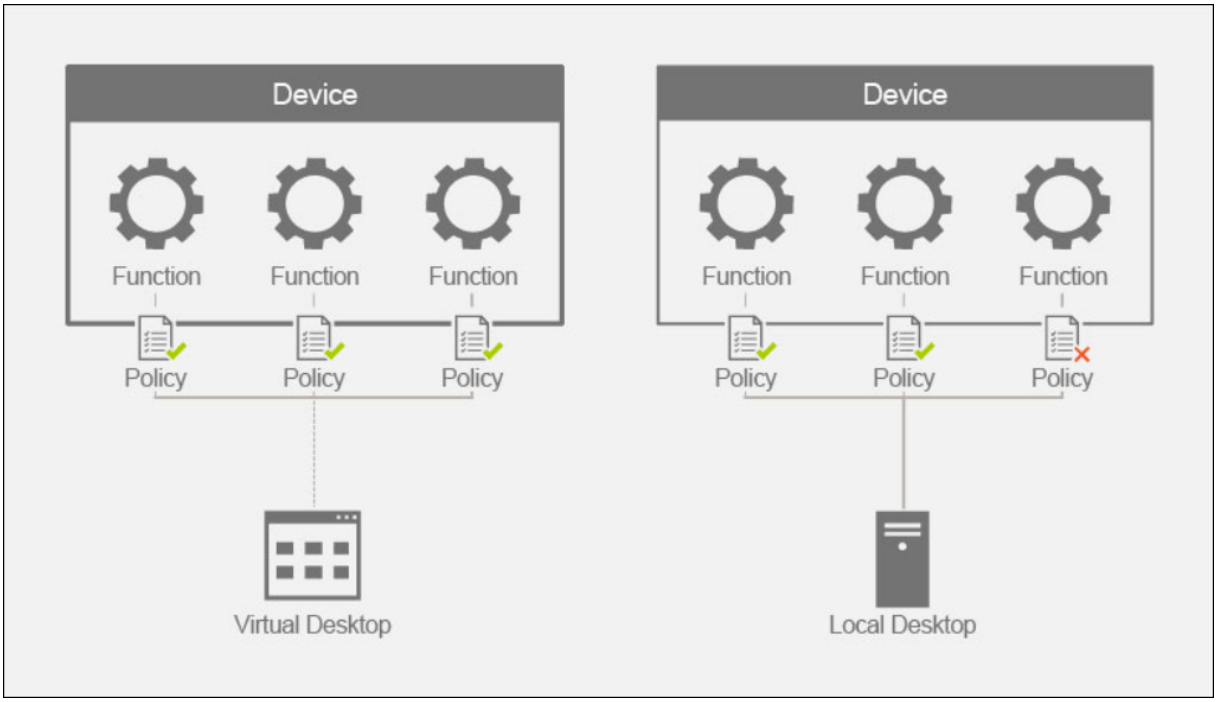
- Permitir que los dispositivos USB existentes se conecten automáticamente
- Permitir que los dispositivos USB recién llegados se conecten automáticamente

1. Abra las **directivas de Citrix Web Studio** y haga clic en la ficha **Directivas** .
2. Haga clic en **Crear directiva** y expanda las **directivas ICA > Dispositivos USB**.
3. Modifique el parámetro **Permitir** que los dispositivos USB existentes se conecten automáticamente.
4. Desmarque la casilla **Usar el valor predeterminado**, seleccione **Redirigir automáticamente los dispositivos USB disponibles** en el menú desplegable y haga clic en **Guardar**.
5. Modifique el parámetro **Permitir** que los dispositivos USB recién llegados se conecten automáticamente.
6. Desmarque la casilla **Usar el valor predeterminado**, seleccione **Redirigir automáticamente los dispositivos USB disponibles** en el menú desplegable y haga clic en **Guardar**.

Dispositivos compuestos y división de dispositivos

August 17, 2024

Un dispositivo USB compuesto es un dispositivo único que actúa como varios dispositivos USB independientes conectados a un equipo. Tiene un solo conector USB, pero puede exponer distintas interfaces al equipo, cada una con un conjunto propio de funcionalidades. Cuando un usuario conecta un dispositivo USB compuesto, el dispositivo host coteja todas las funciones (interfaces) con cada regla de directiva. Si la primera coincidencia para cualquier función (interfaz) es una regla Denegar, la regla se considera definitiva para el dispositivo compuesto y se deniega el dispositivo. Si la primera coincidencia para una función (interfaz) es una regla Permitir, el dispositivo host continúa cotejando las reglas con la siguiente función (interfaz). Si no hay una regla de directiva que deniegue alguna función (interfaz), el dispositivo compuesto se autoriza. Si la coincidencia definitiva para el dispositivo compuesto es una regla Denegar, el dispositivo solo estará disponible en el escritorio local; de lo contrario, el dispositivo se conectará de forma remota al escritorio virtual. Si no hay coincidencias, se usan las reglas predeterminadas.



Para dividir un dispositivo compuesto, podemos usar las reglas correspondientes de la directiva Reglas de redirección de dispositivos (versión 2) a fin de permitir únicamente una funcionalidad específica de un dispositivo compuesto. Por ejemplo, es posible que solo queramos usar las funciones HID de una clave FIDO2, pero no la funcionalidad de la tarjeta inteligente. En ese caso, estableceríamos las reglas como se muestra a continuación:

1. Connect: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Yubikey serie 5: funciones HID de

FIDO2 permitidas.

2. Deny: VID=1050 PID=0407 split=01 intf=02 # Yubikey serie 5: función de tarjeta inteligente bloqueada.

> **Sugerencia:**
>
> Al crear nuevas reglas de directivas, consulte los códigos de clase USB, que están disponibles en el sitio web de USB.

Configurar un panel de firmas

1. Instale el controlador de dispositivo apropiado en el host del VDA.
2. Active la **directiva Redirección de dispositivos USB del cliente** en **Citrix Web Studio**.
3. Modifique la directiva **Reglas de redirección de dispositivos USB del cliente** (**versión 2**).
    a) Establezca la información de **VID** y **PID** del panel de firmas que debe redirigirse y haga clic en **Guardar**. Por ejemplo: **Connect**: VID=056A PID=00A4 #STU-430
4. Modifique la directiva **Reglas de optimización de dispositivos USB del cliente**.
    a) Configure el modo junto con otra información del dispositivo. Por ejemplo: Mode=00000004 VID=056A PID=00A4 class=03 #Dispositivo de entrada funciona en modo de captura
5. Modifique la directiva **Permitir que los dispositivos USB existentes se conecten automáticamente**.
6. Desmarque la casilla **Usar el valor predeterminado**, seleccione **Redirigir automáticamente los dispositivos USB disponibles** en el menú desplegable y haga clic en **Guardar**.
7. Modifique la directiva **Permitir que los dispositivos USB recién llegados se conecten automáticamente**.
8. Desmarque la casilla **Usar el valor predeterminado**, seleccione **Redirigir automáticamente los dispositivos USB disponibles** en el menú desplegable y haga clic en **Guardar**.

Una vez que se hayan establecido estas directivas en la consola de Studio, el dispositivo se redirigirá automáticamente al inicio de sesión y no requerirá ninguna acción adicional por parte del usuario final.

> **Nota:**
>
> Sustituya el VID y el PID por el VID y el PID reales del dispositivo que se va a redirigir.

Configuración del teclado Bloomberg mediante redirección USB

1. Active la **directiva Redirección de dispositivos USB del cliente** en **Citrix Web Studio**.
2. Los teclados Bloomberg 5 están configurados de forma predeterminada en la directiva Reglas de redirección de dispositivos USB del cliente (versión 2) y no es necesaria ninguna acción de administración adicional.
3. Modifique la directiva **Permitir que los dispositivos USB existentes se conecten automáticamente**.
4. Desmarque la casilla **Usar el valor predeterminado**, seleccione **Redirigir automáticamente los dispositivos USB disponibles** en el menú desplegable y haga clic en **Guardar**.
5. Modifique la directiva **Permitir que los dispositivos USB recién llegados se conecten automáticamente**.
6. Desmarque la casilla **Usar el valor predeterminado**, seleccione **Redirigir automáticamente los dispositivos USB disponibles** en el menú desplegable y haga clic en **Guardar**.

Una vez que se hayan establecido estas directivas en la consola de Studio, las claves de Bloomberg se presentarán automáticamente en las sesiones de HDX y no se requerirá ninguna acción adicional por parte del usuario final.

Configuración de una clave FIDO2 mediante redirección USB

Citrix recomienda usar la redirección de FIDO2 para usar las claves FIDO2 en las sesiones HDX. Sin embargo, puede haber situaciones en las que deba redirigir las claves FIDO2 mediante redirección USB. Aquí se incluyen casos en los que la redirección de FIDO2 no está disponible porque el cliente, el VDA o el sistema operativo no admiten la función (por ejemplo, Windows Server 2016).

También puede haber casos en los que la clave tenga varios modos habilitados, pero usted solo quiera permitir un subconjunto de ellos en sus sesiones HDX. Por ejemplo, puede que quiera permitir FIDO2 y OTP, pero bloquear la tarjeta inteligente.

En los pasos siguientes se muestra cómo puede configurar una clave FIDO2 mediante redirección USB (Yubikey vid=1050, pid=0407).

1. Active la **directiva Redirección de dispositivos USB del cliente** en **Citrix Web Studio**.
2. Modifique la directiva **Reglas de redirección de dispositivos USB del cliente** (versión 2).
    a) Establezca la información de **VID** y **PID**, así como la configuración de división del dispositivo para que la clave FIDO2 se redirija en la sesión y haga clic en **Guardar**.
    b) **Connect**: VID=1050 PID=0407 class=03 split=01 intf=00,01 #Yubikey serie 5: funciones HID de FIDO2 permitidas.

c) **Deny**: VID=1050 PID=0407 split=01 intf=02 # Yubikey serie 5: función de tarjeta inteligente bloqueada.

3. Modifique la directiva **Permitir que los dispositivos USB existentes se conecten automáticamente**.
4. Desmarque la casilla **Usar el valor predeterminado**, seleccione **Redirigir automáticamente los dispositivos USB disponibles** en el menú desplegable y haga clic en **Guardar**.
5. Modifique la directiva **Permitir que los dispositivos USB recién llegados se conecten automáticamente**.
6. Desmarque la casilla **Usar el valor predeterminado**, seleccione **Redirigir automáticamente los dispositivos USB disponibles** en el menú desplegable y haga clic en **Guardar**.

Una vez que se hayan establecido estas directivas en la consola de Studio, las claves FIDO2 se presentarán automáticamente en las sesiones de HDX y no se requerirá ninguna acción adicional por parte del usuario final.

Configuración de un mouse 3D mediante redirección USB

En la actualidad, los controladores de SpaceMouse de 3DConnexion solo son compatibles con los sistemas operativos de estación de trabajo (Win10 y Win11). No funcionan con sistemas operativos de servidor. A continuación, se indican los pasos para configurar un dispositivo SpaceMouse Enterprise en un sistema operativo de estación de trabajo (vid=046D, pid=C016).

1. Instale el controlador de Windows más reciente en el host del VDA.
2. Active la **directiva Redirección de dispositivos USB del cliente** en **Citrix Web Studio**.
3. Modifique la directiva **Reglas de redirección de dispositivos USB del cliente** (**versión 2**).

   a) Establezca la información de **VID** y **PID** del panel de firmas que debe redirigirse y haga clic en **Guardar**. Por ejemplo: **Connect**: VID=046D PID=C016 #SpaceMouse Enterprise

4. Modifique la directiva **Reglas de optimización de dispositivos USB del cliente**.

   a) Configure el modo junto con otra información del dispositivo. Por ejemplo: Mode=00000004 VID=046D PID=C016 class=03 #Dispositivo de entrada funciona en modo de captura

5. Modifique la directiva **Permitir que los dispositivos USB existentes se conecten automáticamente**.
6. Desmarque la casilla **Usar el valor predeterminado**, seleccione **Redirigir automáticamente los dispositivos USB disponibles** en el menú desplegable y haga clic en **Guardar**.
7. Modifique la directiva **Permitir que los dispositivos USB recién llegados se conecten automáticamente**.

8. Desmarque la casilla **Usar el valor predeterminado**, seleccione **Redirigir automáticamente los dispositivos USB disponibles** en el menú desplegable y haga clic en **Guardar**.

Solución de problemas

August 17, 2024

Se deben seguir estos pasos para clasificar los problemas relacionados con la redirección USB:

1. Compruebe que se cumplen los requisitos del sistema para la redirección USB. Esto incluye las versiones correctas de CVAD y CWA, la compatibilidad de los dispositivos y los controladores de dispositivos en la plataforma del sistema operativo en cuestión.
2. Asegúrese de que la configuración sea adecuada conforme a las versiones y plataformas de los componentes que se usan en su entorno. Consulte la nota en Configuración de la redirección USB antigua para obtener más información sobre los componentes que requieren parámetros de configuración antiguos.
3. Compruebe que el dispositivo aparece en la lista de dispositivos que el cliente ha enumerado.
    a) Barra de herramientas Preferencias de Workspace: Consulte los dispositivos enumerados en la ficha Dispositivos de la barra de herramientas Preferencias de la aplicación Workspace (haga clic con el botón secundario en el **icono de CWA > Central de conexiones > Preferencias**…Haga clic en la ficha **Dispositivos**).
    b) `CtxUsbDiagnostics.exe` (Recomendado): Ejecute esta herramienta en una ventana del símbolo del sistema. El resultado le ofrece información específica del dispositivo para una sesión específica. Le dirá si un dispositivo se redirige o no. También le indicará si un conjunto de reglas de dispositivo está provocando que el dispositivo no se redirija. Consulte Herramienta de diagnóstico para obtener más información.
    c) USBView u otras herramientas de terceros: Ejecute una herramienta de terceros, como USBView, en el dispositivo de punto final o la máquina cliente para asegurarse de que el dispositivo se detecta en el dispositivo de punto final.
4. Si el dispositivo aparece enumerado:
    a) Si se muestra una regla Denegar (Deny) en el resultado de la herramienta CtxUsbDiagnostics con relación a un dispositivo determinado, compruebe las directivas configuradas en Studio y asegúrese de que las reglas estén configuradas correctamente en la directiva de la versión 2. Si no aparece la regla de denegación en la directiva de Studio, compruebe la directiva del lado del cliente y, por último, la configuración predeterminada del lado del cliente en ese orden para encontrar la regla de denegación correspondiente.

b) Si no hay ninguna regla de denegación en el resultado de CtxUsbDiagnostics, CWA permitirá la redirección del dispositivo marcando o haciendo clic en el botón correspondiente de la ficha Dispositivos de la ventana Preferencias (Dispositivos > Administrar dispositivos). Una vez redirigido, un dispositivo estará disponible en la sesión. Esto se puede verificar comprobando el administrador de dispositivos, USBView o una aplicación similar en la sesión HDX.

5. Si el dispositivo no está presente en la sesión:

   a) Es posible que no esté instalado el controlador de dispositivo correcto en el host del VDA. Asegúrese de que las versiones más recientes de los controladores de dispositivos estén instaladas correctamente en el host del VDA. Algunos controladores de dispositivos no son compatibles con máquinas de servidores Terminal Server; por tanto, asegúrese de que no sea este el caso del dispositivo que está intentando redirigir.

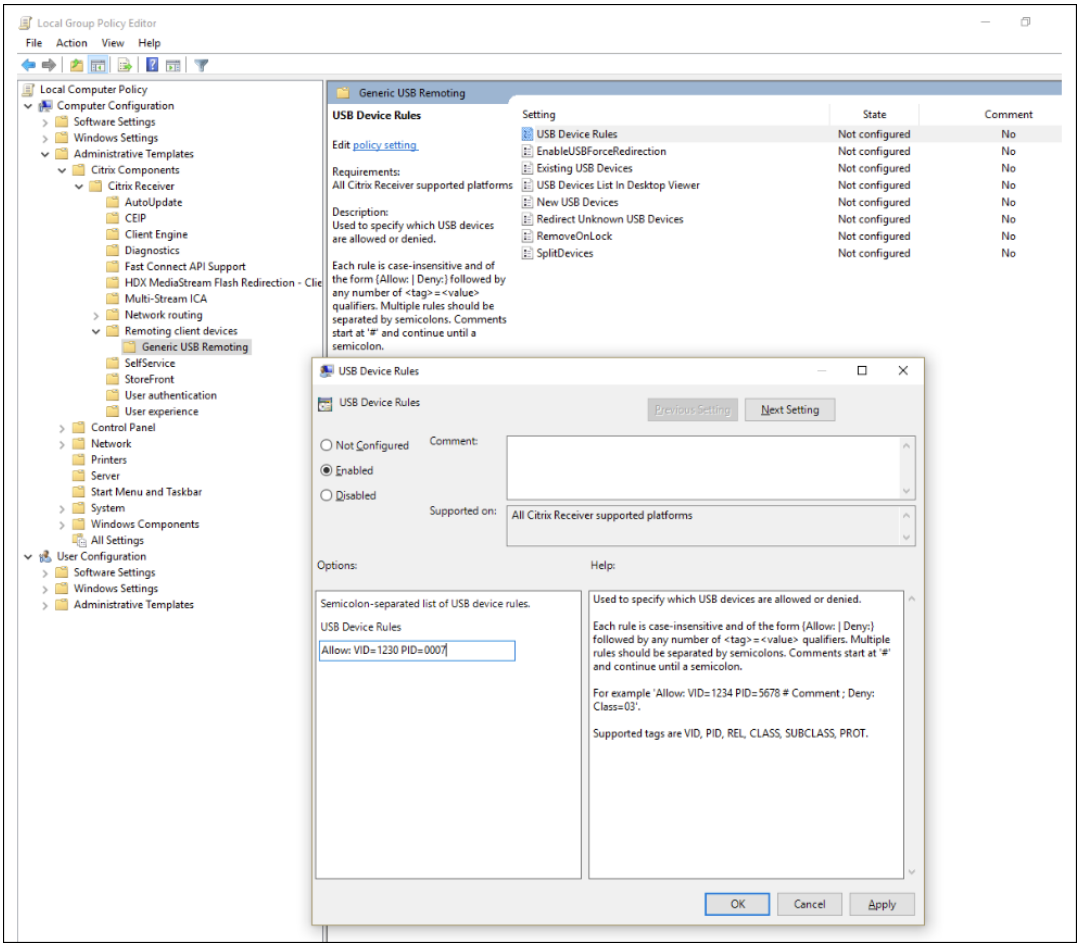
   b) Asegúrese de que el dispositivo no se está usando en el dispositivo de punto final del cliente. Algunos dispositivos también requieren la instalación de controladores en el dispositivo de punto final del cliente, lo que podría impedir que se redirijan en la sesión.

6. Compruebe que las reglas relacionadas con USB estén configuradas correctamente en el dispositivo de punto final del cliente:

   a) **CWA para Windows**:

      i. Compruebe que la directiva de grupo del cliente (agregue más detalles y SS para ello) esté configurada correctamente y no entre en conflicto con las reglas establecidas en Studio.

      ii. Valide esas reglas predeterminadas en el Registro del cliente.



(`HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`) are appropriately set and not in conflict with the rules set in Studio and client group policy.

b) CWA para Linux: Para clasificar los problemas de CWA para Linux, consulte la documentación de USB de CWA para Linux

c) CWA para Mac: Para clasificar los problemas de CWA para Mac, consulte CWA para Mac

Nota:

- En TSVDA, el uso de redirección USB está bloqueado de forma predeterminada para los dispositivos de audio. La forma recomendada de usar esos dispositivos es con Audio VC optimizado.
- A veces, es posible que los dispositivos compuestos USB no se dividan automáticamente aunque se haya establecido una regla de redireccionamiento de dispositivos correcta para dividir el dispositivo. Este problema se produce porque el dispositivo está en modo de bajo consumo. En estos casos, es posible que el dispositivo secundario que entra en el modo

de bajo consumo no esté presente en la lista de dispositivos. Puede utilizar las siguientes soluciones temporales para solucionar este problema:

- Desconecte la sesión, inserte el dispositivo USB y vuelva a conectarse a la sesión.

- Desenchufe el dispositivo USB y vuelva a conectarlo. Esta acción hace que el dispositivo salga del modo de bajo consumo.

- En ocasiones, es posible que la configuración del ahorro de batería con USB esté habilitada para optimizar la duración de la batería. Si el dispositivo de punto final del cliente entra en modo de suspensión, es posible que el dispositivo USB se desconecte. En tal caso, es posible que tenga que desconectar y reconectar el dispositivo para presentarlo de nuevo en la sesión.

Registros de eventos

Los administradores ahora pueden supervisar los dispositivos no autorizados que los usuarios puedan intentar redirigir y adoptar las medidas necesarias. Estos son algunos de los mensajes sobre eventos que se registrarán en el Visor de eventos del host del VDA para los dispositivos que se pueden redirigir y para los dispositivos que no.

Id	1000
Name	UsbEventAcceptDevice
Severity	Informational
Facility	System
Text	The Citrix USB Service allows the USB Device with Product ID: %2, Vendor ID: %3, and Device ID: %4 to be remoted.
Comment	This message logs the device info of a device redirected in an HDX session

Id	1001
Name	UsbEventPolicyRejectsDeviceV1
Severity	Warning
Facility	System
Text	The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules" policy in Citrix Studio.
Comment	This message displays a message of the device not getting redirected if a DENY rule is being enforced by the legacy “Client USB device redirection rules” policy rule.
Arguments	

Id	1002
Name	UsbEventPolicyRejectsDeviceV2
Severity	Warning
Facility	System
Text	The USB device with Product ID: 0x%2, Vendor ID: 0x%3, and Device ID: 0x%4 is not being redirected because the Citrix USB policy, "DENY: ...%5..." is in effect. If you wish to redirect the device, please set an allow rule that matches the device in the "Client USB device redirection rules (Version 2)" policy in Citrix Studio.
Comment	This message displays a message of the device not getting redirected if a DENY rule is being enforced by the "Client USB device redirection rules (Version 2)" policy rule. For instance, if the studio policy rule allows an approved set of devices and denies all other devices and an end user tries to create a new rule on the client endpoint via group policy, this event will get logged. This message would be indicative of an unauthorized device redirection attempt.
Arguments	

Herramienta de diagnóstico USB

August 17, 2024

`CtxUsbDiagnostics.exe` es una herramienta de línea de comandos del VDA que ayuda a los administradores de Citrix a diagnosticar y resolver de forma rápida los problemas de redirección de dispositivos USB que se producen en el cliente. Esta herramienta recopila la información más importante necesaria para clasificar los problemas de configuración asociados a los dispositivos USB conectados al cliente que no se redirigen dentro de una sesión HDX.

```
> **Note :**
>
> Running Command Prompt or Powershell as an administrator is required to ensure the tool has the necessary permissions to perform system-level operations.
```


Requisitos

Host de la sesión

- Sistema operativo
  - Windows 10 1809 o una versión posterior
  - Windows 11 21H2 o posterior
  - Windows Server 2016 o una versión posterior
- VDA
  - Windows: Citrix Virtual Apps and Desktops, versión 2311 o posterior

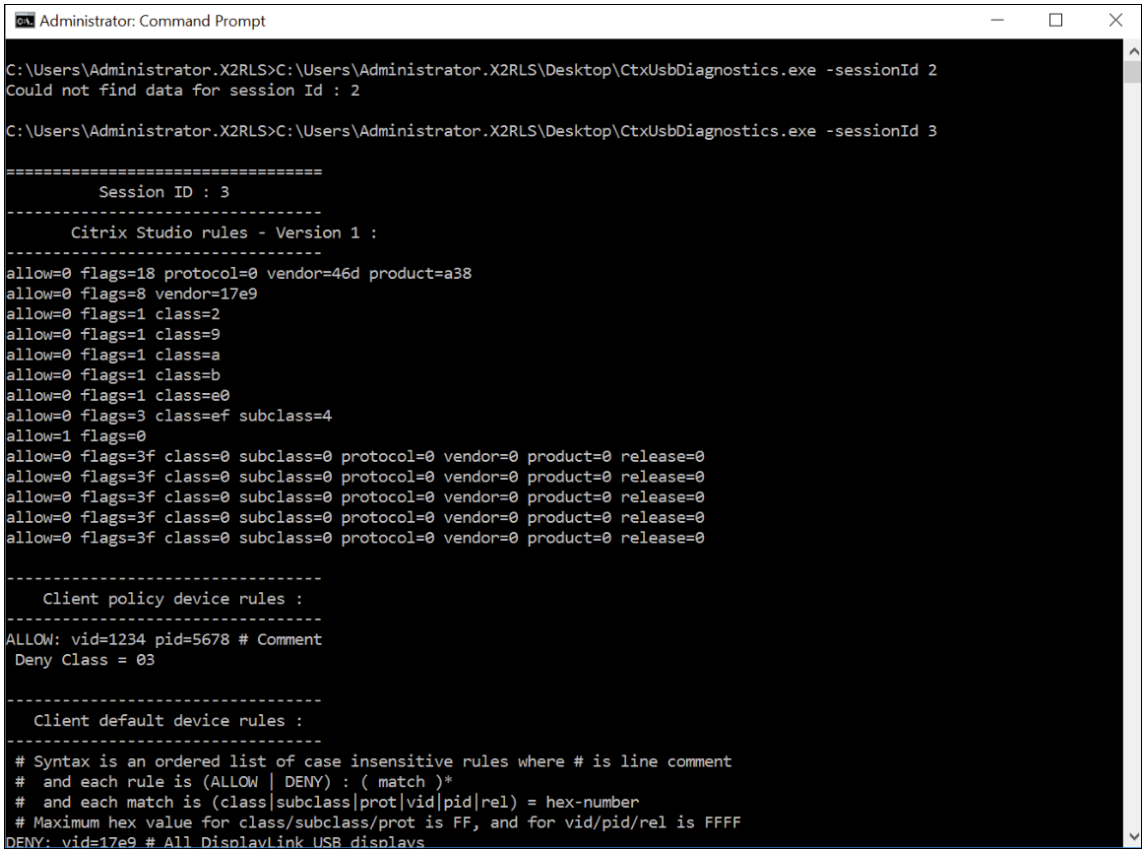
Dispositivo cliente

- Sistema operativo
  - Windows 10 1809 o una versión posterior
- Aplicación Workspace
  - Windows: versión 2311 o posterior

¿Para qué sirve la herramienta?

La herramienta actualmente proporciona:

- SessionID
- Directivas de dispositivos de VDA (reglas de dispositivo definidas en Studio)
- Dispositivos cliente y directivas de dispositivos cliente (reglas de dispositivos)
- Lista de dispositivos, su estado de redirección y motivos por los que se permitieron o rechazaron



> **Nota:**
>
> El administrador puede ver la información de los dispositivos para todas las sesiones activas.

Información mostrada

- **Reglas de Citrix Studio: Versión 1/2**
  - Las reglas de DDC indican el uso de las directivas antiguas **Reglas de redirección de dispositivos USB del cliente** o **Reglas de redirección de dispositivos USB del cliente (versión 2)** en Studio. La información que aparece en esta sección muestra todas las reglas configuradas por el administrador de Citrix.

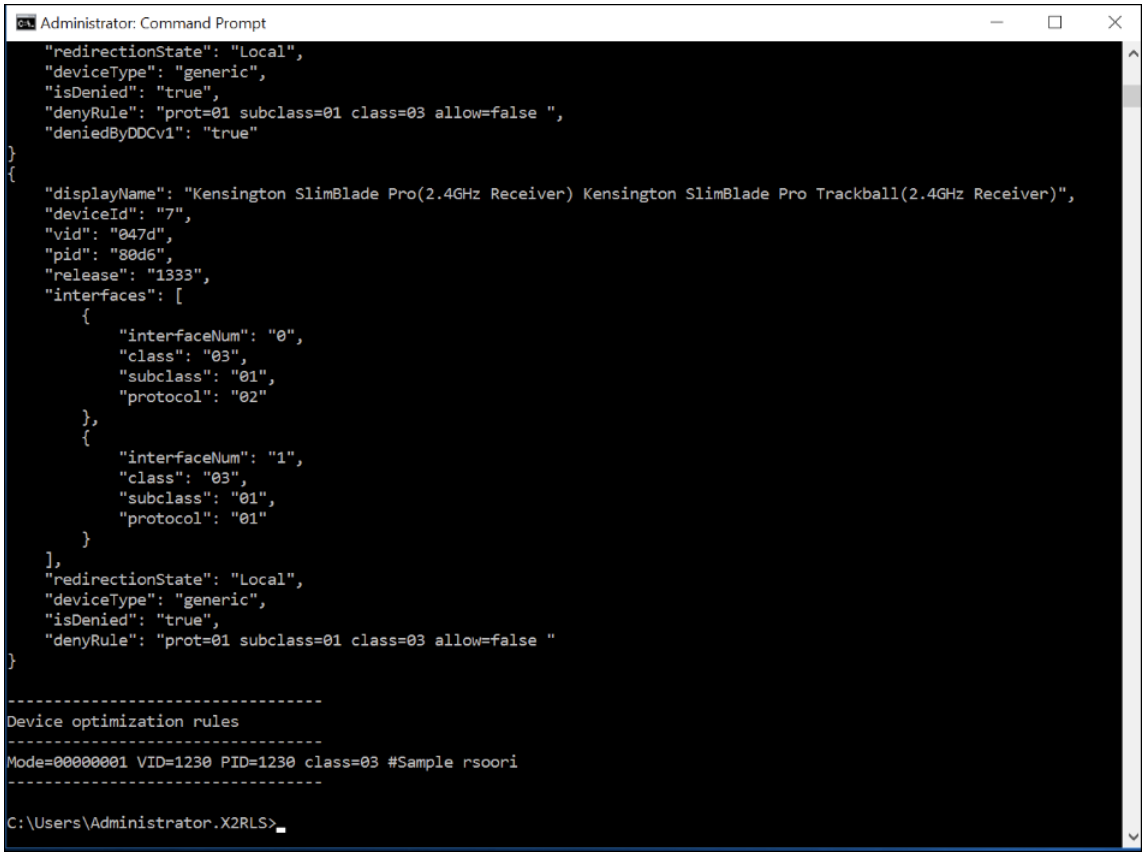

```
C:\Program Files\Citrix\HDX\bin>CtxUsbDiagnostics.exe

---------------------------------
          Session ID : 1
---------------------------------
       Citrix Studio rules - Version 2 :
---------------------------------
DENY: vid=046D pid=0A38
# Block some devices we never want to see
DENY: vid=17e9 # All DisplayLink USB displays
```

- **Reglas de dispositivo predeterminadas del cliente**
  - En esta sección se enumeran las reglas que se establecen en el Registro del cliente.

```
---------------------------------
   Client default device rules :
---------------------------------
 # Syntax is an ordered list of case insensitive rules where # is line comment
 #  and each rule is (ALLOW | DENY) : ( match )*
 #  and each match is (class|subclass|prot|vid|pid|rel) = hex-number
 # Maximum hex value for class/subclass/prot is FF, and for vid/pid/rel is FFFF
DENY: vid=17e9 # All DisplayLink USB displays
CONNECT: vid=1188 pid=A101 # Bloomberg 5 Biometric module
DENY: vid=1188 pid=A001 split=01 intf=00 # Bloomberg 5 Primary keyboard
CONNECT: vid=1188 pid=A001 split=01 intf=01 # Bloomberg 5 Keyboard HID
DENY: vid=1188 pid=A301 split=01 intf=02 # Bloomberg 5 Keyboard Audio Channel
CONNECT: vid=1188 pid=A301 split=01 intf=00,01 # Bloomberg 5 Keyboard Audio HID
DENY: class=02 # Communications and CDC-Control
DENY: class=09 # Hub devices
DENY:vid=045e pid=079A # Microsoft Surface Pro 1 Touch Cover
DENY:vid=045e pid=079c # Microsoft Surface Pro 1 Type Cover
DENY:vid=045e pid=07dc # Microsoft Surface Pro 3 Type Cover
DENY:vid=045e pid=07dd # Microsoft Surface Pro JP 3 Type Cover
DENY:vid=045e pid=07de # Microsoft Surface Pro 3_2 Type Cover
DENY:vid=045e pid=07e2 # Microsoft Surface Pro 3 Type Cover
DENY:vid=045e pid=07e4 # Microsoft Surface Pro 4 Type Cover with fingerprint reader
DENY:vid=045e pid=07e8 # Microsoft Surface Pro 4_2 Type Cover
DENY:vid=03eb pid=8209 # Surface Pro Atmel maXTouch Digitizer
ALLOW:vid=056a pid=0315 class=03 # Wacom Intuos tablet
ALLOW:vid=056a pid=0314 class=03 # Wacom Intuos tablet
ALLOW:vid=056a pid=00fb class=03 # Wacom DTU tablet
DENY: class=03 subclass=01 prot=01 # HID Boot keyboards
DENY: class=03 subclass=01 prot=02 # HID Boot mice
DENY: class=0a # CDC-Data
DENY: class=0b # Smartcard
DENY: class=e0 # Wireless controller
DENY: class=ef subclass=04 # Miscellaneous network devices
ALLOW: # Otherwise allow everything else
```

- **Reglas de optimización de dispositivos**
  - La sección enumera las reglas de optimización del dispositivo tal como se establece en "Reglas de optimización de dispositivos USB del cliente".



Lista de dispositivos

En esta sección se incluye información valiosa sobre cada dispositivo que está conectado al dispositivo de punto final del cliente, la información del hardware, si se redirige o no, si se estableció la regla de redirección de dispositivos correcta o no, etc.

Nombre de la etiqueta	Descripción
displayName	Muestra el nombre común del dispositivo.
vid	ID de proveedor
pid	ID del producto
Interfaces	En esta subsección se enumeran todas las interfaces en caso de que el dispositivo compuesto se haya dividido en varios dispositivos secundarios.
InterfaceNum	Indica el índice del descriptor de la interfaz
class	Código de clase

Nombre de la etiqueta	Descripción
subclass	Código de subclase
protocolo	Protocolo
redirectionState	**Local**indica que el dispositivo no se redirige en la sesión ICA. **ThisSession**indica que el dispositivo se redirige en la sesión ICA. **OtherSession**indica que el dispositivo se redirige en otra sesión ICA.
optiEnabled	**true**indica que el dispositivo está optimizado. **false** indica que el dispositivo no está optimizado y que la transferencia de datos se realiza a través del canal virtual USB.
deviceType	**genérico** indica que el dispositivo no tiene un canal virtual optimizado y que el tráfico fluye a través del canal virtual USB. **optimizado** implica que la transferencia de datos asociada al dispositivo se realiza a través de un canal virtual dedicado.
isDenied	**true**indica que el dispositivo no se redirige debido a una regla de directiva establecida por el administrador. `false` indica que el dispositivo se redirige debido a la directiva aplicada.
denyRule	Este campo es útil si **isDenied** se establece en `true`. Le indica al administrador la regla específica establecida en la directiva que hace que el dispositivo no se redirija.

Configuración de la redirección USB antigua

August 17, 2024

Si usa algún componente anterior a la versión 2212 o CWA para Linux, siga esta guía para configurar la redirección USB en su entorno.

Habilitar la redirección de USB genérico

1. Abra las **directivas de Citrix Web Studio** y haga clic en la ficha **Directivas** .
2. Haga clic en **Crear directiva** y expanda las **directivas ICA > Dispositivos USB**.
3. Modifique la **directiva Redirección de dispositivos USB del cliente**.
4. Seleccione **Permitida** y haga clic en **Guardar**.

Creación de reglas de directiva de redirección USB

Cuando el usuario intenta redirigir un dispositivo USB a un escritorio virtual, se coteja sucesivamente cada regla de directiva USB hasta que encuentra una coincidencia. La primera coincidencia para cualquier dispositivo se considera definitiva. Si la primera coincidencia es una regla para Permitir, se autoriza la redirección del dispositivo al escritorio virtual. Si la primera coincidencia es una regla para Denegar, el dispositivo solamente está disponible en el escritorio local. Si no hay coincidencias, se usan las reglas predeterminadas.

Configuración de la directiva en el DDC:

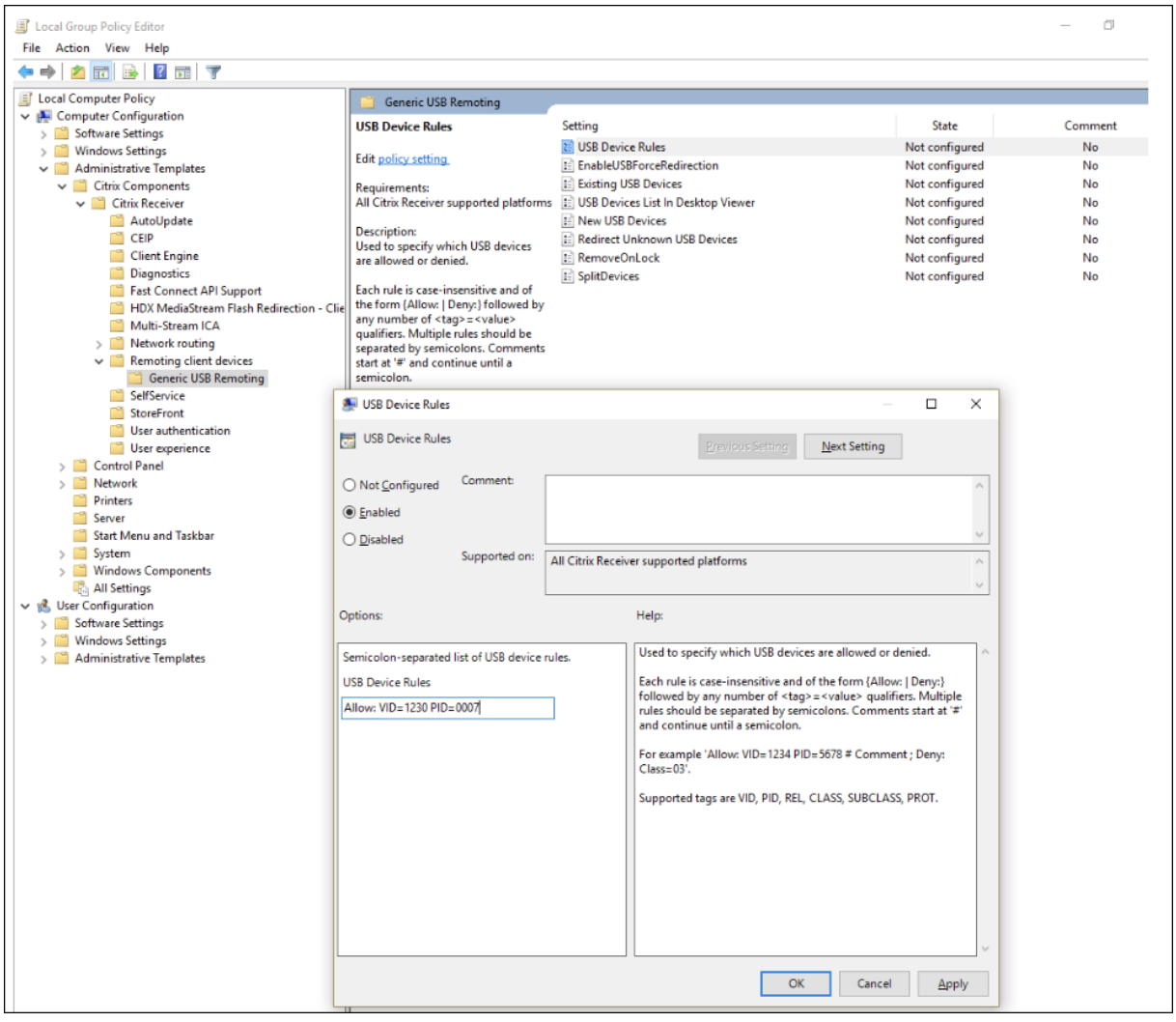
1. Abra las **directivas de Citrix Web Studio** y haga clic en la ficha **Directivas** .
2. Haga clic en **Crear directiva** y expanda las **directivas ICA > Dispositivos USB**.
3. Modifique las **Reglas de redirección de dispositivos USB del cliente**.
4. Establezca el valor conforme a los ejemplos proporcionados en la descripción de cada dispositivo USB que necesite redirigirse y haga clic en Guardar.
   Por ejemplo:
   Allow: VID=056A PID=00A4 #STU-430
   Deny: Class=08 subclass=05 # Almacenamiento masivo

   > **Nota:**
   >
   > Si un administrador de Citrix marca la casilla Usar el valor predeterminado y hace clic en Guardar, las reglas predeterminadas se encuentran en el siguiente registro del VDA.
   >
   > **Precaución:**
   >
   > Consulte la renuncia de responsabilidades al final de este artículo antes de usar el Editor del Registro.
   > `HKLM\SOFTWARE\Wow6432Node\Citrix\PortICA\GenericUSB\DeviceRules`

Uso de objetos de directiva de grupo en el cliente:

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 el **parámetro Reglas de dispositivos USB** y habilítelo. Agregue la regla de dispositivo USB como en este ejemplo:
   La regla Allow: VID=1230 PID=0007 permite el dispositivo con el ID de proveedor 1230 y el ID de producto 0007.

> **Nota:**
>
> Usa la regla Allow: VID=xxxx PID=xxxx cuando un dispositivo específico deba estar en la parte superior de la lista de reglas de dispositivos.



> **Nota:**
>
> Se puede usar una herramienta como USBView o incluso la barra de herramientas de conexión

> para determinar los detalles del dispositivo, como VID y PID (incluya SS aquí).

Configurar redirección automática de dispositivos USB

Los dispositivos USB se redirigen automáticamente cuando se habilita la compatibilidad con USB. Además, la configuración de preferencias de usuario de USB está definida para conectar automáticamente dispositivos USB. 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 aparezcan en la lista o se redirijan, utilice DeviceRules en el dispositivo de punto final del cliente o en la directiva de DDC.

Esta directiva se puede configurar en el DDC, en el cliente mediante un objeto de directiva de grupo, mediante las Preferencias de Citrix Workspace o en la ficha Conexiones, en CDViewer. Todos estos métodos se describen a continuación:

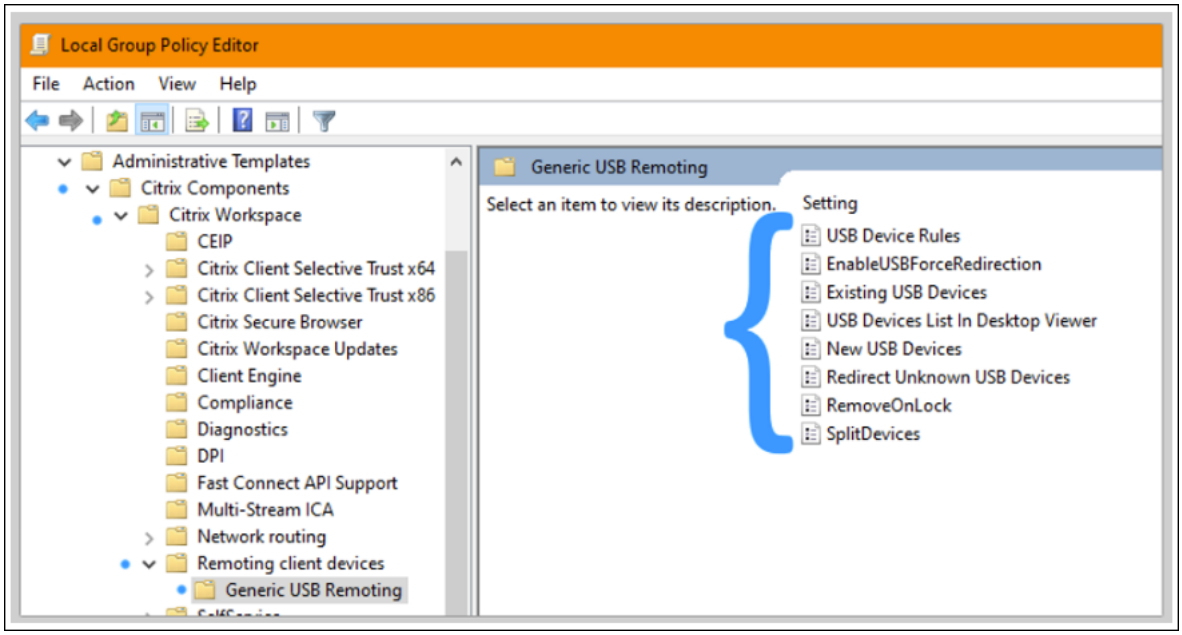
Configuración de la directiva en el DDC:

Hay dos directivas en el DDC que se pueden configurar para permitir la redirección automática de dispositivos USB: "Permitir que los dispositivos USB existentes se conecten automáticamente"y "Permitir que los dispositivos USB recién llegados se conecten automáticamente"

1. Abra las **directivas de Citrix Web Studio** y haga clic en la ficha **Directivas** .
2. Haga clic en **Crear directiva** y expanda las **directivas ICA > Dispositivos USB**.
3. Modifique el parámetro **Permitir que los dispositivos USB existentes se conecten automáticamente**.
4. Desmarque la casilla **Usar el valor predeterminado**, seleccione **Redirigir automáticamente los dispositivos USB disponibles** en el menú desplegable y haga clic en **Guardar**.
5. Modifique el parámetro **Permitir que los dispositivos USB recién llegados se conecten automáticamente**.
6. Desmarque la casilla **Usar el valor predeterminado**, seleccione **Redirigir automáticamente los dispositivos USB disponibles** en el menú desplegable y haga clic en **Guardar**.

Uso de objetos de directiva de grupo en el cliente:

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**.



Uso de Central de conexiones de Citrix:

1. Vaya a **Preferencias de Citrix Workspace > Conexiones**.
2. Asegúrese de que las siguientes opciones estén seleccionadas:

    a) Al iniciar una sesión, conectar los dispositivos automáticamente
    b) Cuando se conecta un nuevo dispositivo mientras se ejecuta una sesión, conectar el dispositivo automáticamente.

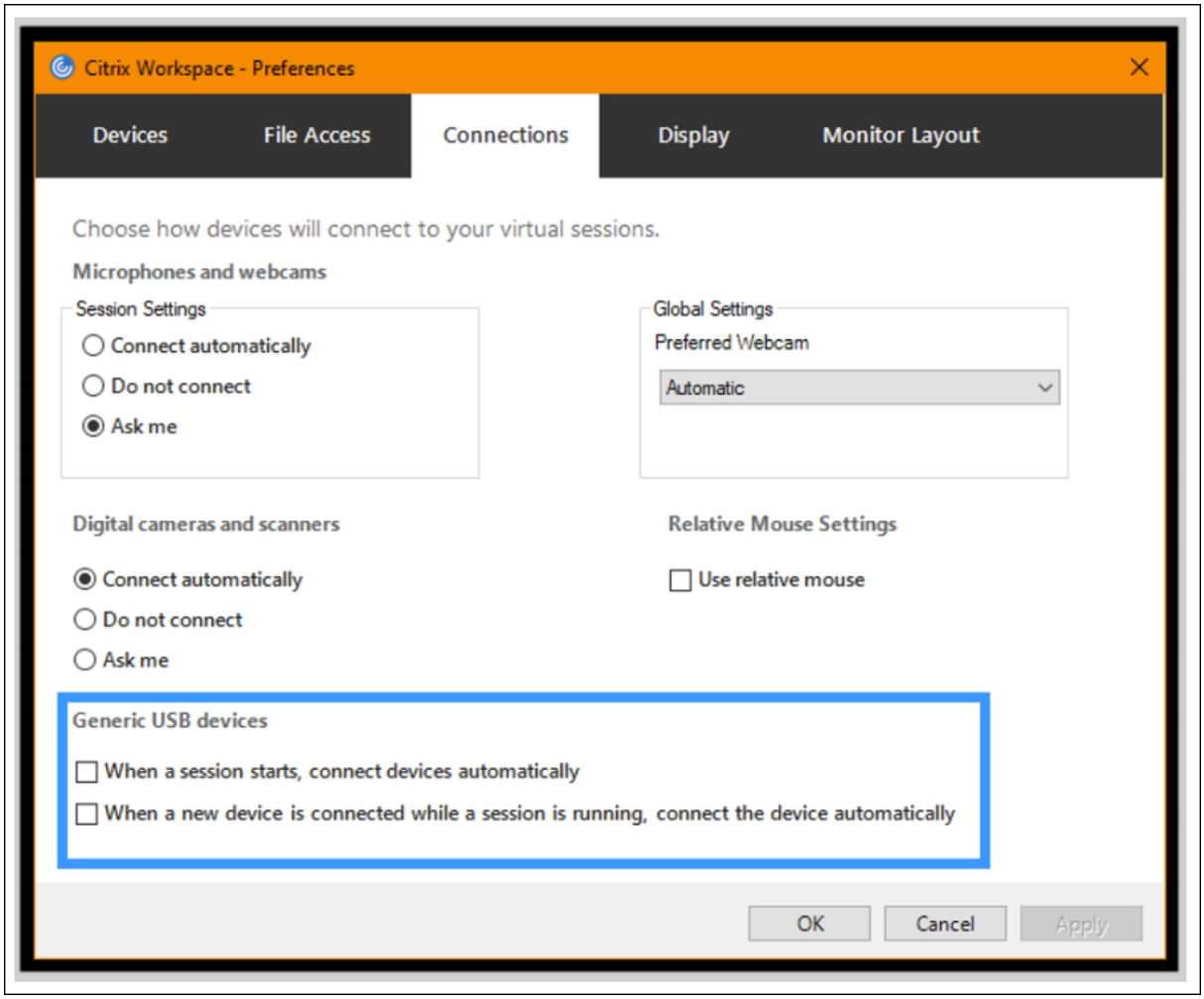
3. Haga clic en **Aceptar**.

Uso de la barra de herramientas Conexión de CDViewer:

1. Tras iniciarse una sesión, haga clic en el menú desplegable **CDViewer** y seleccione la ficha **Preferencias de Citrix Workspace > Conexiones**.
2. Asegúrese de que las siguientes opciones estén seleccionadas:

    a) Al iniciar una sesión, conectar los dispositivos automáticamente
    b) Cuando se conecta un nuevo dispositivo mientras se ejecuta una sesión, conectar el dispositivo automáticamente.

3. Haga clic en **Aplicar** y **Aceptar** para guardar la directiva.



Para las configuraciones basadas en el cliente, las claves de Registro se establecen en el dispositivo cliente en la siguiente ubicación:

> **Precaución:**
>
> Consulte la renuncia de responsabilidades al final de este artículo antes de usar el Editor del Registro.
>
> `HKLM\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB`

Asignación de unidades del cliente (CDM)

August 17, 2024

La asignación de unidades del cliente hace que las unidades de almacenamiento del dispositivo de punto final del cliente estén disponibles dentro de una sesión de Citrix HDX para permitir la transferencia de archivos y carpetas del cliente al host de la sesión, y viceversa. Esta función está habilitada

de forma predeterminada con privilegios de lectura y escritura. 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 este parámetro a una directiva, compruebe que el parámetro **Redirección de unidades del cliente** está establecida en **Permitida** y también se ha agregado a la directiva.

Como medida de seguridad, las unidades de los dispositivos de punto final se asignan sin el permiso de ejecución de forma predeterminada. Para permitir a los usuarios ejecutar ejecutables directamente desde las unidades de cliente asignadas, modifique el valor de Registro **ExecuteFromMappedDrive** en el host de la sesión. Para obtener información, consulte Unidades de cliente asignadas en la sección de **funciones HDX administradas a través del Registro**.

Requisitos

Estos son los requisitos para usar CDM:

Plano de control de Citrix

- Citrix Virtual Apps and Desktops 1912 o versiones posteriores
- Citrix DaaS

Host de la sesión

- Sistema operativo
  - Windows 10 1809 o una versión posterior
  - Windows Server 2016 o una versión posterior
  - Linux: Consulte los requisitos del sistema de Linux VDA
- VDA
  - Windows: Citrix Virtual Apps and Desktops 1912 o versiones posteriores.
  - Linux: Consulte la documentación de Linux VDA

Dispositivo cliente

- Sistema operativo
  - Windows 10 1809 o una versión posterior
  - Linux: Consulte los requisitos del sistema de la aplicación Workspace para Linux.

Directivas relacionadas

Con relación a los parámetros de CDM, consulte la sección Referencia para configuración de directivas.

Supuestos de doble salto

CDM es compatible con supuestos de doble salto. De forma predeterminada, la unidad del dispositivo de punto final del cliente se asigna a la sesión del segundo salto y las unidades del primer salto no están disponibles. Sin embargo, se puede configurar de manera que las unidades del primer salto se asignen en la sesión del segundo salto, en lugar de las unidades del dispositivo de punto final del cliente.

Para configurar esta funcionalidad, modifique este valor de Registro:

- Clave: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advance
- Nombre del valor: NativeDriveMapping
- Tipo de valor: REG_SZ
- Información del valor:
  - True: Asigna las unidades de la sesión del primer salto en la sesión del segundo salto
  - False: Asigna las unidades del dispositivo de punto final del cliente en la sesión del segundo salto

> **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 usa el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Compatibilidad con dispositivos cliente móviles y con pantalla táctil

August 17, 2024

Citrix Virtual Apps and Desktops permite a los usuarios acceder a sus aplicaciones y escritorios publicados desde dispositivos cliente móviles y con pantalla táctil.

Requisitos

Plano de control de Citrix

- Citrix Virtual Apps and Desktops 1912 o versiones posteriores
- Citrix DaaS

Host de la sesión

- Sistema operativo
  - Windows 10 1903 o una versión posterior
  - Windows 11 21H2 o posterior
- VDA
  - Windows: Citrix Virtual Apps and Desktops, versión 7.15 o posterior

Dispositivo cliente

- Sistema operativo
  - Windows 10 1809 o una versión posterior
  - Windows 11 21H2 o posterior
- Aplicación Citrix Workspace para Windows, versión 1808 o posterior

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. Cuando el VDA detecta la presencia de un teclado o mouse en un cliente táctil, coloca al cliente en el modo escritorio. Si el teclado o el mouse no están presentes, el VDA coloca al cliente en el modo móvil o tableta. Esta detección se produce al conectarse y al reconectarse sesiones, y también durante las sesiones, cuando el teclado o el mouse se conectan o se desconectan.

Esta función está habilitada de forma predeterminada. Para inhabilitar esta función, defina la configuración de directiva Cambiar modo tableta (configuración de directiva).

Además de los requisitos para los dispositivos de pantalla táctil mencionados anteriormente, se requieren estos requisitos para Windows Continuum:

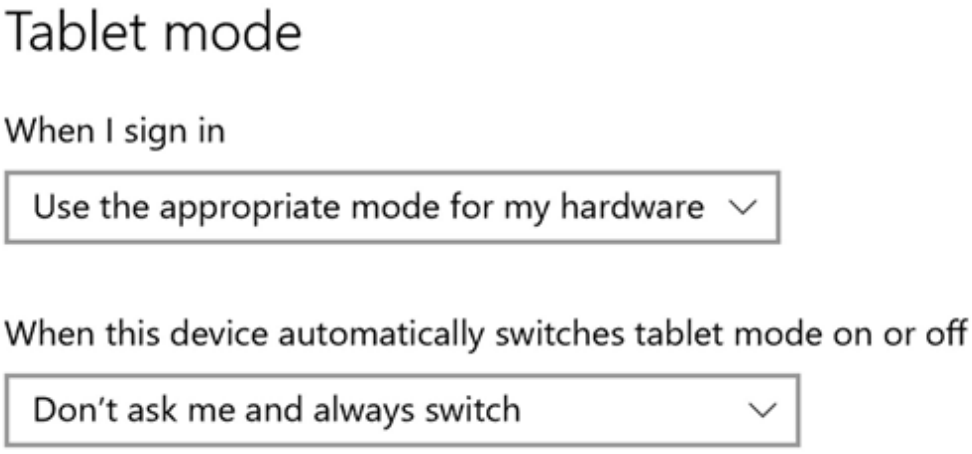
XenServer (anteriormente Citrix Hypervisor)

- Citrix Hypervisor 8.2 o una versión posterior
- 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 aprovisione una nueva máquina con Machine Creation Services (MCS).

Host de la sesión

- Sistema operativo
  - Windows 10 1903 o una versión posterior
  - Windows 11 21H2 o posterior
- VDA
  - Windows: Versión 7.16 o una posterior
  - **Debido a las limitaciones actuales en las configuraciones del sistema operativo, los usuarios tendrán que configurar estas opciones en los menús desplegables después de iniciar la primera sesión ICA y reiniciar el VDA:**
    - **Parámetros > Sistema > Modo tableta**
      - Usar el modo adecuado para mi hardware
      - No preguntarme y cambiar siempre



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.

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 no admite las funciones de Windows Continuum.

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.

Lápices para Microsoft Surface Pro y Surface Book

Se admite la funcionalidad de lápiz estándar en aplicaciones basadas en Windows Ink. 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.

Estos son los requisitos para la funcionalidad del lápiz:

Plano de control de Citrix

- Citrix Virtual Apps and Desktops 1903 o una versión posterior
- Citrix DaaS

Host de la sesión

- Sistema operativo
  - Windows 10 1809 o una versión posterior
  - Windows 11 21H2 o posterior
- VDA
  - Windows: Citrix Virtual Apps and Desktops, versión 1903 o posterior

Dispositivo cliente

- Sistema operativo
  - Windows 10 1809 o una versión posterior
  - Windows 11 21H2 o posterior
- Aplicación Citrix Workspace para Windows 1902 o una versión posterior

Para obtener una demostración de Windows Ink y la funcionalidad del lápiz, haga clic en este gráfico:

Para habilitar o inhabilitar esta función, consulte Lápices para Microsoft Surface Pro y Surface Book en la lista de funciones administradas a través del Registro.

Problemas conocidos

Estos son problemas conocidos relacionados con la compatibilidad con lápices:

- Debido a las limitaciones del sistema operativo de Windows Server 2022, los usuarios no podrán establecer accesos directos del lápiz ni realizar ajustes en la configuración del lápiz o la tinta en el Panel de control cuando se conecten a aplicaciones o escritorios del servidor de 2022.
- Los accesos directos del lápiz no se aceptan en clientes con Windows 11 y lápiz habilitado debido a las limitaciones del sistema operativo.

Puertos serie

August 17, 2024

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.

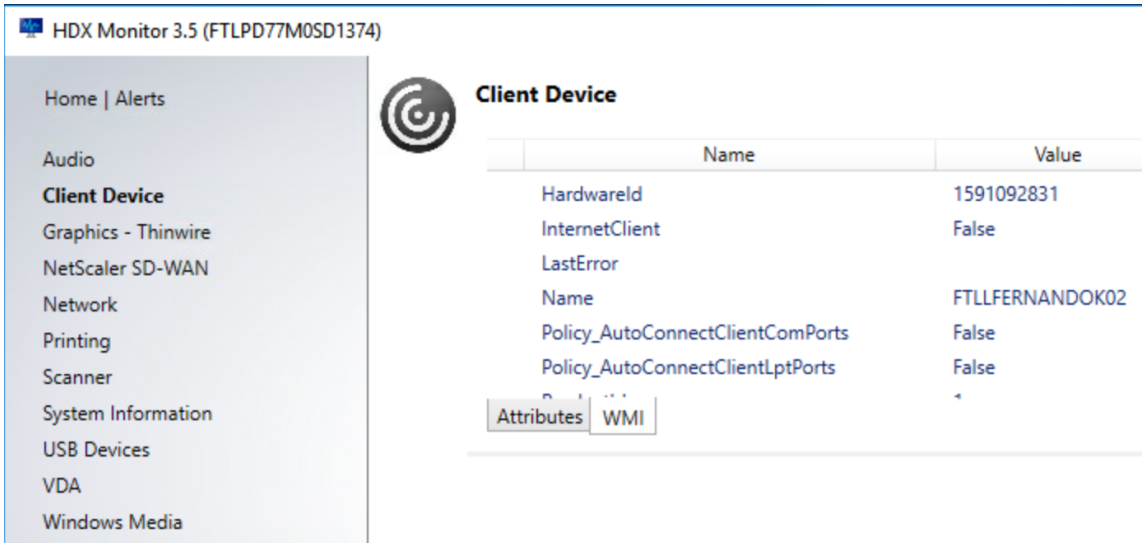
> **Importante:**
>
> El hecho de que un dispositivo se pueda conectar al dispositivo de punto final directamente por USB no significa que ese dispositivo se pueda redirigir mediante la redirección de USB genérico. Algunos dispositivos USB funcionan como puertos COM virtuales, a los que las aplicaciones 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.



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

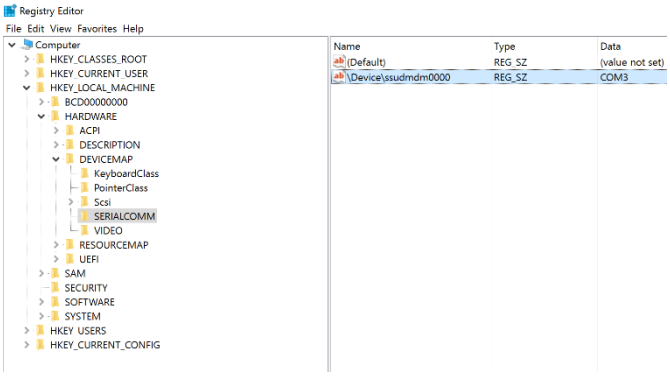
-------------------------------------------------------------------------------
             COM3      \\Client\COM3:            Citrix Client Network
```

3. 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.

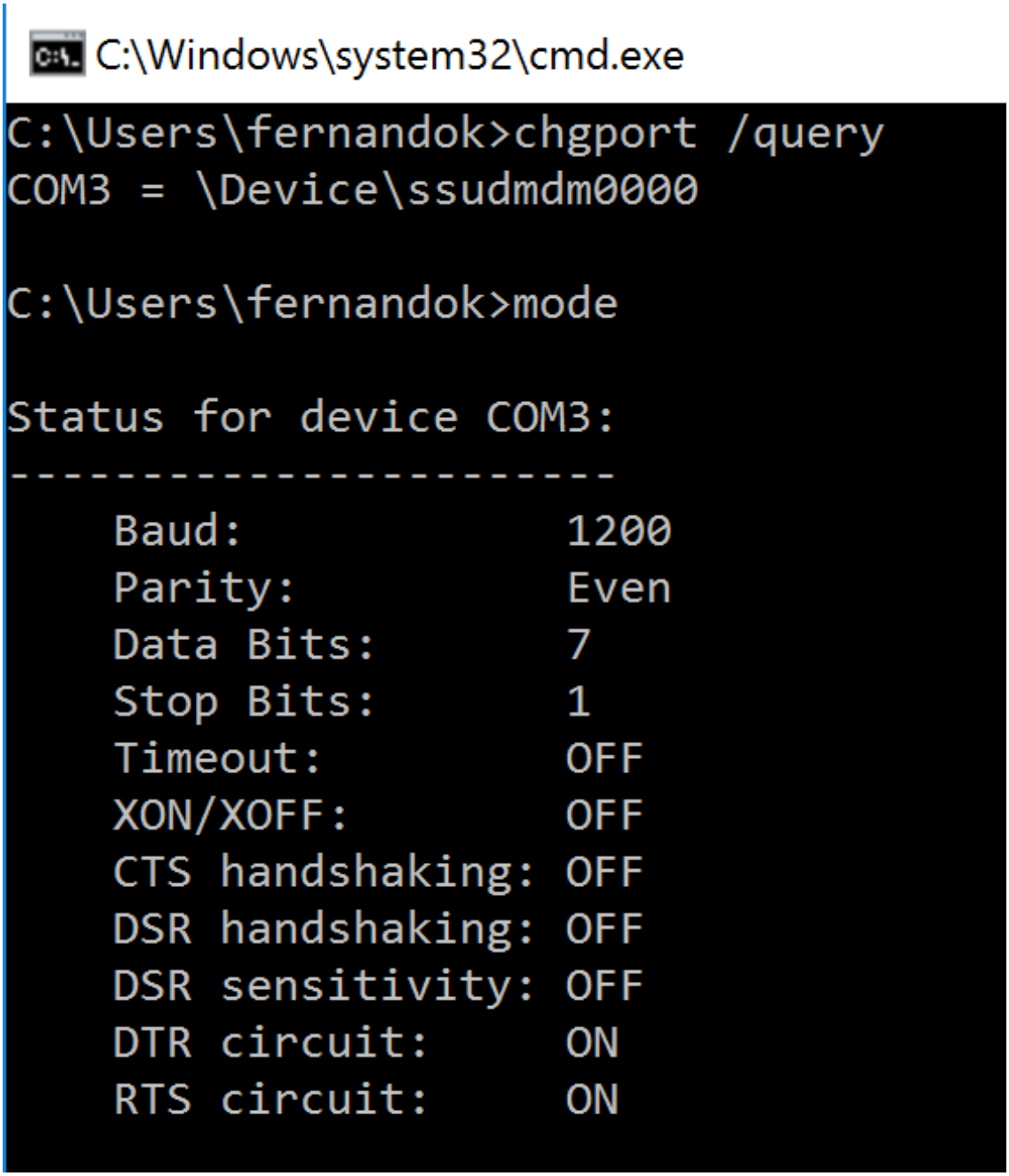
> **Importante:**
>
> La asignación de puertos COM no es compatible con TAPI. No puede asignar dispositivos Windows Telephony Application Programming Interface (TAPI) de Windows a los puertos COM del cliente. TAPI define una forma estándar que tienen las aplicaciones para controlar las funciones del 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).

Solucionar problemas

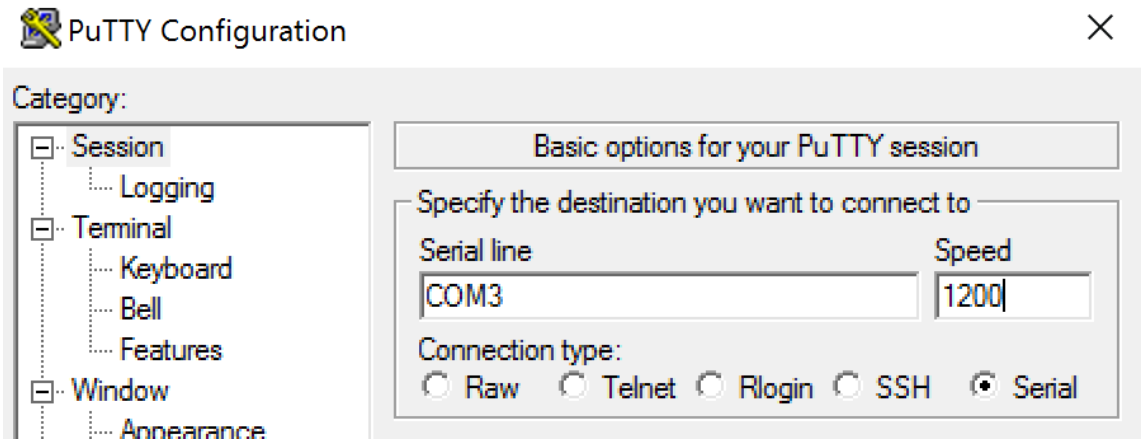
1. Compruebe que puede acceder al dispositivo directamente desde el dispositivo de punto final, sin pasar por Citrix. Mientras el puerto no se asigne al VDA, no podrá conectarse a una sesión de Citrix. Siga las instrucciones de solución de problemas incluidas con el dispositivo y primero compruebe que 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 **chgport /query**.



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 **chgport /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.

Teclados especiales

August 17, 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 usa 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 y modelo 5 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.

> **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 es un dispositivo USB compuesto que consta de varios dispositivos USB en una carcasa física:

- Teclado.
- Lector de huellas dactilares.
- Dispositivo de audio 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.
- Como mínimo la aplicación Citrix Workspace 2207 para Linux para poder usar el modelo 5 del teclado Bloomberg.
- Como mínimo la aplicación Citrix Workspace 2109 para Windows para poder usar el modelo 5 del teclado Bloomberg.
- 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.
- 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.

Para habilitar la compatibilidad con teclados Bloomberg, consulte Teclado Bloomberg en la lista de funciones administradas a través del Registro.

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:

Para el teclado Bloomberg 5:

- Módulo biométrico de Bloomberg LP
- Teclado de Bloomberg LP (dispositivo compuesto con dos interfaces)
- Audio del teclado de Bloomberg LP (dispositivo compuesto con tres interfaces)

Para teclados Bloomberg 3 y 4:

- 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.

Cámaras web

August 17, 2024

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.

Puede usar una clave del Registro para inhabilitar y habilitar la función y, a continuación, configurar una resolución específica. Para obtener más información, consulte Streaming por cámara web de alta definición y Resolución de cámara web de alta definición en la lista de funciones administradas a través del Registro.

Gráficos

August 17, 2024

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 multirruta para ofrecer una experiencia de usuario fluida e interactiva a los usuarios de aplicaciones y escritorios virtuales.

Marca de agua de texto en sesión

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.

Frecuencia de actualización adaptativa

Con las nuevas mejoras de escalabilidad, HDX ajusta la frecuencia de actualización de los monitores virtuales para que coincida con el conjunto de directivas de FPS objetivo. La frecuencia de actualización adaptativa (ARR) está disponible para VDA de sesión única y multisesión, y funciona tanto en escenarios acelerados por GPU como sin GPU.

modo tolerante a pérdidas

El modo tolerante a pérdidas se modificó a fondo para garantizar que la sesión siga siendo interactiva cuando se detecte la pérdida de paquetes.

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 texto en sesión

Alto rango dinámico (HDR) de 10 bits

August 17, 2024

Con las sesiones de escritorio virtual de alto rango dinámico (HDR) de 10 bits, puede usar funciones de codificación y descodificación mejoradas para generar imágenes y vídeos de alta calidad con una gama más amplia de colores y un mayor contraste y brillo. Además, puede personalizar el nivel de luminancia blanca, los datos de identificación de pantalla ampliados (EDID) y la calidad visual para mejorar la experiencia del usuario.

Requisitos del sistema

Dispositivo de punto final:

- Aplicación Citrix Workspace para Windows 2209 o posterior para GPU NVIDIA
- Compatibilidad de GPU de NVIDIA con la decodificación HEVC (H.265) 444 de 10 bits en dispositivos de punto final
- Monitores compatibles con HDR de 10 bits, el HDR de 10 bits debe estar habilitado en todos los monitores que usen la configuración de pantalla.

Servidor:

- Sistema operativo Windows de sesión única VDA 2209 o posterior para GPU NVIDIA y VDA 2308 o posterior para GPU Intel
- Compatibilidad de GPU de NVIDIA con la codificación HEVC 444 de 10 bits en los VDA

Directivas requeridas

Dispositivo de punto final:

- Habilitar la decodificación H.265 para gráficos

Servidor:

- Optimizar para cargas de trabajo de gráficos 3D
- Indicador de estado de gráficos (opcional)

Configuraciones de servidores

Al iniciar una sesión de Citrix con un monitor de punto final compatible con HDR de 10 bits, la sesión HDR se habilita de forma predeterminada. En las sesiones HDR con varios monitores, todos los monitores de punto final deben tener habilitado HDR de 10 bits. Las sesiones HDR son compatibles tanto en modo ventana como en pantalla completa.

Nivel del blanco de referencia

Este parámetro define el nivel de luminancia blanca por valor de nit. Controla el brillo relativo de la pantalla HDR dentro de la sesión. El valor predeterminado es de 80 nits. Configure esta clave del Registro para definir un valor de nit diferente:

- Ruta: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- Tipo: REG_DWORD
- Nombre: RefWhiteLevel

Para activar el parámetro, debe cambiar el tamaño de la sesión o desconectarla e iniciarla de nuevo.

Supeditación de EDID

Puede configurar el VDA para que utilice el EDID del monitor de punto final para sus sesiones de HDR. Esto le permite aprovechar plenamente las prestaciones visuales del monitor al equiparar la gama de colores y el intervalo de luminancia. De forma predeterminada, en las sesiones HDR se presuponen pantallas compatibles con HDR1000.
Puede exportar el EDID del monitor de punto final mediante NVIDIA u otras herramientas. Aplíquelo al VDA con esta clave del Registro:

- Ruta: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics
- Tipo: REG_BINARY
- Nombre: EDIDOverride

Al guardar el EDID en el Registro, no debe contener comas, espacios ni caracteres especiales. Para activar la supeditación del EDID, cierre sesión e inicie una nueva sesión.

Experiencia sin pérdida visual

Habilite estas directivas para obtener una experiencia sin pérdida visual:

- Permitir compresión sin pérdida visual
- Calidad visual: Siempre sin pérdida o Gradual sin pérdida

Una vez establecidas las directivas, puede controlar la calidad de la sesión HDR mediante el indicador de estado de los gráficos con el control deslizante de calidad de la imagen o al cambiar al modo de píxeles perfectos.

Permitir bloqueo de pantalla de Windows

Puede usar esta directiva para permitir que todos los tiempos de espera de visualización de Windows, incluido el bloqueo de pantalla, se apliquen a una sesión de Citrix Virtual Desktops en el sistema operativo de la estación de trabajo. Este parámetro se puede establecer mediante un objeto de directiva de grupo de Citrix en Citrix Studio.

De forma predeterminada, cuando este parámetro no está habilitado, un escritorio virtual Citrix Virtual Desktops no responde a los tiempos de espera para el bloqueo de la sesión, el protector de pantalla o el apagado de pantalla durante una sesión activa.

Cuando se configura un protector de pantalla protegido con contraseña en un VDA de estación de trabajo, este parámetro debe estar habilitado para permitir que la sesión de Citrix Virtual Desktops se bloquee automáticamente cuando se agote el tiempo de espera del protector de pantalla.

Al habilitar este parámetro cuando se configura un tiempo de espera para apagado de la pantalla en el VDA, al vencer ese tiempo de espera, la sesión no se actualiza hasta que el usuario vuelve a interactuar con la misma. Por ejemplo, la hora mostrada no se actualiza y las nuevas notificaciones no se muestran.

Otras consideraciones

- En las GPU virtuales, puede iniciar sesiones HDR de 10 bits en hasta cuatro monitores.
- La sesión de Citrix regresa al modo de 8 bits, no HDR, en estos casos:

- Si algún monitor de punto final no tiene habilitado el HDR de 10 bits
- Al habilitar la pantalla compartida.
- Al configurar un diseño de pantalla virtual en los VDA.
- Al cambiar al modo de píxeles perfectos sin configurar la directiva **Permitir compresión sin pérdida visual**.

HDX 3D Pro

August 17, 2024

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 archivado 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.

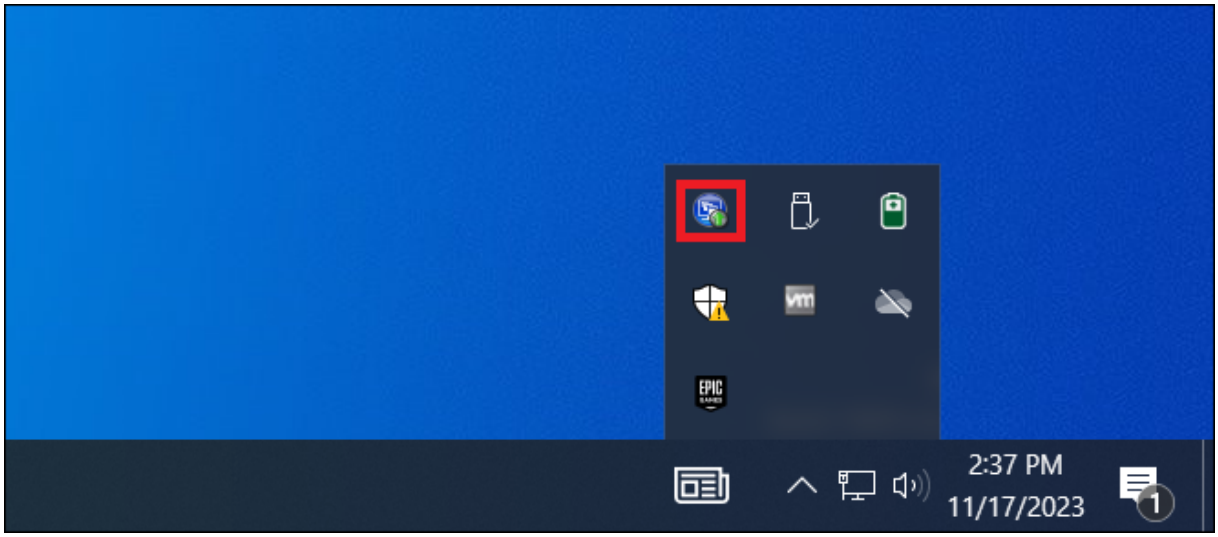
  Puede reemplazar estaciones de trabajo complejas y costosas por dispositivos de usuario más simples, al mover el procesamiento de gráficos al centro de datos para una administración centralizada.

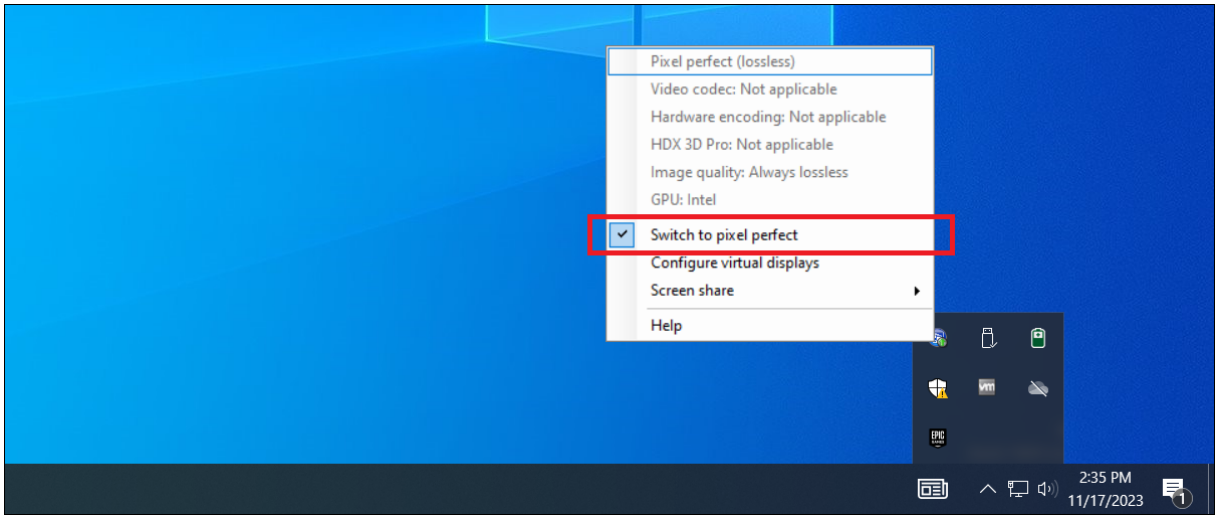
La opción de compresión sin pérdida para casos de uso especiales

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 pérdida en el Indicador del estado de los gráficos, 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 borrar la selección de la **compresión sin pérdida** en la sesión, haga clic con el botón secundario en el icono y haga clic en **Cambiar a Píxel perfecto** 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 de Registro en `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator`.

- Nombre: HKEY_LOCAL_MACHINE_HotKey, Tipo: String

El formato para configurar una combinación de atajos 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, establezca K=0x79
  para Ctrl + F10, establezca C=1, K=0x79
  para Alt + A, establezca A=1, K=A o A=1, K=A o K=A, A=1
  Para Ctrl + Alt + 5, establezca C=1, A=1, K=5 o A=1, K=5, C=1
  Para Ctrl + Shift + F5, establezca A=1, S=1, K=0x74

Optimizar la experiencia del usuario de HDX 3D Pro

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 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.
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. La herramienta está disponible en la carpeta **Support** de los medios de instalación de Citrix Virtual Apps and Desktops.

Aceleración de GPU para SO Windows multisesión

August 17, 2024

Citrix Virtual Apps and Desktops permite que las aplicaciones con muchos gráficos que se ejecutan en sesiones con SO Windows multisesión 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 puede utilizarse de manera más eficiente.

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 podrían obligar 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.

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 XenServer, 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.

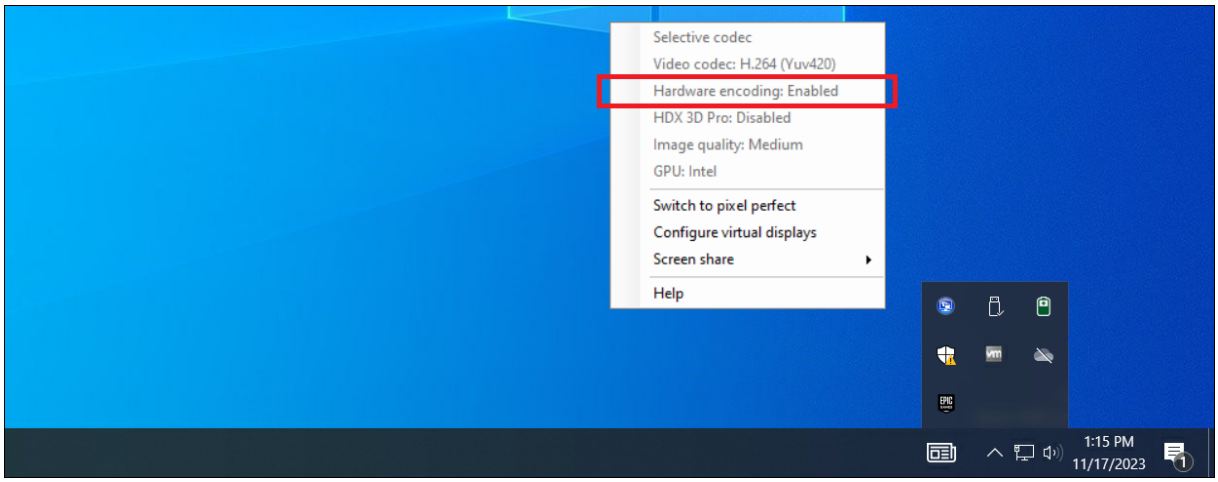
La escalabilidad mediante el uso compartido de GPU depende de varios factores:

- 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.

- 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.

Para confirmar que se está produciendo una aceleración de la GPU, se puede usar el indicador de estado 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 2016 y versiones posteriores, 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 2016 y versiones posteriores, 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 parámetros en el Registro de Windows del servidor que ejecuta sesiones de SO

multisesión Windows. Para obtener información sobre el parámetro de Registro, consulte Representación de Windows Presentation Foundation (WPF) en la lista de funciones administradas a través del Registro.

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 de aceleración de CUDA, habilite los parámetros de Registro. Para obtener información, consulte Aceleración de GPU para aplicaciones OpenCL o CUDA en la lista de funciones administradas a través del Registro.

Aceleración de GPU para SO Windows de sesión única

August 17, 2024

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 XenServer, vSphere, Nutanix y Hyper-V (solo PassThrough).

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.

> **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 usa 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 sistema operativo de sesión única, son compatibles hasta 8 monitores 4K. 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.
- 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.
- 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 e Intel Data Center GPU Flex. Para obtener más información, consulte https://www.intel.com/content/www/us/en/products/details/discrete-gpus/data-center-gpu/flex-series.html.
- Compatibilidad para GPU de AMD.

> Nota:
>
> La compatibilidad para 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 https://www.amd.com/en/graphics/workstation-virtual-graphics.

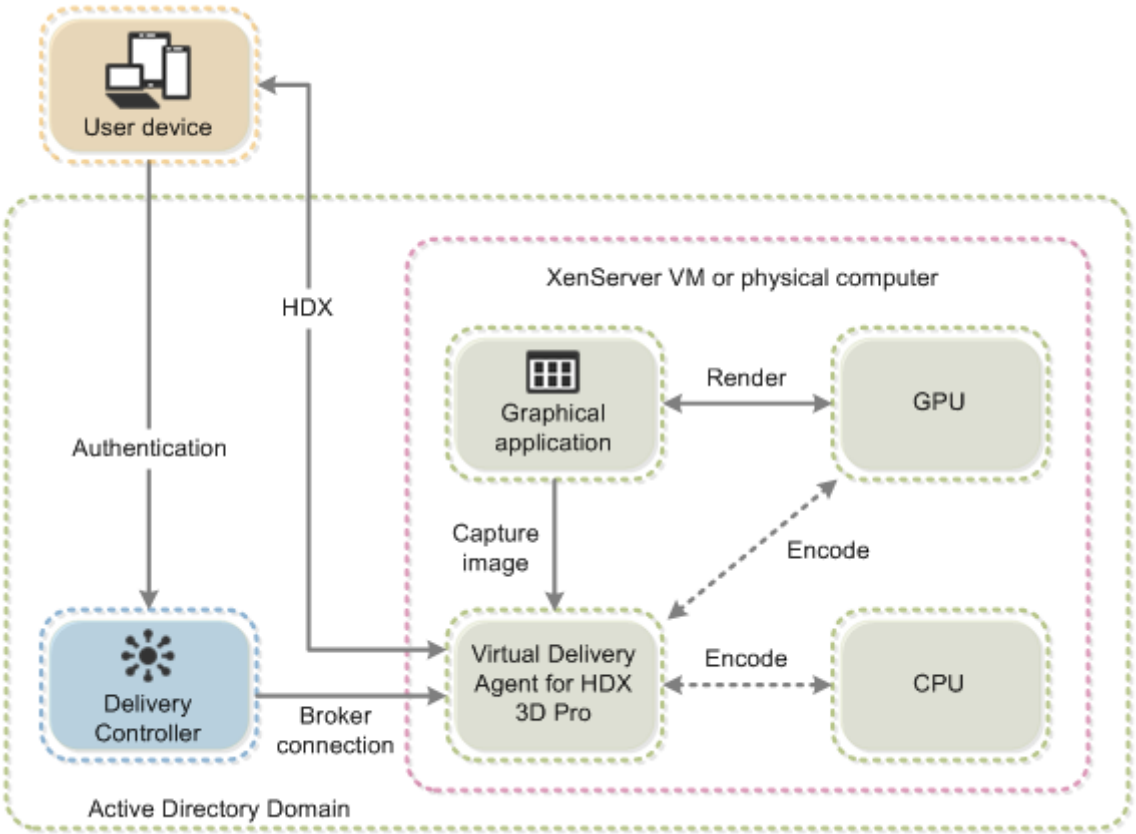
- Acceso a un codificador de vídeo de alto rendimiento para las GPU de NVIDIA, GPU de AMD y GPU de Intel. Una configuración de directiva (habilitada de forma predeterminada) controla esta función. Dicha función permite usar la codificación por hardware para la codificación H.264, H.265 o AV1 (si está 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

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.

Compresión sin pérdida

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 y haga clic en **Cambiar a Píxel perfecto** o use el acceso directo **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**.

Tecla de acceso rápido Sin pérdida

Puede usar la tecla de acceso rápido predeterminada **ALT+SHIFT+1** para seleccionar o cancelar la selección de **Sin pérdida** en cualquier momento dentro de una sesión.

Puede anular el acceso directo predeterminado, **ALT+SHIFT+1**, en el Registro de Windows.
Para configurar un nuevo parámetro del Registro, defina los siguientes valores de Registro:

- **Clave**: `HKEY_CURRENT_USER\SOFTWARE\Citrix\Graphics`
- **Nombre**: `HKLM_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 teclas deben estar separadas por comas (,) sin espacio. El orden de las teclas no importa.

A, C, S, W y K son teclas, donde C=Control, A=ALT, S=MAYÚS, W=Win y K=una tecla válida, donde los valores permitidos para K son 0—9, a—z y 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

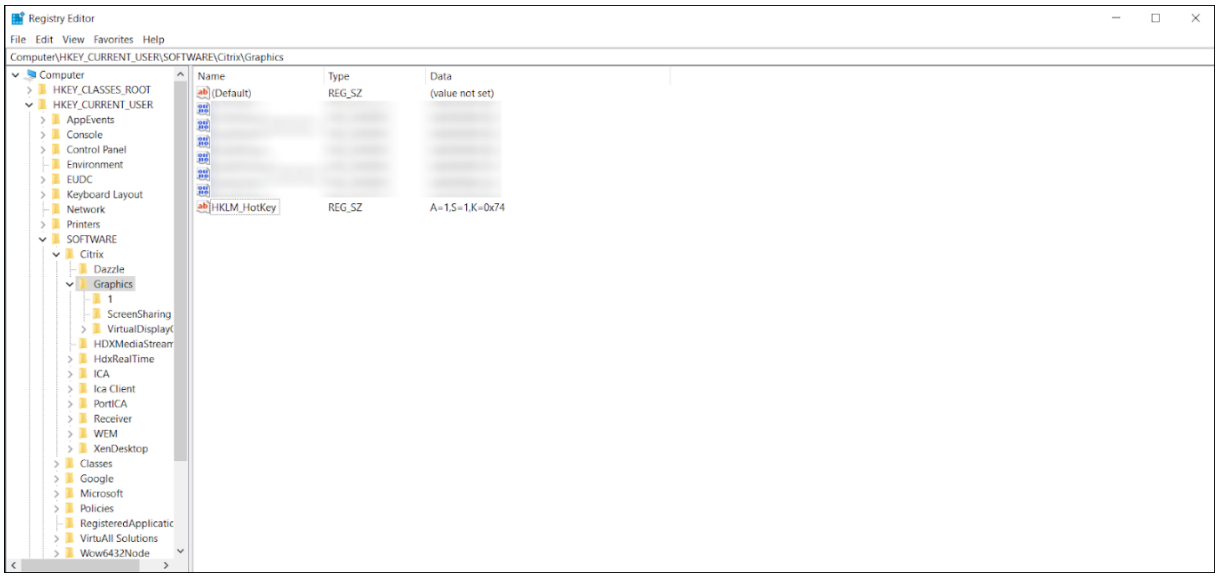
En la siguiente tabla se muestra la lista de ejemplos de códigos de teclas virtuales:

Tecla	Valor
F1	0x70
F2	0x71
F3	0x72
F4	0x73
F5	0x74
F6	0x75
F7	0x76
F8	0x77
F9	0x78
F10	0x79

Tecla	Valor
F11	0x7A
F12	0x7B
Tecla RePág	0x21
Tecla AvPág	0x22
Tecla Fin	0x23
Tecla Inicio	0x24
Flecha izquierda	0x25
Flecha arriba	0x26
Flecha derecha	0x27
Flecha abajo	0x28

Asegúrese de que no haya espacio entre las combinaciones del acceso directo. Por ejemplo:

Correcto:
C=1,K=0x74
Incorrecto:
C=1, K=0x74



> **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 usa el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Thinwire

August 20, 2024

Introducción

Thinwire, una parte de la tecnología de Citrix HDX, 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 ofrece 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.

HDX 3D Pro

En su configuración predeterminada, Thinwire puede entregar gráficos 3D o de interacción elevada y emplear una unidad de procesamiento de gráficos (GPU), si está presente. Sin embargo, se recomienda habilitar el modo HDX 3D Pro mediante las directivas **Optimizar para cargas de trabajo de gráficos 3D** o **Calidad visual > Gradual sin pérdida** para casos en los que las GPU están presentes. Estas directivas configuran Thinwire para que utilice un códec de vídeo (H.264, H.265 o AV1) que codifica toda la pantalla mediante la aceleración de hardware si hay una GPU presente. Esto ofrece una experiencia más fluida para gráficos 3D profesionales. Para obtener más información, consulte H.264 gradual sin pérdida, HDX 3D Pro y Aceleración de GPU para SO Windows de sesión única.

Requisitos

Thinwire está optimizado para sistemas operativos modernos, como Windows Server 2022, Windows Server 2019, Windows 10 y Windows 7. Para Windows Server 2008 R2, se recomienda el modo de gráficos antiguo. Utilice las plantillas de directivas Citrix integradas, 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.

- 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, es posible que algunas aplicaciones Citrix Workspace admitan 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 emplea más recursos de servidor (CPU, memoria) cuando hay 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 bajo ancho de banda o latencia elevada, tenga en cuenta la posibilidad de habilitar los gráficos de 8 o 16 bits para mejorar la interactividad. Es posible que la calidad visual se vea afectada, especialmente a una profundidad de color de 8 bits.

Métodos de codificación

Thinwire puede operar en dos modos de codificación diferentes en función de las prestaciones de las directivas y del cliente:

- Thinwire con la configuración de directiva de JPEG adaptativo
  Usar el códec de vídeo para la compresión: **No usar el códec de vídeo**
- Thinwire con la configuración de directiva de Selective H.264, H.265 o AV1
  Usar el códec de vídeo para la compresión: **Usar el códec de vídeo cuando lo prefiera** o **Para regiones que cambien de forma activa**
- Thinwire con la configuración de directiva con Pantalla completa H.264, H.265 o AV1
  Usar el códec de vídeo para la compresión: **Para toda la pantalla**

H.265

La codificación de vídeo de alta eficiencia (HEVC), también conocida como H.265, es la sucesora de H.264.
La codificación por hardware con el códec de vídeo H.265 es compatible con las siguientes GPU:

- GPU basadas en NVIDIA Maxwell y versiones superiores
- GPU Intel de 6.ª generación y superiores
- GPU basadas en AMD Raven y versiones superiores

AV1

Citrix agregó compatibilidad para el códec de vídeo AV1. La ventaja del AV1 es que tiene una compresión de imagen superior, una mejor calidad de imagen y un menor uso de ancho de banda en comparación con H.264 y H.265.

Se deben cumplir los siguientes requisitos para AV1:

- VDA 2305 o superior para GPU NVIDIA, o
- VDA 2308 o superior para GPU Intel

Las siguientes GPU son compatibles para la codificación:

- GPU NVIDIA basada en Ada Lovelace
- GPU Intel ARC o la serie GPU Flex para centro de datos de Intel

Para obtener más información sobre las GPU Ada Lovelace de NVIDIA, consulte Arquitectura ADA.

Para obtener más información sobre las GPU de la serie Flex para estaciones de trabajo ARC y centros de datos de Intel, consulte la serie Flex y su descripción general.

Selección automática de códecs de vídeo

Puede detectar automáticamente el mejor códec de vídeo para usar cuando la directiva **Usar códec de vídeo para compresión** está habilitada u Optimizar para la carga de trabajo de gráficos 3D está habilitada en el VDA. Durante la instalación de la aplicación Citrix Workspace para Windows, se evalúan las capacidades de decodificación del dispositivo de punto final. En función de esta información, la aplicación Citrix Workspace para Windows negocia el mejor códec para usar con el VDA al conectarse. La siguiente lista muestra el orden en el que se evalúan los códecs de vídeo:

- AV1
- H.265
- H.264

La selección automática solo se aplica a las variantes 4:2:0 de estos códecs. Si el parámetro de **calidad visual** está establecido en "Gradual sin pérdidas"o "Siempre sin pérdidas"y cuando Permitir sin pérdidas visuales está establecido en "habilitado", la selección automática del códec de vídeo está inhabilitada.

Al conectarse a un recurso, la aplicación Citrix Workspace prueba la capacidad del dispositivo de punto final para decodificar H.265 y AV1 y guardar las capacidades en el registro. A continuación, la aplicación Citrix Workspace selecciona automáticamente el mejor códec de vídeo para usar y lo negocia con el VDA. Si tanto el VDA como el cliente pueden usar H.265 y AV1, se selecciona AV1 como códec de vídeo. Si el AV1 no está disponible en el VDA ni en el cliente, se negocia H.265. Si H.265 tampoco está disponible en ninguno de los dos, la sesión usa H.264 como códec de vídeo.

> **Nota:**
>
> Esta función está habilitada de manera predeterminada. Este comportamiento se puede cambiar configurando el nuevo parámetro de Registro del lado del cliente`DisableDecoderCaps`.

Para inhabilitar la selección automática del códec de vídeo, defina 'DisableDecoderCaps'como `HKLM\Software\WOW6432Node\Policies\Citrix\ICA Client\Graphics Engine DWORD DisableDecoderCaps = 1` o `HKCU\Software\Policies\Citrix\ICA Client\Graphics Engine DWORD DisableDecoderCaps = 1`.

Si alguno de estos valores se establece en 1, no se usa la selección automática del códec de vídeo. El indicador de estado de los gráficos y el monitor HDX pueden supervisar el códec de vídeo.

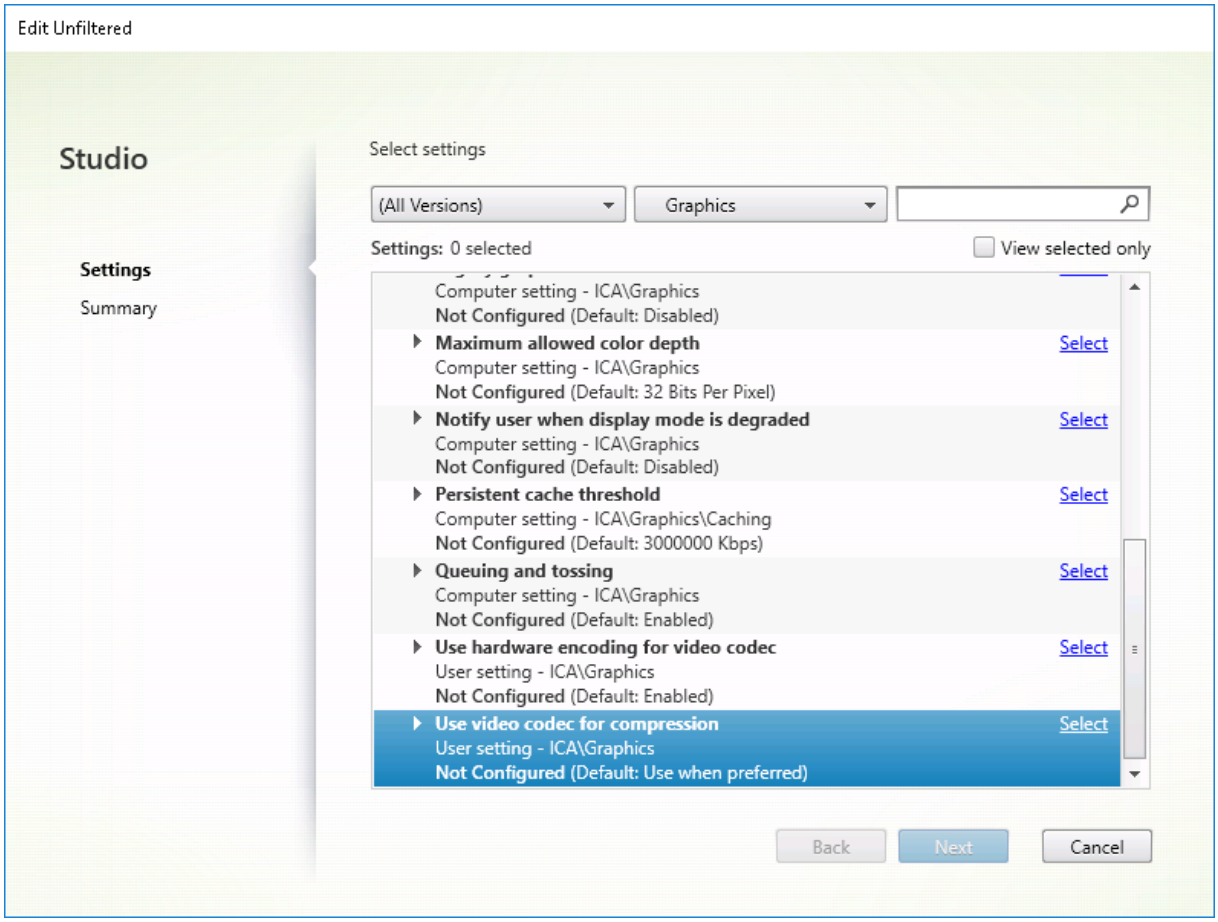
Configuración

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. Esto equivale funcionalmente a la opción **Para áreas en cambio constante**.
- Las demás opciones de esta configuración de directiva siguen utilizando 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, H.265 o AV1 solo en aquella parte de la pantalla donde se mueva la imagen.

- **Para la pantalla entera**. Entrega Thinwire con H.264, H.265 o AV1 en pantalla completa para mejorar la experiencia del usuario y optimizar el ancho de banda cuando haya un uso intensivo de gráficos 3D. En el caso de H.264 4:2:0 (la directiva **Compresión sin pérdida visual** está inhabilitada), la imagen final no es perfecta (sin pérdida), y es posible que no sea adecuada para ciertas situaciones. En tales casos, plantéese usar H.264 Gradual sin pérdida o H.265 Gradual sin pérdida en su lugar.



Hay otras configuraciones de directiva, incluidas las siguientes configuraciones de directiva de Presentación visual, que se pueden emplear para optimizar el rendimiento de la tecnología de pantallas remotas. Thinwire es compatible con todas.

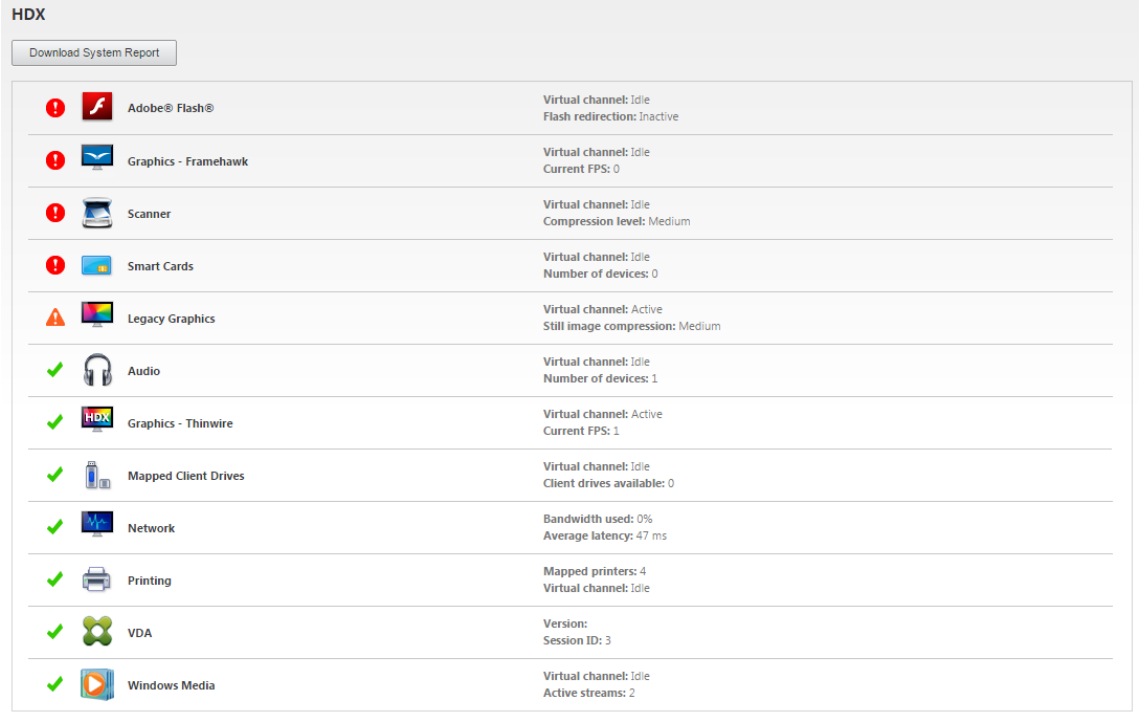
- Profundidad de color preferida para gráficos simples
- Velocidad de fotogramas de destino
- Calidad visual

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.

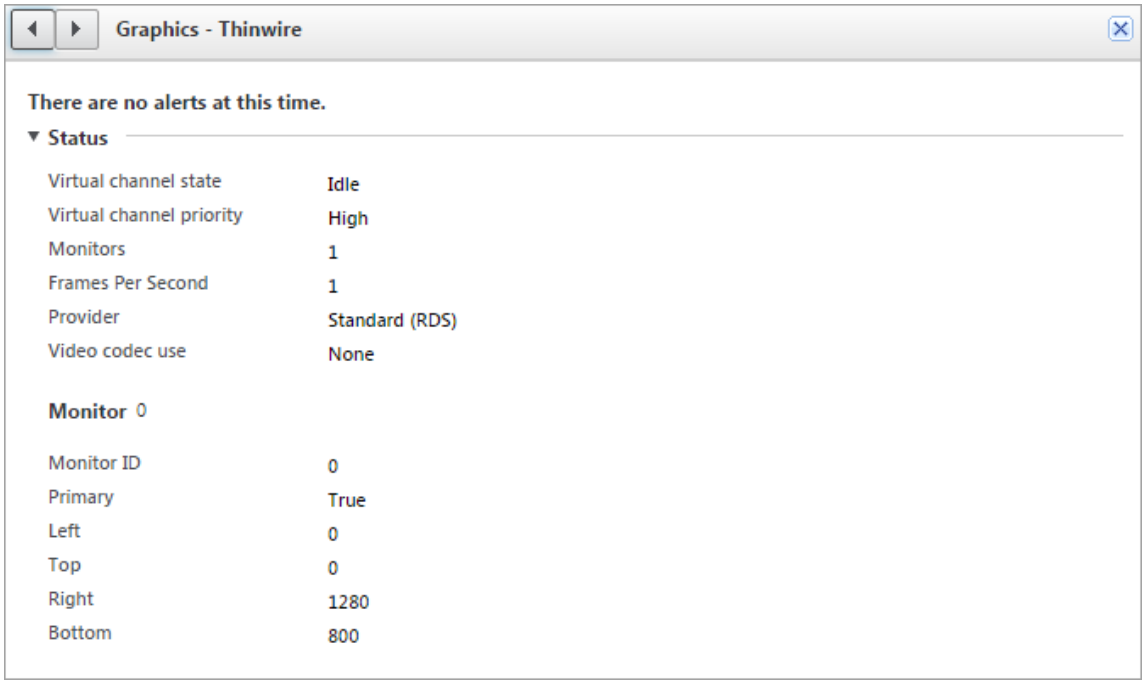
Supervisar Thinwire

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**.



3. Seleccione **Gráficos: Thinwire**.



Códec de compresión sin pérdida (MDRLE)

En una sesión de escritorio estándar, la mayoría de las imágenes son gráficos simples o regiones de texto. Thinwire determina dónde se encuentran estas áreas y las selecciona 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.

En XenApp y XenDesktop 7.17, agregamos un códec MDRLE, con una razón de compresión más alta y menor consumo de ancho de banda que el códec 2DRLE en sesiones de escritorio estándar. Este nuevo códec no afecta a la escalabilidad de los servidores.

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.

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)
- Agentes VDA de XenApp y XenDesktop 7.17 (versión mínima)
- Aplicación Citrix Workspace para Windows 1808 (versión mínima)
- Citrix Receiver para Windows 4.11 (versión mínima)

Modo progresivo

Citrix Virtual Apps and Desktops 1808 presentó el modo progresivo y lo habilitó de forma predeterminada. En condiciones de red restringida (valor predeterminado: ancho de banda < 2 Mbps o latencia > 200 ms), Thinwire aumentó la compresión de texto e imágenes estáticas para mejorar la interactividad durante la actividad en pantalla. Cuando se detiene la actividad en pantalla, el texto y las imágenes altamente comprimidos se vuelven más nítidos de forma progresiva y aleatoria por bloques. Esta compresión y esta mayor nitidez mejoran la interactividad general, reducen la eficiencia de la caché y aumentan el uso del ancho de banda.

A partir de Citrix Virtual Apps and Desktops 1906, el modo progresivo está inhabilitado de forma predeterminada. Ahora empleamos otra estrategia. La calidad de las imágenes estáticas se basa ahora en las condiciones de la red y se halla entre un valor mínimo y un valor máximo predefinidos para cada parámetro de la **calidad visual**. Como no existe ningún paso explícito para aumentar la nitidez, Thinwire optimiza la entrega de imágenes y mantiene la eficiencia de la caché, al tiempo que ofrece casi todos los beneficios del modo progresivo.

Cambiar el comportamiento del modo progresivo

Puede cambiar el estado del modo progresivo con la clave de Registro. Para obtener información, consulte Modo progresivo en la lista de funciones administradas a través del Registro.

Gradual sin pérdida

Gradual sin pérdida es una configuración especial de Thinwire que optimiza la entrega de gráficos en pos de la interactividad y la calidad final de las imágenes. Para habilitar esta configuración, establezca la directiva **Calidad visual** en **Gradual sin pérdida**.

La opción Gradual sin pérdida comprime la pantalla mediante H.264, H.265 o AV1 durante la actividad en pantalla y la vuelve totalmente nítida (sin pérdida) al cesar la actividad. La calidad de las imágenes se adapta a los recursos disponibles para mantener la mejor velocidad de fotogramas posible. La fase de nitidez se realiza de forma gradual. Por ejemplo: al seleccionar un modelo y girarlo.

La opción Gradual sin pérdida ofrece todas las ventajas de utilizar un códec de vídeo para la pantalla completa, incluida la aceleración de hardware, pero con el beneficio adicional de una pantalla final y sin pérdida garantizada. Esto es fundamental para cargas de trabajo de tipo 3D que requieren una imagen final totalmente nítida. Por ejemplo: al manipular imágenes médicas. Además, la opción **Gradual sin pérdida** de H.264 emplea menos recursos que H.264 en pantalla completa 4:4:4. Como resultado, la opción **Gradual sin pérdida** generalmente proporciona una velocidad de fotogramas mayor que H.264 en Compresión sin pérdida visual 4:4:4.

> **Nota:**
>
> Puede inhabilitar el uso de un códec de vídeo cuando uses una compilación sin pérdidas. Simplemente defina la directiva de **uso de códecs de vídeo** en `Do not use video codec`. El resultado es la codificación de las imágenes en movimiento con JPEG adaptativo.

Codificación sin pérdidas visuales

La codificación sin pérdidas visuales usa el espacio de color YUV 4:4:4 en lugar del espacio de color YUV 4:2:0 submuestreado con cromas para la compresión de códecs de vídeo. Esto garantiza que no se pierda información de color durante la conversión del espacio de color y, una vez decodificada, sea visualmente imperceptible desde la imagen RGB original.

Fíjese en este ejemplo. Si usa un códec de vídeo para comprimir toda la pantalla, la compresión de color 4:2:0 puede degradar los detalles de alto contraste, como el texto, haciendo que sean borrosos y difíciles de leer. Por el contrario, el formato 4:4:4 conserva casi toda la información de color y no presenta ninguna degradación perceptible visualmente.

Las cargas de trabajo que requieren una calidad de píxeles perfecta o una visualización precisa en color pueden beneficiarse de la codificación sin pérdidas visuales.

La codificación sin pérdida visual está disponible con H.264 y H.265. La codificación H.264 4:4:4 es una solución basada exclusivamente en software y, como resultado, puede tener un impacto significativo en el uso de la CPU tanto en el VDA como en el cliente. Esto también puede afectar a la velocidad de fotogramas.

La compatibilidad con H.265 4:4:4 se agregó con el lanzamiento de la aplicación Citrix Workspace 2305, lo que permitió a Thinwire usar tanto una GPU en el VDA como un cliente para la codificación H.265 4:4:4, lo que mejoró considerablemente el rendimiento.

Para permitir la codificación 4:4:4 de Sin pérdidas visuales, es necesario habilitar dos directivas:

- **Calidad visual**: establecida en `Build to Lossless` o `Always Lossless`
- **Permitir sin pérdidas visuales**: establecido en `Enabled`

> **Nota:**
>
> Si la opción **Permitir sin pérdidas visuales** no está habilitada, cambiamos a nuestro codificador Thinwire en `Build to lossless` o `Always Lossless`.

H.265 4:4:4 visualmente sin pérdidas tiene estos requisitos adicionales:

- Las GPU NVIDIA requieren la versión 2209 o superior de VDA
- Las GPU Intel requieren la versión 2308 de VDA o superior

Las siguientes GPU son compatibles con H.265 4:4:4:

- GPU NVIDIA de la generación Pascal y posteriores
- GPU Intel de 10.ª generación y posteriores

Para el cliente, se requiere la versión 2305 de la aplicación Citrix Workspace para Windows (se recomienda la versión 2309.1).

La decodificación por hardware de H.265 4:4:4 es posible con las siguientes GPU de dispositivos cliente:

- GPU NVIDIA de generación Turing y posteriores
- GPU Intel de 10.ª generación y posteriores

Marca de agua de texto en sesión

August 17, 2024

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 las sesiones solo es compatible con el modo de gráficos Thinwire.
- 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.

Uso compartido de pantalla

August 17, 2024

El uso compartido de pantalla permite a un usuario compartir una sesión de Citrix Virtual Desktop con otros usuarios, incluidos el contenido de la pantalla, el teclado y los controles del mouse.

Requisitos del sistema

- Windows: VDA para SO de sesión única o multisesión
- Linux: consulte la documentación de Linux VDA para obtener más información sobre cómo compartir sesiones de Linux.
- Solo se pueden compartir sesiones de escritorio.
- Debe haber conectividad de red entre el VDA que aloja la sesión y las máquinas que se conectan a las sesiones compartidas. Los requisitos de puerto de red se basan en los puertos ICA en uso (TCP/UDP 1494 o 2598) y en la configuración de la directiva de uso compartido de pantalla (TCP 52525 a 52625 de forma predeterminada).

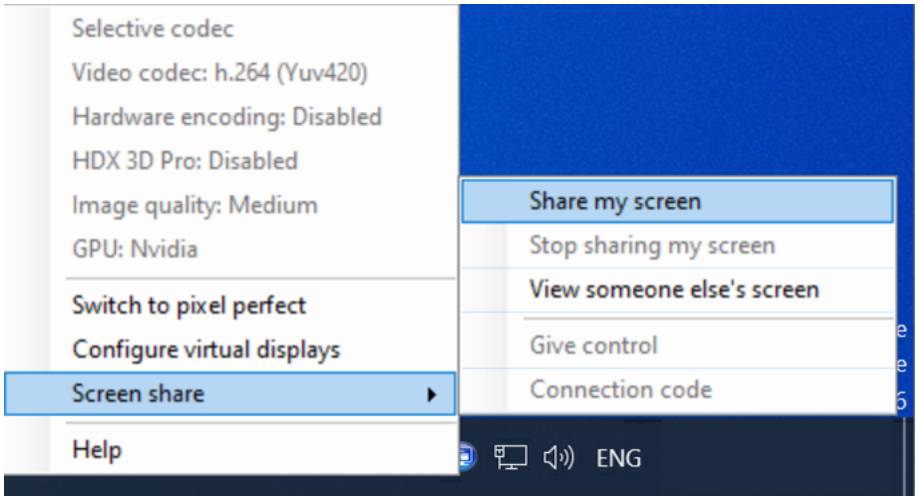
Configuración

El uso compartido de pantalla debe habilitarse mediante directivas de Citrix. El uso compartido de pantalla está inhabilitado de forma predeterminada Configure la directiva de uso compartido de pantalla para habilitar o inhabilitar la función y asignar el rango de puertos de red utilizables.

Habilite la directiva del indicador de estado de gráficos para que se muestre la interfaz de usuario que incluye controles para compartir y conectarse a las sesiones.

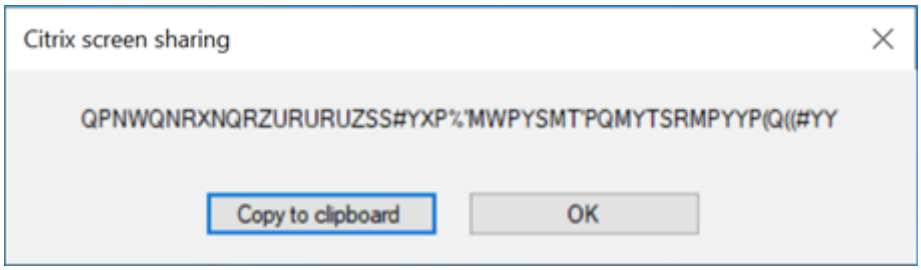
Compartir una sesión

Para compartir una sesión, busque el icono del indicador de estado de gráficos HDX en el área de notificaciones de Windows. Haga clic con el botón secundario en él para mostrar el menú y seleccione **Pantalla compartida > Compartir mi pantalla**.



Haga clic en **Copiar al portapapeles** o seleccione y copie manualmente toda la cadena que se muestra en el cuadro de diálogo. La cadena se puede pegar en distintas aplicaciones, como un programa de correo electrónico o un cliente de mensajería instantánea, para distribuirla a otros usuarios.

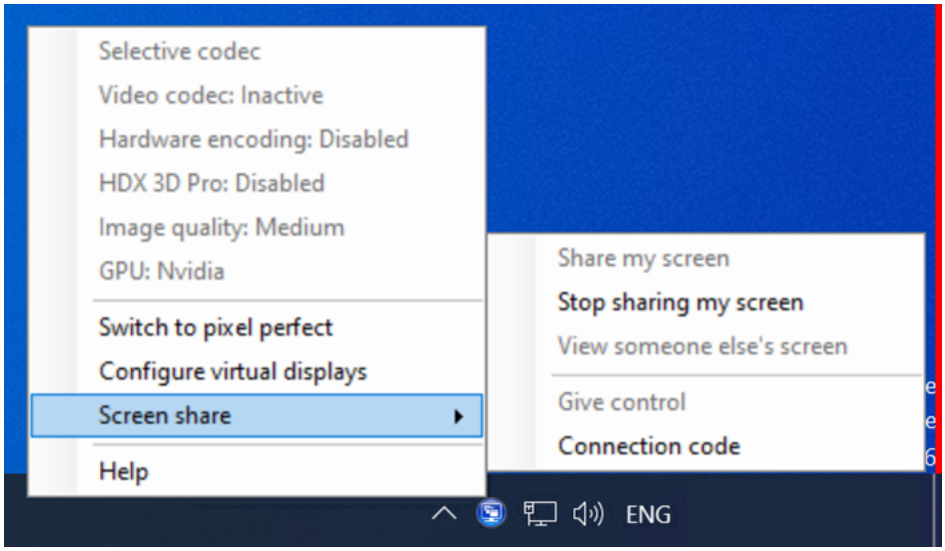
Haga clic en **Aceptar** o en la **x** para cerrar el cuadro de diálogo. El código de conexión se puede obtener de la opción de menú **Pantalla compartida > Código de conexión** en cualquier momento mientras se comparte la sesión.



Aparecerá un contorno rojo alrededor de la pantalla como indicador de que la sesión ahora se está compartiendo y que otros usuarios la pueden ver.

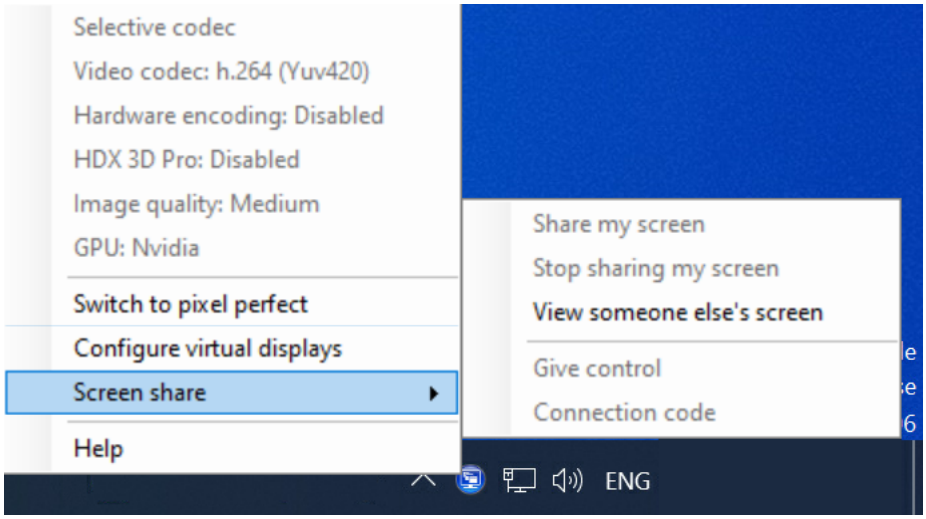
Los controles del teclado y el mouse también se pueden compartir con otros usuarios mediante la opción de menú **Pantalla compartida > Dar control**.

Use la opción de menú **Pantalla compartida > Dejar de compartir mi pantalla** para dejar de compartir la sesión y desconectar a todos los usuarios.

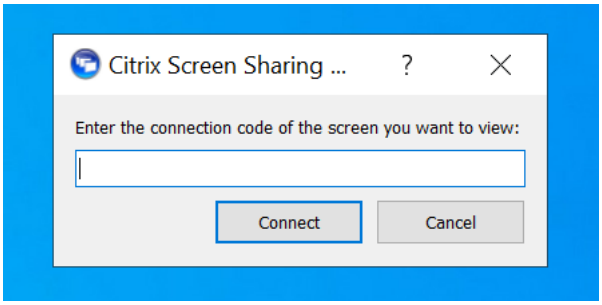


Conectarse a una sesión compartida

Para conectarse a las sesiones de otros usuarios, busque el icono del indicador de estado de gráficos HDX en el área de notificaciones de Windows. Haga clic con el botón secundario en él para mostrar el menú y seleccione **Pantalla compartida > Ver la pantalla de otra persona**.

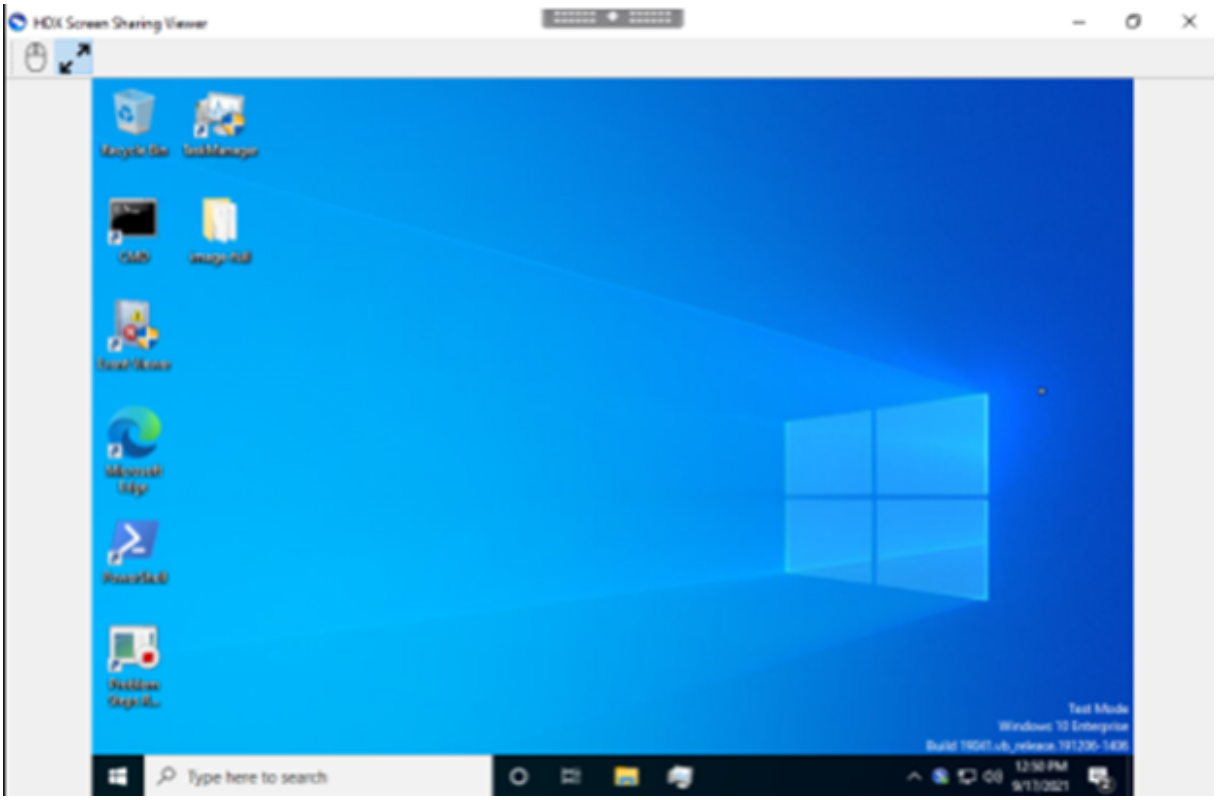


Escriba o pegue en el cuadro de texto la cadena de conexión que proporcionó el usuario que compartió la sesión. Haga clic en **Conectar** para establecer la conexión.



Puede solicitar controles de teclado y mouse haciendo clic en el icono de mouse situado en la esquina superior izquierda de la ventana **Visor de pantalla compartida de HDX**.

Puede desconectarse de la sesión compartida en cualquier momento cerrando la ventana **Visor de pantalla compartida de HDX**.



Otras consideraciones

- La aplicación de visor de pantalla compartida se incluye con el VDA en *C:\Archivos de programa\Citrix\HDX\bin\TwPlayer.exe* y puede implementarse como aplicación publicada utilizando un servidor de Virtual Apps. Este modelo de implementación alternativo permite colaborar con usuarios que no tienen acceso a un escritorio virtual.
- La cantidad de usuarios a los que se permite conectarse a una sesión compartida se puede limitar mediante el rango de puertos de red en la directiva de uso compartido de pantalla. Se re-

quiere un puerto por cada usuario. El rango predeterminado permite 100 usuarios como máximo.
- Se comparten todos los monitores conectados a la sesión. No puede seleccionar monitores individuales.
- El códec de vídeo H.265 no es compatible.

Distribución de pantallas virtuales

August 17, 2024

La interfaz de usuario para configuración de pantalla virtual permite definir un diseño de pantalla virtual por monitor de sesión en el VDA, dentro de una sesión en directo. Esta función le permite dividir cada monitor de sesión de forma independiente en varios monitores virtuales. Puede dividirse en un total de 8 monitores virtuales en el escritorio remoto. Además, puede actualizar el monitor principal de la sesión y la configuración de PPP para las pantallas.

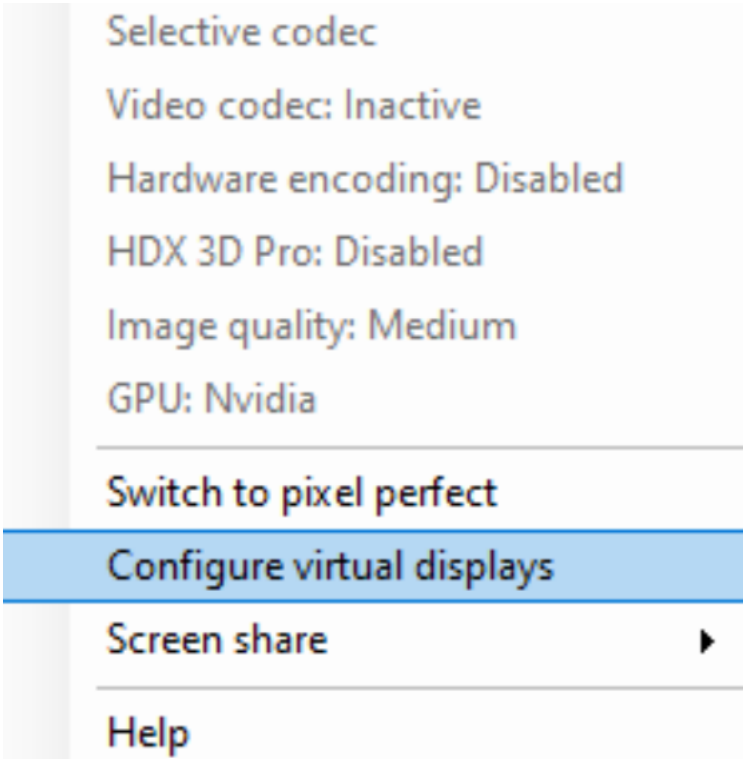
La configuración de pantalla virtual se almacena por usuario y dispositivo cliente. La configuración se aplica a todas las conexiones posteriores de un cliente determinado para un usuario concreto. Se conserva durante el cambio de tamaño de las sesiones, la desconexión o reconexión de sesiones y el cierre o inicio de sesión. El restablecimiento del diseño de pantalla virtual configurado se produce al cambiar el tamaño de una sesión y al cambiar la cantidad de monitores de la sesión.

Requisitos del sistema

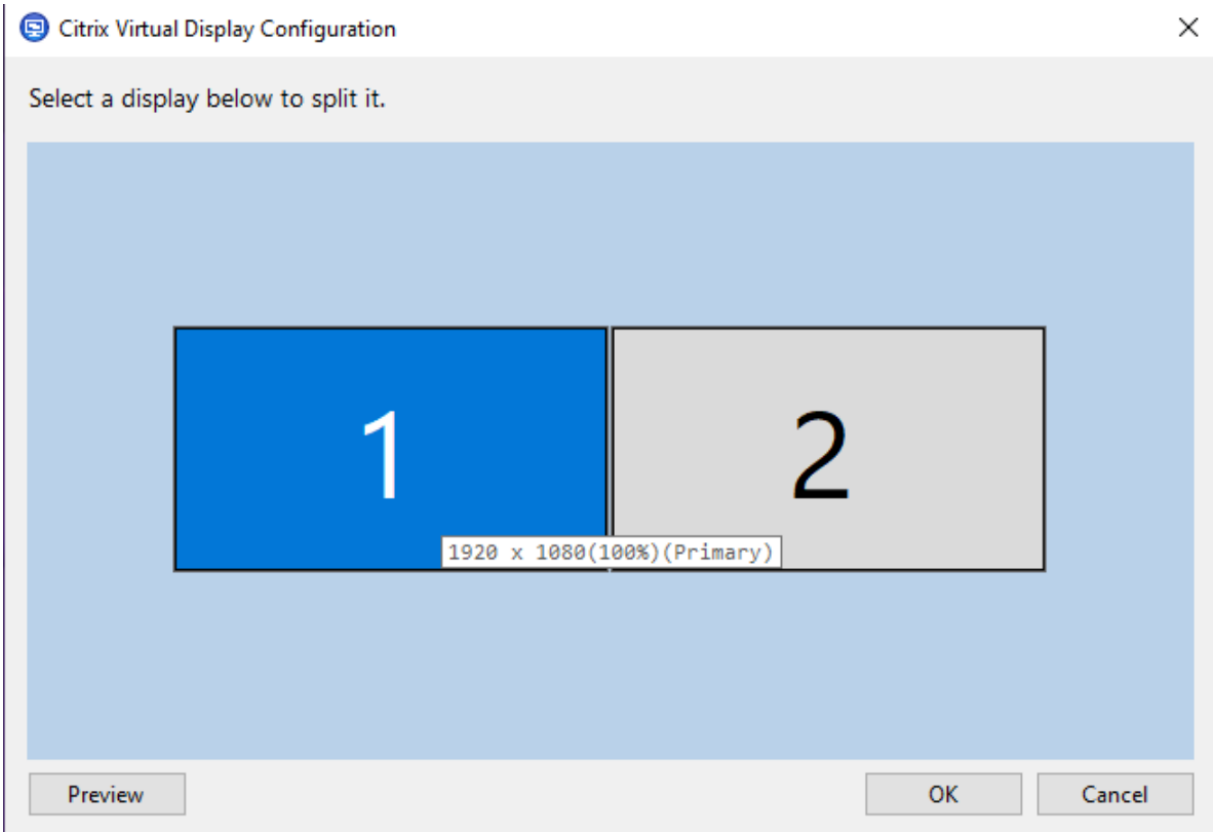
- Windows: VDA para SO de sesión única o multisesión
- La directiva Indicador de estado de gráficos debe estar activada
- Solo se pueden configurar las sesiones de escritorio.

Configuración

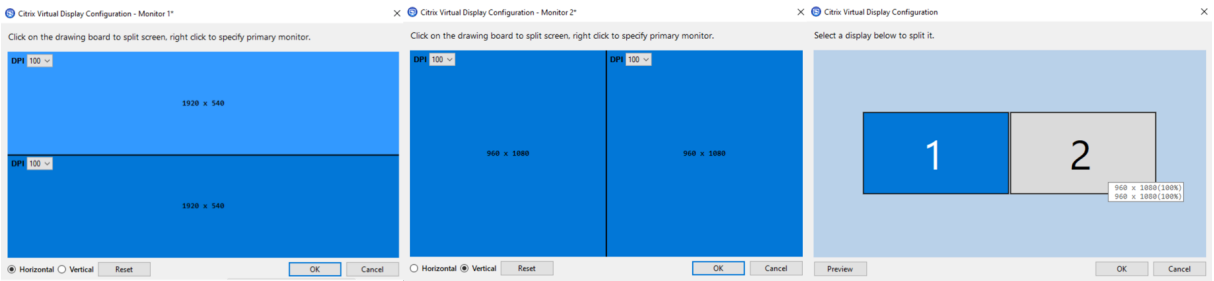
Para configurar el diseño de pantalla virtual, haga clic con el botón secundario en el icono del indicador de estado de los gráficos y seleccione la opción Configurar pantallas virtuales. Se iniciará la interfaz de usuario de configuración de pantalla virtual.



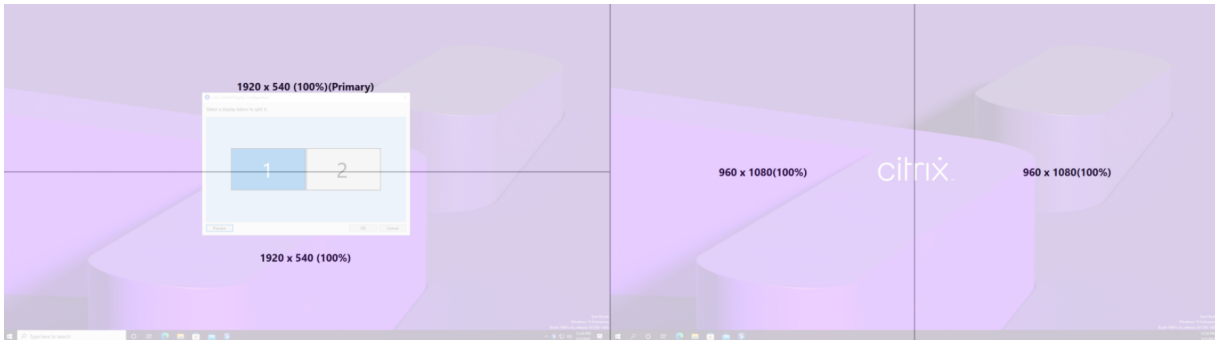
La interfaz de usuario muestra el diseño de pantalla de la sesión actual, y el monitor principal de la sesión se indica en color azul. Puede ver el texto de ayuda de la configuración de pantalla al pasar el cursor por una pantalla. El texto de ayuda proporciona información sobre el diseño de pantalla virtual definido actualmente en un monitor de sesión determinado.



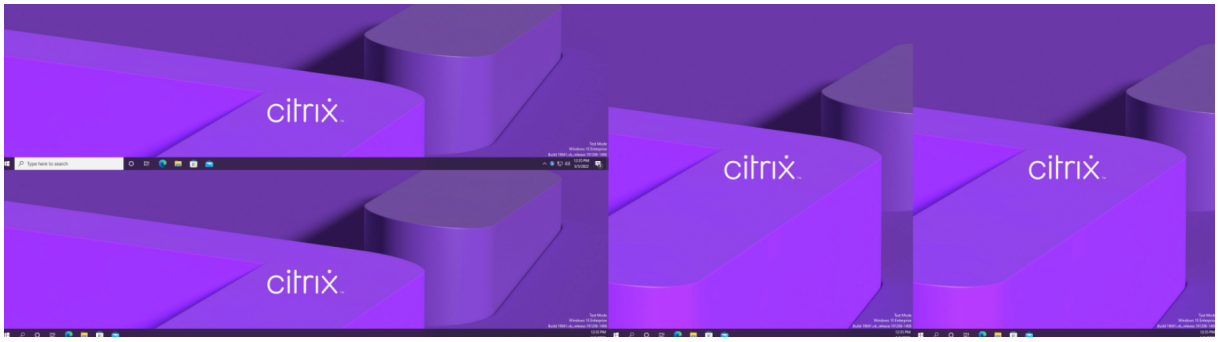
Seleccione una pantalla para cambiar a una interfaz de usuario interactiva, que le permite configurar las pantallas virtuales para el monitor de sesión seleccionado. Puede dibujar líneas horizontales o verticales para dividir la pantalla en monitores virtuales. La pantalla se divide en función de porcentajes especificados en la resolución del monitor de la sesión. Haga clic con el botón secundario en una pantalla virtual para marcarla como monitor principal y utilice la lista desplegable de PPP para establecer un factor de escala preferido para la pantalla virtual. Después de definir un diseño de pantalla virtual, haga clic en **Aceptar** para guardar temporalmente el diseño o en **Cancelar** para descartar los cambios. Puede usar la opción **Restablecer** para deshacer la configuración y restaurar el diseño original del monitor de sesión.



Para obtener una vista previa del diseño de pantalla virtual configurado actualmente, haga clic en el botón **Vista previa**. Aparecerá una ventana para resaltar la posición y resolución previstas de las pantallas virtuales en la sesión.



Haga clic en **Aceptar** para aplicar inmediatamente y guardar el diseño de pantalla virtual. Haga clic en **Cancelar** para cerrar la interfaz de usuario y descartar todos los cambios.



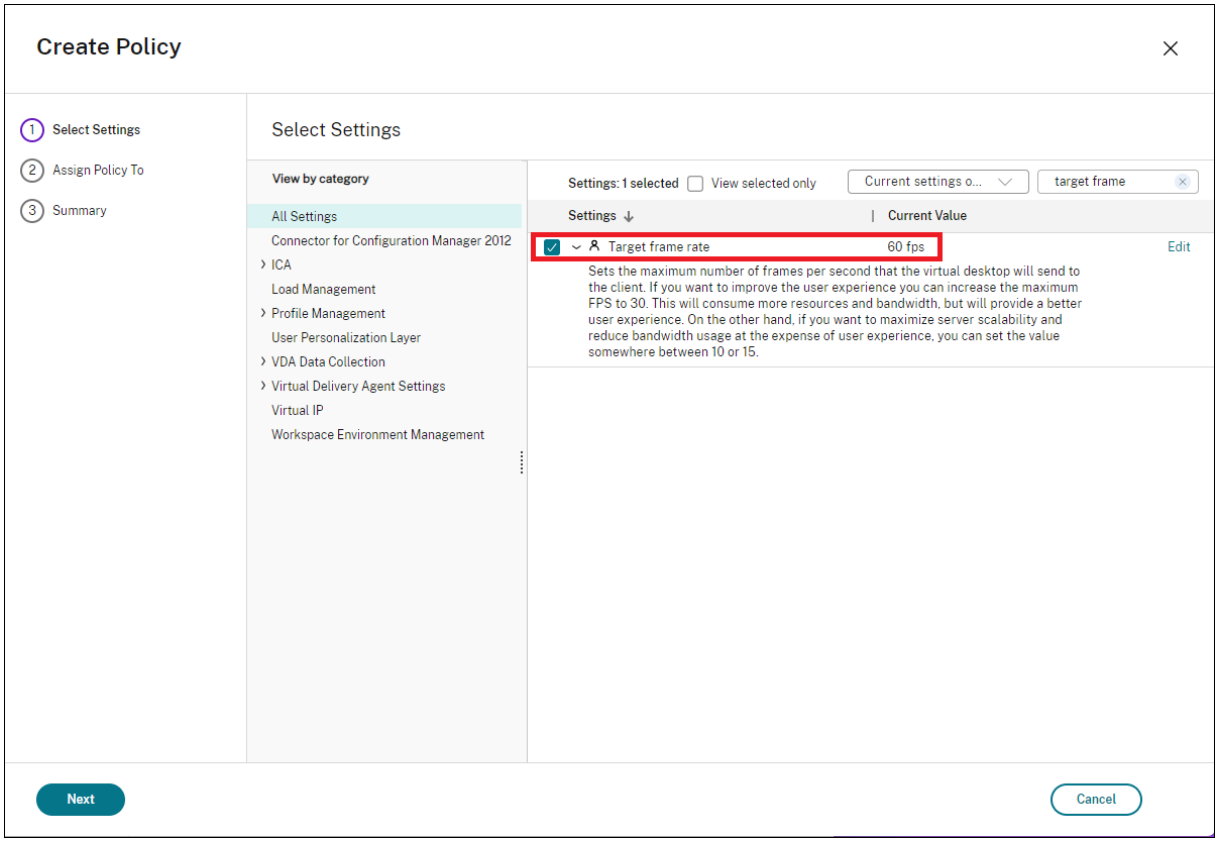
Otras consideraciones

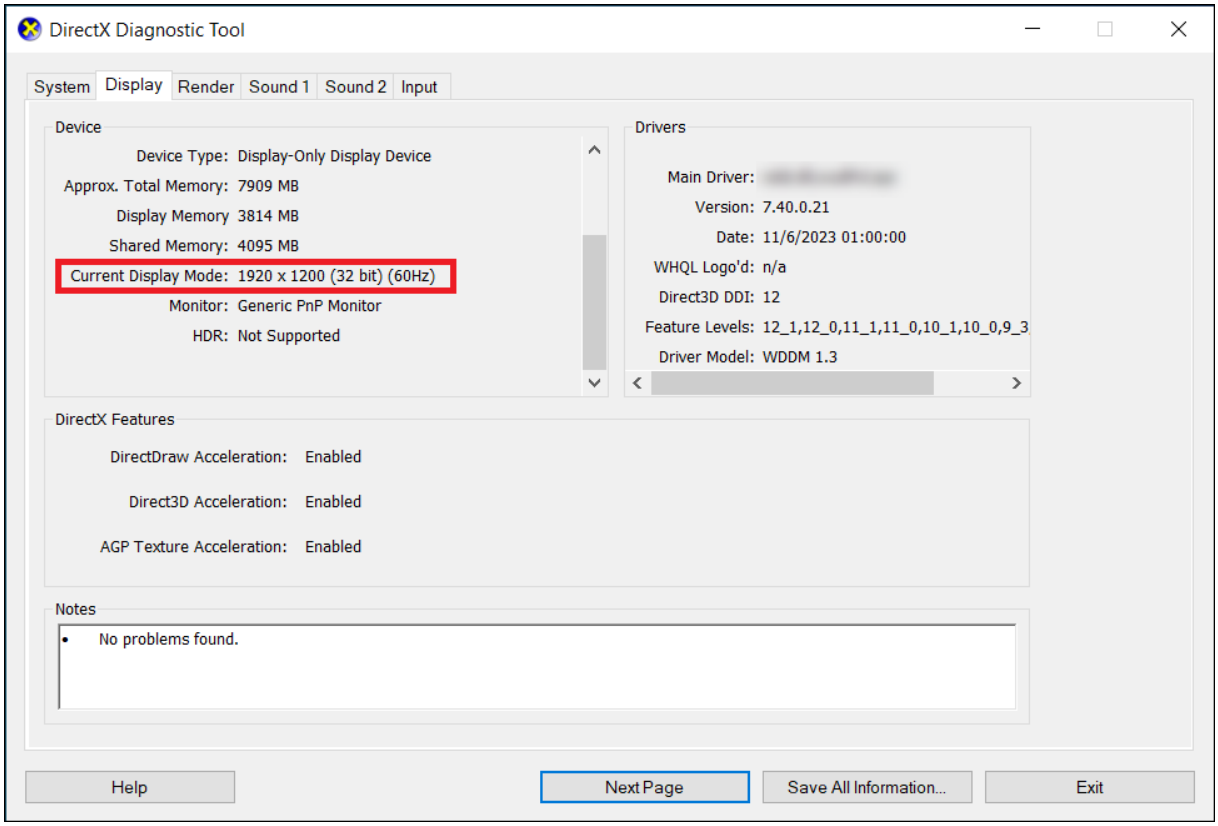
- La resolución mínima de pantalla virtual requerida es de 640 x 480.
- El valor de puntos por pulgada (PPP) de pantalla virtual definido a través de la interfaz de usuario depende de la compatibilidad del SO con la resolución de pantalla dada
- No use esta funcionalidad simultáneamente con la funcionalidad de pantalla virtual existente en la aplicación Citrix Workspace.
- La función de vista previa no se admite en Server 2016.

Frecuencia de actualización adaptativa

August 17, 2024

Con las nuevas mejoras de escalabilidad, HDX ajusta la frecuencia de actualización de los monitores virtuales para que coincida con el conjunto de directivas de FPS objetivo. La frecuencia de actualización adaptativa (ARR) está disponible para VDA de sesión única y multisesión, y funciona tanto en escenarios acelerados por GPU como sin GPU.





> **Nota**
>
> La frecuencia de actualización adaptativa solo está disponible cuando se usa Citrix Indirect Display o IDD (según la configuración predeterminada de Citrix Virtual Apps and Desktops) y no está disponible cuando se usan los adaptadores de pantalla suministrados por el proveedor.

Modo tolerante a pérdidas para gráficos

August 17, 2024

El modo tolerante a pérdidas para gráficos se modificó por completo para garantizar que la sesión siga siendo interactiva cuando se detecte la pérdida de paquetes. Cuando las condiciones de la red se degradan más allá de los umbrales predefinidos de ancho de banda, latencia y pérdida de paquetes, el codificador de gráficos Citrix cambia automáticamente a un modo más agresivo de entrega de paquetes para superar el efecto de la pérdida de paquetes. Como resultado, el uso del ancho de banda aumenta en una cantidad proporcional a la cantidad de pérdida de paquetes. Si las condiciones mejoran más adelante, el codificador de gráficos Citrix vuelve a funcionar sin problemas. Los umbrales se pueden configurar mediante directivas, siendo los valores predeterminados una latencia de 300 ms y una pérdida de paquetes del 5 %.

Actualmente, es compatible la aplicación Citrix Workspace para Windows 2311. La compatibilidad con otras plataformas se agregará en versiones posteriores de la aplicación Citrix Workspace. Al igual que en las versiones anteriores de esta función, HDX Adaptive Transport (EDT) debe estar habilitado para que esta función funcione. Además, si se conecta a través del Citrix Gateway Service, el modo tolerante a pérdidas para gráficos también debe estar habilitado en el Gateway.

Contenido multimedia

August 17, 2024

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.

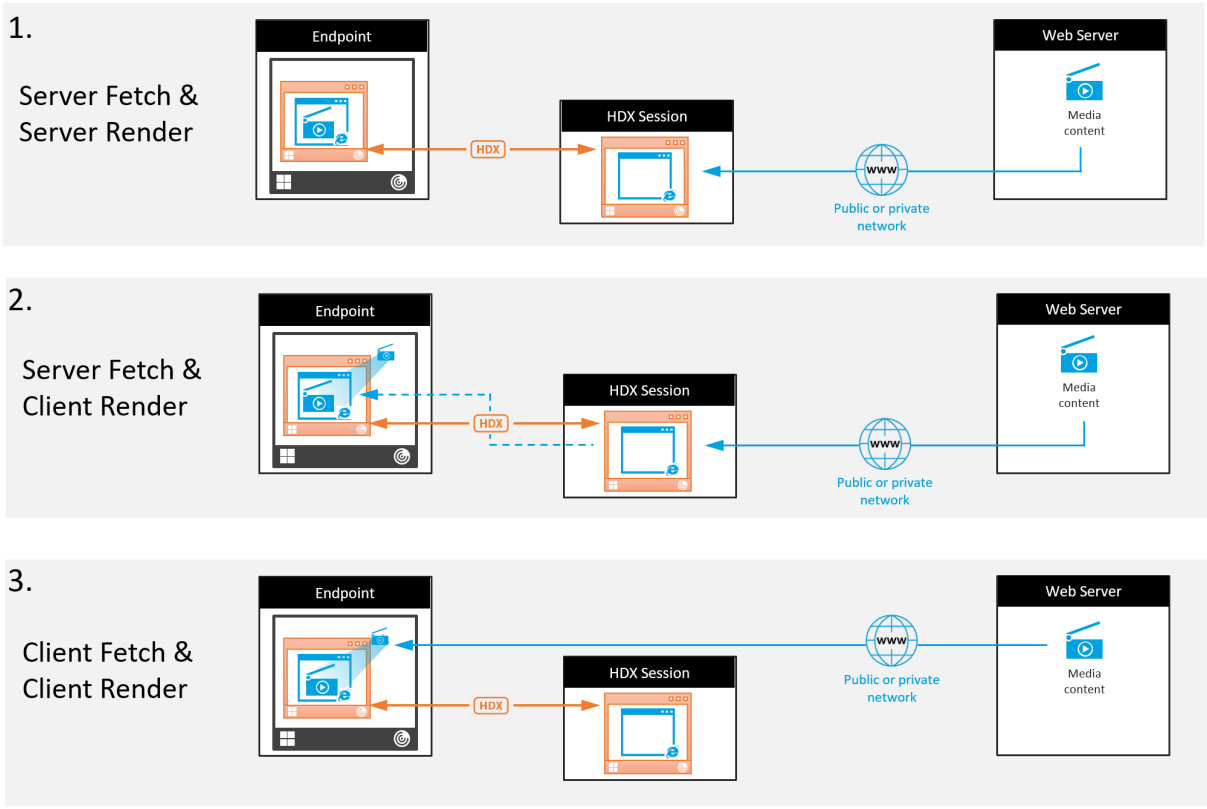
Con la entrega de contenido multimedia generado en el servidor, la aplicación decodifica y genera el contenido de audio y vídeo en el servidor de Citrix Virtual Apps and Desktops. Una vez recibido, el contenido se comprime y se entrega por protocolo ICA a la aplicación Citrix Workspace presente en el 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	Plataforma
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 del explorador web	No
	Redirección de cámara web HDX	Sí
	Redirección de vídeo HTML5	Sí
	Redirección de Windows Media	Sí

Funciones de audio

August 17, 2024

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 multisecuencia.

Audio adaptable

Con el audio adaptable, no es necesario configurar manualmente las directivas de calidad de audio en los VDA. El audio adaptable optimiza los parámetros del entorno y sustituye los formatos de compresión de audio obsoletos para proporcionar una excelente experiencia de usuario.

El audio adaptable está habilitado de forma predeterminada. Para inhabilitar el audio adaptable, consulte Configuraciones de directiva de audio.

> **Importante:**
>
> Citrix recomienda entregar el audio mediante el protocolo de datagramas de usuario (UDP) en lugar de TCP cuando se necesiten aplicaciones de audio en tiempo real. Las siguientes opciones de transporte de audio están disponibles a través de UDP:
>
> - Audio sobre UDP
> - Transporte adaptable HDX (Enlightened Data Transport, EDT)
>
> 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.
>
> Para obtener más información sobre el audio adaptable y el audio UDP, consulte Transporte de audio en tiempo real por UDP e Intervalo de puertos UDP de audio.

Modo tolerante a pérdidas para audio

El modo tolerante a pérdidas admite audio. Esta función amplía la experiencia del usuario para la transmisión en tiempo real y mejora la calidad del audio en comparación con EDT cuando los usuarios se conectan a través de redes con alta latencia y pérdida de paquetes. Esta función está inhabilitada de forma predeterminada.

> **Nota:**
>
> Tanto las directivas de **transporte adaptable de HDX (EDT)** como de **modo tolerante a pérdidas para audio** deben estar habilitadas para que esta función funcione.

Requisitos del sistema

Asegúrese de que estos productos tienen las versiones mínimas compatibles con el modo tolerante a pérdidas:

- Citrix Virtual Delivery Agent (VDA) 2308
- Aplicación Citrix Workspace para Windows 2309

Además, deben estar habilitadas estas funciones:

- Directiva de transporte adaptable HDX.
- (Opcional) Para conexiones remotas, se requiere Citrix Gateway Service.

> **Nota:**
>
> Si no se cumplen las condiciones anteriores, el audio se envía mediante el transporte EDT de confianza.

Información adicional

El modo tolerante a pérdidas es un protocolo de transporte tolerante a pérdidas que permite la pérdida de paquetes en la transmisión sin reenviar contenido multimedia, lo que resulta en una experiencia más cercana al tiempo real para los usuarios.

Enlightened Data Transport (EDT) es un protocolo de transporte patentado por Citrix que ofrece una experiencia de usuario superior en conexiones de larga distancia exigentes y, al mismo tiempo, mantiene la escalabilidad de los servidores. El modo tolerante a pérdidas es una función de Citrix Gateway Service que utiliza dicho modo como protocolo de transporte para mantener una conexión estable incluso en caso de congestión de la red. Esto garantiza una experiencia uniforme y estable para los empleados remotos. En condiciones normales, tanto el modo EDT como el modo tolerante a pérdidas proporcionan resultados similares. Sin embargo, en condiciones de red con pérdida de paquetes, el modo tolerante a pérdidas proporciona una mejor experiencia de audio en comparación con EDT. Esto la convierte en una función esencial para teletrabajadores que dependen de multimedia en tiempo real para su trabajo.

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 softphone). 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:

- Audio adaptable (predeterminado)
  - Velocidad de bits: Variable adaptable
  - Número de canales: 2 (estéreo) para reproducción, 1 (mono) para captura de micrófono
  - Frecuencia: 48000 Hz
  - Profundidad de bits: 16 bits
- Alta calidad
  - 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.

> **Nota:**
>
> Si el transporte de audio en tiempo real por UDP no es necesario para el audio adaptable, Citrix recomienda inhabilitar la configuración de la directiva. Esto ayuda a evitar que los clientes de la aplicación Citrix Workspace soliciten conexiones UDP abiertas o activen ventanas de diálogo no deseadas sobre la configuración del firewall del cliente de la aplicación Citrix Workspace.

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 multisecuencia. 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. Para obtener información, consulte Evitar eco durante conferencias multimedia en la lista de funciones administradas a través del Registro.

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 de HDX 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 multisecuencia: 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 multisecuencia, 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.

Herramienta de línea de comandos de diagnóstico de audio

La herramienta de línea de comandos de diagnóstico de audio del VDA se puede utilizar para consultar datos de sesión relacionados con las directivas de audio, la configuración y el transporte de datos.

Uso

Abra una línea de comando y ejecute `CtxAudio.exe` desde la carpeta `C:\Program Files\Citrix\HDX\bin`.

- Al ejecutar la herramienta como administrador, se muestra la información de audio de todas las sesiones ICA activas.
- Al ejecutar la herramienta sin ser administrador, se muestra la información de audio de la sesión ICA del usuario actual.

Resultado

La herramienta genera varios parámetros de configuración que pueden ayudar a diagnosticar problemas relacionados con el audio dentro de una sesión.

Sección	Descripción
Información de directiva	Directivas de audio aplicadas a las sesiones actuales.
Información sobre los parámetros	Los parámetros de configuración relacionados con el audio se almacenan en el Registro.
Información sobre el estado	El estado, la versión, los códecs y el transporte del audio que se aplican a las sesiones actuales.
Información sobre los dispositivos	Los nombres de los dispositivos, sus roles y sus estados empleados en la sesión.

> **Nota:**
>
> El resultado varía en función de si ejecuta la herramienta en un VDA multisesión (TS) o en un VDA de sesión única (WSVDA).

Limitación

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 la clave al Registro en la máquina RDS y reiníciela. Para obtener información, consulte Limitación de audio en la lista de funciones administradas a través del Registro.

Redirección de contenido del explorador web

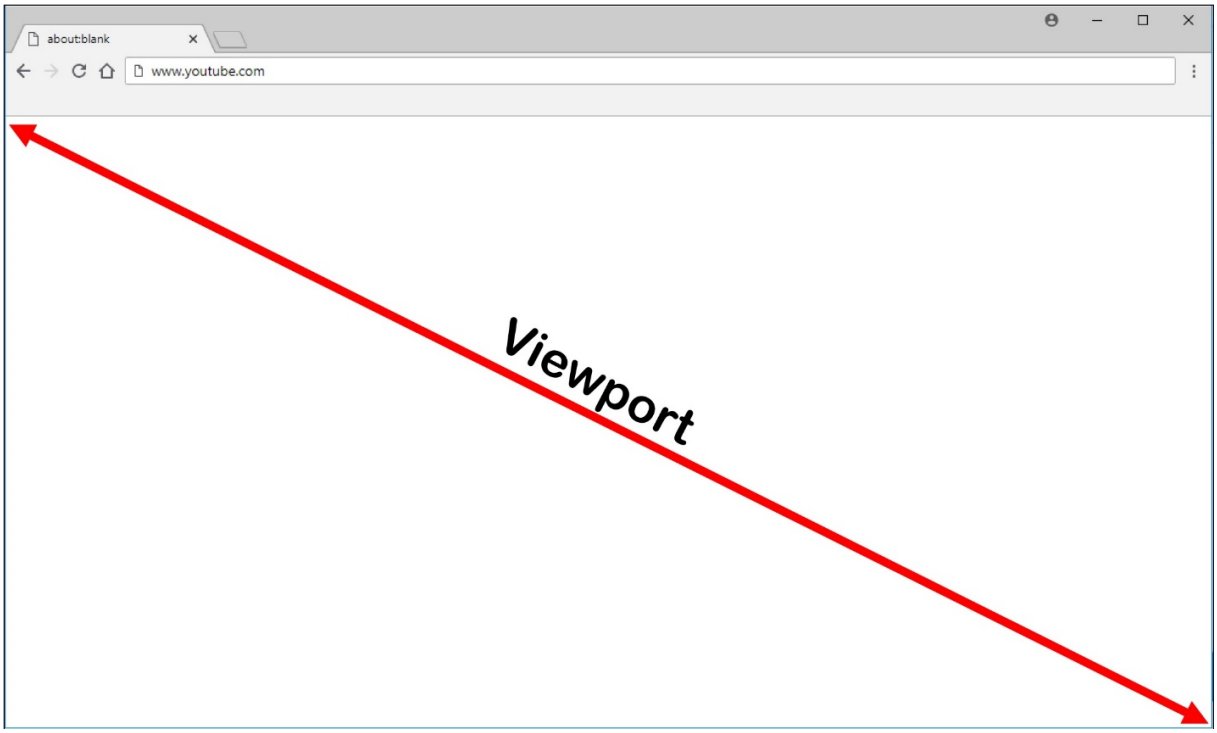
August 17, 2024

Redirección de 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 Windows o Citrix Workspace para Linux 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 ejecuta en el explorador en el VDA.



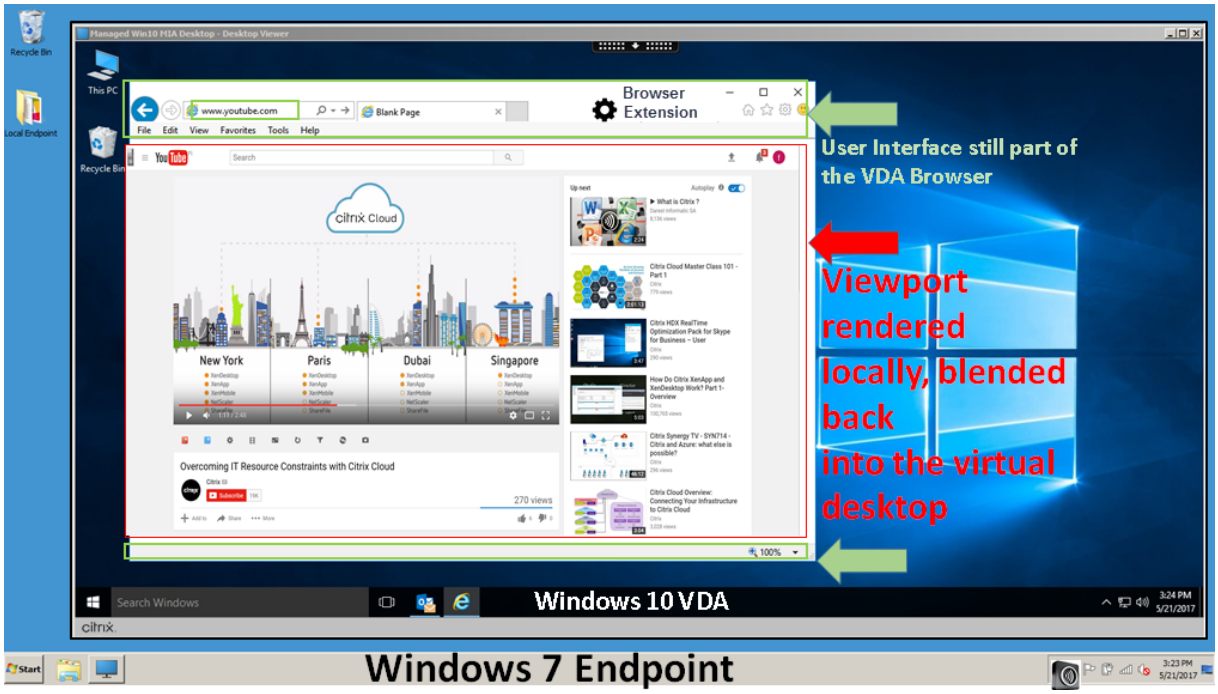
1. Configure una directiva de Studio que especifique una lista de control de acceso que contenga las URL incluidas en la lista de permitidos para permitir redirecciones o la lista de bloqueados para inhabilitar la redirección de URL específicas. Para que el explorador web presente en el VDA detecte que 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. Para Chrome, la extensión del explorador está disponible en Chrome Web Store y puede implementarla mediante directivas de grupo y archivos ADMX. Las extensiones de Chrome se instalan basándose en el usuario. No es necesario actualizar una imagen maestra para agregar o quitar una extensión. Para Microsoft Edge, la extensión no está disponible directamente. Debe permitir que las extensiones de la tienda de aplicaciones de Chrome la encuentren e instalen.
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.

> **Nota:**
>
> Para obtener más información sobre las novedades y las correcciones de la extensión de redirección de contenido del explorador, vaya a Chrome Web Store y busque `citrix bcr` para encontrar la extensión.

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.



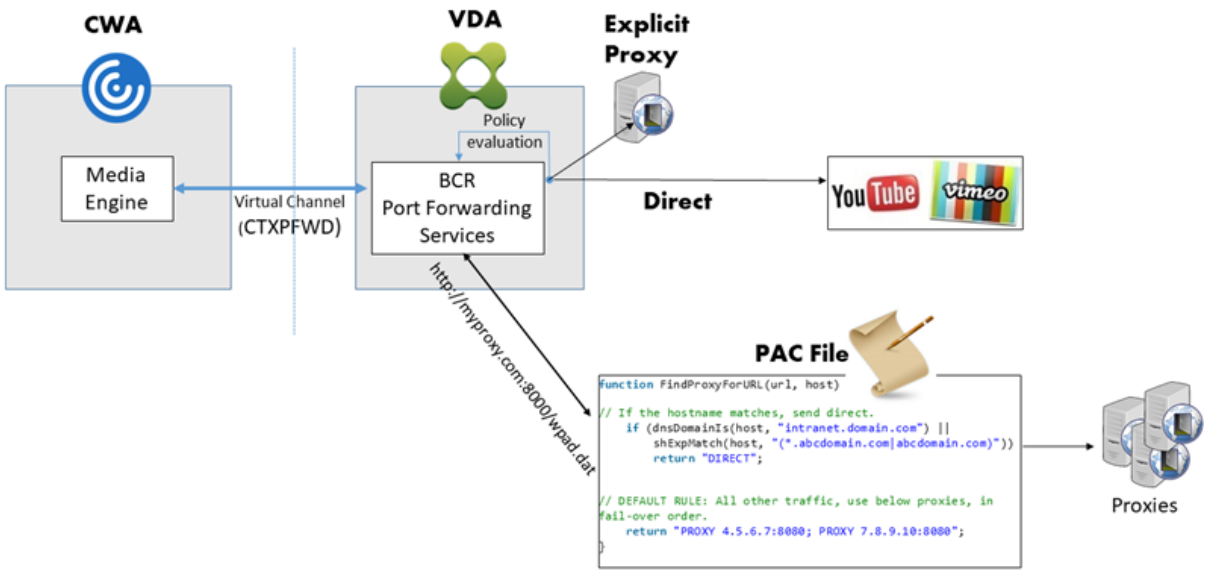
La aplicación Citrix Workspace obtiene el contenido de estas maneras:

- **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 quitar 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 (CTXPFWD). 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 en 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:

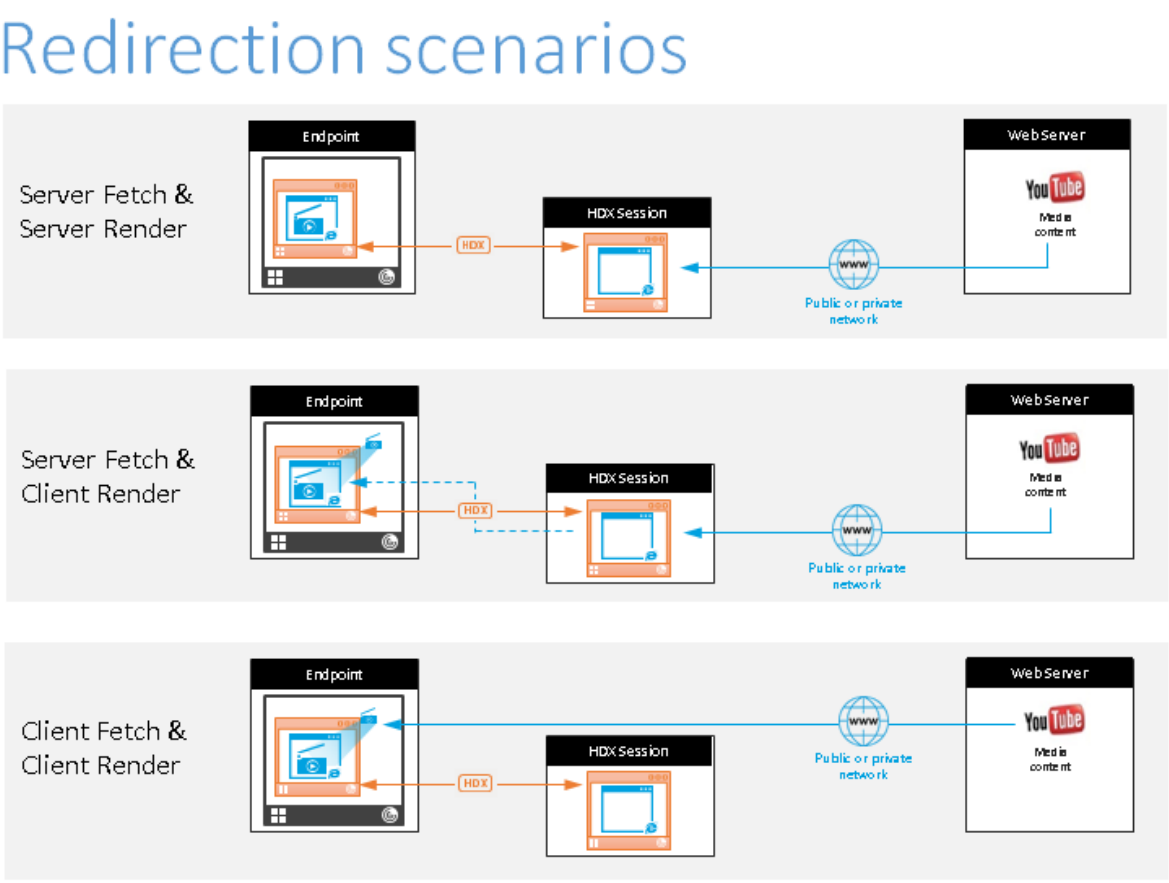
- **Proxy explícito**: Si tiene un solo proxy explícito en su centro de datos.
- **Directo o transparente**: Si no tiene proxies o si usa proxies transparentes.
- **Archivos PAC**: Si confía en archivos PAC, los exploradores del VDA pueden elegir automáticamente el servidor proxy apropiado para obtener la URL especificada.



- **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 de los sitios de XenApp y XenDesktop.

  Ventajas:

  - Mejor experiencia para el usuario final [velocidad de bits adaptable (ABR)]
  - Uso reducido de recursos de VDA (CPU / RAM / E/S)
  - Consumo reducido del ancho de banda



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 dirección URL no puede estar en la directiva de lista de bloqueados.

Requisitos del sistema

Citrix Virtual Apps and Desktops

- Citrix Virtual Apps and Desktops 7 1808 o versiones posteriores
- XenApp y XenDesktop 7.15 CU5 o posterior

- SO de VDA: Windows 10 y 11, Windows Server 2016/2019/2022
- Explorador en el VDA:
  - La versión más reciente de Google Chrome
  - La versión más reciente de Microsoft Edge
- Extensión BCR de Chrome Web Store instalada en el explorador web del VDA

Dispositivos de punto final Windows

- Windows 10 y 11
- Aplicación Citrix Workspace para Windows 1809 o versiones posteriores

> **Nota:**
>
> La redirección de contenido del explorador no se admite en las versiones LTSR 1912 y 2203.1 de la aplicación Citrix Workspace.

Dispositivos de punto final Linux

- Aplicación Citrix Workspace 1808 para Linux o versiones posteriores
- Los terminales de clientes ligeros deben incluir WebKitGTK+

Dispositivos de punto final Mac (Technical Preview)

- macOS 11 Big Sur
- macOS 12 Monterrey
- macOS 13 Ventura
- macOS 14 Sonoma (hasta 14.2.1) con la versión mínima 2311 de la aplicación Citrix Workspace

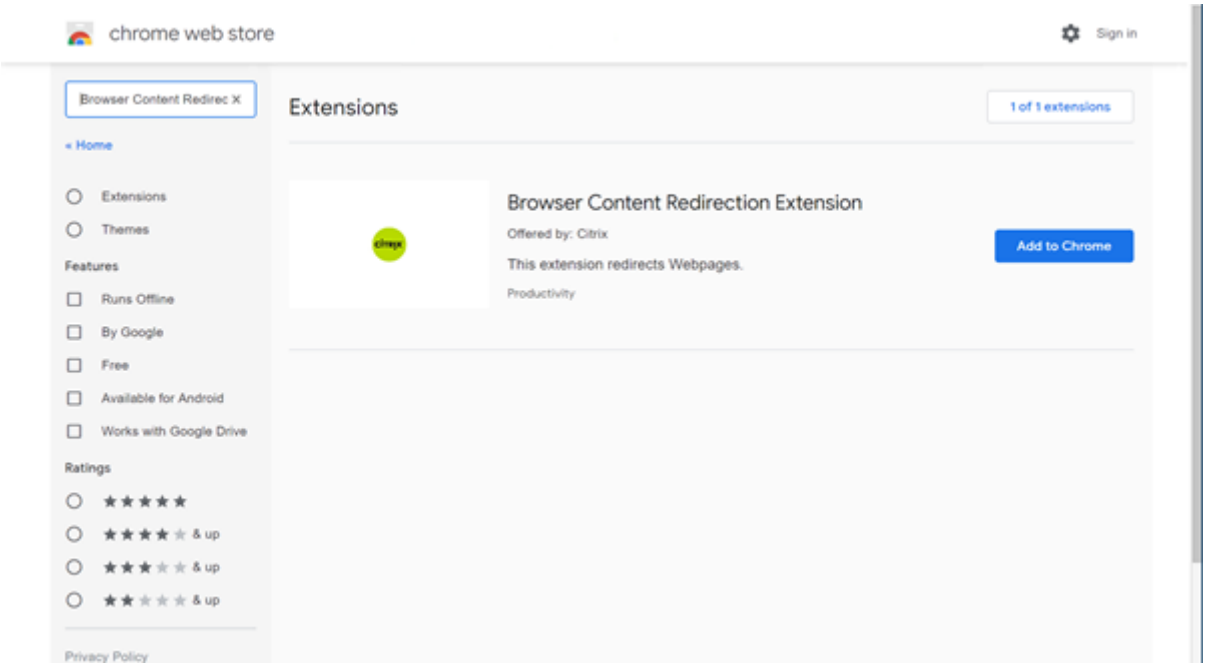
Solución de problemas

Para obtener información sobre solución de problemas, consulte el artículo How to troubleshoot browser content redirection de Knowledge Center.

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 **Agregar a Chrome** en el entorno de Citrix Virtual Apps and Desktops.

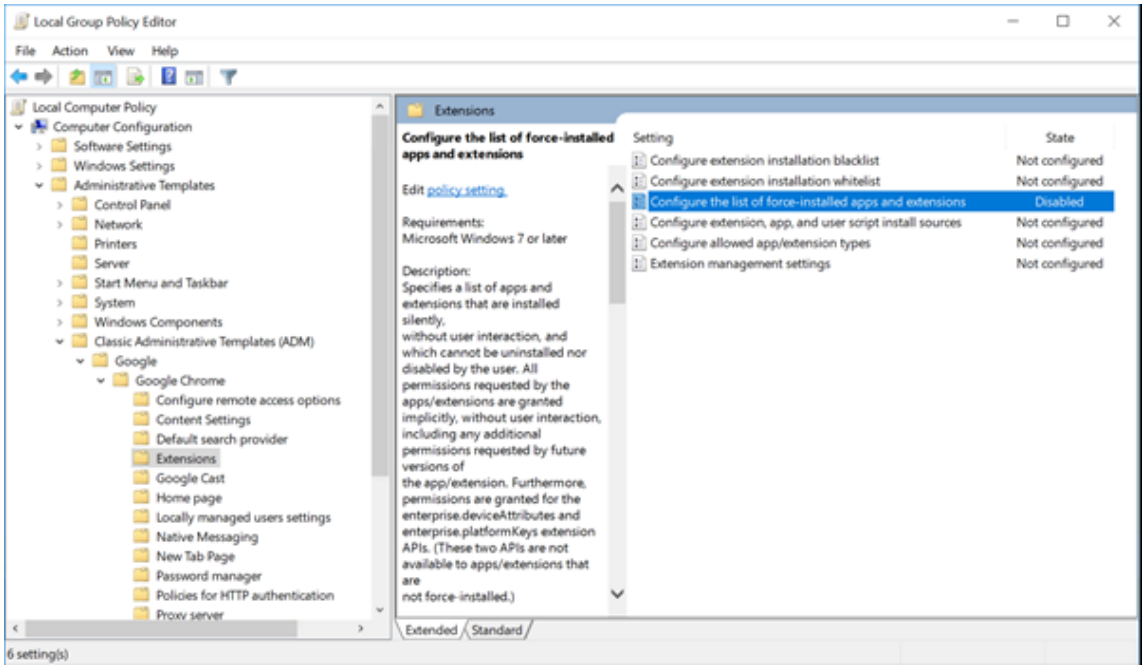
La extensión **no** se requiere en la máquina cliente del usuario, solo en el VDA.



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.

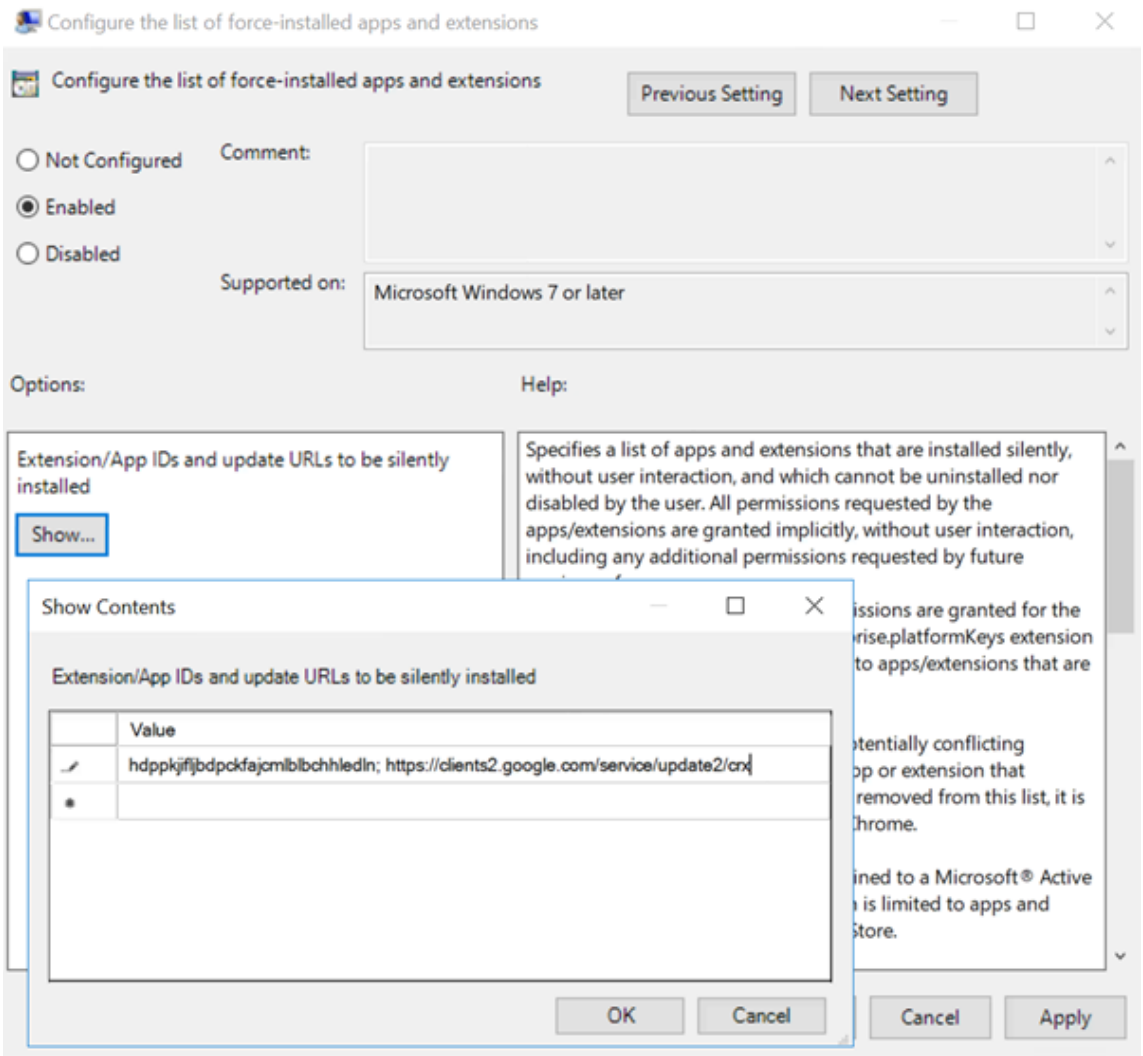
Implementar la extensión mediante la directiva de grupo

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 Definir políticas del explorador Chrome en equipos gestionados.
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 al 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.

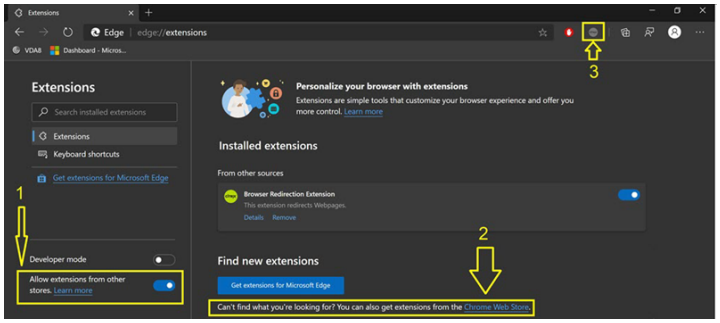
   Todas las actualizaciones de la extensión se instalan automáticamente en las máquinas de los usuarios a través de la URL de actualización que especificó en la configuración.

   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**. Elija **Administrar extensión**. 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

Cuando se usa la redirección de contenido del explorador con los PPP (escalado) establecidos por encima del 100% en la máquina del usuario, la pantalla de contenido redirigido del explorador 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 clave de Registro en la máquina del usuario. Para obtener información, consulte PPP y redirección de contenido del explorador en la lista de funciones administradas a través del Registro.

Single Sign-On con autenticación de Windows integrada (IWA)

La redirección de contenido del explorador web mejora la superposición para usar el esquema **Negotiate** para la autenticación en servidores web configurados con autenticación de Windows integrada (IWA) en el mismo dominio que el VDA.

De forma predeterminada, la redirección de contenido del explorador web utiliza un esquema de autenticación básico que requiere que los usuarios se autentiquen con sus credenciales de VDA cada vez que accedan al servidor web. Para el inicio de sesión único (Single Sign-On/SSO), puede habilitar la configuración de directiva **Redirección de contenido de explorador Web compatible con autenticación de Windows integrada (IWA)** o crear una clave de Registro en el VDA.

Antes de habilitar Single Sign-On, complete lo siguiente:

- Configure la infraestructura Kerberos para emitir tíquets para nombres principales de servicio (SPN) construidos a partir del nombre de host. Por ejemplo, `HTTP/serverhostname.com`.

- Para obtención de servidor: Cuando utilice la redirección de contenido del explorador Web en el modo de obtención de servidor, asegúrese de que el DNS está configurado correctamente en el VDA.
- Para obtención de cliente: Cuando utilice la redirección de contenido del explorador web en el modo de obtención de cliente, asegúrese de que el DNS está configurado correctamente en el dispositivo cliente y que permite conexiones TCP desde la superposición a la dirección IP del servidor web.

Para configurar Single Sign-On mediante la directiva Redirección de contenido de explorador web, consulte el parámetro Redirección de contenido del explorador compatible con autenticación de Windows integrada.

Como alternativa, para habilitar Single Sign-On en un servidor web, agregue una clave de registro en el VDA. Para obtener información, consulte Single Sign-On con autenticación de Windows integrada para redirección de contenido del explorador web en la lista de funciones administradas a través del Registro.

Encabezado de solicitud user-agent

El encabezado user-agent ayuda a identificar las solicitudes HTTP enviadas desde la redirección de contenido del explorador web. Este parámetro puede ser útil al configurar reglas de proxy y firewall. Por ejemplo: si el servidor bloquea las solicitudes enviadas desde la redirección de contenido del explorador web, puede crear una regla que contenga el encabezado user-agent para omitir ciertos requisitos.

Solo los dispositivos con Windows admiten el encabezado de solicitud user-agent.

De forma predeterminada, la cadena del encabezado de solicitud user-agent está inhabilitada. Para habilitar el encabezado user-agent para el contenido generado en el cliente, utilice el Editor del Registro. Para obtener información, consulte Encabezado de solicitud user-agent en la lista de funciones administradas a través del Registro.

Compatibilidad del cliente con redirección de contenido del explorador

Puede utilizar WMI para comprobar si su cliente es compatible con la redirección de contenido del explorador. Funciona cualquier método de acceso a WMI. A continuación se muestra un ejemplo en el que se utiliza PowerShell.

1. Abra PowerShell.
2. Ejecute `Get-WmiObject -Class CTXBCRStatus`.
3. Compruebe el parámetro `BCR_Capable`.
    - Si es `True`, el cliente es compatible con redirección de contenido del explorador.

- Si es `False`, el cliente no es compatible con redirección de contenido del explorador.

Información adicional

- Si `CtxBrowserSvc` no está disponible, no se muestran resultados al ejecutar el comando.
- Si `CtxBrowserSvc` no se ha ejecutado nunca, los resultados devuelven un error de clase no válida.

Limitaciones de redirección de contenido del explorador

La redirección de contenido del explorador no admite los siguientes casos de uso:

- No se admiten las aplicaciones web que requieren ventanas emergentes.
- Tampoco se admiten las aplicaciones web que requieren persistencia de las cookies de sesión. Las aplicaciones que dependen del servicio de autenticación de Google (por ejemplo, Google Meet) pueden bloquearse.
- El plug-in de extensión no se publica oficialmente en la tienda de aplicaciones de Microsoft Edge. Sin embargo, puede usar la tienda de aplicaciones de Chrome para instalar las extensiones.
- La directiva de redirección de vídeo HTML5 debe estar inhabilitada cuando se utilice la redirección de contenido del explorador.
- La redirección de contenido del explorador no es compatible con el marco ARMhf (ARM hard-float).
- En ocasiones, las sesiones de usuario se pueden desconectar debido a redes poco fiables, una latencia en la red muy variable o limitaciones en el alcance de los dispositivos inalámbricos. Actualmente, la redirección de contenido del explorador (BCR) no cuenta con suficientes mecanismos alternativos o de generación de informes para esos casos.
- No puede descargar archivos ni imprimirlos en el explorador superpuesto de BCR.

Conferencias de vídeo de HDX y compresión de vídeo para cámaras web de HDX

August 17, 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 usa el Editor del Reg-

> istro, 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. La redirección de USB genérico de HDX solo se recomienda cuando hay problemas de compatibilidad de las aplicaciones con compresión de vídeo de HDX o cuando se requieren funcionalidades nativas avanzadas de la cámara web. Para obtener un mejor rendimiento, Citrix recomienda que Virtual Delivery Agent tenga al menos dos CPU virtuales.

Para evitar que los usuarios cambien la compresión de vídeo de cámaras web de HDX, inhabilite la redirección de dispositivos USB desde los parámetros en **Configuraciones de la directiva ICA > Configuraciones de directiva de 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**.

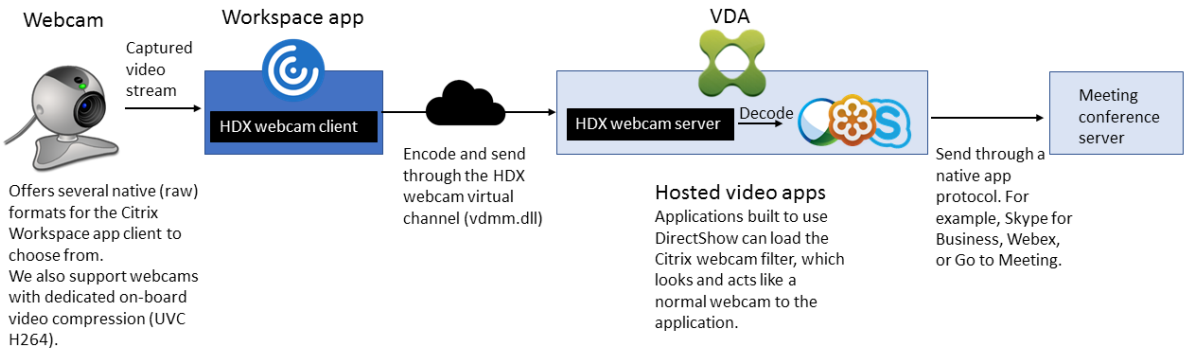
Compresión de vídeo de cámara web HDX

La compresión de vídeo de cámaras web de HDX también se llama modo de cámara web **optimizado**. Este tipo de compresión de vídeo por cámara web envía el vídeo en H.264 directamente a la aplicación de videoconferencias de la sesión virtual. Para optimizar los recursos de los VDA, la compresión de cámaras web de HDX no codifica, transcodifica ni decodifica el vídeo de las cámaras web. Esta función está habilitada de manera predeterminada.

Para inhabilitar el streaming directo de vídeo del servidor a la aplicación de videoconferencias, establezca la clave de Registro en 0 en el VDA. Para obtener información, consulte Compresión de vídeo de cámara web en la lista de funciones administradas a través del Registro.

Si inhabilita la funcionalidad predeterminada para los recursos de streaming de vídeo, la compresión de vídeo de cámaras web de HDX utiliza la tecnología marco multimedia que forma parte del sistema operativo cliente para interceptar vídeo de 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 su integración le ofrece 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 directiva de **conferencias multimedia** debe estar habilitada para la compresión de vídeo de cámara web HDX. Esta directiva está habilitada de forma predeterminada.

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, modifique la clave de Registro en el cliente. Para obtener información, consulte Compresión de software de cámara web en la lista de funciones administradas a través del Registro.

Requisitos para la compresión de vídeo de cámaras web de HDX

La compresión de vídeo de cámaras web de HDX admite las siguientes versiones de la aplicación Citrix Workspace:

Plataforma	Procesador
Aplicación Citrix Workspace para Windows	La aplicación Citrix Workspace para Windows admite la compresión de vídeo de cámara web para aplicaciones de 32 y 64 bits en XenApp y XenDesktop 7.17 y versiones posteriores. En versiones anteriores, la aplicación Citrix Workspace para Windows solo es compatible con aplicaciones de 32 bits.
Aplicación Citrix Workspace para Mac	La aplicación Citrix Workspace para Mac 2006 o versiones posteriores admite la compresión de vídeo de cámara web para aplicaciones de 64 bits en XenApp y XenDesktop 7.17 y versiones posteriores. En versiones anteriores, la aplicación Citrix Workspace para Mac solo es compatible con aplicaciones de 32 bits.

Plataforma	Procesador
Aplicación Citrix Workspace para Linux	La aplicación Citrix Workspace para Linux admite tanto aplicaciones de 32 bits como de 64 bits en el escritorio virtual.
Aplicación Citrix Workspace para Chrome	Debido a que algunos dispositivos Chromebook ARM no son compatibles con la codificación H.264, solo las aplicaciones de 32 bits pueden utilizar la compresión de vídeo de cámaras web de HDX optimizada.

Las aplicaciones de vídeo basadas en Media Foundation admiten la compresión de vídeo de cámaras web de HDX en Windows 10 o posterior, Windows Server 2019 y versiones posteriores. Para obtener más información, consulte el artículo CTX132764 de Knowledge Center.

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 por 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. No es necesario instalar los controladores del dispositivo en el servidor.

Las distintas cámaras web ofrecen diferentes velocidades de fotogramas y tienen diferentes niveles de brillo y contraste. Ajustar el contraste de la cámara web puede reducir considerablemente el tráfico ascendente. Citrix utiliza las siguientes cámaras web para la validación inicial de funciones:

- Modelos de Microsoft LifeCam VX (2000, 3000, 5000, 7000)
- Creative Live! Cam Optia Pro
- Logitech QuickCam Messenger
- Logitech C600, C920
- HP Deluxe Webcam

Para ajustar la velocidad de fotogramas de vídeo preferida, modifique la clave de Registro en el cliente: Para obtener información, consulte Velocidad de fotogramas en compresión de vídeo por cámara web en la lista de funciones administradas a través del Registro.

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 de videoconferencias admiten la generación de alta definición, la aplicación usa la resolución de alta definición. Admitimos todas las resoluciones de cámara web.

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 y habilitar la función. Para obtener más información, consulte Streaming por cámara web de alta definición en la lista de funciones administradas a través del Registro.

Si la negociación del tipo de medios falla, HDX recurre a la resolución VGA predeterminada (640 x 480 píxeles). Puede usar claves de Registro en el cliente para configurar la resolución predeterminada. Compruebe que la cámara admite la resolución especificada. Para obtener más información, consulte Resolución de cámara web de alta definición en la lista de funciones administradas a través del Registro.

La compresión de vídeo de cámaras web de HDX utiliza considerablemente menos ancho de banda en comparación con la redirección de USB genérico Plug-n-Play y funciona bien en conexiones WAN. Para ajustar el ancho de banda, establezca la clave de Registro en el cliente. Para obtener más información, consulte Ancho de banda de cámara web de alta definición en la lista de funciones administradas a través del Registro.

Introduzca un valor en bits por segundo. Si no especifica el ancho de banda, las aplicaciones de videoconferencias utilizan 350 000 bps de forma predeterminada.

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 Plug-n-Play de HDX 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 en el servidor 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

August 17, 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, el sector de los exploradores 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, 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 propios, incluidas:

- 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

Función	HTML5	Flash
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

Versión mínima del explorador web en el VDA	SO Windows versión/compilación/SP
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 https://wiki.mozilla.org/CA:AddRootToFirefox	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 de 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 and XenDesktop Engineering; CN = Citrix XenApp and 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 and XenDesktop Engineering; CN = Citrix XenApp and 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

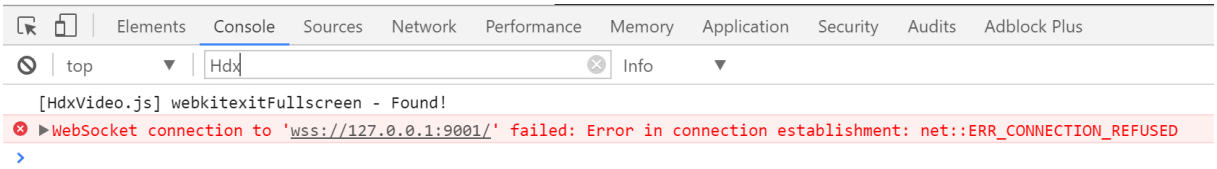
En esta versión, esta funcionalidad está disponible solo para las páginas web controladas. Requiere que se agregue HdxVideo.js de JavaScript (incluido en los medios de instalación de Citrix Virtual Apps and Desktops) a las páginas web donde está disponible el contenido multimedia HTML5. Por ejemplo: 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

August 17, 2024

> **Nota:**
>
> El nuevo Microsoft Teams 2.1 ya está disponible de forma generalizada para VDA. Esta versión de Microsoft Teams es compatible con la Optimización para Microsoft Teams de Citrix mediante WebRTC (VDI 1.0).
>
> A partir de Citrix Virtual Apps and Desktops 2402, no es necesario configurar manualmente la entrada `msedgewebview2.exe` del Registro, ya que aparece en la lista de permitidos de forma predeterminada.
>
> Las aplicaciones publicadas ahora son compatibles con el nuevo Microsoft Teams.

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).

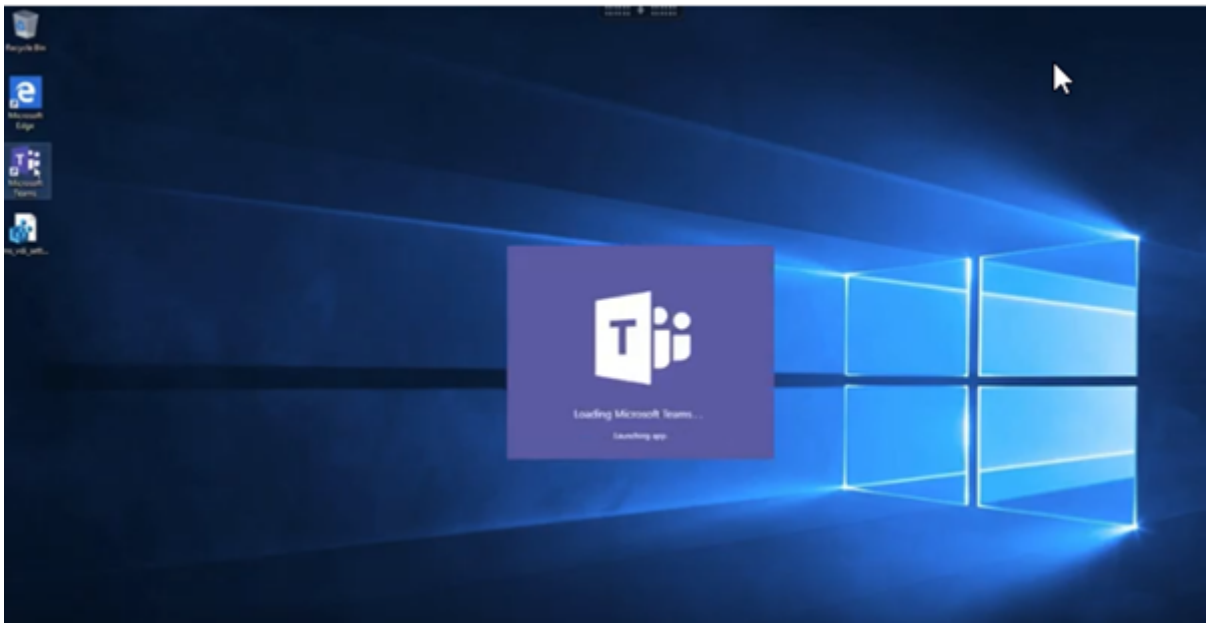
Nuestra optimización para Microsoft Teams incluye una API y servicios de HDX del lado de VDA para interactuar con la aplicación alojada Teams y recibir comandos. Estos componentes abren un canal virtual de control (CTXMTOP) en el motor de medios de la aplicación Citrix Workspace. El dispositivo de punto final descodifica y proporciona 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

Citrix y Microsoft recomiendan la última versión disponible de Microsoft Teams y mantenerla actualizada.
No se admiten las versiones de la aplicación de escritorio de Microsoft Teams con fechas de publicación que son más de 90 días anteriores a la fecha de publicación de la versión actual.
Las versiones no compatibles de la aplicación de escritorio de Microsoft Teams muestran una página de bloqueo a los usuarios y solicitan actualizar la aplicación.

Para obtener información sobre las últimas versiones disponibles, consulte Update history for Microsoft Teams App (Desktop and Mac).

Le recomendamos que siga las directrices de instalación para toda la máquina de Microsoft Teams. No utilice el instalador EXE que instala Microsoft 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 usa el parámetro `ALLUSERS=1`. Al establecer este parámetro, el instalador de Microsoft Teams a nivel de equipo aparece en **Programas y funciones**, en el **Panel de control**. También en **Aplicaciones y funciones**, en Configuración de Windows, para todos los usuarios del equipo. Todos los usuarios pueden desinstalar Microsoft 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 Microsoft Teams no se actualiza automáticamente cuando hay una nueva versión. Recomendamos este modo para entornos no persistentes, como 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).

Supongamos que tiene un entorno VDI persistente dedicado en Windows 10. Quiere que la aplicación Microsoft Teams se actualice automáticamente y prefiere que Microsoft Teams se instale por usuario en `Appdata/Local`. En este caso, utilice el instalador `.exe` o el MSI sin `ALLUSER=1`.

> **Nota:**
>
> Citrix recomienda instalar el VDA antes de instalar Microsoft Teams en la imagen dorada. Este orden de instalación es necesario para que el indicador `ALLUSER=1` surta efecto. Si la máquina virtual tenía Microsoft Teams instalado antes de instalar el VDA, desinstale Microsoft Teams y vuelva a instalarlo.

Para el acceso con Remote PC

Citrix recomienda instalar la versión 1.4.00.22472 de Microsoft Teams o una posterior después de instalar el VDA. De lo contrario, deberá cerrar sesión e iniciar sesión de nuevo para que Microsoft Teams detecte el VDA según lo previsto. A partir de la versión 1.4.00.22472, se incluye lógica aumentada ejecutada en el inicio de Microsoft Teams y en el inicio de sesión para la detección de VDA. En estas versiones también se incluye la identificación del tipo de sesión activa (HDX, RDP o conectada localmente a la máquina cliente). Si se conectó localmente, es posible que las versiones anteriores de Microsoft Teams no detecten ni inhabiliten determinadas funciones o elementos de la interfaz de usuario. Por ejemplo, salas para sesión de subgrupo, ventanas emergentes para reuniones y chats o reacciones en las reuniones.

> **Importante:**
>
> Al pasar de una sesión local a una sesión HDX y si Microsoft Teams se mantiene abierto y ejecutándose en segundo plano, debe salir y volver a iniciar Microsoft Teams para optimizar la sesión con HDX correctamente.
> Por el contrario, si utiliza Microsoft Teams de forma remota a través de una sesión HDX optimizada, desconecte la sesión HDX y vuelva a conectarse a la misma sesión de Windows localmente en el dispositivo. Cuando trabaje desde la oficina, deberá volver a iniciar Microsoft Teams para que pueda detectar correctamente el estado de Acceso con Remote PC (HDX o local). Esto se debe a que Microsoft Teams solo puede evaluar el modo VDI en el momento de iniciarse la aplicación, y no mientras ya se está ejecutando en segundo plano. Sin un reinicio, es posible que Microsoft Teams no cargue funciones como ventanas emergentes, grupos de trabajo o reacciones en las reuniones.

Para App Layering

Si utiliza Citrix App Layering para administrar instalaciones de VDA y Microsoft Teams en diferentes capas, deberá crear una clave de Registro en los VDA con Windows antes de instalar Microsoft Teams con el indicador `ALLUSER=1` desde la línea de comandos. Para obtener más información, consulte la sección *Optimización para Microsoft Teams con Citrix App Layering* en Multimedia.

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 Microsoft Teams se instala en `C:\Program Files (x86)` (unos 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.

> **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 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 Microsoft Teams en cualquier máquina virtual Windows Server de 64 bits:

Carpeta:

- `C:\Program Files (x86)\Microsoft\Teams`
- `C:\Users\<username>\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`
- Nombre: `Teams`
- Tipo: `REG_SZ`
- Valor: `C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

> **Nota:**
>
> La ubicación del Registro varía según los sistemas operativos subyacentes y la cantidad de bits.

Recomendaciones

- Recomendamos inhabilitar el inicio automático eliminando las claves de Registro de Microsoft Teams. Al hacerlo, se evita que muchos inicios de sesión que ocurren al mismo tiempo (por ejemplo, al comenzar la jornada laboral) saturen la CPU de la máquina virtual.
- Si el escritorio virtual no tiene una GPU/vGPU, se recomienda **Inhabilitar la aceleración de hardware de GPU** en la **Configuración** de Microsoft Teams para mejorar el rendimiento. Este parámetro (`"disableGpu":true`) se almacena en `%Appdata%\Microsoft\Teams`, en `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 Microsoft Teams.

Instalador por usuario

Cuando se utiliza el instalador `.exe`, el proceso de instalación es diferente. Todos los archivos se colocan en AppData.

Carpeta:

- `C:\Users\<username>\AppData\Local\Microsoft\Teams`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsPresenceAddin`
- `C:\Users\<username>\AppData\Local\Microsoft\TeamsMeetingAddin`
- `C:\Users\<username>\AppData\Local\SquirrelTemp`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

Acceso directo de escritorio:

```
C:\Users\<username>\AppData\Local\Microsoft\Teams\Update.exe --
processStart "Teams.exe"
```

Registro:

```
HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

Prácticas recomendadas

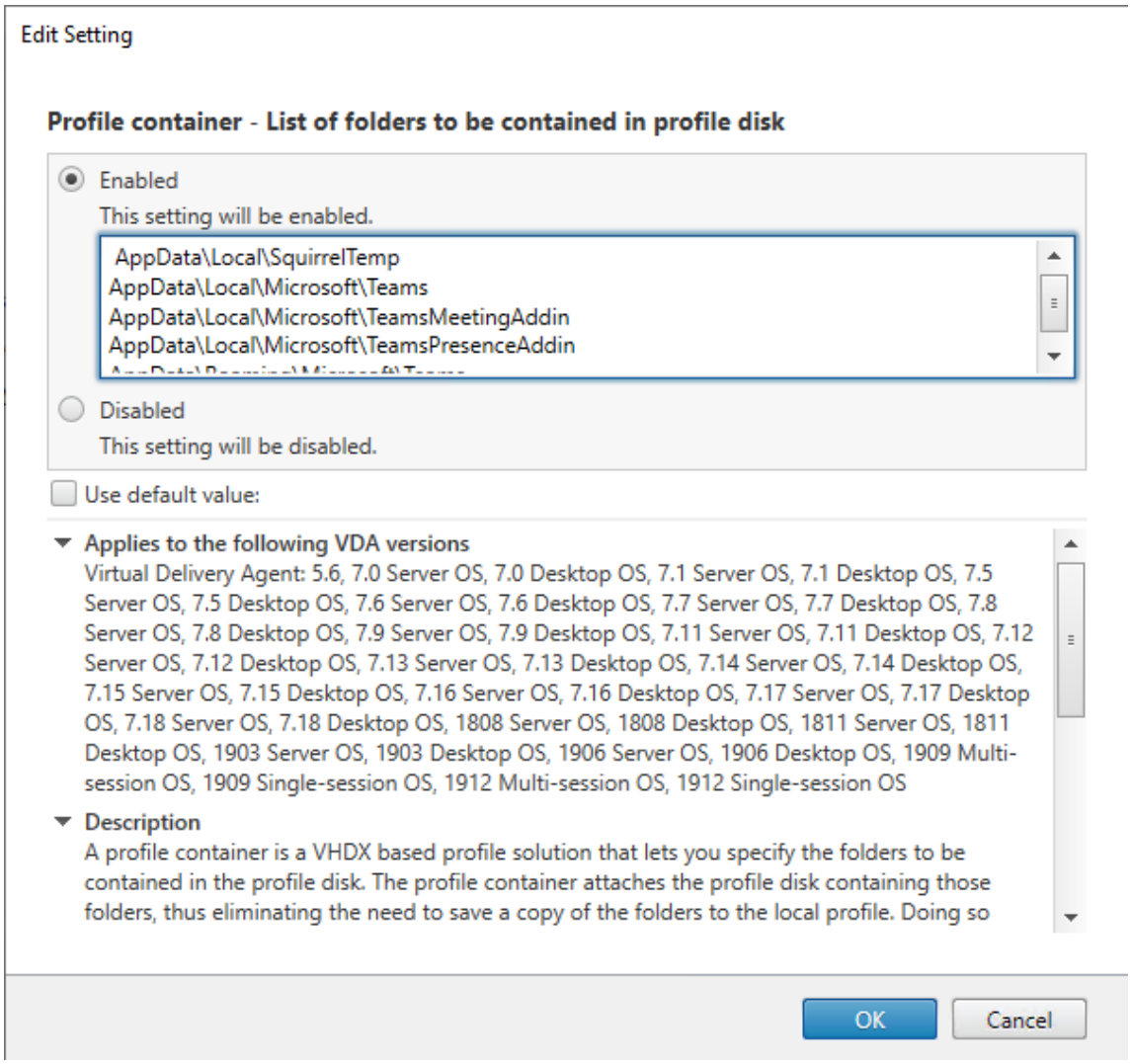
Las recomendaciones se basan en casos de uso.
El uso de Microsoft Teams con una configuración no persistente requiere un administrador de almacenamiento en caché de perfiles para una sincronización eficiente de los datos de runtime de Microsoft Teams. Con un administrador de almacenamiento en caché de perfiles, la información específica del usuario necesaria se almacena en caché durante la sesión de usuario. La información específica del usuario incluye los datos de usuario, el perfil y la configuración. Sincronice los datos de estas dos carpetas:

- `C:\Users\<username>\AppData\Local\Microsoft\IdentityCache`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

Lista de exclusión de contenido almacenado en caché de Microsoft Teams para una configuración no persistente Excluya los archivos y directorios de la carpeta de almacenamiento en caché de Microsoft Teams como se describe en la documentación de Microsoft. Esta acción ayuda a reducir el tamaño del almacenamiento en caché del usuario para optimizar aún más la configuración no persistente.

Caso de uso: Sesión única En este caso, el usuario final utiliza Microsoft Teams en una ubicación cada vez. No es necesario que ejecuten Microsoft Teams en dos sesiones de Windows al mismo tiempo. En una implementación de escritorio virtual común, cada usuario se asigna a un escritorio y Microsoft Teams se implementa en el escritorio virtual como una aplicación.
Se recomienda habilitar el contenedor de perfiles de Citrix y redirigir los directorios por usuario que se indican en Instalador por usuario 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**.



Enumera todos los directorios por usuario 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 2022, 2019, 2016, 2012R2 ediciones Standard y Datacenter, y con opción Server Core

Versión mínima: Virtual Delivery Agent (VDA) 1906.2

Sistemas operativos compatibles:

- Windows 11
- Windows 10 de 64 bits, versión 1607 y versiones posteriores. Las aplicaciones alojadas en máquinas virtuales se admiten en la aplicación Citrix Workspace para Windows 2109.1 y versiones posteriores.
- Windows Server 2022, 2019, 2016 y 2012 R2 (ediciones Standard y Datacenter)

Requisitos:

- BCR_x64.msi: El MSI que incluye 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: La versión Current Release más reciente de la aplicación Citrix Workspace para Windows; versión mínima: aplicación Citrix Workspace 1907 para Windows

- Windows 11.
- Windows 10 (ediciones de 32 y 64 bits, incluidas las ediciones Embedded; la compatibilidad con Windows 7 dejó de ofrecerse en la versión 2006, y la compatibilidad con Windows 8.1 dejó de ofrecerse en la versión 2204.1).
- 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 y AIO.
- 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 disco y 1 GB de RAM.
- El requisito mínimo de Microsoft .NET Framework es la versión 4.8. La aplicación Citrix Workspace descarga e instala automáticamente .NET Framework, si no está presente en el sistema.

Los administradores pueden habilitar/inhabilitar Microsoft Teams iniciando en el modo optimizado y cambiando la directiva Optimización de Microsoft Teams. Los usuarios que inician en modo optimizado en la aplicación Citrix Workspace no pueden inhabilitar Microsoft Teams.

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
- `libnsl`
- Ubuntu 20.04 o posterior

Mejora en la autenticación:

- Biblioteca libsecret
- Biblioteca libunwind-12. Para obtener más información, consulte Incorporar la dependencia de "libunwind-12 library"para llvm-12.

Hardware:

- Como mínimo, una CPU de doble núcleo de 1,8 GHz que admita una resolución de 720p HD durante llamadas de conferencia 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 una lista completa de dispositivos de punto final verificados, consulte Clientes ligeros.

Para obtener más información, consulte Requisitos previos para instalar la aplicación Citrix Workspace.

Puede inhabilitar la optimización para Microsoft Teams. Para ello, actualice el valor del campo **VDWEBRTC** a Off en el archivo `/opt/Citrix/ICAClient/config/module.ini`. El valor predeterminado es VDWEBRTC = On. Una vez finalizada la actualización, reinicie la sesión. (se requiere permiso en la raíz).

Versión mínima: Aplicación Citrix Workspace 2012 para Mac

Sistemas operativos compatibles:

- macOS Catalina (10.15).
- macOS Big Sur 11.0.1 y versiones posteriores.
- macOS Monterrey.

Funciones compatibles:

- Audio
- Vídeo
- Optimización para compartir pantalla (entrante y saliente)

> **Nota:**
>
> La aplicación Citrix Viewer necesita acceder a las preferencias de Seguridad y privacidad de macOS para que el uso compartido de la pantalla funcione. Los usuarios configuran esta preferencia en el **menú Apple > Preferencias del Sistema > Seguridad y privacidad > Ficha Privacidad > Grabación de pantalla** y al seleccionar **Citrix Viewer**.

La optimización para Microsoft Teams funciona de forma predeterminada con la aplicación Citrix Workspace 2012 y versiones posteriores y macOS 10.15.

Si quiere desactivar la optimización de Microsoft Teams, ejecute este comando en el terminal y reinicie la aplicación Citrix Workspace:

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

Versión mínima: La versión más reciente de la aplicación Citrix Workspace para ChromeOS activa en la versión más reciente de ChromeOS

Hardware:

- Procesadores que funcionan igual o mejor que el Intel i3 de cuatro núcleos a 2,4 GHz.

Funciones compatibles:

- Audio
- Vídeo
- Optimización para compartir pantalla (entrante y saliente): Inhabilitada de forma predeterminada. Consulte estos parámetros para obtener instrucciones sobre cómo activarla.

Escalabilidad de un solo servidor

En esta sección se ofrecen recomendaciones y orientación para estimar cuántos usuarios o máquinas virtuales (VM) puede admitir un único host físico. Esto se conoce comúnmente como "escalabilidad de un solo servidor"(SSS/Single Server Scalability) de Citrix Virtual Apps and Desktops. En el contexto de Citrix Virtual Apps (CVA) o virtualización de sesiones, también se conoce comúnmente como densidad de usuarios. La idea es averiguar cuántos usuarios o máquinas virtuales pueden trabajar en un único componente de hardware que ejecute un hipervisor principal.

> **Nota:**
>
> Esta sección incluye información para estimar la escalabilidad de un solo servidor (SSS). La información es general y no necesariamente aplicable a su situación o entorno en particular. La única forma de entender realmente el valor de SSS en Citrix Virtual Apps and Desktops es utilizando una herramienta para pruebas de carga o escalabilidad como Login VSI. Citrix recomienda usar esta información y estas reglas simples únicamente para estimar rápidamente el valor SSS. Sin embargo, Citrix recomienda usar Login VSI o la herramienta de pruebas de carga que elija para validar los resultados, especialmente antes de comprar hardware o tomar cualquier decisión de carácter financiero.

Hardware (sistema sometido a prueba)

- Dell PowerEdge R740
- Intel Xeon (Gold) 6126 a 2,60 GHz (máx. Turbo 3,70 GHz), 12 núcleos por socket, socket doble con Hyper-Threading habilitado
- 382 GB de RAM
- Almacenamiento SSD RAID 0 local (11 discos) 6 TB

Software

Una sola máquina virtual (40 procesadores lógicos) con Windows 2019 (TSVDA) que ejecute Citrix Virtual Apps and Desktops 2106
VMware ESXi 6.7

Terminología

- Carga de trabajo de los trabajadores del conocimiento: Incluye Acrobat Reader, Freemind/Java, visor de fotos, Edge y aplicaciones de MS Office como Excel, Outlook, PowerPoint y Word.
- Base de referencia: Las pruebas de escalabilidad del servidor se ejecutan con la carga de trabajo los trabajadores del conocimiento (sin Microsoft Teams).
- Carga de trabajo de Microsoft Teams: Carga de trabajo típica de trabajador del conocimiento + Microsoft Teams

Cómo es la prueba de estrés de Microsoft Teams

- Microsoft Teams se optimiza con HDX. Por lo tanto, todo el procesamiento multimedia se envía al dispositivo de punto final o al cliente y no forma parte de la medición.
- Todos los procesos de Microsoft Teams se detienen o finalizan antes del comienzo de la carga de trabajo.
- Abra Microsoft Teams (arranque en frío).
- Mida el tiempo que tarda Microsoft Teams en cargar y captar el foco de la ventana principal de Microsoft Teams.
- Cambie a la ventana de chat con los atajos de teclado.
- Cambie a la ventana del calendario con los atajos de teclado.
- Envíe el mensaje de chat a un usuario específico con los atajos de teclado.
- Cambie a la ventana de Microsoft Teams con los atajos de teclado.

Resultados

- Impacto de escalabilidad del 40 % con la carga de trabajo de Microsoft Teams (81 usuarios), en comparación con la base de referencia (137 usuarios).
- Al aumentar la capacidad del servidor en un 40 % aproximadamente (en CPU), se restaura la cantidad de usuarios como ocurre con la carga de trabajo de referencia.
- Se requiere un 20 % de memoria adicional con la carga de trabajo de Microsoft Teams, en comparación con la base de referencia.
- Aumento del tamaño de almacenamiento por usuario de 512 a 1024 MB.
- ~50 % de aumento en la escritura de IOPS, ~100 % de aumento en las lecturas de IOPS. Microsoft Teams puede tener un impacto significativo en entornos con un almacenamiento más lento.

Tabla de funciones y compatibilidad de versiones

Función	Microsoft Teams (versión mínima)	VDA (versión mínima)	Aplicación Citrix Workspace para Windows CR (versión mínima)	Aplicación Citrix Workspace para Mac (versión mínima)	Aplicación Citrix Workspace para Linux (versión mínima)	Aplicación Citrix Workspace para ChromeOS (versión mínima)
Audio/vídeo (P2P y conferencias)	versión actual menos 90 días	1906	1907	2009	2004	2105.5
Uso compartido de pantalla	Versión actual menos 90 días	1906	1907	2012	2006	2105.5
i. Borde rojo del indicador de la pantalla	Versión actual menos 90 días	1906	2002	2012	2006	No
ii. Limitar la captura a Desktop Viewer	Versión actual menos 90 días	1906	2009.5	2012	2006	No
iii. Varios monitores	Versión actual menos 90 días	1912 CU6+	2106 (1)	2106	2106	No
DTMF	Versión actual menos 90 días	N/D	2102	2101	2101	2111.1
Compatibilidad con servidores proxy	Versión actual menos 90 días	N/D	2012 (2)	2104 (3)	2101 (3)	2305

Función	Microsoft Teams (versión mínima)	VDA (versión mínima)	Aplicación Citrix Workspace para Windows CR (versión mínima)	Aplicación Citrix Workspace para Mac (versión mínima)	Aplicación Citrix Workspace para Linux (versión mínima)	Aplicación Citrix Workspace para ChromeOS (versión mínima)
Uso compartido de aplica-ciones	Versión actual menos 90 días	2109	2109.1	2203.1	2209	No
Subtítulos en directo	Versión actual menos 90 días	N/A (4)	2109.1	2109	2109	2303
e911 dinámico	Versión actual menos 90 días	N/D	2112.1	2112	2112	2112
Dar control	Versión actual menos 90 días	N/D	2112.1	2203.1	No	No
Solicitar el control	Versión actual menos 90 días	N/D	2112.1	2203.1	2203	2303
Multiventana	1.5.00.11865	2112, 1912 CU6 (5)	2112.1	2203.1	2203	2303
Transcripciones de reuniones	Versión actual menos 90 días	2112.1, 1912 CU6 y versiones posteriores	2112	2203.1	2203	2303
Desenfoque de fondo	Versión actual menos 90 días	2112, 1912 CU6 y versiones posteriores	2207	2301	2212	2303

1. El visor del CD en modo de pantalla completa solamente. MAYÚS+F2 no está disponible.

2. Negotiate/Kerberos, NTLM, Basic y Digest. Los archivos Pac también son compatibles.
3. Anónimos solamente.
4. Si el VDA tiene la versión 2112 o una posterior, los subtítulos en directo solo funcionan si la versión de la aplicación Citrix Workspace es 2203.1 para MAC y 2203 para Linux o 2112 para Windows. Esto se debe a que los subtítulos en directo se comportan de manera diferente si Microsoft Teams está en modo de interfaz de ventana única o en modo de varias ventanas.
5. El modo multiventana se introdujo en la versión 2112 de VDA, pero se transfirió a la versión 1912 LTSR CU6 de VDA.

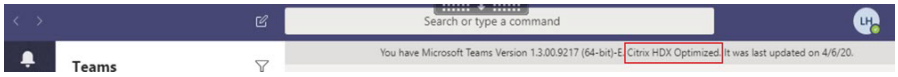
> **Nota:**
>
> - Todas las funciones enumeradas en la **Aplicación Citrix Workspace para Windows 1912 CU6 (o una versión posterior)** son válidas para la aplicación Citrix Workspace para Windows 2203.1 LTSR CU1.
> - Microsoft ha retirado el modo de ventana única en Microsoft Teams. Para cumplir con las normas, debe actualizar su VDA a 1912 CU6 LTSR o a una versión posterior y a la aplicación Citrix Workspace 2203 CU2 o a una versión posterior, la cual ofrece el modo multiventana.

Habilitar la optimización de Microsoft Teams

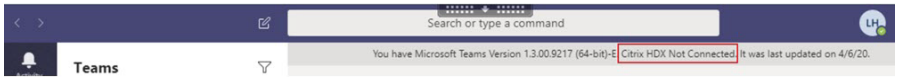
Para habilitar la optimización de Microsoft Teams, utilice la directiva de la consola Administrar descrita en la directiva de redirección de Microsoft Teams. Esta directiva está **activada** de forma predeterminada. Además de habilitar esta directiva, HDX comprueba si la versión de la aplicación Citrix Workspace es, al menos, la mínima requerida. Si se ha habilitado la directiva y se admite la versión de la aplicación Citrix Workspace, **HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupp** se establece en **1** automáticamente en el VDA. Microsoft Teams lee la clave para cargar en modo VDI.

> **Nota:**
>
> Si utiliza agentes VDA de la versión 1906.2, o una posterior, con versiones de controladores anteriores (por ejemplo, versión 7.15) que no tienen la directiva disponible en la consola Administrar (Studio), el VDA aún puede optimizarse. La optimización HDX para Microsoft Teams está habilitada de forma predeterminada en el VDA.

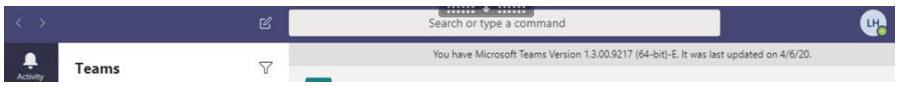
Si hace clic en **Acerca de > Versión**, aparecerá la leyenda **Optimizado para Citrix HDX**:



Si se muestra que **Citrix HDX no está conectado**, la API de Citrix se carga en Microsoft Teams. Cargar la API es el primer paso hacia la redirección. Pero hay un error en las partes 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, Microsoft Teams no pudo cargar la API de Citrix. Salga de Microsoft Teams haciendo clic con el botón secundario en el icono del área de notificaciones y reiniciando. Asegúrese de que la directiva de la consola Administrar no esté establecida en **Prohibido** y de que la versión de la aplicación Citrix Workspace sea compatible.



Importante: Reconexiones de sesión

- Es posible que tenga que iniciar Microsoft Teams de nuevo para obtener una sesión optimizada para HDX cuando su conectividad cambia. Por ejemplo, si se traslada de un dispositivo de punto final no compatible (aplicación Workspace para iOS, Android o versiones anteriores de Windows/Linux/Mac) a uno compatible (aplicación Workspace para Windows/Linux/Mac/Chrome OS/HTML5) o viceversa.
- También es necesario reiniciar Microsoft Teams si ha instalado la aplicación con el instalador EXE de Microsoft Teams en el VDA. Se recomienda el instalador EXE para implementaciones de VDI persistentes. En estos casos, Microsoft Teams puede actualizarse automáticamente mientras la sesión HDX está en estado desconectado. Por lo tanto, los usuarios que se reconectan a una sesión HDX descubren que Microsoft Teams no se ejecuta de forma optimizada.
- Al pasar de una sesión local a una sesión HDX, debe iniciar Microsoft Teams de nuevo para optimizar la sesión con HDX. Esta acción es necesaria en caso de acceso con Remote PC.

Requisitos de la red

Microsoft Teams se basa en servidores Media Processor (procesador de multimedia) en Microsoft 365 para las reuniones o llamadas con múltiples participantes. Además, Microsoft Teams se basa en Transport Relay (traspaso de transporte) de Microsoft 365 para estos casos:

- Dos pares en una llamada punto a punto sin conectividad directa
- Un participante no tiene conectividad directa con el procesador de multimedia.

Así, el estado de la red entre el par y la nube de Microsoft 365 determina el rendimiento de la llamada. Para obtener pautas detalladas sobre la planificación de redes, consulte Principios de conectividad de red de Microsoft 365.

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 for Business 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 Microsoft 365 de la forma más directa posible desde la sucursal.
- Planifique y proporcione suficiente ancho de banda en la sucursal.
- Compruebe la conectividad y la calidad de la red en cada sucursal.
- Si debe usar una de estas opciones en la sucursal, asegúrese de que el tráfico RTP/UDP (gestionado por HdxRtcEngine.exe en la aplicación Citrix Workspace) no se vea obstaculizado.
  - Omitir servidores proxy
  - Interceptación SSL de red
  - Dispositivos de inspección profunda de paquetes (PPP)
  - Bifurcaciones VPN (utilice túnel dividido si es posible)

> **Importante: Configuración de túneles divididos de VPN**
>
> El tráfico de HdxRtcEngine.exe debe desviarse del túnel VPN y debe poder usar la conexión a Internet local del usuario para conectarse directamente al servicio. El modo varía según el producto de la VPN y la plataforma de la máquina que se usen, pero la mayoría de las soluciones de VPN admiten una configuración simple de la directiva para aplicar esta lógica. Para obtener más información sobre las instrucciones de túneles divididos específicas de cada plataforma VPN, consulte este artículo de Microsoft.

El motor multimedia WebRTC en la aplicación Workspace (HdxRtcEngine.exe) utiliza el protocolo de transporte seguro en tiempo real (SRTP) para secuencias multimedia que se descargan en el cliente. SRTP proporciona confidencialidad y autenticación a RTP. Para esta funcionalidad, se utilizan claves simétricas (negociadas con DTLS) para cifrar el contenido multimedia y los mensajes de control mediante cifrado AES.

Para lograr una experiencia de usuario positiva, se recomiendan las siguientes métricas:

Métrica	Del dispositivo de punto final a Microsoft 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 los 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).

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
Audio (en cada sentido)	~ 60 Kbps	Opus*
Vídeo (en cada sentido)	~ 700 Kbps	H264 360p @ 30 fps 16:9
Uso compartido de pantalla	~ 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 H264 son los códecs preferidos para llamadas de conferencias y entre dos usuarios.

> **Importante:**
>
> En cuanto concierne al rendimiento, el uso de CPU es más elevado en la codificación que en la descodificación en la máquina cliente. Puede integrar como parte del código la resolución máxima de codificación en la aplicación Citrix Workspace para Linux y Windows. Consulte Estimador de rendimiento del codificador y Optimización para Microsoft Teams.

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 redirige 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 omitir `127.0.0.1:9002`.

  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, estas versiones admiten servidores proxy:

- Aplicación Citrix Workspace para Windows versión 2012 (Negotiate/Kerberos, NTLM, Basic y Digest. Los archivos Pac también son compatibles)
- Aplicación Citrix Workspace para Windows versión 1912 CU5 (Negotiate/Kerberos, NTLM, Basic y Digest. Los archivos Pac también son compatibles)
- Aplicación Citrix Workspace para Linux versión 2101 (autenticación anónima)
- Aplicación Citrix Workspace para Mac versión 2104 (autenticación anónima)

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 Microsoft 365.

> **Importante:**
>
> - Compruebe que el dispositivo cliente se puede conectar al servidor DNS para procesar resoluciones DNS. Un dispositivo cliente debe poder resolver estos FQDN del servidor de retransmisión de Microsoft Teams:
>   - `worldaz.relay.teams.microsoft.com`
>   - `inaz.relay.teams.microsoft.com`
>   - `uaeaz.relay.teams.microsoft.com`
>   - `euaz.relay.teams.microsoft.com`
>   - `usaz.relay.teams.microsoft.com`
>   - `turn.dod.teams.microsoft.us`
>   - `turn.gov.teams.microsoft.us`
>
> Si las solicitudes de DNS no se realizan correctamente, fallan las llamadas P2P con usuarios externos y el establecimiento de archivos multimedia con llamadas de conferencias.
>
> - La ubicación del servidor de conferencias se selecciona en función de la ubicación del escritorio virtual del primer participante (y no del cliente).

Establecimiento de llamadas y rutas de flujo de medios

Cuando sea posible, el motor de medios HDX WebRTC de la aplicación Citrix Workspace (HdxRtcEngine.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 homologo a otro. Si los puertos UDP altos están bloqueados, el motor de medios recurre a TCP 443 con TLS.

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. Esta compatibilidad significa que el dispositivo de punto final debe ser capaz de procesar resoluciones DNS.

Supongamos que no hay una ruta directa entre los dos pares o entre un par y un servidor de conferencias y se une a una llamada o reunión de varios participantes. HdxRtcEngine.exe utiliza un servidor de traspaso de transporte de Microsoft Teams en Microsoft 365 para llegar al otro par o al procesador multimedia, donde se alojan las reuniones. La máquina cliente debe tener acceso a tres intervalos de direcciones IP de subred de Microsoft 365 y a cuatro puertos UDP (o a TCP 443 con TLS como alternativa si UDP está bloqueado). Para obtener más información, consulte el diagrama de arquitectura en Configuración de llamadas 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, 52.122.0.0/15	**UDP:** 3478, 3479, 3480, 3481, **TCP:** 443 (reserva)

Estos intervalos incluyen tanto servidores de traspaso de transporte como procesadores de multimedia, con un front-end de Azure Load Balancer.
Los servidores de traspaso de transporte de Microsoft Teams proporcionan funcionalidad para los protocolos STUN y TURN, pero no son dispositivos de punto final ICE. Además, los servidores de traspaso de transporte de Microsoft Teams no finalizan el contenido multimedia, TLS ni hacen ninguna transcodificación. Pueden puentear TCP (si HdxRtcEngine.exe utiliza TCP) a UDP cuando reenvían tráfico a otros pares o procesadores de multimedia.

El motor de medios WebRTC de la aplicación Workspace conecta con el servidor de traspaso de transporte de Microsoft Teams más cercano en la nube de Microsoft 365. El motor de medios 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 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 Microsoft Teams se carga en modo optimizado y HdxRtcEngine.exe se está ejecutando en el terminal, los errores de 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. Para obtener más información sobre el proceso de recopilación de candidatos de ICE, consulte "Recopilar registros"en la sección Asistencia.

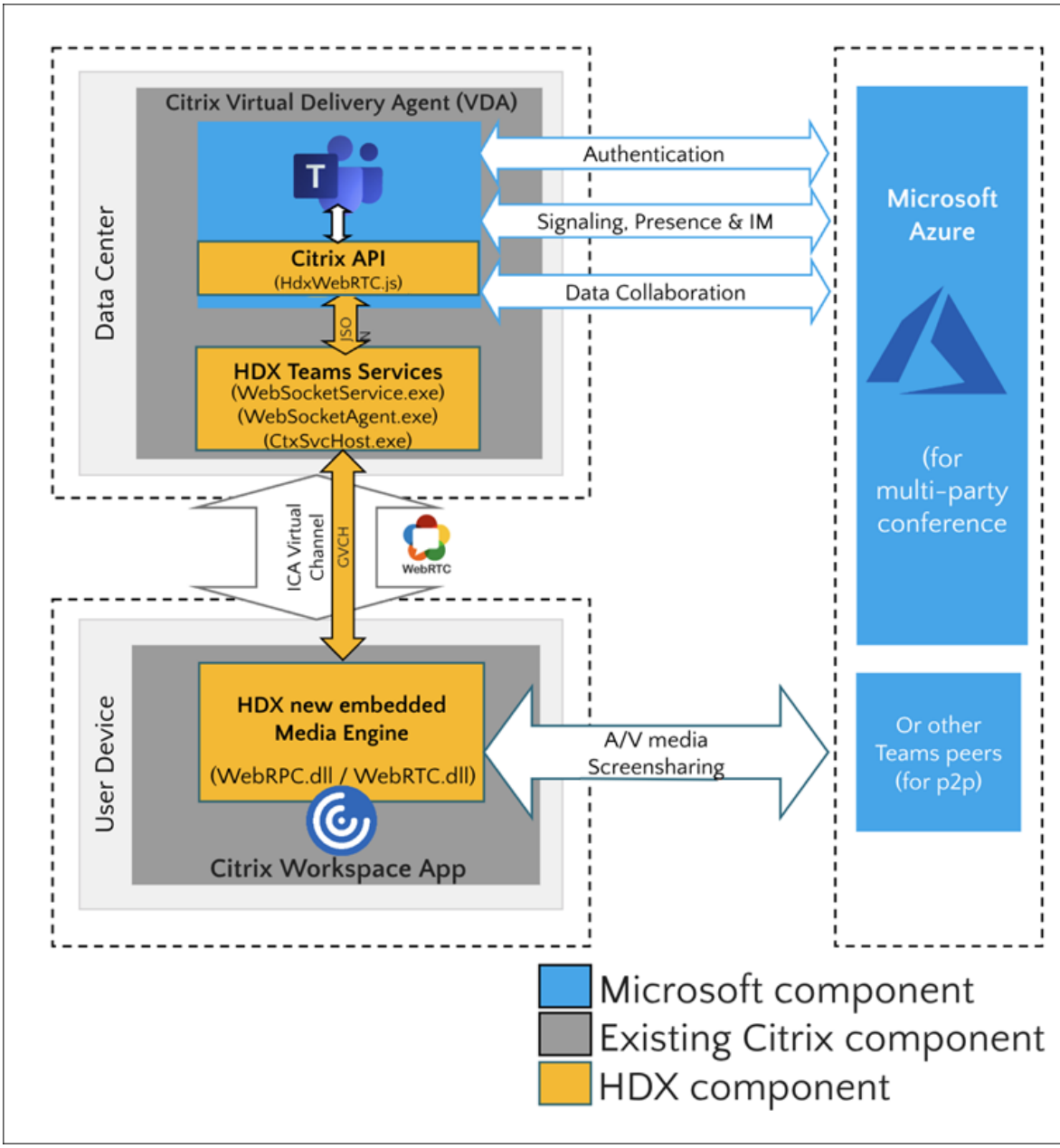
> **Nota:**
>
> Si los dispositivos de punto final no tienen acceso a Internet, es posible que los usuarios aún

> puedan 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. Microsoft Teams se autentica en O365. Las directivas de arrendatario se envían al cliente de Microsoft Teams, y la información pertinente del canal de señalización y del protocolo TURN se transmite a la aplicación.
3. Microsoft Teams detecta que se ejecuta en un VDA y realiza llamadas API a la API de JavaScript de Citrix.
4. JavaScript de Citrix en Microsoft Teams abre una conexión WebSocket segura con WebSocketService.exe en el VDA, 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 Microsoft Teams para Citrix HDX (CtxSvcHost.exe).
6. El archivo wfica32.exe (motor de HDX) de la aplicación Citrix Workspace genera un nuevo proceso denominado HdxRtcEngine.exe, que es el nuevo motor de WebRTC utilizado para la optimización de Microsoft Teams.
7. El motor de medios de Citrix 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 Microsoft Teams de Microsoft 365 y establece una ruta de señalización de extremo a extremo con el **interlocutor B**. Microsoft Teams solicita a HdxRtcEngine 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 Microsoft Teams en Microsoft 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 solicitudes de enlace STUN) se completan. A continuación, el contenido multimedia con Secure Real-Time Transport Protocol (SRTP) circula directamente entre HdxRtcEngine.exe y el otro interlocutor (o servidores de conferencia de Microsoft 365 si se trata de una reunión).

Sistema telefónico de Microsoft

Sistema telefónico es la tecnología de Microsoft que posibilita el control de llamadas y las funciones de central de conmutación (PBX) en la nube de Microsoft 365 con Microsoft Teams. La optimización para Microsoft Teams es compatible con el sistema telefónico mediante planes de llamada de Microsoft 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.
Se admiten colas de llamadas, transferencia, reenvío, retención, silenciamiento y reanudación de una llamada.

DTMF

Las siguientes versiones de la aplicación Citrix Workspace (y posteriores) son compatibles con la funcionalidad multifrecuencia de doble tono (DTMF):

- Versión 2102 de la aplicación Citrix Workspace para Windows
- Aplicación Citrix Workspace 1912 LTSR CU5 para Windows (solo SO con Windows 10)
- Versión 2101 de la aplicación Citrix Workspace para Linux
- Versión 2101 de la aplicación Citrix Workspace para Mac
- Aplicación Citrix Workspace para ChromeOS versión 2111.1

Compatibilidad con e911 dinámico

A partir de la versión 2112, la aplicación Citrix Workspace admite llamadas de emergencia dinámicas. Cuando se usa en los planes de llamadas de Microsoft, Operator Connect y enrutamiento directo, le permite:

- Configurar y redirigir llamadas de emergencia.
- Notificar al personal de seguridad.

La notificación se proporciona en función de la ubicación actual de la aplicación Citrix Workspace que se ejecuta en el dispositivo de punto final, en lugar del cliente de Microsoft Teams que se ejecuta en el VDA.

La ley de Ray Baum exige que la ubicación transmitible de la persona que llama al 911 se transmita al Punto de Respuesta de Seguridad Pública (PSAP) correspondiente. La optimización de Microsoft Teams con HDX es conforme a la ley de Ray Baum cuando se utiliza con las siguientes versiones de la aplicación Citrix Workspace:

- Aplicación Citrix Workspace para Windows 2112.1 y versiones posteriores
- Aplicación Citrix Workspace para Linux 2112 y versiones posteriores
- Aplicación Citrix Workspace para Mac 2112 y versiones posteriores
- Aplicación Citrix Workspace para ChromeOS 2112 y versiones posteriores

Para habilitar las llamadas de emergencia dinámicas, el administrador debe usar Centro de administración de Microsoft Teams y configurar lo siguiente para crear un mapa de ubicación de emergencia o de red:

- Parámetros de red

- Servicio de información de ubicación (LIS)

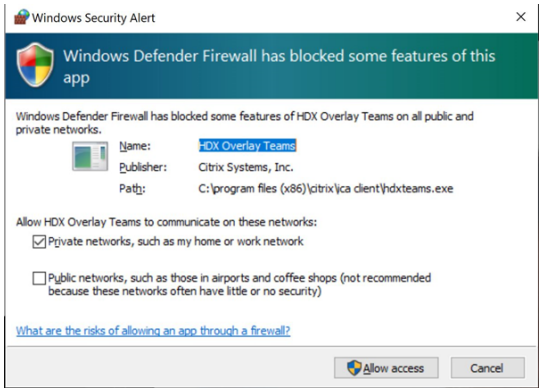
Para obtener más información sobre las llamadas de emergencia dinámicas, consulte la documentación de Microsoft.

La información de ubicación transmisible que la aplicación Citrix Workspace transmite a Microsoft Teams es:

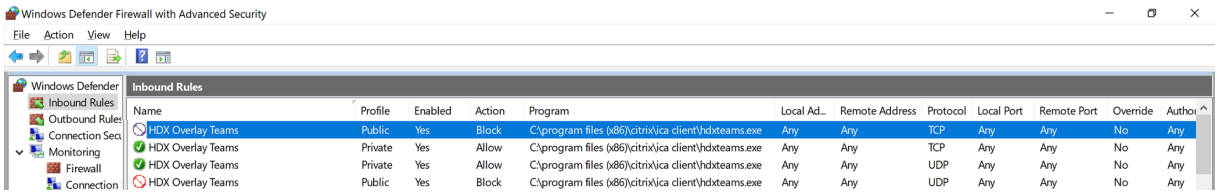
- ID de chasis o ID de puerto mediante el protocolo de detección de la capa de enlace (LLDP) para conexiones Ethernet/Switch. Ethernet/Switch (LLDP) se admite en:
  - Versiones 8.1 y 10 de Windows
  - macOS, que requiere software de habilitación de LLDP. Para descargar el software de habilitación de LLDP, vaya a `www.microsoft.com` y busque el software de habilitación de LLDP.
  - Linux, que requiere que la biblioteca LLDP se incluya en la distribución del sistema operativo (SO) del cliente ligero.
- BSSID de WLAN y {IPv4-IPv6; subred; dirección MAC} del dispositivo de punto final en el que está instalada la aplicación Citrix Workspace.
  - Las ubicaciones basadas en subredes y Wi-Fi son compatibles con la aplicación Workspace para Windows, Linux y Mac.
- Latitud y longitud, si se concede el permiso de usuario en el nivel de SO donde está instalada la aplicación Citrix Workspace (permiso establecido en HDX RTC Engine).
  - Compatible con todas las plataformas de la aplicación Workspace. Sin embargo, para Citrix Workspace para Linux, debe incluir la biblioteca `libgps` en la distribución del sistema operativo del cliente ligero (>sudo apt-get install libgps23 gpsd lldpd).

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 o HdxRtcEngine.exe (HDX Overlay Microsoft 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 quiere.

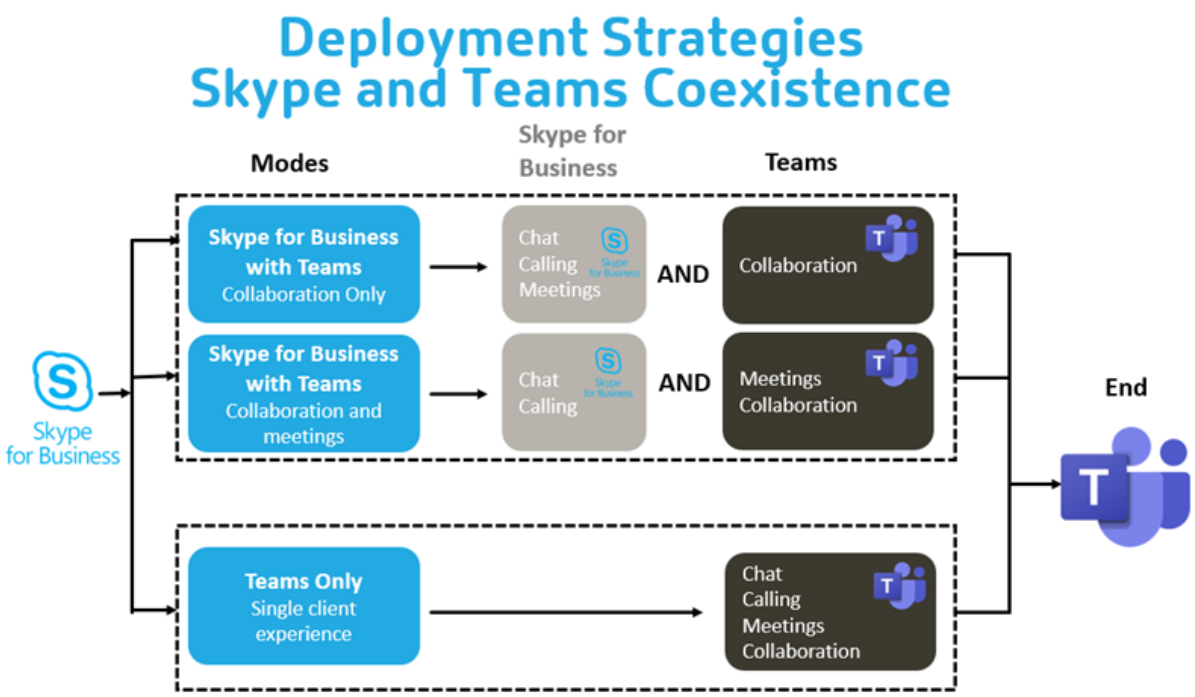


Coexistencia de Microsoft Teams y Skype for Business

Puede implementar Microsoft Teams y Skype for Business en paralelo, como dos soluciones independientes con prestaciones superpuestas.
Para obtener más información, consulte Coexistencia e interoperabilidad de Microsoft Teams y Skype for Business.

Citrix RealTime Optimization Pack y Optimización de HDX para motores multimedia de Microsoft Teams respetan la configuración establecida en su entorno. Los ejemplos incluyen modos de isla y Skype for Business con la colaboración de Microsoft Teams. Asimismo, Skype for Business con las reuniones y la colaboración de Microsoft 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 libera, está disponible para Microsoft Teams.



Citrix SD-WAN: conectividad de red optimizada para Microsoft Teams

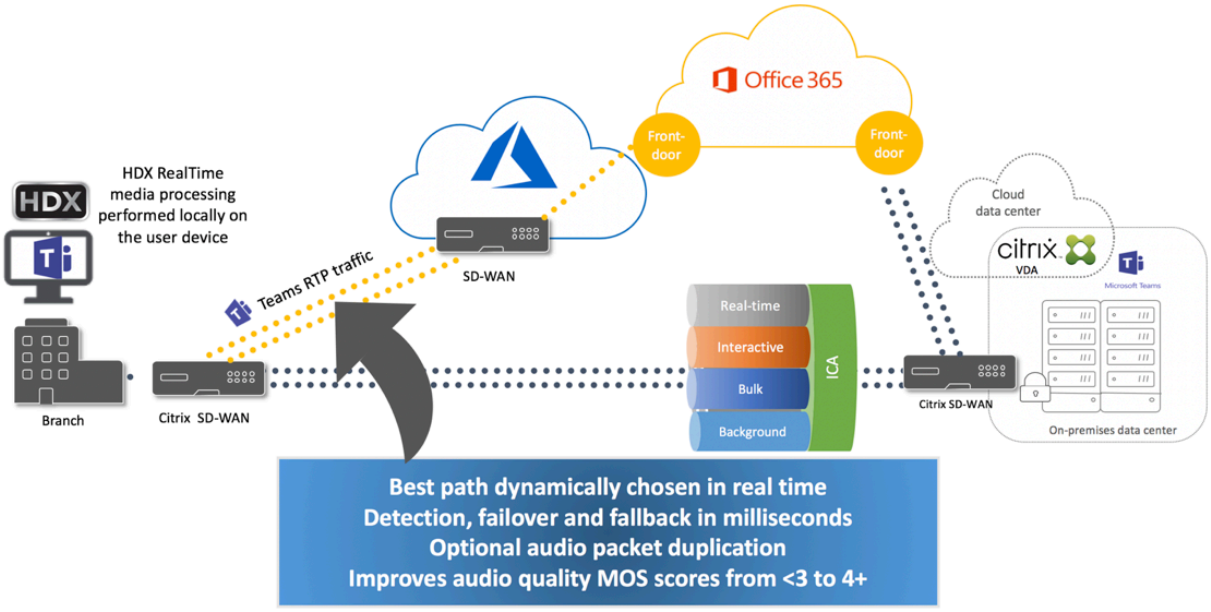
Para lograr una calidad de audio y vídeo óptima, se requiere una conexión de red a la nube de Microsoft 365 que tenga baja latencia, baja vibración y baja pérdida de paquetes. El uso de una red de retorno (backhaul) para canalizar el tráfico RTP de audio y vídeo de Microsoft Teams desde los usuarios 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. También podría provocar congestión en los vínculos WAN. Citrix SD-WAN optimiza la conectividad para Microsoft Teams en base a los principios de conectividad de red de Microsoft 365. Citrix SD-WAN utiliza la dirección IP y el servicio web de Microsoft 365 basados en REST de Microsoft y DNS próximo. Este uso sirve 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.
- Los clientes de Citrix SD-WAN pueden conectarse a Microsoft 365 a través de Citrix Cloud Direct Service. 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. Dirija el tráfico de Microsoft Teams directamente desde el dispositivo de sucursal Citrix SD-WAN a la puerta de entrada de Microsoft 365 más cercana para minimizar la latencia. Para obtener más información, consulte Optimización de Citrix SD-WAN Office 365.



Reuniones y chat en modo multiventana

En Windows, puede utilizar varias ventanas de reuniones o chat para Microsoft Teams. Para obtener más información sobre la función emergente, consulte Microsoft Teams Pop-Out Windows for Chats and Meetings en el sitio de Microsoft 365.

> **Nota:**
>
> Esta función está disponible en la aplicación Citrix Workspace para Windows 2112.1, Mac 2203, Linux 2203 y ChromeOS 2303. Requiere un VDA 2112 o una versión posterior, y se transfirió a 1912 CU6 LTSR y versiones posteriores.

Desenfoque y efectos de fondo

La aplicación Citrix Workspace para Windows, Mac, Linux y ChromeOS/HTML5 admite efectos y desenfoque de fondo en la optimización de Microsoft Teams con HDX.

Puede difuminar o reemplazar el fondo por una imagen predeterminada y evitar distracciones inesperadas al ayudar a que la conversación se centre en la silueta (cuerpo y rostro). Puede utilizar esta función con llamadas de conferencia o P2P.

> **Nota:**
>
> Esta función está integrada en los botones y la interfaz de usuario de Microsoft Teams. La compatibilidad con varias ventanas es un requisito previo que necesita una actualización de VDA a la versión 2112 o a una posterior. Para obtener más información, consulte Reuniones y chat en modo multiventana.

Los controles de la interfaz de usuario de Microsoft Teams para desenfoque y efectos de fondo requieren las siguientes versiones mínimas:

- Aplicación Citrix Workspace para Windows 2207
- Aplicación Citrix Workspace para Mac 2301
- Aplicación Citrix Workspace para Linux 2307
- Aplicación Citrix Workspace para ChromeOS 2303

Limitaciones:

- El cliente debe estar conectado a Internet mientras se reemplaza la imagen de fondo por una imagen predeterminada de Microsoft Teams.
- La interfaz de usuario de Microsoft Teams no admite el reemplazo de imágenes de fondo definidas por el administrador y el usuario. Las imágenes de fondo personalizadas se pueden configurar mediante los parámetros de configuración del cliente, si la imagen también está almacenada en el cliente.

Establecimiento de una imagen de fondo personalizada

Las siguientes claves de Registro solo son necesarias si no tiene previsto utilizar la interfaz de usuario de Microsoft Teams para controlar la función o si un administrador quiere anular el funcionamiento predeterminado. Por ejemplo: inhabilitar el desenfoque de fondo porque el dispositivo de punto final no es lo suficientemente potente.

En Windows Para establecer una imagen de fondo personalizada, los administradores o los usuarios finales deben configurar la siguiente clave del Registro en el cliente o el dispositivo de punto final:

Ubicación: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`

- Nombre: VideoBackgroundEffect
- Tipo: DWORD
- Valor: 0 (inhabilitado), 1 (habilitado), 2 (reemplazo de imagen de fondo)

Al establecer el valor en 1, se desenfoca el fondo. El usuario final o el administrador pueden establecer este valor.

Si se establece el valor en 2, también debe estar presente la clave **VideoBackgroundImage**. Este valor solo puede establecerlo el administrador. Esta clave solo es necesaria si quiere reemplazar la imagen de fondo, no desenfocarla:

- Nombre: VideoBackgroundImage
- Tipo: REG_SZ
- Valor: nombre_de_imagen.jpeg

La imagen de fondo del vídeo debe estar presente en el directorio `C:\Program Files (x86)\Citrix\ICA Client`.

Esta configuración del Registro también sirve para habilitar el desenfoque de fondo o el reemplazo de imágenes en la aplicación Citrix Workspace 2206 sin el selector de interfaz de usuario de Microsoft Teams. En otras palabras, si su entorno o VDA no admiten el modo multiventana, puede usar la solución alternativa (claves del Registro en HKCU) con la aplicación Citrix Workspace 2206 o posterior para lograr un resultado parecido, aunque el usuario no podrá controlar la funcionalidad en medio de la sesión HDX o la llamada de Microsoft Teams.

Los cambios en las claves del Registro solo surten efecto cuando se conecta la sesión HDX.

En Mac Ubicación de la imagen descargada por el usuario: */Usuarios/nombre_de_usuario/Descargas/cualquier_i*

Ejecute los siguientes comandos para establecer la imagen personalizada como imagen predeterminada:

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundEffect -int 2
```

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundImage -string "
/Users/username/Downloads/any_image.png"
```

En Linux Ubicación de la imagen descargada por el usuario: */home/nombre_de_usuario/Downloads/cualquier_ir*

Cree el archivo */var/.config/citrix/hdx_rtc_engine/config.json* y agregue estas claves de configuración en formato JSON. Por ejemplo,

```
{


"VideoBackgroundEffect":2,

"VideoBackgroundImage":"/home/username/Downloads/any_image.jpg"

 }
```

En HTML5

1. Vaya al archivo **configuration.js** que se encuentra en la carpeta **HTML5Client**.
2. Agregue el atributo **backgroundEffects** y establezca el atributo en **true**. Por ejemplo,

```
'features' : {

    'msTeamsOptimization' :
    {

        'backgroundEffects' : true
     }

 }
```

3. Guarde los cambios.

Consideraciones sobre el consumo de CPU

Si bien la funcionalidad de desenfoque es frugal en cuanto respecta a la CPU, puede esperar un aumento del consumo. Por ejemplo: en un cliente ligero con un chip Intel® Pentium® Silver de 4 núcleos y 1,5 GHz con TurboBoost de hasta 2,8 GHz, el desenfoque del fondo agrega aproximadamente un 2% al uso de CPU. El uso medio de CPU es inferior al 20%.

Vista de galería y participantes activos en Microsoft Teams

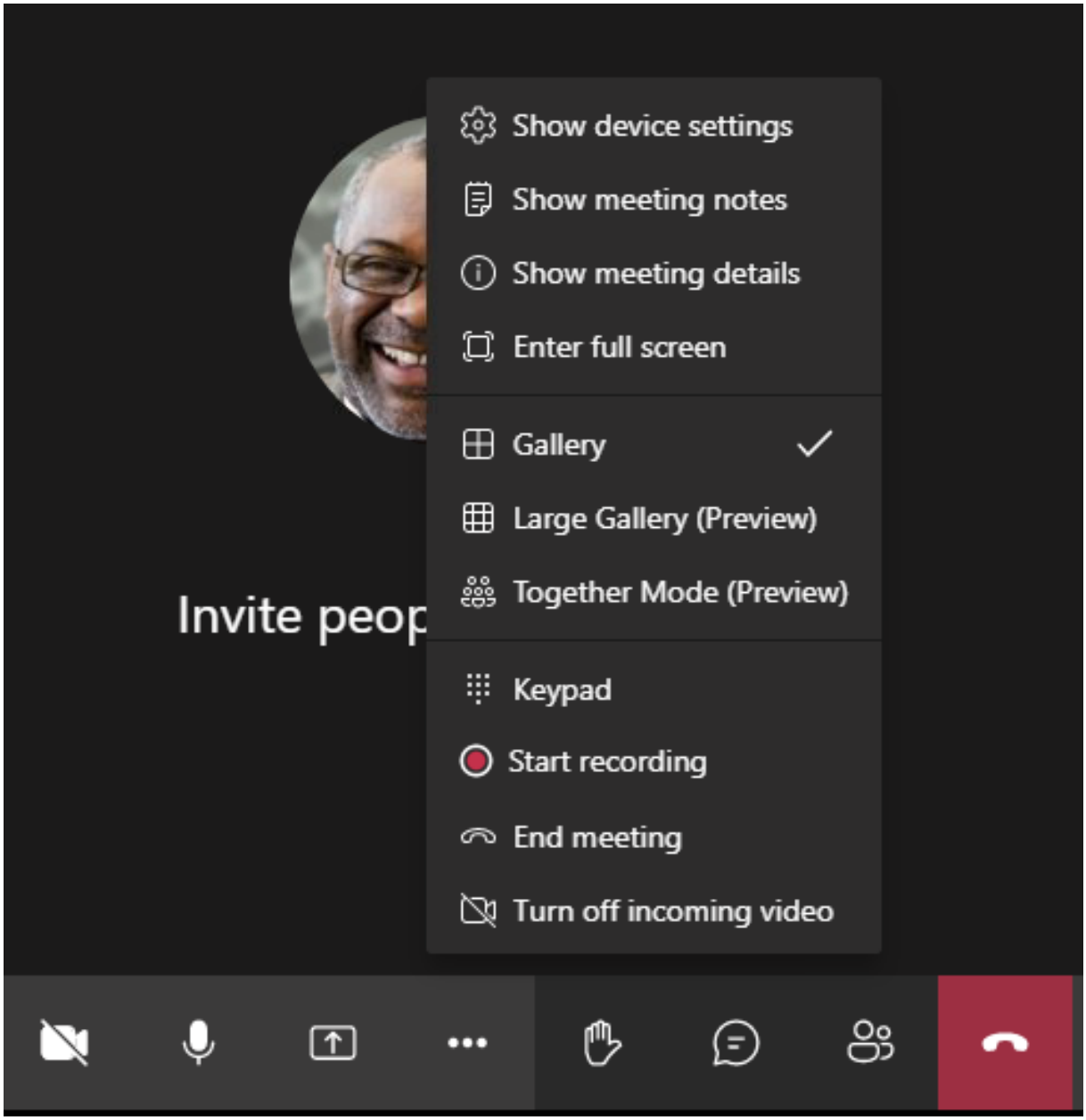
Microsoft Teams permite los modos **Gallery**, **Large Gallery** y **Together**.

Microsoft Teams muestra una cuadrícula 2x2 con secuencias de vídeo de cuatro participantes (denominada **Gallery**). En este caso, Microsoft Teams envía cuatro secuencias de vídeo al dispositivo cliente para su decodificación. Cuando hay más de cuatro participantes que comparten un 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 Microsoft Teams compone un único feed de vídeo y lo envía al dispositivo cliente para su descodificación, lo que reduce el consumo de CPU. Es posible que este único feed de tipo tabla también incluya vídeos 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, Microsoft 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.



Compatibilidad con restricciones de relación de aspecto de vídeo (aplicación Citrix Workspace para Windows 2102, aplicación Citrix Workspace para Linux 2106, aplicación Citrix Workspace para Mac 2106 y versiones posteriores):

- La opción **Fit to frame** está disponible en la vista Gallery/Large Gallery. Esta opción recorta el tamaño del vídeo para ajustarlo a la subventana. **Fill to frame**, por otro lado, muestra barras negras (buzón) en los laterales del vídeo para que no haya recortes.

En esta tabla se ofrece una comparación de los diseños Gallery y Large Gallery:

	Vista Gallery 2x2 (predeterminada)	Vista Large Gallery
Diseño / Cuadrícula	Muestra una cuadrícula 2x2 con secuencias de vídeo de cuatro participantes. Solo los cuatro últimos participantes más activos aparecen en la pantalla, y los demás participantes no aparecen en la cuadrícula.	Muestra una cuadrícula de 7x7 con transmisiones de vídeo de 49 participantes.
Técnica de mezcla	Un enrutador multimedia reenvía transmisiones individuales de cada participante a cada usuario.	Un servidor central de conferencias mezcla y transcodifica todo el audio o vídeo para crear un diseño compuesto personalizado para cada participante. Esta acción agrega alguna latencia adicional.
Participante activo	El nuevo participante activo sustituye al participante menos activo de la cuadrícula.	Muestra todos los participantes independientemente de si están activos o inactivos.
Codificación en el dispositivo de punto final	Es posible que se codifiquen al menos una secuencia de vídeo en el dispositivo de punto final si la transmisión simultánea está habilitada. Para obtener más información sobre la compatibilidad con la transmisión simultánea, consulte Transmisión simultánea.	Es posible que se codifiquen al menos una secuencia de vídeo en el dispositivo de punto final si la transmisión simultánea está habilitada. Para obtener más información sobre la compatibilidad con la transmisión simultánea, consulte Transmisión simultánea.
Descodificación en el dispositivo de punto final	Cada participante recibe hasta cuatro transmisiones multimedia individuales. Esto aumenta el consumo de CPU en el dispositivo de punto final por parte de HdxRtcEngine.exe (para la descodificación/generación).	Cada participante recibe una única transmisión de audio y vídeo. Esta configuración reduce el consumo de CPU en el dispositivo de punto final.

	Vista Gallery 2x2 (predeterminada)	Vista Large Gallery
Resolución máxima	720p. Cuando cuatro participantes comparten vídeo, la resolución máxima es de 360p por fuente de vídeo. Si menos de cuatro participantes comparten vídeo, es posible que la resolución por fuente de vídeo sea más alta.	720p para el diseño compuesto o la mezcla. No hay necesidad de una transmisión de vídeo de alta calidad para cada participante en un diseño compuesto. Debido a esta condición, cada usuario remitente reduce la resolución o la velocidad de bits de carga.
Problema de "usuarios lentos"	El usuario remitente modifica la calidad de cada modalidad (audio/vídeo/pantalla compartida) a la calidad común más baja de las redes de los participantes. Esta transmisión multimedia se reenvía a todos los demás participantes. Como resultado, un participante con una red en mal estado afecta a la calidad de todos los demás participantes de la llamada.	Menos susceptible al caso de calidad común más baja de las redes. El servidor de conferencias ofrece diferentes calidades en función de las condiciones de red de cada participante.
Vista previa propia	Aparece usted en una miniatura pequeña en directo.	Aparece usted en una miniatura y se mezcla con el resto de las fuentes de vídeo. Como resultado, es posible que usted se incluya en el diseño principal de los vídeos con una ligera demora adicional.

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.

A partir de la aplicación Citrix Workspace 2109 o versiones posteriores para Windows, Linux o Mac y la aplicación Citrix Workspace 2303 para ChromeOS, los usuarios pueden compartir sus pantallas y

cámaras de vídeo simultáneamente.

Con versiones anteriores, 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.

> **Nota para PowerPoint Live**
>
> Esta limitación no existe si comparte contenido de PowerPoint Live. En ese caso, otros compañeros pueden ver su cámara web y el contenido, además de desplazarse hacia adelante y hacia atrás para revisar otras diapositivas. En este caso, las diapositivas se generan en el VDA. Para acceder a una presentación con diapositivas de PowerPoint Live, haga clic en el botón "Share tray" y seleccione una de las diapositivas sugeridas de PowerPoint, o haga clic en "Browse"y busque un archivo de PowerPoint en su equipo o en OneDrive.

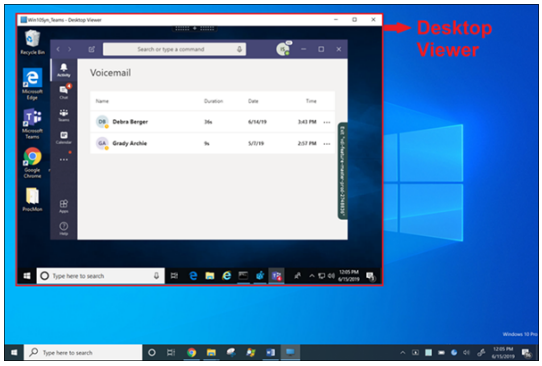
El uso compartido saliente de la pantalla también se optimiza y se descarga en la aplicación Citrix Workspace. En este caso, el motor de medios captura y transmite solo la ventana de Citrix Desktop Viewer (CDViewer.exe), con un borde rojo a su alrededor. Las aplicaciones locales que se superponen con Desktop Viewer no se capturan.

> **Nota**
>
> Establezca permisos específicos en la aplicación Citrix Workspace para Mac para habilitar el uso compartido de la pantalla. Para obtener más información, consulte Requisitos del sistema.

Limitación conocida:

- Si Desktop Viewer está inhabilitado o si se está utilizando Desktop Lock, la selección de varios monitores no está disponible en el selector de pantallas de Microsoft Teams. Es posible que Desktop Viewer se inhabilite al modificar la plantilla de archivo `.ICA` o `StoreFront web.config`. La tecla de acceso rápido MAYÚS+F2 no es compatible con el uso compartido de la pantalla en varios monitores.
- En las versiones de la aplicación Workspace anteriores a 2106, solo se comparte el monitor principal. Arrastre la aplicación del escritorio virtual al monitor principal para que los otros participantes de la llamada la puedan ver.
- Es posible que el uso compartido de la pantalla para varios monitores no funcione si configura la aplicación Citrix Workspace con la función de diseño de monitores virtuales (partición lógica de un único monitor físico). En este caso, todos los monitores virtuales se comparten en una imagen compuesta.
- Las versiones anteriores de la aplicación Citrix Workspace para Windows (de 1907 a 2008) también comparten una aplicación local que se ejecuta en la máquina cliente. Este uso compartido solo es posible si la aplicación local se superpone a Desktop Viewer. Este comportamiento se eliminó a partir de las versiones 2009.6 y 1912 CU5.

- Al compartir la pantalla, si pasa del modo de ventana a la pantalla completa, se detiene el uso compartido de la pantalla. Debe dejar de compartir la pantalla y compartirla de nuevo para que funcione.
- No es posible anclar los controles de uso compartido en una ubicación específica en Microsoft Teams optimizado.
- Al compartir una aplicación minimizada, es posible que también se comparta la barra de título de la aplicación.



Uso compartido de la pantalla desde una aplicación integrada:

Si publica Microsoft Teams como aplicación independiente integrada, el uso compartido de la pantalla captura el escritorio local del dispositivo de punto final físico. Se requiere la versión 1909 de la aplicación Citrix Workspace para Windows como mínimo.

Uso compartido de aplicaciones

A partir de la aplicación Citrix Workspace para Windows 2112.1 y el VDA 2112, Microsoft Teams admite el uso compartido de aplicaciones.

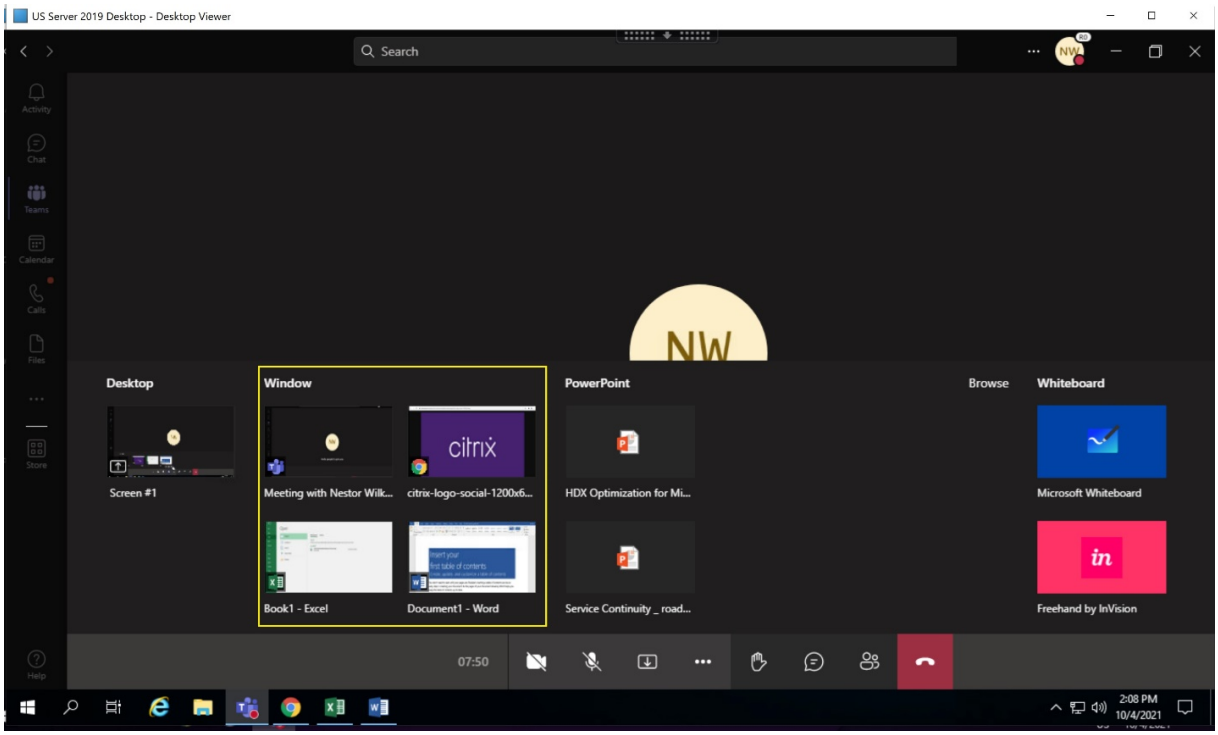
A partir de la aplicación Citrix Workspace para Windows 2109, para Mac 2203, para Linux 2209 y para VDA 2109, Microsoft Teams admite el uso compartido de la pantalla de aplicaciones específicas que se ejecutan en la sesión virtual. También puede compartir aplicaciones internas personalizadas, como Java, mediante Microsoft Teams optimizado. Para compartir una aplicación específica:

1. Vaya a la aplicación Microsoft Teams de su sesión remota.
2. Haga clic en **Compartir contenido** en la interfaz de usuario de Microsoft Teams.
3. Seleccione una aplicación para compartirla en la reunión. Aparecerá un borde rojo alrededor de la aplicación seleccionada y los interlocutores de la llamada podrán ver la aplicación compartida.

Para compartir una aplicación diferente, haga clic en **Compartir contenido** de nuevo y seleccione otra aplicación.

Si quiere inhabilitar el uso compartido de aplicaciones, cree esta clave del Registro en el VDA en `HKLM\SOFTWARE\Citrix\Graphics`:
Nombre: `UseWsProvider`
Tipo: `DWORD`
Valor: 0

> **Nota:**
>
> - Si minimiza una aplicación, Microsoft Teams muestra la última imagen de la aplicación compartida. Puede maximizar la ventana para reanudar el uso compartido de la pantalla.
> - La pantalla compartida depende de la captura de la ventana en el lado del VDA. A continuación, el contenido se transmite a velocidad máxima a la aplicación Citrix Workspace. La velocidad máxima es de 30 fotogramas por segundo. La aplicación Citrix Workspace reenvía el contenido al otro usuario o al servidor de conferencias.



Limitaciones conocidas en el uso compartido de la pantalla de una aplicación específica:

- El puntero del mouse no se muestra al compartir la pantalla de una aplicación.
- Si minimiza una aplicación al compartirla, solo aparece el icono de la aplicación en el selector de pantallas. La miniatura de la aplicación no se previsualiza en el selector de pantallas. No se puede compartir el contenido y el borde rojo no aparece hasta que se maximiza la aplicación.
- Acceso a aplicaciones locales (LAA) muestra una lista de aplicaciones que se pueden compartir con aplicaciones de escritorio en las instancias de Microsoft Teams optimizadas del VDA. Sin embargo, al seleccionar la aplicación de la lista, es posible que el resultado no sea el previsto.

Compatibilidad con App Protection
El uso compartido de la pantalla de una aplicación específica es compatible con la función de App Protection de Microsoft Teams optimizado para HDX. Puede compartir la pantalla de una aplicación específica si ha iniciado la aplicación o el escritorio desde un grupo de entrega que tiene habilitada App Protection.

Al hacer clic en **Compartir contenido** en la interfaz de usuario de Microsoft Teams, el selector de pantallas quita la opción **Escritorio**. Solo se puede seleccionar la opción **Ventana** para compartir cualquier aplicación abierta.

> **Nota:**
>
> Cuando se inician aplicaciones o escritorios desde un grupo de entrega con la protección de aplicaciones habilitada, no se puede ver el vídeo entrante ni compartir la pantalla si se usa la aplicación Citrix Workspace para Windows 2202 o una versión anterior.

Dar y solicitar el control en Microsoft Teams Esta función se admite en las siguientes versiones de la aplicación Citrix Workspace (no depende de la versión del VDA ni del sistema operativo, sesión única o multisesión):

- Aplicación Citrix Workspace para Windows 2112.1 o una versión posterior
- Aplicación Citrix Workspace para Mac 2203.1 o una versión posterior
- Aplicación Citrix Workspace para Linux 2203 o una versión posterior
- Aplicación Citrix Workspace para ChromeOS 2303 o versiones posteriores

Durante una llamada de Microsoft Teams, puede solicitar el control cuando un participante comparte la pantalla. Una vez que tiene el control, puede hacer selecciones, modificaciones u otras actividades con el teclado y el mouse en la pantalla compartida.

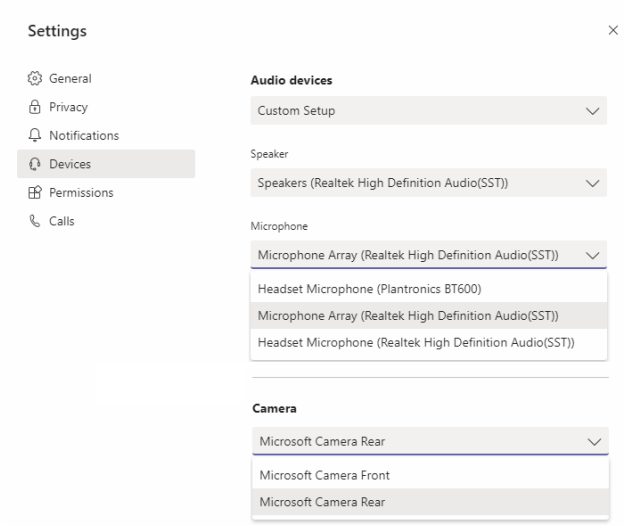
Para tomar el control cuando se comparte una pantalla, haga clic en el botón **Solicitar control** de la interfaz de usuario de Microsoft Teams. El participante de la reunión que comparte la pantalla puede aceptar o rechazar su solicitud.

Mientras tenga el control, puede realizar selecciones, modificaciones y otras acciones en la pantalla compartida. Para estas acciones, puede usar un teclado y un mouse. Cuando haya terminado, haga clic en **Solicitar el control**.

> **Limitaciones:**
>
> - La entrega y solicitud de controles no están disponibles si el usuario comparte una sola aplicación (también conocido como uso compartido de aplicaciones). Se debe compartir todo el escritorio o monitor.
> - La función para anclar la barra de control en una ubicación específica no está disponible.

Periféricos en Microsoft Teams

Cuando la optimización para Microsoft Teams está activa, la aplicación Citrix Workspace accede a los periféricos (auriculares, micrófonos, 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, recurre al motor de medios WebRTC de la aplicación Workspace para adquirir, capturar y procesar los objetos multimedia. Microsoft Teams indica los dispositivos que debe seleccionar el usuario.

Los periféricos que se insertan mientras Microsoft Teams está activo no están seleccionados de forma predeterminada. Tiene que seleccionar manualmente los periféricos en la pantalla **Configuración > Dispositivos** de la interfaz de usuario de Microsoft Teams. Una vez seleccionado un periférico, Microsoft Teams almacena en caché la información correspondiente. Como resultado, los periféricos se seleccionan automáticamente cuando se vuelve a conectar a una sesión desde el mismo dispositivo de punto final.

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. Además, colóquelos lejos de cualquier superficie que pueda refractar el sonido hacia el micrófono. Para obtener más información, consulte `www.microsoft.com` y busque auriculares con micrófono certificados por Microsoft Teams.
- Cámaras certificadas por Microsoft Teams, aunque los periféricos certificados por Skype Empresarial son compatibles con Microsoft Teams. Para obtener más información, vaya a y busque cámaras certificadas por Microsoft Teams y periféricos certificados por Skype for Business.

- El motor de medios de la aplicación Citrix Workspace no puede aprovechar la descarga de CPU con cámaras web que emplean codificación H.264 integrada UVC 1.1 y 1.5.

> **Nota:**
>
> La aplicación Workspace 2009.6 para Windows ahora puede adquirir periféricos con formatos de audio de 24 bits o con frecuencias superiores a 96 kHz.
>
> HdxTeams.exe (en la aplicación Citrix Workspace para Windows 2009 o versiones anteriores) solo admite estos formatos específicos de dispositivo de audio (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 Microsoft 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, inhabilite el dispositivo en cuestión o:
>
> 1. Abra el **Panel de control Audio** (mmsys.cpl).
> 2. Seleccione el dispositivo de reproducción o grabación.
> 3. Vaya a **Propiedades > Avanzadas** y cambie la configuración a un modo compatible.

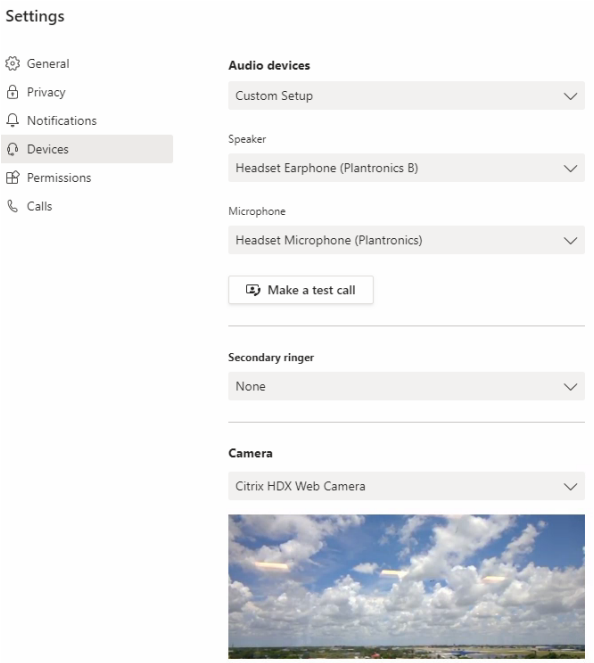
Modo de reserva

Si Microsoft Teams no se carga en el modo VDI optimizado (“Citrix HDX no está conectado”en Microsoft Teams/Acerca de/Versión), el VDA recurre a tecnologías HDX heredadas. Las tecnologías HDX heredadas pueden ser la redirección de cámara web y la redirección de audio y micrófono del cliente. Si está utilizando un SO de plataforma o versión de la aplicación Workspace que no admite la optimización de Microsoft Teams, no se aplicarán las claves de registro de reserva.
En el modo de reserva, 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 estableciendo las claves de Registro en el VDA. Para obtener más información, consulte Modo de reserva de Microsoft Teams en la lista de funciones administradas a través del Registro.

Esta función requiere Microsoft Teams 1.3.0.13565 o una versión posterior.

Para determinar si está en el modo optimizado o no en la ficha **Configuración > Dispositivos** de la aplicación Microsoft 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:

- Botones HID: Respuesta y finalización de llamada no disponibles. Compatible con subir y bajar el volumen.
- Los parámetros de calidad de servicio que ofrece el Centro de administración de Microsoft Teams no se aplican a los usuarios de VDI.

- Los usuarios no pueden hacer capturas de pantalla del contenido de Microsoft Teams con una herramienta de recorte en el VDA. Sin embargo, si la herramienta de recorte se utiliza en el lado del cliente, se puede capturar el contenido.

Limitación en el VDA:

- Al configurar el parámetro **PPP elevado de la aplicación Citrix Workspace** en `Yes`, la ventana de vídeo redirigido aparece fuera de lugar. Esta limitación se produce cuando el factor de escalado de PPP del monitor está configurado en un valor superior al 100%.

Limitaciones en la aplicación Citrix Workspace y el VDA:

- Solo se puede controlar el volumen de una llamada optimizada desde la barra de volumen presente en la máquina cliente, no en el VDA.

Transmisión simultánea

La función de transmisión simultánea está habilitada para llamadas de videoconferencias en Microsoft Teams optimizado tanto en Windows como en Mac. Para Linux, consulte con el proveedor de su cliente ligero.
Con la transmisión simultánea, la calidad y la experiencia de las videoconferencias en diferentes dispositivos de punto final mejoran al adaptarse a la resolución adecuada para ofrecer la mejor experiencia en llamadas a todos los usuarios.

Con esta experiencia mejorada, es posible que cada usuario cuente con varias transmisiones de vídeo en diferentes resoluciones (por ejemplo, 720p, 360p…) en función de varios factores, como la capacidad del dispositivo de punto final, las condiciones de la red y más. El dispositivo de punto final receptor solicita entonces la resolución de máxima calidad que pueda gestionar, lo que ofrece a todos los usuarios una experiencia de vídeo óptima.

> **Nota:**
>
> Esta función está disponible solamente después de la implantación de una actualización de Microsoft Teams. Para obtener información sobre el valor de ETA, vaya a https://www.microsoft.com/ y busque la hoja de ruta de Microsoft 365. Cuando Microsoft implante la actualización, consulte CTX253754 para obtener información sobre la actualización de la documentación y el anuncio.

Limitaciones de Microsoft

- No se ofrece la vista de galería 3x3. Dependencia de Microsoft Teams: Póngase en contacto con Microsoft para saber cuándo esperar una cuadrícula 3x3.

- La interoperabilidad con Skype for Business se limita a llamadas de audio, sin modalidad de vídeo.
- La resolución máxima de transmisión de vídeo entrante y saliente es 720p.
- No se admite el tono de espera de las llamadas RTC.
- No se admite la omisión de medios para enrutamiento directo.
- Los roles de productor y presentador para difusión y eventos en directo no están disponibles. El rol de asistente está disponible, pero no está optimizado (renderizado en el VDA).
- No está disponible la función de zoom en Microsoft Teams.
- No se admiten el enrutamiento basado en ubicación ni la omisión de medios.
- No se permite la combinación de llamadas (la opción no se muestra en la interfaz de usuario).

Limitaciones de Citrix y Microsoft

- Al hacer uso compartido de pantalla, la opción de **incluir audio del sistema** no está disponible.
- La transmisión simultánea no es compatible con ChromeOS.

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 M365s (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.

> **Nota:**
>
> Para seguir usando Microsoft Teams en modo optimizado para compartir pantallas y vídeo, Citrix recomienda actualizar su VDA y la aplicación Citrix Workspace a las versiones compatibles. Si no actualiza su infraestructura y sus terminales para que tengan disponibles las funciones de multiventana, sus llamadas, videollamadas y uso compartido de pantalla dejarán de estar optimizadas. Esto puede provocar problemas de calidad de las llamadas, aumentar la latencia y aumentar la carga del servidor.

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 (1)	Versión LTSR compatible (2)	Versión recomendada (3)
Microsoft Teams	1.5.00.11865	No aplicable	Más reciente
VDA	1912 CU6 LTSR, 2109 CR, 2203 LTSR	1912 CU8+, 2203 LTSR CU2+ (4)	2308 CR+
Aplicación Citrix Workspace para Windows	2112.1 CR	2203 CU2+ (4)	2309 CR+
Aplicación Citrix Workspace para Mac	2203 CR	No aplicable	2308 CR+
Aplicación Citrix Workspace para Linux	2202 CR	No aplicable	2308 CR+
Aplicación Citrix Workspace para ChromeOS o HTML5	2303 CR	No aplicable	2309 CR+

Notas:

1. Versión mínima: esta es la versión en la que se introdujo por primera vez la multiventana. Es posible que algunas de las versiones mínimas que se enumeran aquí hayan llegado al final de su vida.
2. Versión compatible con LTSR: esta es la versión LTSR compatible con Citrix para multiventana. Es posible que las versiones anteriores de estas versiones de LTSR funcionen, pero no se garantiza la compatibilidad para esas versiones cuando se publique una nueva versión de LTSR CU. Para obtener más información sobre las directivas de compatibilidad de LTSR, consultehttps://support.citrix.com/article/CTX205549/faq-citrix-virtual-apps-and-desktops-and-citrix-hypervisor-long-term-service-release-ltsr.
3. Versión recomendada: es la versión del software que Citrix recomienda si el usuario/cliente decide actualizar su software. Todas estas son versiones CR.
4. La versión 2203 LTSR para las versiones base de VDA y CWA incluye la funcionalidad de multiventana. Estas versiones han sido reemplazadas por la última CU, que es la versión compatible oficial. Los clientes pueden seguir usando estas versiones no compatibles según su criterio. Citrix anima a los clientes de la versión LTSR a que se actualicen a la versión CU más reciente.

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 de recibir asistencia en marzo de 2023 y debe actualizarse a una versión más reciente. Para obtener más información sobre la compatibilidad de versiones de la aplicación Citrix Workspace, 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 Microsoft Teams en la VM
- Instalar Microsoft Teams mediante MSI (sección Instalación de VDI)
- Clientes ligeros
- Herramienta de evaluación de la red de Skype for Business
- Coexistencia e interoperabilidad de Microsoft Teams y Skype for Business

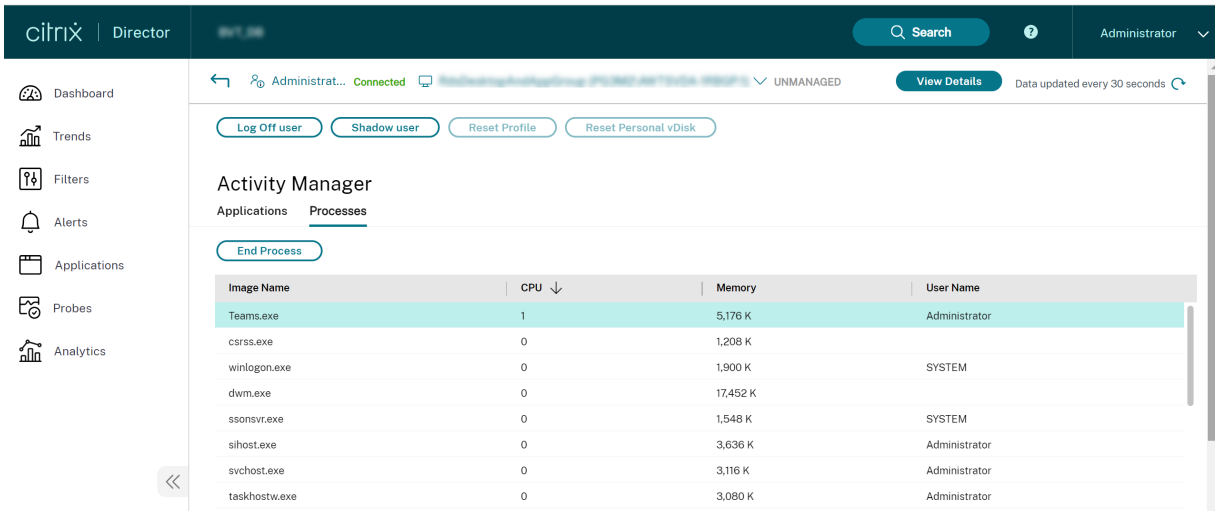
Supervisión, solución de problemas y asistencia para Microsoft Teams

August 17, 2024

Supervisar Teams

En esta sección, se ofrecen líneas generales para supervisar la optimización de Microsoft Teams con HDX.

Si está ejecutando en modo optimizado y `HdxRtcEngine.exe` se está ejecutando en la máquina cliente, un proceso en el VDA llamado `WebSocketAgent.exe` se ejecuta en la sesión. Utilice **Administrador de actividades** en Director para ver la aplicación.



El estado de optimización de Microsoft Teams se puede ver en Director > página **Detalles del usuario** > Panel **Detalles de la sesión** > Campo **Optimización de MS Teams**. La optimización de Microsoft Teams es fundamental para una mejor experiencia de usuario, como audio y vídeo nítidos. Esta función está disponible para la versión 2311 y posteriores de VDA. Las versiones de la aplicación Citrix Workspace compatibles se enumeran en Optimización para Microsoft Teams. Director muestra el estado de la optimización de Microsoft Teams solo si Microsoft Teams se ejecuta como una aplicación publicada o dentro de un escritorio publicado.

Para obtener más información, consulte estado de Optimización de Microsoft Teams.

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 último versión de `hdxmonitor.msi` en la carpeta `layout\image-full\Support\HDX Monitor`.

Con la versión mínima de VDA 1912, puede supervisar las llamadas activas de Microsoft Teams a través de Citrix HDX Monitor (versión mínima 3.11). La imagen ISO del producto Citrix Virtual Apps and

Desktops contiene la último versión de `hdxmonitor.msi` en la carpeta `layout\image-full\Support\HDX Monitor`.

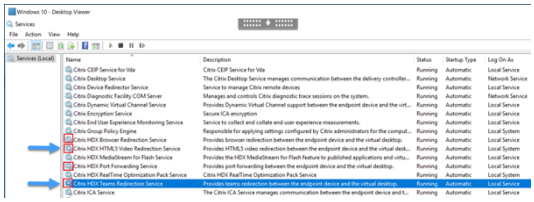
Para obtener más información, consulte *Supervisión* en el artículo CTX253754 de Knowledge Center.

Solucionar problemas

En esta sección se proporcionan sugerencias para solucionar problemas que pueden surgir al usar la optimización para Microsoft Teams. Para obtener más información, consulte 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.

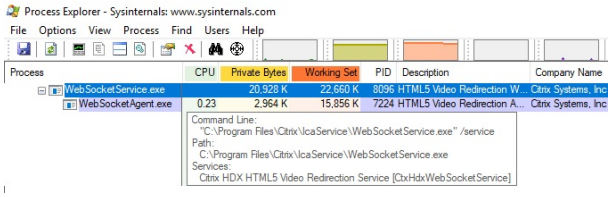


- **Citrix HDX Teams Redirection Service** establece el canal virtual utilizado en Microsoft Teams. El servicio se basa en CtxSvcHost.exe.
- **Citrix HDX HTML5 Video Redirection Service** se ejecuta como WebSocketService.exe y escucha el puerto TCP 127.0.0.1:9002. WebSocketService.exe realiza dos funciones 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 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 o HdxRtcEngine.exe. Lo hace cuando Microsoft Teams se inicia en el VDA y el usuario intenta llamar o acceder a los 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 o HdxRtcEngine.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 iniciarán HdxTeams.exe o HdxRtcEngine.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 o HdxRtcEngine.exe se inician 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.

3. Registros de WebRPC: Son los registros más importantes que registran la ejecución del empaquetado de la biblioteca WebRTC.

   Ubicación: /Users/<USERNAME>/Library/Logs/HdxRtcEngine/<W_M_D_H_M_S_Y>/webrpc.log

Registros de Linux:

Puede localizar los registros de Linux en las carpetas /tmp/webrpc/<current date>/ and /tmp/hdxrtcengine/<current date>/.
Registro de WebRTC: /tmp/webrpc/<current date>/webrtc.log
Registro del kernel: /var/log/syslog

Registros ICE/STUN/TURN/:

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 HdxRtcEngine.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 realice correctamente. Consulte el siguiente fragmento de muestra para la fase de recopilación:


```
RPCStubs Info: -> device id = \?\display#int3470#4&1835d135&0&uid13424#{
 65e8773d-8f56-11d0-a3b9-00a0c9223196 }
 {
 bf89b5a5-61f7-4127-a279-e187013d7caf }
  label = Microsoft Camera Front groupId =

webrtcapi.RTCPeerConnection Info: createOffer. audio = 1 video = 1
webrtcapi.RTCPeerConnection Info: setLocalDescription.
>>> begin:sdp
[...]

webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state = HaveLocalOffer

webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Gathering

[...]
>>> begin:sdp
candidate:840548147 1 udp 2122194687 10.108.124.215 56927 typ host generation 0 ufrag oVk6 network-id 1
<<< end:sdp
[...]
>>> begin:sdp
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
<<< end:sdp
[...]
>>> begin:sdp
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
<<< end:sdp
[...]

webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state = Complete webrtcapi.RTCPeerConnection Info: setRemoteDescription.
>>> begin:sdp
[...]

webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state = HaveRemotelOffer
```

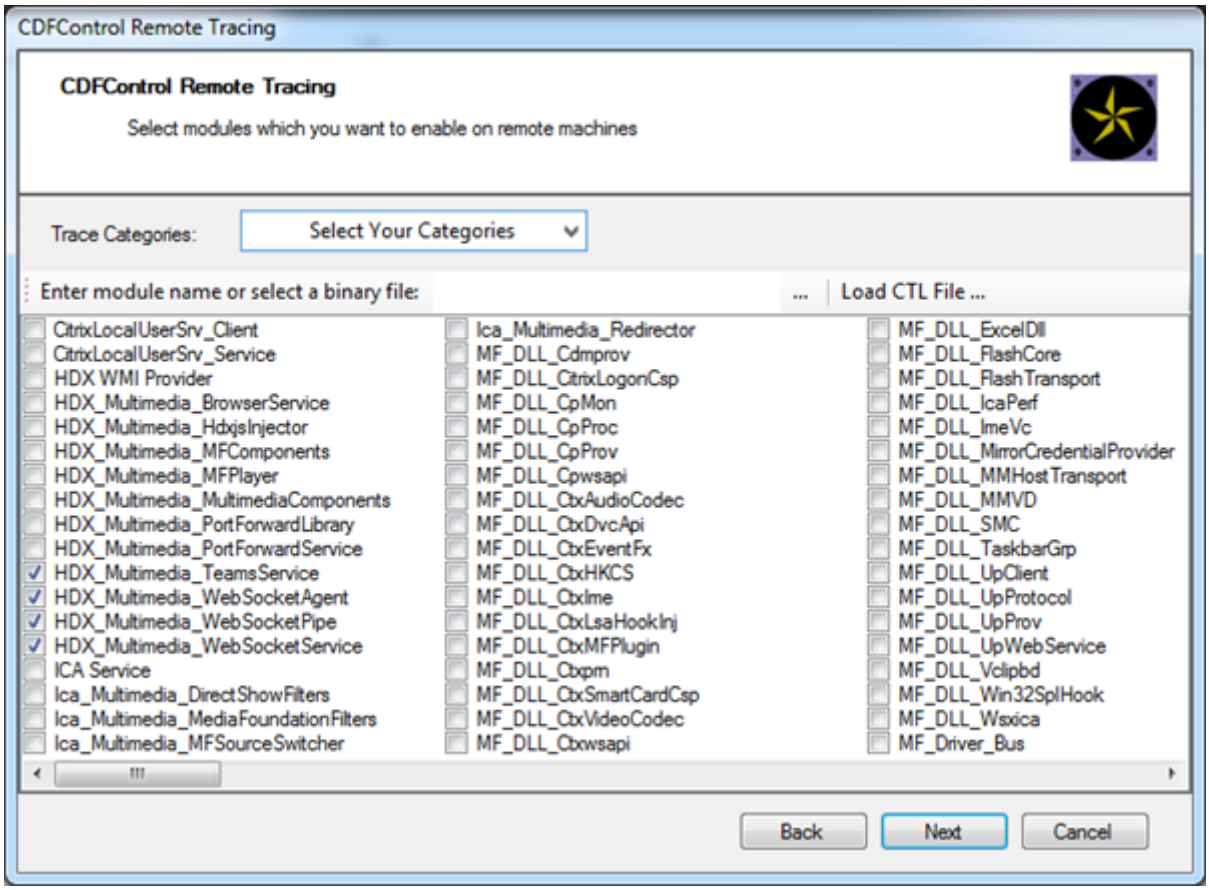
Si hay varios candidatos de ICE, el orden de preferencia es el siguiente:

1. host
2. par reflexivo
3. servidor reflexivo
4. traspaso de transporte

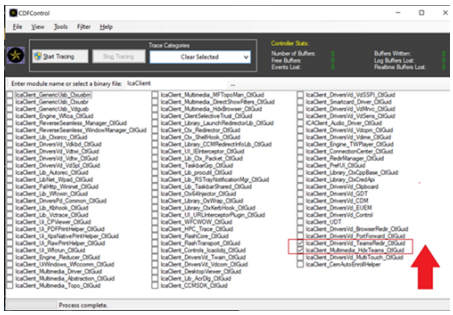
Si encuentra un problema y puede reproducirlo, le recomendamos que haga clic en**Ayuda > Informar de un problema** en Microsoft Teams. Citrix y Microsoft comparten los registros para resolver los problemas técnicos si abre un caso con Microsoft.
La captura de rastros CDF antes de ponerse en contacto 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:



- IcaClient_DriversVd_TeamsRedir (opcional)
- IcaClient_Multimedia_HdxTeams (requiere la aplicación Citrix Workspace 2012 o una versión posterior)

Redirección de Windows Media

August 17, 2024

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

August 17, 2024

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 de 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 de cliente

August 17, 2024

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 2022
- Windows Server 2019, 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)

Para habilitar la redirección de carpetas del cliente en el servidor, consulte Redirección de carpetas del cliente en la lista de funciones administradas a través del Registro.

En el dispositivo de usuario, especifique qué carpetas quiere redirigir:

1. Compruebe que está instalada la versión más reciente de la aplicación Citrix Workspace.
2. En el directorio de instalación de la aplicación Citrix Workspace, inicie CtxCFRUI.exe.
3. Seleccione el botón de opción **Personalizada** y agregue, modifique o quite carpetas.
4. Desconecte y vuelva a conectar sus sesiones para que la configuración tenga efecto.

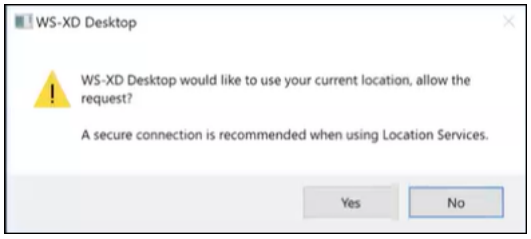
Redirección de la ubicación del cliente

August 17, 2024

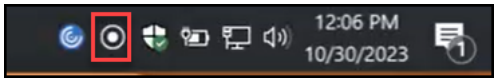
La redirección de la ubicación del cliente, cuando está habilitada, permite que las sesiones de escritorio y aplicaciones alojadas en VDA accedan sin problemas a la ubicación actual del cliente. En un sistema operativo multisesión (TS VDA o WS VDA multisesión), cada sesión tiene su propia ubicación única proporcionada por el cliente conectado. Con esta función, las aplicaciones del VDA que dependen de la ubicación tienen la ubicación exacta del cliente.

Para obtener más información, consulte la documentación de Microsoft.

Una vez habilitada la redirección de la ubicación del cliente y permitido el acceso a la ubicación tanto en el lado del servidor como en el del cliente, al iniciar una aplicación o un escritorio de acceso a la ubicación, el cliente le pedirá que comparta su ubicación actual en el siguiente cuadro de diálogo:



Al habilitar la redirección de la ubicación del cliente, aparece el siguiente icono en la barra de tareas del cliente siempre y cuando la aplicación o el escritorio alojados en el VDA consulten la información de ubicación actual.



Requisitos del sistema

Para servidores:

- VDA OS de sesión única (Win10/11) o multisesión (Win 11 22H2 y Server 2022 23H2 o posterior)
- Aplicación Citrix Workspace para Windows, iOS o Android

Configuración

La redirección de la ubicación del cliente debe habilitarse mediante la directiva de Citrix para que la función funcione. La redirección de la ubicación del cliente está inhabilitada de forma predeterminada.

Para habilitar la redirección de la ubicación del cliente, siga estos pasos:

En el lado de Windows VDA y del cliente:

1. En **Parámetros > Privacidad > Ubicación** , habilite las siguientes opciones:
    - **Permitir el acceso a la ubicación de este dispositivo**
    - **Permitir que las aplicaciones accedan a su ubicación**
    - **Permitir que las aplicaciones de escritorio accedan a su ubicación**
2. Para sistemas operativos multisesión, habilite el ajuste de **anulación de ubicación**.

En el lado del Controller/DDC:

Habilite la directiva **Studio > Directivas > Ubicación > Configuración > Permitir que la aplicación use la ubicación física del dispositivo cliente**.
Para obtener más información, consulte Parámetros de directivas de sensores de cliente.

Redirección bidireccional de contenido

August 17, 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

Exploradores web:

- Google Chrome con extensión de redireccionamiento de explorador Citrix (disponible en Google Chrome Web Store)
- Microsoft Edge (Chromium) con extensión de redireccionamiento de explorador Citrix (disponible en Google Chrome Web Store)

Configuración

A partir de la versión 2311 de Citrix Virtual Apps and Desktops, la redirección de contenido bidireccional se configura únicamente a través de Citrix Studio. Las versiones anteriores tenían configuraciones de directivas configuradas tanto en el dispositivo de punto final del cliente como en Studio. La redirección bidireccional de contenido está inhabilitada de forma predeterminada.

Para la configuración del VDA, consulte Redirección bidireccional de contenido en Configuración de **directiva de ICA**.

Para que funcione la redirección del explorador, las extensiones del explorador deben registrarse en el explorador de origen (desde donde se redirige la URL) mediante los comandos que se muestran. Ejecute los comandos según sea necesario en el VDA y en el cliente en función del explorador en uso.

Explorador web	VDA	Cliente
Google Chrome	%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regChrome	%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /regChrome
Microsoft Edge	%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regEdge	%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /regEdge
Todos los exploradores disponibles	%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regall	%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe/regall

Para cancelar el registro de una extensión del explorador:

Explorador web	VDA	Cliente
Google Chrome	%%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe/unregChrome	%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /unregChrome

Explorador web	VDA	Cliente
Microsoft Edge	%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirect.exe /unregEdge	%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /unregEdge
Todos los exploradores disponibles	%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirect.exe /unregall	%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /unregall

> **Nota:**
>
> El comando "register"hace que los exploradores Chrome y Edge soliciten a los usuarios que habiliten la extensión de redirección de explorador web Citrix durante el primer inicio. La extensión de explorador también se puede instalar manualmente desde Google Chrome Web Store. Para Microsoft Edge, consulte también Agregar una extensión a Microsoft Edge desde Chrome Web Store.

Redirección con comodines de Citrix VDA al cliente

La redirección bidireccional de contenido admite el uso de comodines al definir las URL que se van a redirigir. Para configurar la redirección bidireccional de contenido, consulte las instrucciones de configuración.

Redirección de protocolos personalizados del VDA al cliente

La redirección bidireccional de contenido admite la redirección de protocolos personalizados desde el VDA de Citrix al cliente. Se admiten protocolos distintos de HTTP o HTTPS. Para configurar la redirección bidireccional de contenido, consulte las instrucciones de configuración.

En Web Studio, defina el protocolo personalizado en **Redirección de contenido bidireccional**.

> **Nota:**
>
> - Debe tener privilegios de administrador para ejecutar estos comandos.
> - El cliente debe tener una aplicación registrada para gestionar el protocolo. De lo contrario, la URL redirige al cliente y no se inicia.
> - Las URL de protocolo personalizado que introduce o inicia en los exploradores Chrome y Edge no son compatibles ni se redirigen.
> - No se admiten los siguientes protocolos: `rtsp://`, `rtspu://`, `pnm://`, `mms://`.

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.
- 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.

Redirección del host al cliente

August 17, 2024

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.

```
<?xml version="1.0" encoding="UTF-8"?>

<DefaultAssociations>

<Association Identifier="http" ProgId="ServerFTAHTML" ApplicationName="
    ServerFTA" />

<Association Identifier="https" ProgId="ServerFTAHTML" ApplicationName=
    "ServerFTA" />

</DefaultAssociations>
```

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 usa 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://;custometype2://`

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 usar la clave **ValidSites** 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.

Acceso a aplicaciones locales y redirección de URL

August 17, 2024

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 URL bloqueadas de

su explorador) tras seleccionar enlaces insertados en un explorador en una sesión de escritorio. Si va a una URL que no está en la lista de URL bloqueadas, 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 redirige 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 URL permitidas ni la de URL bloqueadas.

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 URL permitidas y la lista de 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:

- Edge, la versión más reciente
- Firefox, la versión más reciente y la versión de asistencia extendida
- Chrome, la versión más reciente

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. De forma predeterminada, el acceso a aplicaciones locales está prohibido.

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 predeterminada. 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 URL permitidas y la lista de 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 sesión en Web Studio y haga clic en **Directivas** en el panel de la izquierda.
2. En la barra de acciones, haga clic en **Crear directiva**.
3. En la ventana Crear directiva, escriba "Permitir acceso a aplicaciones locales"en el cuadro de búsqueda y, a continuación, haga clic en **Seleccionar**.
4. 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.
5. En la ventana Crear directiva, escriba "Lista de redirección de URL permitidas"en el cuadro de búsqueda y, a continuación, haga clic en **Seleccionar**. La lista de permitidos para la redirección de URL especifica las URL que se pueden abrir en el explorador predeterminado de la sesión remota.
6. En la ventana Modificar configuración, haga clic en **Agregar** para agregar las URL y, a continuación, haga clic en **Aceptar**.
7. En la ventana Crear directiva, escriba "Lista de redirección de URL bloqueadas"en el cuadro de búsqueda y, a continuación, haga clic en **Seleccionar**. La lista de bloqueados de redirección de URL especifica las URL que se redirigen al explorador predeterminado que se ejecuta en el dispositivo de punto final.
8. En la ventana Modificar configuración, haga clic en **Agregar** para agregar las URL y, a continuación, haga clic en **Aceptar**.
9. En la página Parámetros, haga clic en **Siguiente**.
10. En la página Usuarios y máquinas, asigne la directiva a los grupos de entrega correspondientes y, a continuación, haga clic en **Siguiente**.
11. 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_CLIENTHOSTEDAPPSURL=1`.
    - Para CitrixReceiverWeb.exe, utilice `/ALLOW_CLIENTHOSTEDAPPSURL=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 directivas 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 las aplicaciones publicadas mediante el Editor del Registro o el SDK de PowerShell.

Para el Editor del Registro, consulte Acceso a aplicaciones locales para aplicaciones publicadas en la lista de funciones administradas a través del Registro.

Para usar 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 DaaS. Para obtener más información, consulte SDK de PowerShell remoto de Citrix DaaS.

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-configsitemetadata -name "studio_clientHostedApps"-value "true"`.

Después de completar los pasos correspondientes anteriores, siga estos pasos para continuar.

1. Inicie sesión en Web Studio y seleccione **Aplicaciones** en el panel de la izquierda.
2. 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 la barra de acciones. Para mostrar la opción Agregar aplicación de acceso local en la barra de acciones, haga clic en **Actualizar**.
3. 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 será 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 multisesión Windows.

C:\Archivos de programa (x86)\Citrix\HDX\bin\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 ficha. 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.

Para configurar el comportamiento de la aplicación local al cerrar sesión y al desconectar, consulte Comportamiento de la aplicación local al cerrar sesión y al desconectar en la lista de funciones administradas a través del Registro.

Consideraciones sobre unidades del cliente y redirección de USB genérico

August 17, 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 en Reglas de optimización de dispositivos USB del cliente de Citrix es una configuración específica para la redirección de USB genérico, para un determinado de dispositivo USB. No se aplica a la optimización que se describe aquí.

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 multisecuencia.

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 dicha aplicación 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, Windows Server 2016, Windows Server 2019 o Windows Server 2022.
- 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:

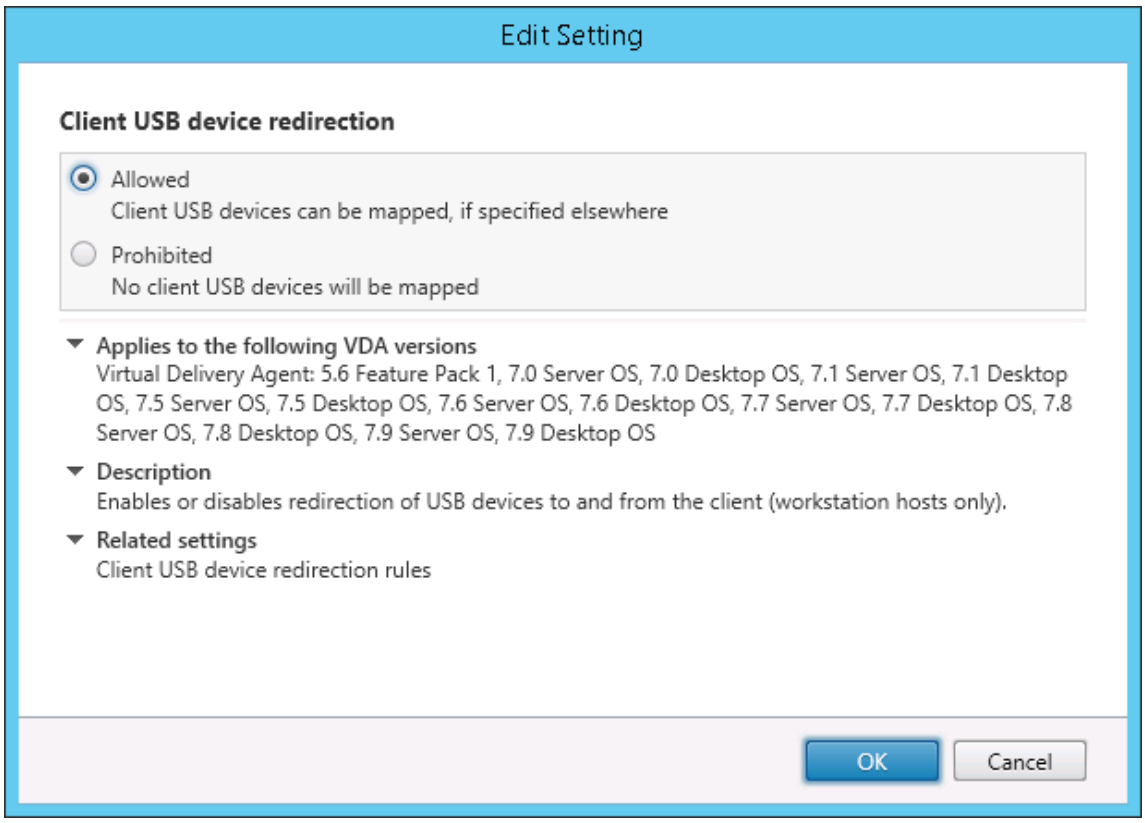
- Si dos departamentos o empresas diferentes se encargan de la aplicación Citrix Workspace y del VDA, pueden aplicar medidas de control por separado. Esta configuración se aplica cuando un usuario, ubicado en una empresa, acceda a una aplicación ubicada en otra empresa.
- Las configuraciones de directivas 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:

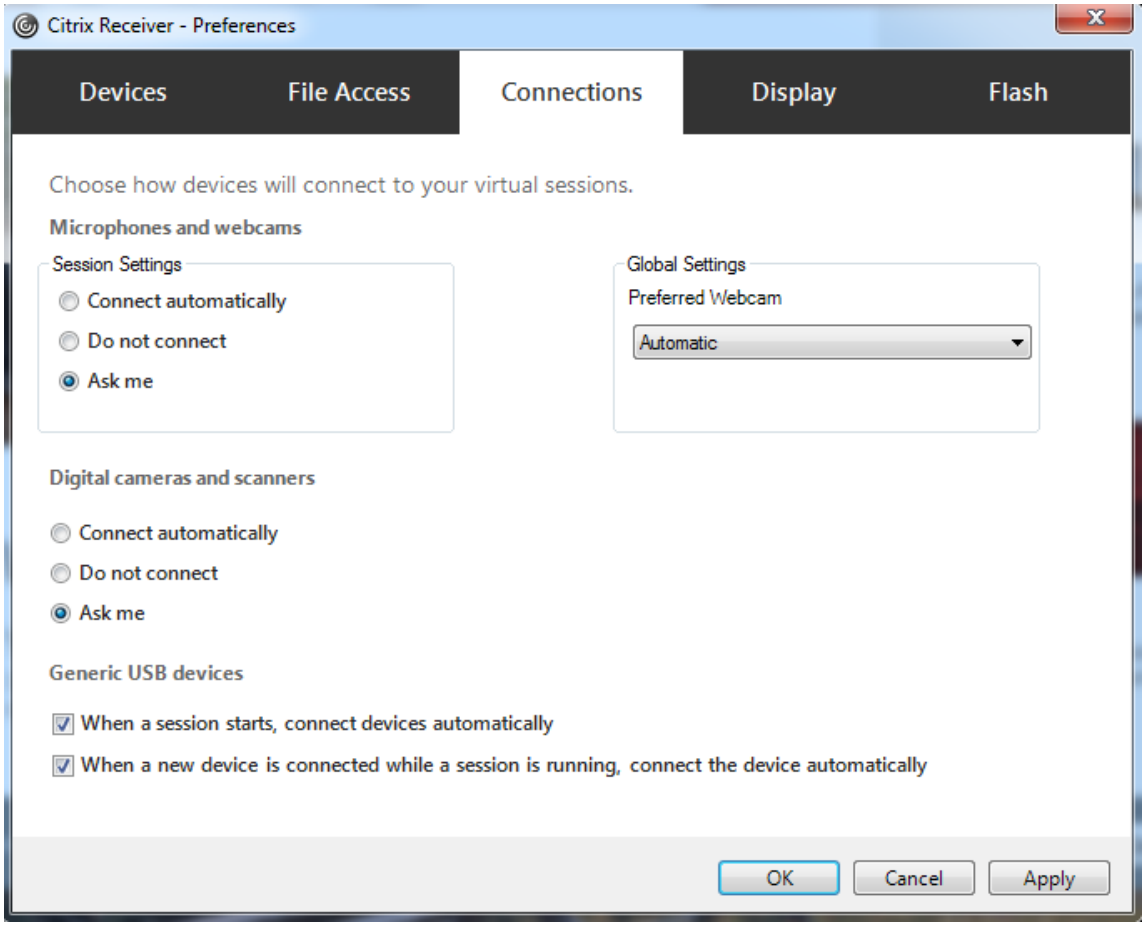
1. Agregue Redirección de dispositivos USB del cliente a una directiva y establezca su valor en **Permitida**.



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.

   Una vez que se haya completado la configuración de la directiva, 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**.



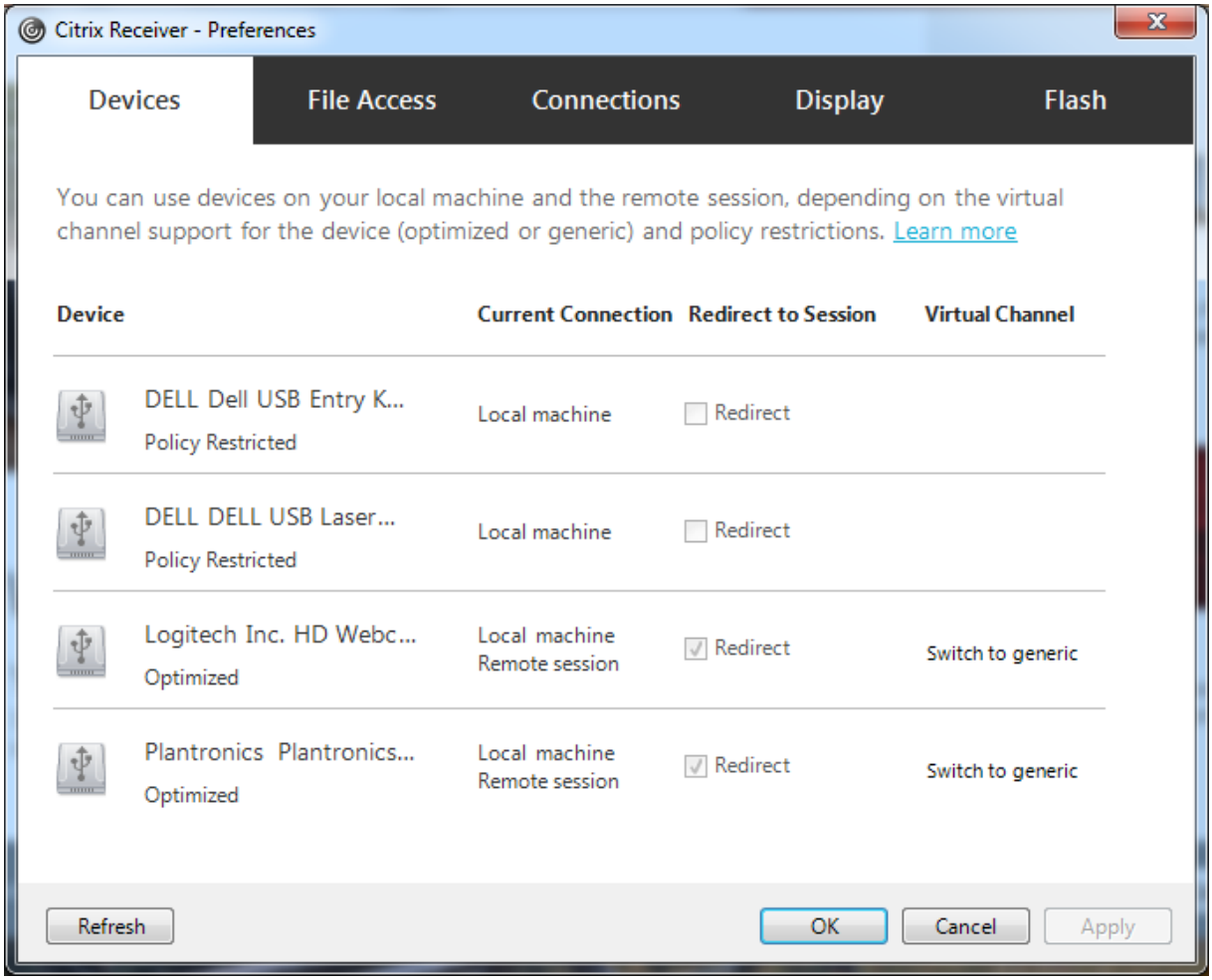
Si especificó las reglas de directiva USB para el VDA en el paso anterior, especifique las mismas reglas de directiva para la aplicación Citrix Workspace.

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 para supeditar las reglas predeterminadas de la directiva de USB.

Citrix DaaS (antes, Citrix Virtual Apps and Desktops Service):

- En la mayoría de los casos, descargue el archivo MSI (`CitrixGroupPolicyManagement_x64.msi`) de la Consola de administración de directivas de grupo de Citrix, instálelo en su sistema de Active Directory y, a continuación, administre las directivas de grupo de AD (no instale el MSI en un VDA).
- Para la aplicación Citrix Workspace para Windows, modifique el Registro del dispositivo del usuario. En los medios de instalación se incluye una plantilla administrativa (un archivo ADM) que le permite cambiar el dispositivo del usuario mediante la Directiva de grupo de Active Directory: dvd root `\os\lang\Support\Configuration\icaclient_usb.adm`

Citrix Virtual Apps and Desktops local:

- Para el VDA, modifique las reglas de supeditación del administrador para las máquinas con sistema operativo multisesión mediante las reglas de directiva de grupo. La Consola de administración de directivas de grupo se incluye en los medios de instalación:
  - x64: dvd root `\os\lang\x64\Citrix Policy\CitrixGroupPolicyManagement_x64.msi`
  - x86: dvd root `\os\lang\x86\Citrix Policy\CitrixGroupPolicyManagement_x86.msi`
- Para la aplicación Citrix Workspace para Windows, modifique el Registro del dispositivo del usuario. En los medios de instalación se incluye una plantilla administrativa (un archivo ADM)

que le permite cambiar el dispositivo del usuario 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 usa 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 HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Ci
Client\GenericUSB. 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 HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\
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 http://www.usb.org/ 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:**
>
> - A partir de la versión 2212 de Citrix Virtual Apps and Desktops, algunos de los dispositivos USB no pueden utilizar la función de redirección de USB genérico. Debe agregar estos dispositivos de forma explícita con sus respectivos ID de proveedor (VID) e ID de producto (PID).
> - 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.

Imprimir

August 17, 2024

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.

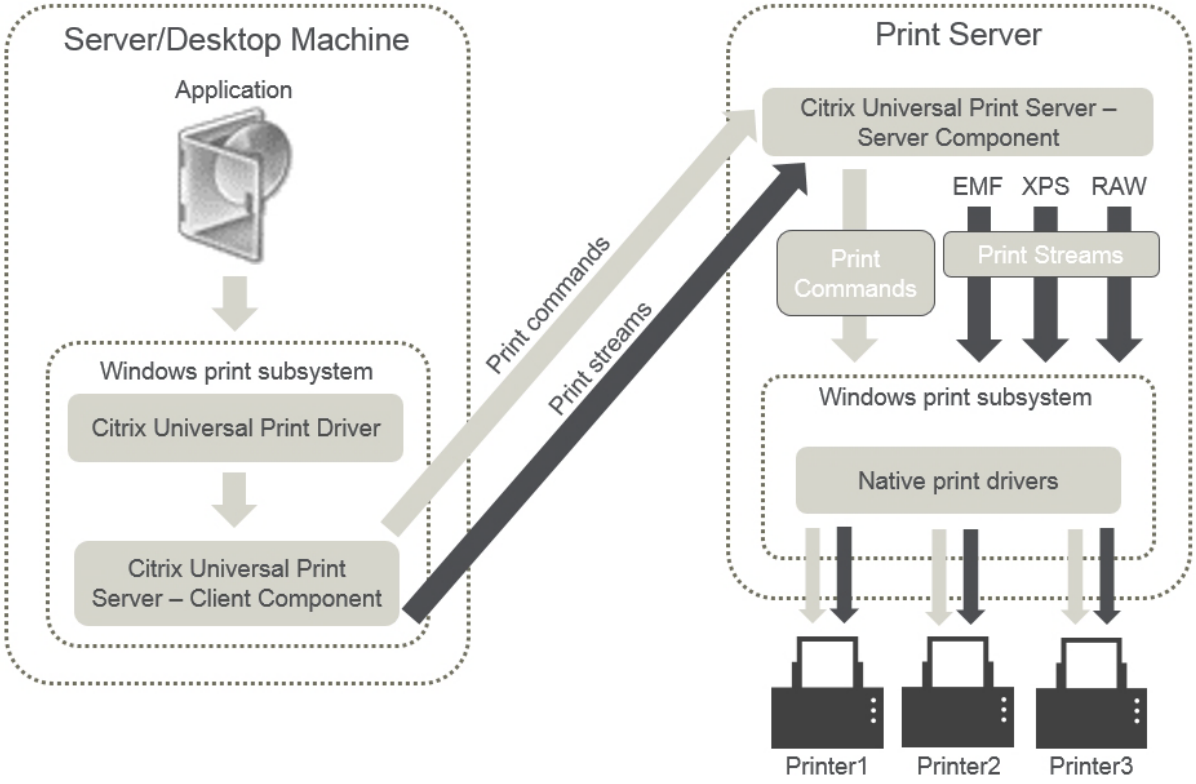
La función de Universal Print Server consta de:

Un componente de cliente, **UPClient**: Habilite UPClient en cada máquina con sistema operativo multisesión 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.

- **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.

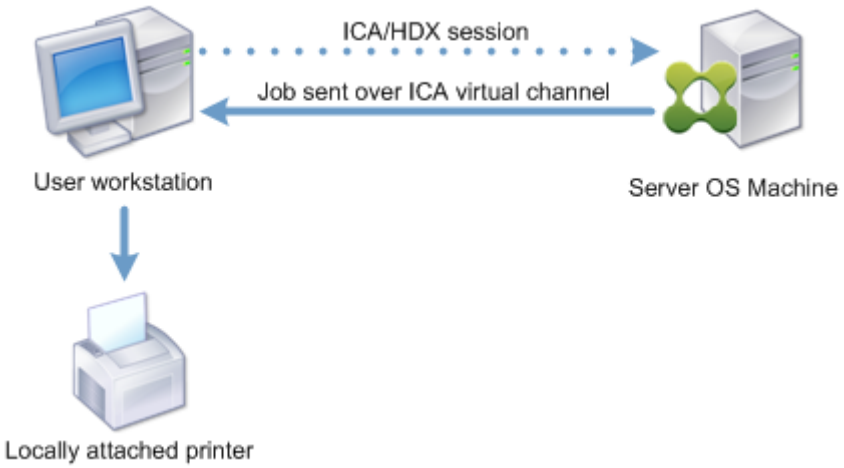
Enrutamiento de trabajos de impresión

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 multisesión, 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.



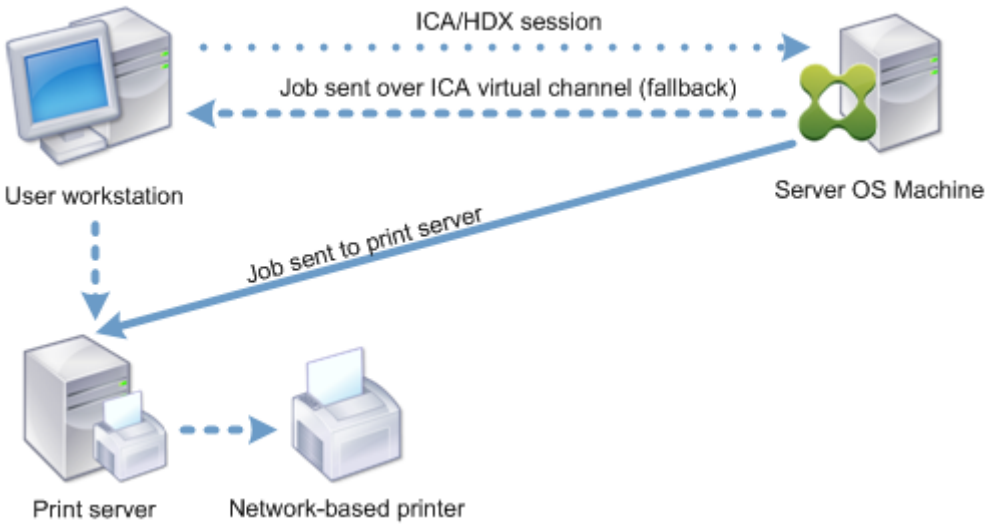
Impresoras de red

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.

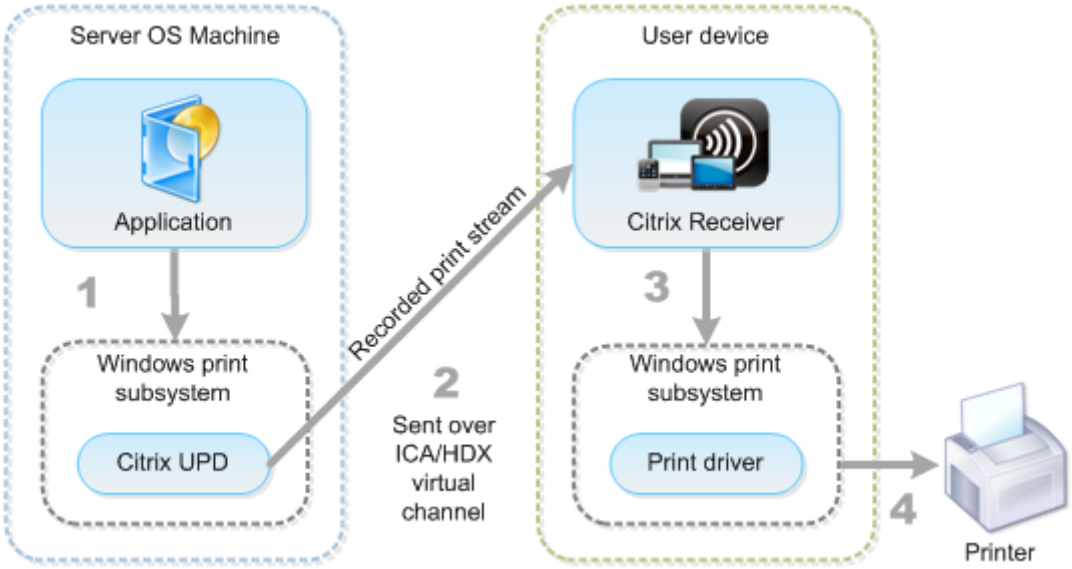
El controlador de impresora universal de Citrix admite los siguientes formatos de impresión:

- 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.

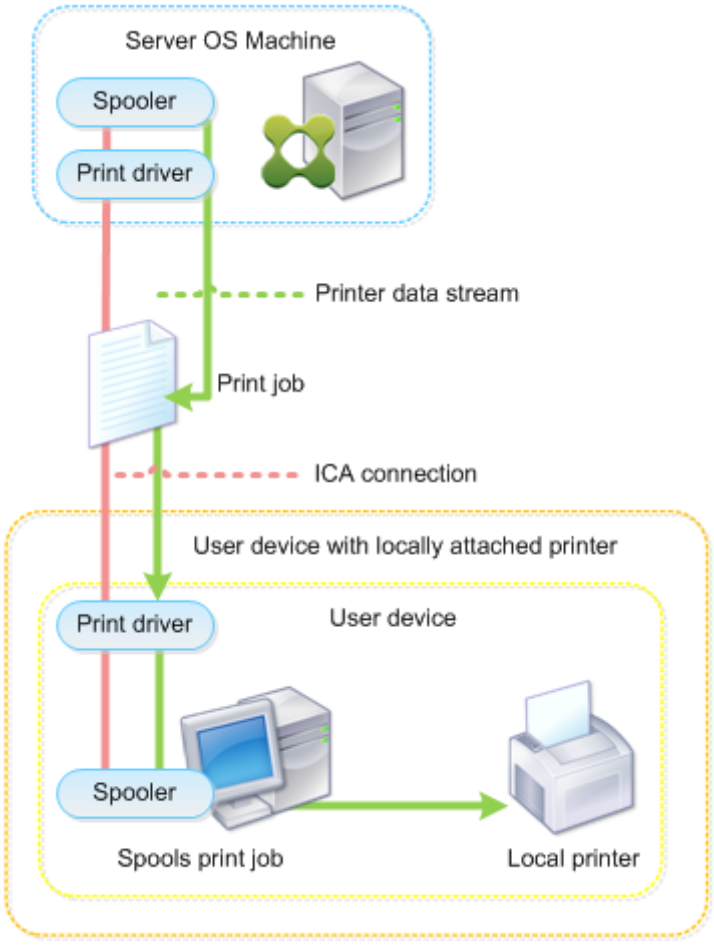
La siguiente ilustración muestra los componentes del controlador de impresión universal y el flujo de trabajo típico de una impresora conectada localmente a un dispositivo.



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

August 17, 2024

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).

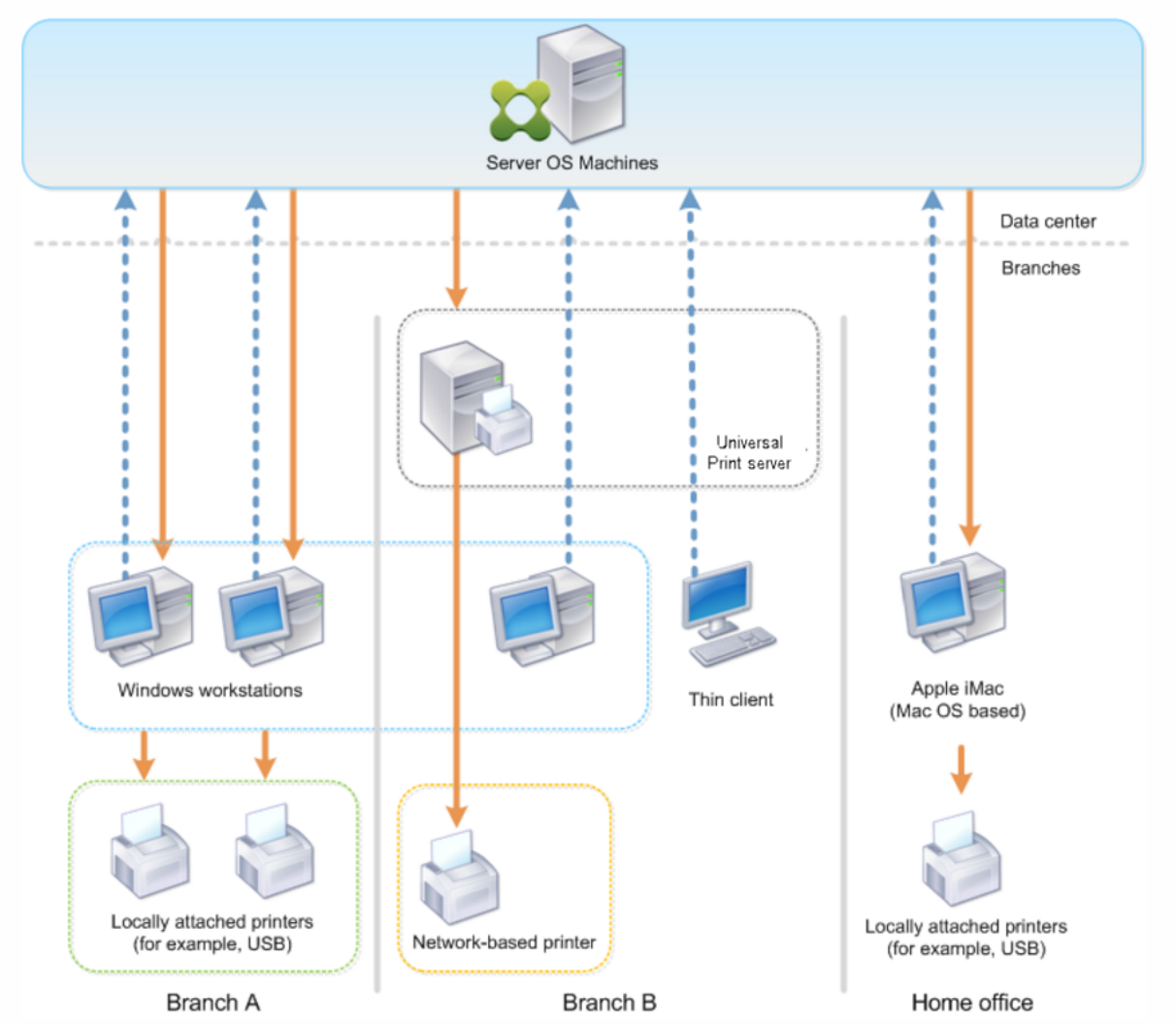
- Si los usuarios necesitan imprimir desde lugares distintos de su ubicación de trabajo principal: por ejemplo, empleados que usan varias estaciones de trabajo o realizan frecuentes viajes de negocios.

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 multisecuencia. 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 multisecuencia 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

August 17, 2024

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.

  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

August 17, 2024

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

August 17, 2024

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 usa 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.

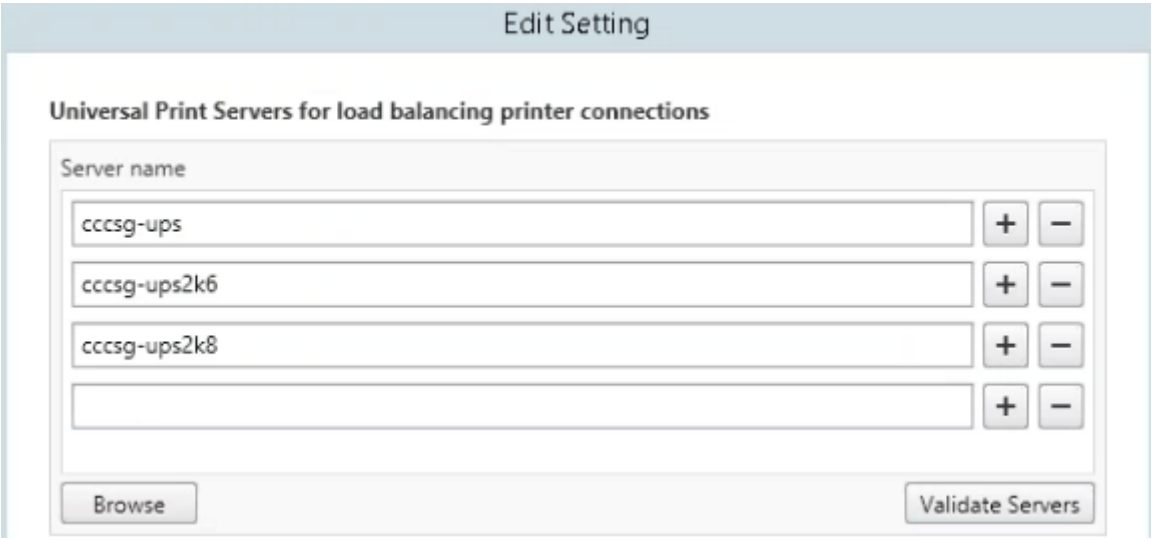
- **Habilitar Universal Print Server**. De forma predeterminada, Universal Print Server está inhabilitado. Al habilitar Universal Print Server, puede elegir si desea usar el proveedor de impresión de Windows en caso de que Universal Print Server no esté disponible. Después de habilitar Universal Print 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.

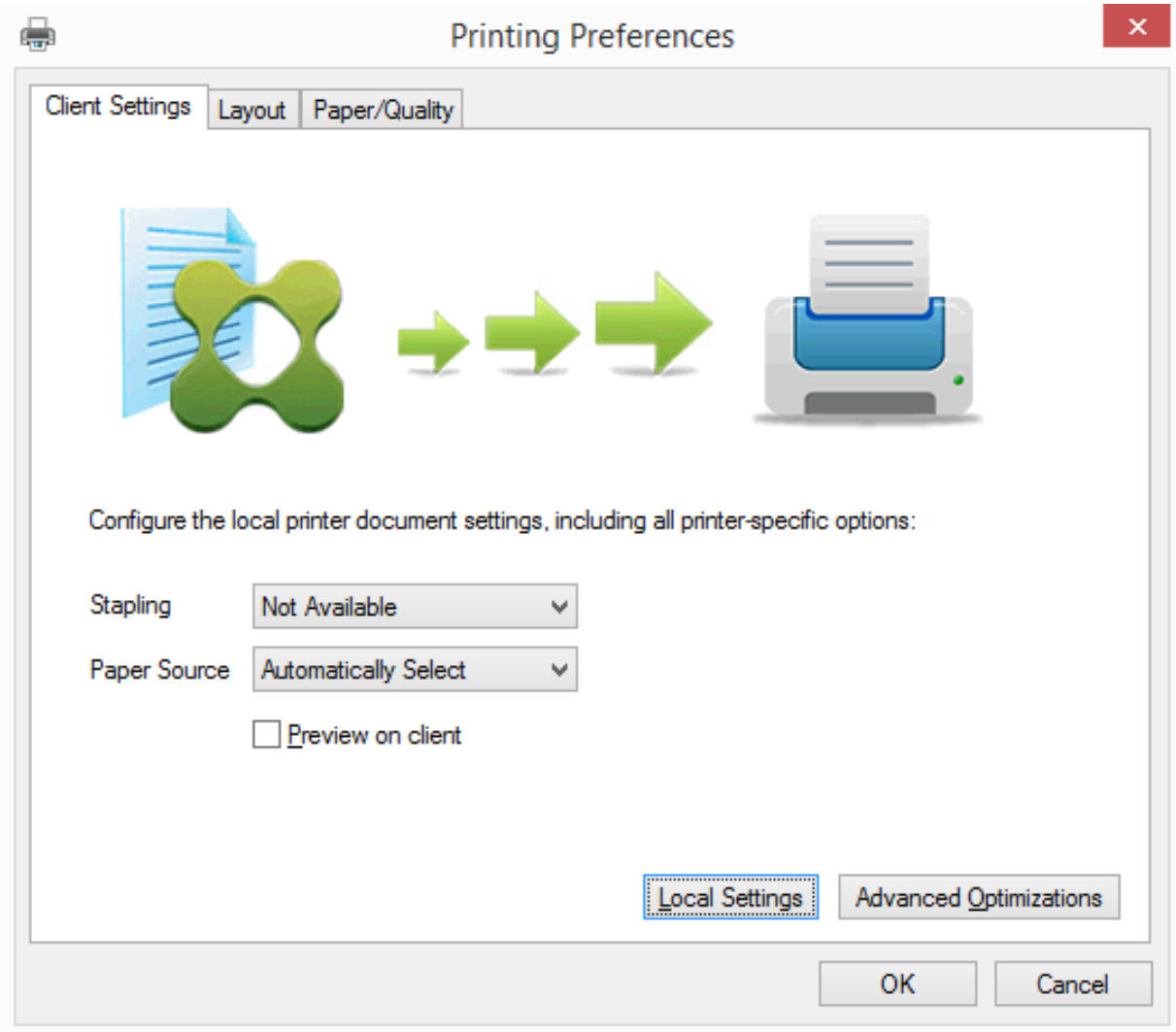
Configuración de directiva	Interacción
Redirección de impresoras del cliente, Crear automáticamente las impresoras del cliente	Después de habilitar Universal Print Server, las impresoras de red del cliente se crean mediante el controlador de impresión universal en lugar de los controladores nativos. 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

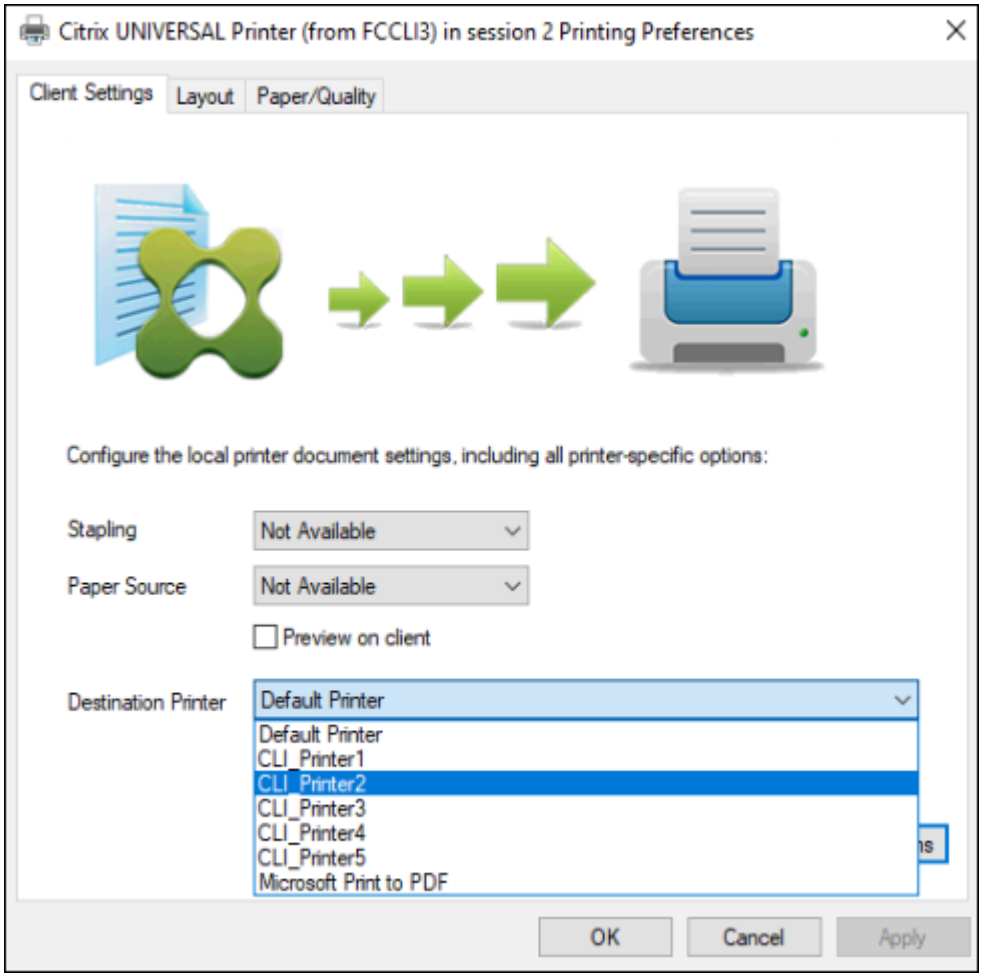
Se suministran estas soluciones de impresión universal para las impresoras cliente:

- **Impresora universal de Citrix:** Una impresora genérica, creada al comienzo de las sesiones, que no está vinculada a ningún dispositivo de impresión. Si crea automáticamente y usa únicamente la Impresora universal de Citrix, es posible que note una reducción del uso de recursos y del tiempo de inicio de sesión de los usuarios. 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.

  Para 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 o PCL.

  La Impresora universal de Citrix le permite seleccionar la impresora predeterminada del cliente o una impresora de cliente específica como destino de impresión. Para elegir una impresora específica para un trabajo de impresión, abra el cuadro de diálogo **Preferencias de impresión**. Seleccione el menú desplegable **Impresora de destino**. La opción **Impresora predeterminada** envía los trabajos de impresión a la impresora predeterminada del cliente. También se enumeran todas las impresoras redirigidas por el cliente que estén conectadas al dispositivo de punto final que se ejecuta la sesión. La impresora que seleccione se guardará como impresora de destino para cualquier trabajo de impresión futuro.



- **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

August 17, 2024

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
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

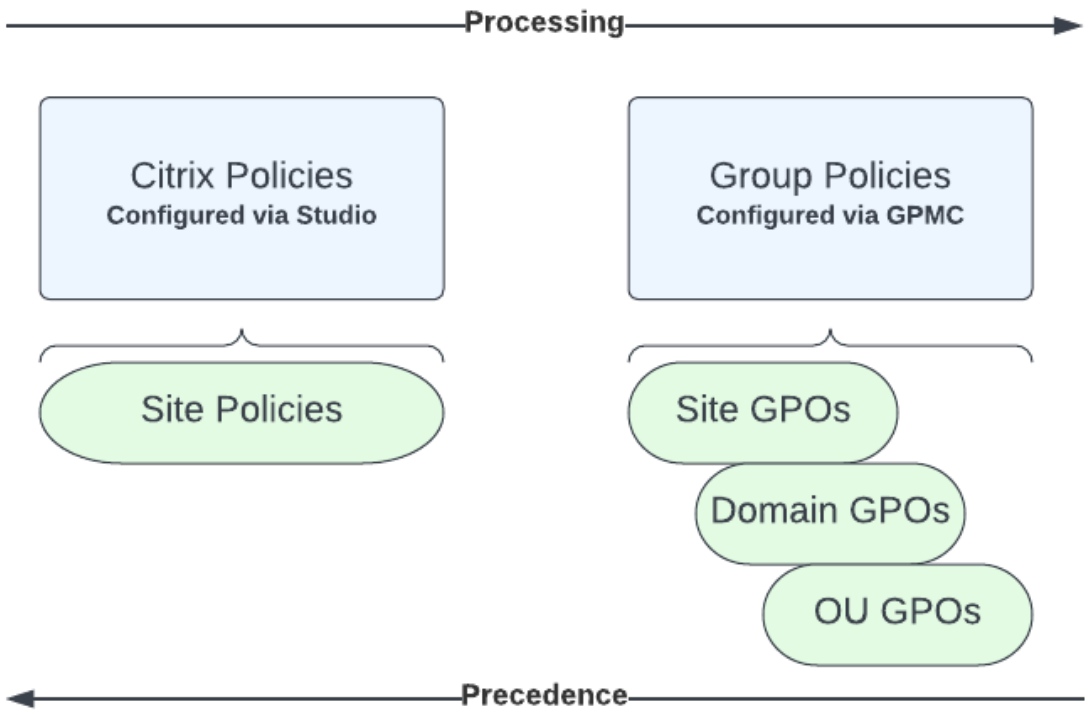
> **Nota:**
>
> Las colas de impresión de las impresoras de red que usan la ruta de impresión en red son privadas y no se pueden administrar en el sistema.

Directivas

August 17, 2024

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 en el nivel de grupo GPO del dominio anulan las directivas de GPO del sitio. Las directivas en el nivel de GPO del sitio, 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 Web 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. Además, pueden aplicarlos a un conjunto de usuarios de destino en diferentes niveles de la red.

Estos GPO se guardan en Active Directory. 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

August 17, 2024

> **Nota:**
>
> Puede administrar la implementación de Citrix Virtual Apps and Desktops mediante dos consolas de administración: Web Studio (basada en la web) y Citrix Studio (basada en Windows). Este artículo se refiere únicamente a Web Studio. Para obtener información sobre Citrix Studio, consulte el artículo equivalente en Citrix Virtual Apps and Desktops 7 2212 o versiones anteriores.

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 con las directivas de Citrix.

- **Web Studio.** Si usted es un administrador Citrix y no tiene permisos para administrar directivas de grupo, utilice Web Studio para crear directivas para su sitio. Las directivas que se crean mediante Web Studio se almacenan en la base de datos del sitio, y las actualizaciones se envían al VDA cuando ese VDA se registra con el intermediario o cuando un usuario se conecta a ese VDA.
- **Editor de directivas de grupo local** (complemento de la consola de administración de Microsoft). Si su entorno de red usa Active Directory y tiene permiso para administrar la directiva de grupo, puede usar el Editor de directivas de grupo local para crear directivas para su 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:**
>
> Se recomienda utilizar el Editor de directivas de grupos locales para configurar algunos parámetros de directivas. Los ejemplos incluyen parámetros relacionados con el registro de VDA con un Controller y parámetros relacionados con servidores de Microsoft App-V.
> Se agregan validaciones de directivas adicionales. Como resultado, realizar una actualización en contexto podría provocar la pérdida de datos de la directiva si hay una configuración de directiva no válida. Si crea o modifica las directivas mediante un método que no sea Web Studio, Citrix recomienda usar la versión más reciente del SDK y el complemento.

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 Virtual Apps and Desktops (almacenados en la base de datos del sitio)
3. GPO de sitio
4. GPO de dominio
5. Unidades organizativas

No obstante, si hay un conflicto, las configuraciones de directiva que se procesan en último lugar pueden anular a las procesadas con anterioridad. El orden de prioridad de los parámetros de directivas es el siguiente:

1. Unidades organizativas
2. GPO de dominio
3. GPO de sitio
4. GPO del sitio de Virtual Apps and Desktops (almacenados en la base de datos del sitio)
5. GPO locales

Por ejemplo: un administrador de Citrix usa Web 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 se ignora la directiva A. El motivo es que la directiva B se procesa en el nivel de dominio, mientras que la directiva A se procesa en el nivel de GPO del sitio de Virtual Apps and Desktops.

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. Esta configuración incluye parámetros relacionados con la configuración típica de conexión del cliente RDP. Los parámetros de la configuración de conexión del

cliente RDP son Fondo de pantalla de escritorio, Animación de menús y Ver contenido de las ventanas al arrastrar.

Cuando se utilizan varias directivas, puede priorizar las que contienen configuraciones conflictivas. Para obtener más información, consulte Comparación, prioridad, modelado y solución de problemas de directivas.

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.

   > **Nota:**
   >
   > Para abrir el asistente de modelado de directivas de grupo de Citrix, vaya a la ficha **Directivas > Modelado** y, a continuación, haga clic en **Iniciar asistente de modelado** en la barra de acciones. La ficha **Modelado** no está disponible en las instancias de Web Studio a petición del cliente.

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 Web Studio, las configuraciones de directiva se ordenan en categorías según la funcionalidad o la función a la que afectan. Por ejemplo, la sección **Profile Management** incluye 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 la izquierda de Web Studio.

  - La ficha **Directivas** muestra todas las directivas. Al seleccionar una directiva, las fichas en la parte inferior muestran lo siguiente:
    * Resumen: Muestra el nombre, prioridad, estado habilitado/inhabilitado y descripción
    * Parámetros: Muestra todos los parámetros configurados
    * Asignado a: Muestra objetos de usuario y máquina a los que está asignada la directiva. Para obtener más información, consulte Creación de directivas.
  - La ficha **Plantillas** enumera las plantillas suministradas por Citrix y las plantillas que usted haya creado. Al seleccionar una plantilla, las fichas de la parte inferior muestran lo siguiente:
    * Descripción (por qué le podría interesar utilizar la plantilla)
    * Parámetros (lista de parámetros configurados). 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.

  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 la barra de acciones.
  3. En la página **Parámetros**, escriba el nombre del parámetro en el campo de **búsqueda**:

     Puede refinar la búsqueda si selecciona:

     - Una versión de producto específica
     - Una categoría (por ejemplo, Ancho de banda)
     - Palabras clave en el nombre del parámetro
     - La casilla de verificación **Ver solo seleccionadas**
     - Para buscar solo 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:

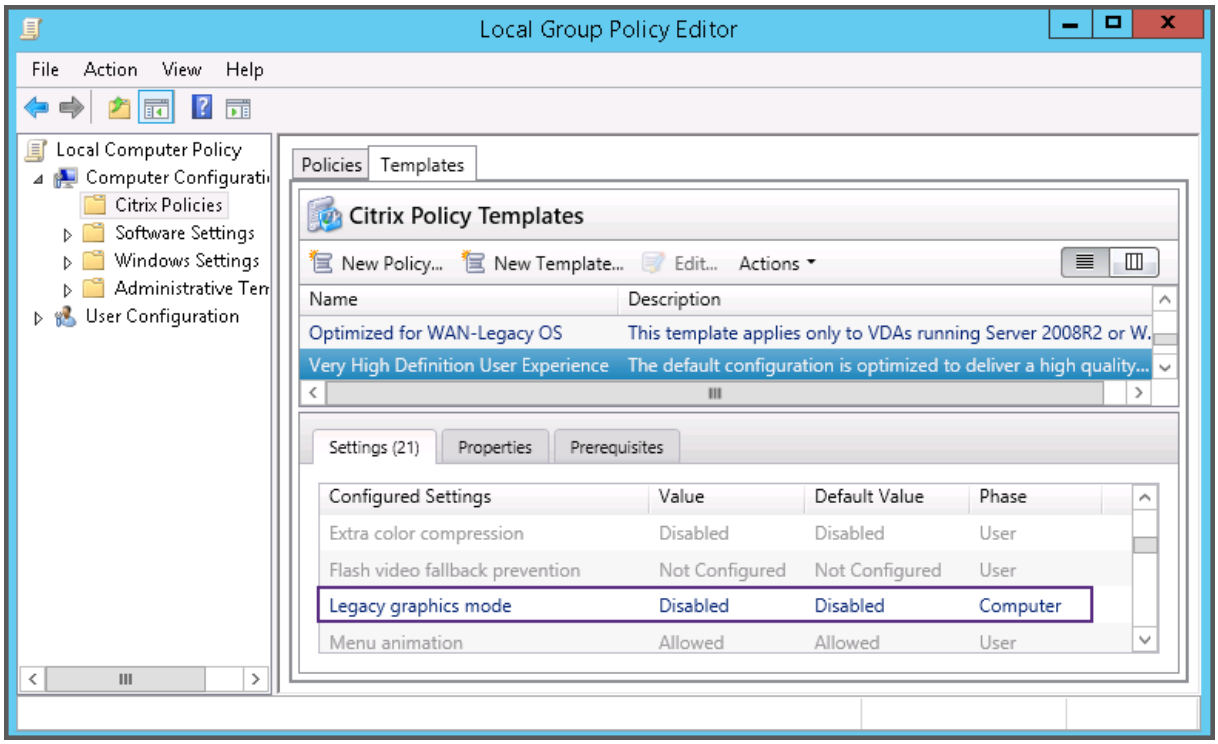
1. Seleccione la directiva.
2. Seleccione la ficha **Configuraciones** y comience a escribir el nombre de la configuración.

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 independiente de la plantilla utilizada. Puede usar el campo **Descripción** de una nueva directiva para realizar un rastreo de la plantilla de origen utilizada.

En el Editor de directivas de grupo, las configuraciones de equipo y de usuario se deben aplicar de forma independiente, incluso si se han 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 usa en una directiva creada a partir de esta plantilla.
- Las configuraciones de usuario, en gris, no se usan en una directiva creada a partir de esta plantilla.



Plantillas de directiva

August 17, 2024

> **Nota:**
>
> Puede administrar la implementación de Citrix Virtual Apps and Desktops mediante dos consolas de administración: Web Studio (basada en la web) y Citrix Studio (basada en Windows). Este artículo se refiere únicamente a Web Studio. Para obtener información sobre Citrix Studio, consulte el artículo equivalente en Citrix Virtual Apps and Desktops 7 2212 o versiones anteriores.

Las plantillas son colecciones de parámetros que se recomienda usar en la creación de directivas para lograr algunos resultados específicos. Por ejemplo, para crear directivas a fin de ofrecer una experiencia de alta definición a los usuarios finales, se pueden usar los parámetros definidos en la plantilla Experiencia de usuario de muy alta definición como referencia y punto de partida.

Las plantillas no son directivas. Las plantillas son documentación complementaria a los parámetros de directivas de Citrix. Demuestran las funcionalidades colectivas de ciertos parámetros relacionados con el usuario.

El uso de plantillas es opcional. Los administradores pueden crear directivas sin usar plantillas. Las plantillas son útiles para los administradores que tienen una idea general sobre cómo se debe configurar un sitio, pero no están seguros de qué opciones usar para lograr la configuración deseada.

Los administradores pueden crear plantillas a partir de una plantilla o una directiva existente, o bien partiendo de cero.

ADMX/ADML

Las plantillas de directivas de grupo de Citrix que se describen aquí no tienen nada que ver con las plantillas de directivas de Windows. Las plantillas que se describen aquí y las plantillas de directivas de Windows son dos conceptos diferentes. Las plantillas de directivas de grupo de Citrix no son archivos ADMX.

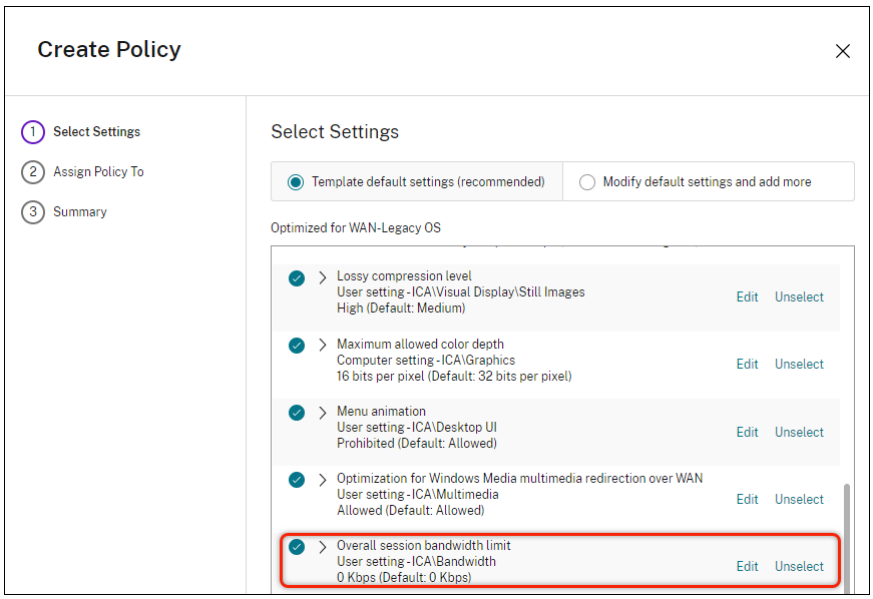
Plantillas integradas de Citrix

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 con Web Studio

Para crear una plantilla basada, a su vez, en una plantilla:

1. Inicie sesión en Web Studio y seleccione **Directivas** en el panel de la izquierda.
2. Haga clic en la ficha **Plantillas** y seleccione la plantilla a partir de la cual creará otra.
3. Seleccione la ficha **Crear plantilla**. Aparecerá la pantalla **Seleccionar configuraciones**.
4. Seleccione y configure las configuraciones de directiva que desea incluir en la plantilla.
5. Haga clic en **Siguiente**. Aparecerá la pantalla **Resumen** .
6. Introduzca un nombre para la plantilla.
7. Haga clic en **Finalizar**. La nueva plantilla aparece en la ficha **Plantillas**.

Para crear una plantilla basada en una directiva:

1. Inicie sesión en Web Studio y seleccione **Directivas** en el panel de la izquierda.
2. Haga clic en la ficha **Directivas** y seleccione la directiva a partir de la cual crea la plantilla.
3. Haz clic en la ficha **Más**.
4. Seleccione **Guardar como plantilla**. Aparecerá la pantalla **Seleccionar configuraciones**.
5. Seleccione y defina las configuraciones de directiva que desea incluir en la plantilla.
6. Haga clic en **Siguiente**. Aparecerá la pantalla **Resumen** .

7. Introduzca un nombre y una descripción para la nueva plantilla y haga clic en **Finalizar**.

Plantillas y administración delegada

Las plantillas de Web Studio se almacenan en la base de datos del sitio, a diferencia de las plantillas de Citrix Studio, que se almacenan como archivos en la carpeta de perfiles de usuario del administrador actual con una extensión `.gpt`. Las plantillas de Citrix Studio creadas por un administrador no son visibles para otros administradores ni para el mismo administrador en una máquina diferente. Las plantillas de Web Studio son visibles para todos los administradores, sujeto a permisos y administración delegada.

Crear directivas

August 17, 2024

> **Nota:**
>
> Puede administrar la implementación de Citrix Virtual Apps and Desktops mediante dos consolas de administración: Web Studio (basada en la web) y Citrix Studio (basada en Windows). Este artículo se refiere únicamente a Web Studio. Para obtener información sobre Citrix Studio, consulte el artículo equivalente en Citrix Virtual Apps and Desktops 7 2212 o versiones anteriores.

Antes de crear una directiva, decida a qué grupo de usuarios o dispositivos puede afectar. Puede crear una directiva según las funciones laborales del usuario, el tipo de conexión, el dispositivo de usuario o la ubicación geográfica. También 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, en lugar de crear otra directiva nueva. Después de modificar la directiva, configure los parámetros correspondientes. Evite la creación de una directiva exclusivamente para habilitar una configuración específica o para excluir la aplicación de la directiva a determinados usuarios.

Al crear una directiva, puede basarla en las configuraciones de una plantilla de directiva y personalizarlas según sea necesario. También puede crearla sin usar una plantilla y agregar las configuraciones que necesite.

En Web Studio, las nuevas directivas creadas se establecen como inhabilitadas a menos que se marque explícitamente la casilla **Habilitar directiva**.

Durante la creación de directivas y al configurar los parámetros, el sistema ofrece una opción para ver el tipo de parámetros. Puede ver los siguientes tipos de parámetros:

- Todos los parámetros: Ver todos los aplicables de todas las versiones de VDA
- Solo parámetros actuales: Ver los parámetros específicos de la versión actual de VDA
- Solo parámetros antiguos: Ver solo los parámetros aplicables de las versiones retiradas de VDA

Para ver los parámetros mientras los configura:

1. Inicie sesión en Web Studio y seleccione **Directivas** en el panel de la izquierda.
2. En la ficha **Directivas**, haga clic en **Crear directiva**.
3. En la tabla **Seleccionar configuraciones**, haga clic en el menú desplegable situado junto a **Parámetros**.
4. Seleccione una de las siguientes opciones de la lista desplegable:

- Todos los parámetros: Ver todos los parámetros de todas las versiones de VDA
- Solo parámetros actuales: Ver solo los parámetros de las versiones actuales de VDA
- Solo parámetros antiguos: Ver solo los parámetros de las versiones retiradas de VDA

1. La tabla **Parámetros** muestra los parámetros disponibles en función del paso anterior.

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. A veces, se permite o se impide que los usuarios administren la acción de la configuración en la sesión. Por ejemplo: si se define la configuración de 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 este parámetro como el parámetro **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 estas configuraciones de directiva 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. Esta selección impide configurar el parámetro y permite usar solo el valor predeterminado al aplicar la directiva. Esta selección es independiente del valor que se haya introducido antes de seleccionar Usar valor predeterminado.

Si el parámetro seguro predeterminado está habilitada, durante la instalación del VDA, la prioridad de la configuración de directiva se ve afectada de la siguiente manera:

- La configuración personalizada tiene la máxima prioridad
- La configuración predeterminada segura tiene la segunda prioridad
- La configuración predeterminada tiene la prioridad más baja

Para ver la configuración segura predeterminada de una directiva:

1. Inicie sesión en Web Studio.
2. En el panel de navegación de la izquierda, haga clic en **Directivas**.
3. En la ficha **Directivas**, haga clic en **Crear directiva**.
4. En la tabla **Seleccionar parámetros** , ¿al pasar el cursor sobre las configuraciones que tienen **¿Permitido?** como valor actual, se muestra el **Valor predeterminado seguro: Prohibido**.

   Parámetro predeterminado seguro

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, se asigna a determinados objetos de usuario y máquina. Esa directiva se aplica a las conexiones según criterios o reglas específicos. Por lo general, es posible agregar tantas asigna-

ciones como se desee a una directiva, según una combinación de criterios.

Si no especifica ninguna asignación o especifica asignaciones, pero las inhabilita, la directiva se aplica a **todas** las conexiones.

> **Nota:**
>
> Las asignaciones de directivas también se conocen como filtros de directivas. Para obtener información adicional, consulte los siguientes temas:
>
> - Crear, modificar o eliminar un filtro para una directiva
> - ¿Cómo se aplican los filtros?

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. *Tipo de conexión*: Si se debe aplicar la directiva a las conexiones realizadas con o sin NetScaler Gateway. *Nombre de la comunidad de NetScaler Gateway*: Nombre del servidor virtual de NetScaler Gateway. *Condición de acceso*: 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 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.

Nombre de asignación	Aplica una directiva según
Tipo de grupo de entrega	Tipo de escritorio o aplicación: escritorio privado, escritorio compartido, aplicación privada o aplicación compartida. **Nota:** 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 CTX219153.
Unidad organizativa (UO)	Unidad organizativa.
Etiqueta	Etiquetas. **Nota:** Aplique esta directiva a todas las máquinas etiquetadas. 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 Web 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 usa el Editor de directivas de grupo local para administrar las directivas de Citrix, las configuraciones que agregue a la directiva sin filtro se aplican a todos los sitios y conexiones. Los sitios y las conexiones deben estar en el ámbito de los objetos de directiva de grupo (GPO) que incluye la directiva. Por ejemplo: la unidad organizativa Ventas incluye 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 jefe de Ventas-EE. UU. inicia sesión en el sitio, la configuración de la directiva sin filtro se aplica automáticamente a la sesión. Esto se debe a 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. El modo está establecido en Permitir.
  - La asignación B especifica la cuenta del jefe de ventas. El modo está establecido en 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. El modo está establecido en Permitir.
  - La asignación D es una asignación de dirección IP del cliente que especifica 10.8.169.* (la red de la empresa). El modo está establecido en 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. El modo está establecido en Permitir.
  - La asignación F es una asignación de control de acceso que especifica condiciones de conexión de NetScaler Gateway. El modo está establecido en 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 Web Studio

1. Inicie sesión en Web Studio y seleccione **Directivas** en el panel de la izquierda.
2. Seleccione la ficha **Plantillas** y seleccione una plantilla.
3. Seleccione **Crear directiva a partir de una plantilla** en la barra de acciones.
4. De forma predeterminada, la nueva directiva utiliza todos los valores predeterminados de la plantilla. En este caso, se selecciona **Configuraciones de plantilla predeterminadas (recomendado)**. Si quiere cambiar configuraciones, seleccione **Modificar configuraciones predeterminadas y agregar más** y, a continuación, agregue o quite configuraciones.
5. Para especificar cómo se aplica la directiva, seleccione una de las siguientes opciones:
   - **Objetos de usuario y máquina seleccionados**. Para aplicar la directiva a objetos de usuario y máquina seleccionados. A continuación, haga clic en **Asignar** para seleccionar los objetos de usuario y máquina a los que debe aplicarse la directiva.
   - **Todos los objetos del sitio**. Para aplicar la directiva a todos los objetos de usuario y máquina del sitio.
6. Introduzca un nombre para la directiva. 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 inhabilitada de forma predeterminada; se puede habilitar. 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 Web Studio

1. Inicie sesión en Web Studio y seleccione **Directivas** en el panel de la izquierda.
2. Seleccione la ficha **Directivas**.
3. Seleccione **Crear directiva** en la barra de 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 debe aplicarse 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 valor 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 del 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**.
Crear una directiva a partir de una plantilla existente	En la ficha **Plantillas**, seleccione la plantilla y, a continuación, haga clic en **Nueva directiva**.

Conjuntos de directivas

August 17, 2024

Los conjuntos de directivas son objetos de Citrix Virtual Apps and Desktops que acumulan directivas para permitir un acceso simplificado y basado en roles, y una administración sencilla. Puede crear conjuntos de directivas para reflejar las divisiones lógicas de su empresa y su equipo de administradores. Por ejemplo, puede crear un conjunto de directivas para cada región geográfica, unidad de negocio o caso de uso específico. Una vez creados, los ámbitos y los grupos de entrega se asignan a conjuntos de directivas para que solo los administradores autorizados puedan administrar las directivas que se aplican a sus usuarios y máquinas pertinentes.

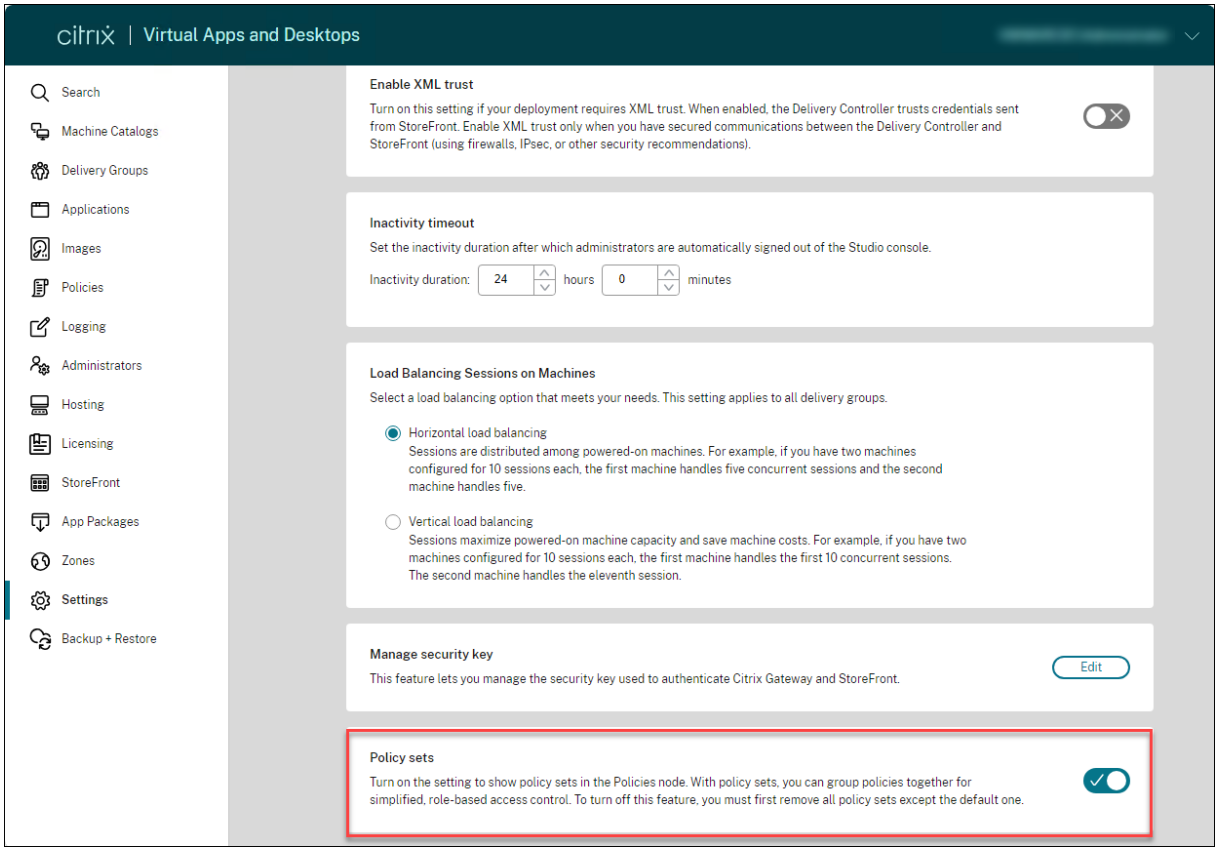
> **Nota:**
>
> Antes de habilitar los conjuntos de directivas, Citrix recomienda tomar nota de lo siguiente:
>
> - Se agregan validaciones de directivas adicionales. Como resultado, realizar una actualización en contexto podría provocar la pérdida de datos de la directiva si hay una configuración de directiva no válida.
> - Para detectar los datos no válidos, utilice la herramienta de análisis de GPO y realice las modificaciones necesarias antes de realizar la actualización de versión. Para obtener más información, consulte CTX676686.
> - Para todas las actualizaciones futuras, Citrix recomienda usar el SDK más reciente. El uso de un SDK anterior para actualizar las directivas podría permitir agregar datos no válidos a las configuraciones de las directivas, lo que podría conllevar el riesgo de perder los datos de las directivas.

Ventajas

- Control de acceso por roles para equipos de administradores distribuidos
- Fusiones, adquisiciones y consolidaciones simplificadas
- Dominio de errores limitado
- Función multiarrendataria para directivas

Habilitar conjuntos de directivas

En la ficha **Administrar** de Virtual Apps and Desktops, vaya a **Parámetros** y active el parámetro **Conjuntos de directivas**.



> **Nota:**
>
> Debe habilitar conjuntos de directivas antes de crear un conjunto de directivas.

Comparación de funciones

Antes de aplicar conjuntos de directivas	Tras aplicar conjuntos de directivas
Las directivas, los parámetros, los filtros y las prioridades de directivas de todo el sitio se configuran en un solo lugar dentro de Citrix Studio.	Las directivas, los parámetros, los filtros y las prioridades de directivas se configuran por separado para cada conjunto de directivas.
Si administra una directiva, debe administrar todas las directivas.	Los administradores totales pueden delegar en administradores de nivel inferior la capacidad de administrar un conjunto de directivas determinado de forma individual.
Las directivas de entornos grandes y distribuidos se vuelven complejas y difíciles de administrar.	Las directivas de entornos grandes y distribuidos se pueden dividir y administrar fácilmente.

¿Cómo funcionan los conjuntos de directivas?

Descripción general

- Los conjuntos de directivas se asignan a grupos de entrega
- Los conjuntos de directivas tienen uno o varios ámbitos
- Los grupos de entrega sin ningún conjunto de directivas asignado reciben el conjunto de directivas predeterminado
- Un grupo de entrega solo puede tener asignado un conjunto de directivas
- Varios grupos de entrega pueden usar el mismo conjunto de directivas
- Aunque los conjuntos de directivas se asignen a grupos de entrega, las directivas mantienen sus filtros

Para obtener más información, consulte How do filters get applied. No hay ningún cambio en la forma en la que funcionan las asignaciones de directivas o los filtros de directivas para los conjuntos de directivas. Es decir, funcionan de la misma manera que lo hacen para las directivas individuales.

Conjunto de directivas predeterminado

- Cuando el parámetro del conjunto de directivas está activado, todas las directivas existentes se agrupan en el conjunto de directivas predeterminado
- Cada grupo de entrega recibe el conjunto de directivas predeterminado, a menos que el equipo de administradores cree un conjunto de directivas y lo asigne a un grupo de entrega.
- Cuando a un grupo de entrega se le asigna un conjunto de directivas diferente, ya no recibirá directivas del conjunto de directivas predeterminado

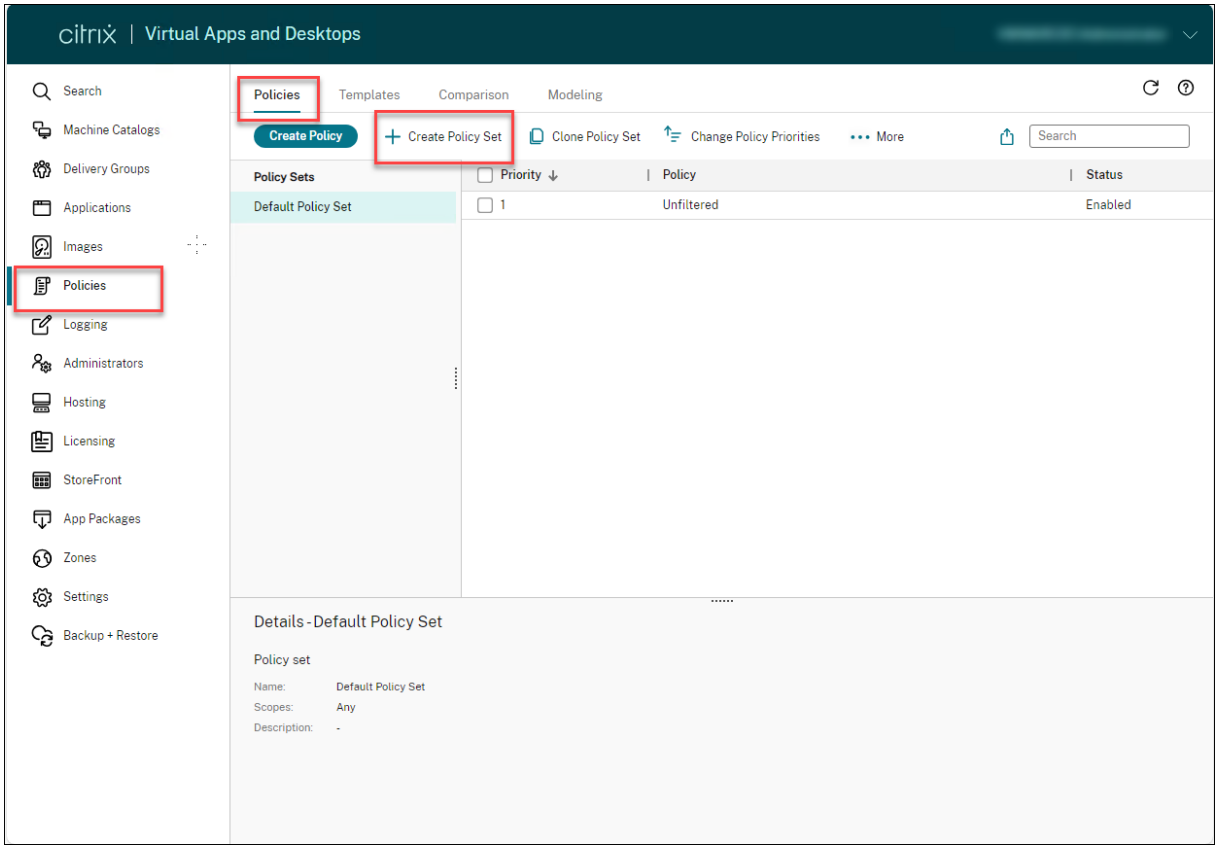
Creación de conjuntos de directivas

Los conjuntos de directivas se pueden crear de estas dos maneras:

- Crear conjunto de directivas: Esta acción crea un conjunto de directivas vacío
- Clonar conjunto de directivas: Esta acción crea un conjunto de directivas basado en un conjunto de directivas existente

Crear conjuntos de directivas

1. Inicie sesión en Web Studio y seleccione **Directivas** en el panel de la izquierda.



1. Seleccione **Crear conjunto de directivas**. Aparece la ficha **Introducción**.
2. Haga clic en **Siguiente** o en la ficha **Nombre y descripción**.
3. Introduzca el nombre y la descripción del conjunto de directivas.
4. Haga clic en **Siguiente** o en la ficha **Asignaciones**.
5. Seleccione uno o más grupos de entrega a los que quiera asignar el conjunto de directivas.
6. Haga clic en **Siguiente** o en la ficha **Ámbitos**.
7. Seleccione los ámbitos del conjunto de directivas.
8. Haga clic en **Crear**. El conjunto de directivas se crea con la asignación y el ámbito definidos.

Clonar conjuntos de directivas

1. Inicie sesión en Web Studio y seleccione **Directivas** en el panel de la izquierda.
2. Seleccione **Clonar conjunto de directivas**.
3. Modifique el nombre del conjunto de directivas.
4. Modifique o cree asignaciones para el conjunto de directivas y haga clic en **Siguiente**.
5. Seleccione o anule la selección de directivas que quiera incluir en el conjunto de directivas clonado.
6. Modifique el ámbito de la directiva.
7. Haga clic en **Crear**. Se crea el conjunto de directivas.

Modificar conjuntos de directivas

1. Inicie sesión en Web Studio y seleccione **Directivas** en el panel de la izquierda.
2. Seleccione **Modificar conjunto de directivas**.
3. Modifique el nombre del conjunto de directivas y haga clic en **Siguiente**.
4. Modifique o cree asignaciones para el conjunto de directivas y haga clic en **Siguiente**.
5. Modifique el ámbito de la directiva.
6. Haga clic en **Crear**.

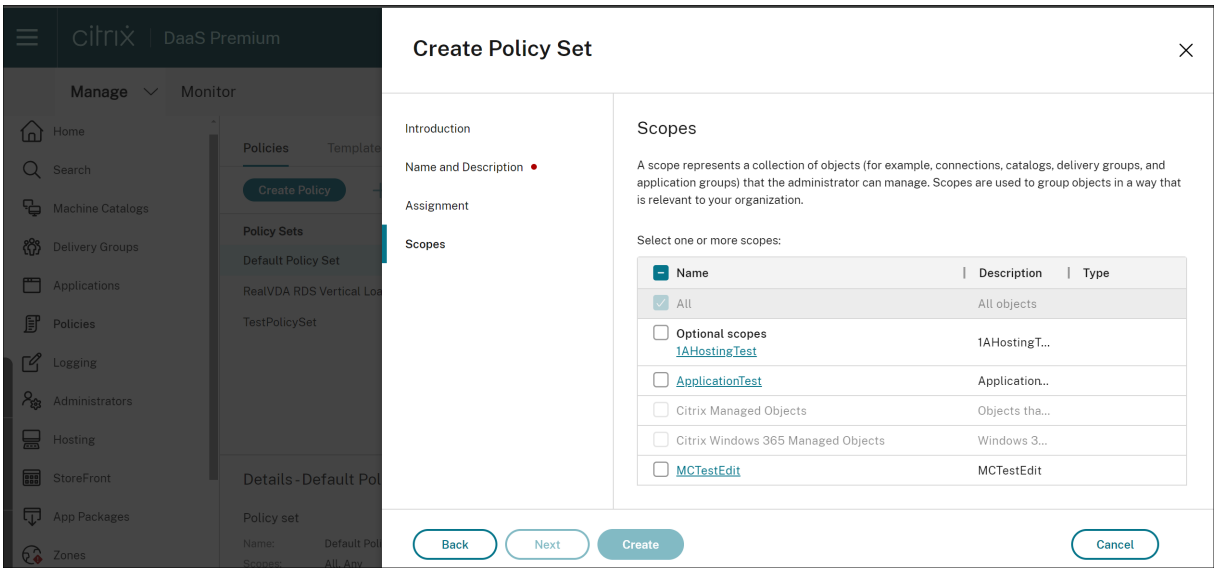
Asignación de conjuntos de directivas

Los conjuntos de directivas se asignan a grupos de entrega. Puede configurar asignaciones cuando se crea o se modifica el conjunto de directivas. También puede configurar asignaciones al crear o modificar grupos de entrega.

Ámbitos de conjuntos de directivas

Los administradores pueden definir el ámbito del conjunto de directivas para que solo administradores autorizados puedan verlo o modificarlo. Puede configurar los ámbitos al crear o al modificar el conjunto de directivas.

Con la introducción de los conjuntos de directivas, también puede crear y administrar directivas de Citrix mediante la API. Para obtener más información, consulte How to create a policy set in Citrix DaaS.



Comparar, priorizar y solucionar problemas de directivas

August 17, 2024

> **Nota:**
>
> Puede administrar la implementación de Citrix Virtual Apps and Desktops mediante dos consolas de administración: Web Studio (basada en la web) y Citrix Studio (basada en Windows). Este artículo se refiere únicamente a Web Studio. Para obtener información sobre Citrix Studio, consulte el artículo equivalente en Citrix Virtual Apps and Desktops 7 2212 o versiones anteriores.

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: por motivos de seguridad, deba establecer restricciones en los grupos de usuarios que interactúan regularmente con datos confidenciales.

Además, 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 usuarios del grupo 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. Al usar diversas directivas, debe determinar:

- Cómo priorizar las directivas
- Cómo crear excepciones
- Cómo ver la directiva efectiva cuando las directivas entran en conflicto.

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 de su entorno siempre anula a las demás configuraciones y directivas. La configuración de cifrado más exigente incluye el sistema operativo y la configuración de remedo más restrictiva.

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. Esta configuración incluye parámetros relacionados con la configuración típica de conexión del cliente RDP. La configuración típica de RDP incluye parámetros como el fondo de pantalla de escritorio, la animación de menús y la visualización del contenido de la ventana mientras se arrastra.

Algunas opciones de configuración de directivas, como Secure ICA, deben 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, tenga en cuenta que un VDA de SO de sesión única se conecta a un VDA de SO multisesión. En este caso, las directivas de Citrix actúan en el VDA de SO de sesión única como si fuera el dispositivo del usuario. Por ejemplo: considere que las directivas están configuradas para guardar en caché las imágenes en el dispositivo del usuario. En este ejemplo, las imágenes almacenadas en caché para el segundo salto en un escenario de doble salto se almacenan en caché en la máquina VDA con SO de sesión única.

Usar el asistente de modelado de directivas

El modelado de directivas le ayuda a simular directivas habilitadas con filtros a efectos de planificación y prueba. Solo se modelan las directivas habilitadas con filtros. Las directivas inhabilitadas nunca se aplican y las directivas habilitadas sin filtros siempre se aplican.

Siga estos pasos para abrir el asistente de **Modelado de directivas**:

1. Seleccione **Directivas** en el menú de navegación de la izquierda.
2. Seleccione la ficha **Modelado**.
3. Seleccione **Modelado de directivas** en la barra de acciones.
4. Lea la página **Introducción** y haga clic en **Siguiente**.
5. Seleccione usuarios o equipos. Puede buscar contenedores o usuarios o equipos específicos. Haga clic en **Siguiente**.
6. Elija una evidencia de filtro. Si lo desea, puede obtener una simulación más detallada introduciendo detalles adicionales, como el **grupo de entrega**, las **etiquetas**, la **dirección IP del cliente**, etc. Haga clic en **Siguiente**.
7. Revise el resumen de opciones elegidas y haga clic en **Ejecutar**.

Al hacer clic en **Ejecutar**, el asistente genera un informe de los resultados del modelado. Mientras consulta este informe, puede hacer lo siguiente:

- Seleccionar si quiere ver **Todas las configuraciones**, la **Configuración de equipo** o los **Parámetros de usuario** en el menú desplegable.
- Usar la barra de búsqueda para buscar configuraciones específicas.
- Hacer clic en una configuración específica para ver sus detalles. Por ejemplo, si no se aplicaron todos los parámetros de usuario a una directiva específica, el panel **Detalles** muestra el motivo por el que no se aplicaron.
- Haga clic en **Exportar** para exportar los resultados del modelado en formato JSON, HTML o ambos.

Tras ejecutar el modelado de directivas, dispondrá de más opciones. Puede hacer lo siguiente:

- **Ver informe de modelado**: Se abre el mismo informe de modelado de arriba para que pueda volver a verlo o exportarlo.
- **Ejecutar de nuevo el modelado de directivas**: Esto le permite volver a ejecutar el modelado de directivas con el mismo conjunto de criterios seleccionado anteriormente y generar nuevos resultados de modelado. Puede resultar útil si algunas directivas han cambiado y quiere ver cómo afectan esos cambios al modelo actual.
- **Eliminar informe de modelado**: Elimina el informe de modelado actual.

Comparar directivas y plantillas

Puede comparar la configuración de una directiva o plantilla con las de otras directivas o plantillas. Por ejemplo: puede que necesite verificar los valores de configuración para garantizar que se cumplan las directrices recomendadas. También puede comparar las configuraciones de una directiva o plantilla con las configuraciones predeterminadas proporcionadas por Citrix.

1. Inicie sesión en Web Studio y seleccione **Directivas** en el panel de la izquierda.
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. Al hacer 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. 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 fusionan según su condición y prioridad. Por ejemplo: si la configuración está inhabilitada o habilitada. 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 la izquierda. Asegúrese de seleccionar la ficha **Directivas**.
2. En la ficha **Directivas**, seleccione **Cambiar prioridades de directiva** en la barra de acciones. Aparecerá la página **Cambiar prioridades de directiva**.
3. En la lista de prioridades, lleve a cabo una de las siguientes opciones para cambiar la prioridad de una directiva:
    - Arrastre la directiva a la posición que quiera.
    - Para moverla una posición hacia arriba o hacia abajo, haga clic en el icono de flecha arriba o abajo, respectivamente.
    - Para moverla a la parte superior o inferior de la lista, haga clic en el icono de flecha superior o inferior, respectivamente.
    - Para cambiar el número de prioridad, haga clic en el icono **Modificar**, introduzca un número y, a continuación, haga clic en **Guardar**.
4. Haga clic en **Guardar**.

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 incluye las siguientes asignaciones:

- La asignación A es una asignación de dirección IP del cliente que especifica el intervalo 208.77.88.*. El modo está establecido en Permitir
- La asignación B es una asignación de usuario que especifica una cuenta de usuario determinada. El modo está establecido en 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.

Determinar las directivas que se aplican a una conexión

Es posible que una conexión no responda como se esperaba porque 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 calcular el Conjunto resultante de directivas o RSOP (Resultant Set of Policies) y determinar cómo se combinan las configuraciones de directiva finales para una conexión.

El Conjunto resultante de directivas se puede calcular de diversas maneras:

- Con el **asistente de modelado de directivas de grupo de Citrix**, puede simular un caso de conexión y observar la forma en que se aplicarían las directivas de Citrix. Puede especificar condiciones para un escenario de conexión, por ejemplo:
  - Controlador de dominio
  - Usuarios
  - Valores de prueba de asignación de directivas Citrix
  - Configuración de entorno simulado, como conexión de red lenta

    El informe que genera el asistente enumera las directivas de Citrix que entran en vigor en el caso concreto. Como inicia sesión en el Controller como un usuario del dominio, el asistente calcula los resultados mediante la configuración de directivas del sitio y 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 le ayuda a evaluar el estado actual de los GPO en su entorno y genera un informe. El informe generado 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 de Citrix en Web Studio. También puede iniciar la herramienta de resultados de directivas de grupo a través de la Consola de administración de directivas de grupo de Windows.

La configuración de directivas de sitio creada con Web Studio no se incluye en el conjunto resultante de directivas en los siguientes casos:

- Si ejecuta el asistente de modelado de directivas de grupo de Citrix desde la Consola de administración de directivas de grupo
- Si ejecuta la herramienta Resultados de directivas de grupo desde la Consola de administración de directivas de grupo

Para verificar que obtiene el grupo de directivas resultante más completo, Citrix recomienda iniciar el asistente de Modelado de Directivas de grupo Citrix desde Web Studio, a menos que cree las directivas mediante solo la Consola de administración de directivas de grupo.

Solucionar problemas de directivas

Los usuarios, las direcciones IP y otros objetos asignados pueden tener varias directivas que se aplican de forma simultánea. Este supuesto 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. En este caso, 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 se produce 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

August 17, 2024

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	Desactivado. 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
Formatos permitidos de escritura en el portapapeles del cliente	No se han especificado formatos	Desde VDA 7.6 hasta la actual

Nombre	Configuración predeterminada	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
Limitar el cliente del portapapeles al tamaño de la transferencia de la sesión	Inhabilitado	VDA 2009
Limitar la sesión del portapapeles al tamaño de transferencia del cliente	Inhabilitado	VDA 2009
Modo tolerante a pérdidas	Se permite	VDA 2003. Nota: El modo de tolerancia a pérdidas aún no está disponible. Esta versión del VDA lo admite desde que está disponible.
Umbrales de tolerancia a pérdidas	Cuando el modo tolerante a pérdidas está disponible: Pérdida de paquetes: 5%, Latencia: 300 ms (RTT)	VDA 2003 hasta la versión actual
Protocolo Rendezvous	Inhabilitado	Se aplica solo a las sesiones HDX establecidas a través de Citrix Cloud.
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.

Nombre	Configuración predeterminada	VDA
Lista de canales virtuales permitidos	Habilitado	Desde VDA 2109 hasta la actual
Recopilación de métricas de sesión	Se permite	7.42 hasta la actual

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
Audio adaptable	Habilitado	Se aplica tanto a las sesiones de SO de sesión única como a las sesiones de SO multisesión de los VDA que utilizan Citrix Virtual Apps and Desktops 2109 o una versión posterior.
Transporte de audio en tiempo real sobre UDP	Se permite	Todas las versiones de VDA
Audio Plug and Play	Se permite	VDA para SO multisesión, desde la versión 7 hasta la actual
Calidad de audio	Alta: sonido de alta definición	Todas las versiones de VDA
Redirección de audio del cliente	Se permite	Todas las versiones de VDA
Redirección de micrófonos del cliente	Se permite	Todas las versiones de VDA
Modo tolerante a pérdidas para audio	Prohibida	VDA versiones 2402 y posteriores

ICA/Reconexión automática de clientes

Nombre	Configuración predeterminada	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 bidireccional de contenido	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
Configuración de redirección bidireccional de contenido	Inhabilitado	Desde VDA 2311 hasta la actual

ICA/Redirección de contenido de explorador web

Nombre	Configuración predeterminada	VDA
Redirección de contenido del explorador web	Se permite	Desde VDA 7.16 hasta la actual
Configuración de lista ACL para redirección de contenido del explorador web	`https://www.youtube.com/*`	Desde VDA 7.16 hasta la actual
Redirección de contenido del explorador compatible con autenticación de Windows integrada	Prohibida	Desde VDA 2106 hasta la actual
Configuración de proxy para redirección de contenido del explorador web	vacío	Desde VDA 7.16 hasta la actual
Autenticación de proxies web de la obtención del servidor de redirección de contenido del explorador	Prohibida	Desde VDA 2012 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	Inhabilitado	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	Inhabilitado	VDA para SO multisesión, desde la versión 7 hasta la actual
Conservar las letras de unidad del cliente	Inhabilitado	VDA 5, 5.5, 5.6 FP1, VDA para SO de sesión única, desde la versión 7 hasta la actual
Acceso de lectura solamente a unidades del cliente	Inhabilitado	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	Inhabilitado	Todas las versiones de VDA

ICA/Gráficos

Nombre	Configuración predeterminada	VDA
Permitir compresión sin pérdida visual	Inhabilitado	Desde VDA 7.6 hasta la actual
Límite de memoria de presentación	65 536 KB	VDA 5, 5.5, 5.6 FP1, VDA para SO de sesión única, desde la versión 7 hasta la actual

Nombre	Configuración predeterminada	VDA
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
Indicador de estado de gráficos	Inhabilitado	Desde VDA 7.16 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	Inhabilitado	VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual
Profundidad de color máxima permitida	32 bits por píxel	Todas las versiones de VDA
Notificar al usuario cuando se degrada la presentación	Inhabilitado	VDA para SO multisesión, desde la versión 7 hasta la actual
Optimizar para cargas de trabajo de gráficos 3D	Inhabilitado	Desde VDA 7.17 hasta la actual
Cola y descarte	Habilitado	Todas las versiones de VDA
Uso compartido de pantalla	Inhabilitado	VDA 2112
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 bps	VDA para SO multisesión, desde la versión 7 hasta la actual

ICA/Gráficos/Framehawk

Nombre	Configuración predeterminada	VDA
Canal de presentación Framehawk	Inhabilitado	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
ICA Keep Alive	No enviar mensajes de ICA Keep Alive	Todas las versiones de VDA

ICA/Teclado e IME

Nombre	Configuración predeterminada	VDA
Sincronización de la distribución del teclado del cliente y mejora de IME	Inhabilitado	Se aplica solo a 1912 LTSR CU2 y versiones posteriores.
Habilitar la asignación de distribución de teclado Unicode	Prohibida	Se aplica solo a 1912 LTSR CU2 y versiones posteriores.
Ocultar cuadro de mensaje emergente del botón de distribución del teclado	Prohibida	Se aplica solo a 1912 LTSR CU2 y versiones posteriores.

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 bloqueados de redirección de URL	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 permitidos de redirección de URL	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
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.

Nombre	Configuración predeterminada	VDA
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
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

Nombre	Configuración predeterminada	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	Inhabilitado	Desde VDA 5, 5.5, 5.6 FP1 hasta la actual

ICA/Conexiones de multisecuencia

Nombre	Configuración predeterminada	VDA
Audio sobre UDP	Se permite	VDA para SO multisesión, desde la versión 7 hasta la actual
Intervalo de puertos UDP de audio	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 multisecuencia	Inhabilitado	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 usuario para multisecuencia	Inhabilitado	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 multisecuencia	Consulte Parámetro de asignación de canales virtuales multisecuencia para conocer las asignaciones de secuencias predeterminadas	VDA 2003

ICA/Redirección de puertos

Nombre	Configuración predeterminada	VDA
Conectar automáticamente puertos COM del cliente	Inhabilitado	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	Inhabilitado	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

Nombre	Configuración predeterminada	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)	Inhabilitado	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	Inhabilitado	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

Nombre	Configuración predeterminada	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	Inhabilitado	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
Límite de compresión de imagen para la impresión universal	Mejor calidad (compresión sin pérdida)	Todas las versiones de VDA

Nombre	Configuración predeterminada	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 sesiones desconectadas	Inhabilitado	VDA 5, 5.5, 5.6 FP1, VDA para SO de sesión única, desde la versión 7 hasta la actual
Temporizador de sesión desconectada de acceso con Remote PC	Inhabilitado	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	Inhabilitado	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

> **Nota:**
>
> La directiva de **Velocidad de fotogramas mínima objetivo** ha quedado obsoleta.

ICA/Presentación visual/Imágenes fijas

Nombre	Configuración predeterminada	VDA
Compresión de color adicional	Inhabilitado	Todas las versiones de VDA
Umbral de compresión de color adicional	8192 Kbps	Todas las versiones de VDA
Compresión intensa	Inhabilitado	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	Inhabilitado	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	Inhabilitado	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	Inhabilitado	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	Inhabilitado	Todas las versiones de VDA
Cerrar la sesión del usuario si hay algún problema	Inhabilitado	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	Inhabilitado	Todas las versiones de VDA

Profile Management/Parámetros básicos

Nombre	Configuración predeterminada	VDA
Reescritura activa	Inhabilitado	Todas las versiones de VDA
Habilitar Profile Management	Inhabilitado	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	Inhabilitado	Todas las versiones de VDA
Ruta al almacén de usuarios	Windows	Todas las versiones de VDA
Procesar inicios de sesión de administradores locales	Inhabilitado	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	Inhabilitado	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	Inhabilitado	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 que 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	Inhabilitado	Todas las versiones de VDA
Incluir nombre de dominio	Inhabilitado	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	Inhabilitado	Todas las versiones de VDA
Información común	Inhabilitado	Todas las versiones de VDA
Advertencias comunes	Inhabilitado	Todas las versiones de VDA
Habilitar registro	Inhabilitado	Todas las versiones de VDA
Acciones del sistema de archivos	Inhabilitado	Todas las versiones de VDA
Notificaciones del sistema de archivos	Inhabilitado	Todas las versiones de VDA
Cierre de sesión	Inhabilitado	Todas las versiones de VDA
Inicio de sesión	Inhabilitado	Todas las versiones de VDA
Tamaño máximo del archivo de registros	1048576	Todas las versiones de VDA

Nombre	Configuración predeterminada	VDA
Ruta al archivo de registros	Inhabilitado. Los archivos de registro se guardan en la ubicación predeterminada: %SystemRoot%\System32 \Logfiles\UserProfileManager.	Todas las versiones de VDA
Información de usuario personalizada	Inhabilitado	Todas las versiones de VDA
Valores de directivas al iniciar y cerrar la sesión	Inhabilitado	Todas las versiones de VDA
Acciones del Registro del sistema	Inhabilitado	Todas las versiones de VDA
Diferencias en el Registro del sistema al cerrar la sesión	Inhabilitado	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	Inhabilitado	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	Inhabilitado	Todas las versiones de VDA
El perfil de plantilla sobrescribe el perfil móvil	Inhabilitado	Todas las versiones de VDA

Nombre	Configuración predeterminada	VDA
Perfil de plantilla utilizado como perfil de Citrix obligatorio para todos los inicios de sesión	Inhabilitado	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	Inhabilitado	Todas las versiones de VDA
Tamaño de caché	0 MB	Todas las versiones de VDA
Streaming de perfiles	Inhabilitado	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	10 GB. Una capa de usuarios es un disco de aprovisionamiento ligero que se expande al tamaño establecido. Las capas de usuarios nunca disminuyen de tamaño.	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

Nombre	Configuración predeterminada	VDA
Usar solo el registro de Controller con IPv6	Inhabilitado	VDA para SO multisesión, desde la versión 7 hasta la actual, VDA para SO de sesión única, desde la versión 7 hasta la actual
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	Inhabilitado	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	Inhabilitado	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

August 17, 2024

Las directivas incluyen configuraciones que se aplican cuando estas 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 intermediario (Delivery Controller). También puede descargar la versión más reciente de las configuraciones de directivas haciendo clic aquí.

Audio

Para esta tarea	Use esta configuración de directiva
Controlar si se permite el uso de varios dispositivos de sonido	Audio 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 audio
Controlar la asignación de sonido a los altavoces del dispositivo de usuario	Redirección de audio 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 un portapapeles local	Límite de ancho de banda de redirección del portapapeles o Porcentaje límite de ancho de banda de redirección del portapapeles
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, o no, 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

Para esta tarea	Use esta configuración de directiva
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
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 multisecuencia

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 multisecuencia entre servidores y dispositivos de usuario	Multisecuencia (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

August 17, 2024

> **Nota:**
>
> En esta página se proporcionan descripciones y valores de configuración admitidos para las configuraciones de la directiva ICA. Para obtener más información sobre cómo trabajar con directivas, consulte la sección Trabajar con directivas.

Transporte adaptable

Esta configuración permite o impide el transporte de datos por EDT como opción principal o por TCP como opción de reserva.

De forma predeterminada, el transporte adaptable está habilitado (**Preferido**), y se usa EDT cuando sea posible (cuando no sea posible, se recurre a TCP). Puede cambiar su configuración según lo que necesite:

- **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.

Configuración de arrastrar y colocar

Esta configuración permite o impide arrastrar archivos entre el cliente y las aplicaciones o los escritorios virtuales. De forma predeterminada, la directiva de arrastrar y colocar está inhabilitada. Puede habilitar esta directiva si es necesario.

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 copiar 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 configuración 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:

- Verifique que la configuración **Redirección del portapapeles del cliente** está **permitida**.
- Verifique 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 la directiva **Redirección del portapapeles del cliente** se establece en **Prohibida** o si la directiva **Restringir escritura en el portapapeles del cliente** se establece en **Inhabilitada**.

> **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.

Limitar el cliente del portapapeles al tamaño de la transferencia de la sesión

Este parámetro especifica el tamaño máximo de los datos del portapapeles que un usuario puede transferir desde un dispositivo de punto final de cliente a una sesión virtual durante una sola operación de copiar y pegar.

Para limitar el tamaño de transferencia del portapapeles, habilite la opción **Limitar el cliente del portapapeles al tamaño de la transferencia de la sesión**. A continuación, en el campo **Límite de tamaño**, introduzca un valor en kilobytes para definir el tamaño de la transferencia de datos entre el portapapeles local y una sesión.

De forma predeterminada, esta configuración está inhabilitada y no hay límite en las transferencias de cliente a sesión.

HDX Direct

HDX Direct permite al cliente establecer automáticamente una conexión directa con el host de la sesión cuando hay una comunicación directa disponible. Las conexiones se establecen de forma segura mediante el cifrado a nivel de red.

Modo HDX Direct

HDX Direct se puede usar para establecer conexiones directas con los hosts de sesión para clientes internos y externos. Esta configuración determina si HDX Direct está disponible solo para clientes internos o para clientes internos y externos.

Cuando se establece en **Interno** solo, HDX Direct intenta establecer conexiones directas solo para los clientes de la red interna.

Cuando se establece en **Interno** y **Externo**, HDX Direct intenta establecer conexiones directas para los clientes internos y externos.

De forma predeterminada, HDX Direct está configurado solo para clientes internos.

Intervalo de puertos HDX Direct

El intervalo de puertos que usa HDX Direct para las conexiones de usuarios externos.
De forma predeterminada, HDX Direct usa el intervalo de puertos: 55000—55250.

Limitar la sesión del portapapeles al tamaño de transferencia del cliente

Este parámetro especifica el tamaño máximo de los datos del portapapeles que un usuario puede transferir desde una sesión virtual a un dispositivo de punto final de cliente durante una sola operación de cortar y pegar.

Para limitar el tamaño de la transferencia del portapapeles, habilite la opción **Limitar la sesión del portapapeles al tamaño de la transferencia del cliente**. A continuación, en el campo **Límite de**

tamaño, introduzca un valor en kilobytes para definir el tamaño de la transferencia de datos entre una sesión y el portapapeles local.

De forma predeterminada, esta configuración está inhabilitada y no hay límite en las transferencias de cliente a sesión.

Restringir escritura en el portapapeles del cliente

Si este parámetro está **habilitado**, los datos del portapapeles del host no se pueden compartir con el dispositivo de punto final del cliente. Puede permitir algunos formatos específicos, habilitando la configuración **Formatos permitidos de escritura en el portapapeles del cliente**.

De forma predeterminada, esta configuración está **inhabilitada**.

Restringir escritura en el portapapeles de la sesión

Cuando esta configuración está **habilitada**, los datos del portapapeles del cliente no se pueden compartir en la sesión de 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 **inhabilitada**.

Formatos permitidos de escritura en el portapapeles de la sesión

Cuando la configuración **Restringir escritura en el portapapeles de la sesión** está **habilitada**, 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:

- Verifique que la configuración **Redirección del portapapeles del cliente** está **permitida**.
- Verifique 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 la directiva **Redirección del portapapeles del cliente** se establece en **Prohibida** o si la directiva **Restringir escritura en el portapapeles de la sesión** se establece en **Inhabilitada**.

> **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 de 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 de un grupo de usuarios de acceso directo en un VDA. Estos usuarios no pueden conectarse al VDA tanto si esta configuración está habilitada como si no.

Redirección FIDO2

Esta configuración habilita o inhabilita la redirección FIDO2. La redirección FIDO2 permite a los usuarios aprovechar los componentes FIDO2 de los dispositivos de punto final local en máquinas virtuales. Los usuarios pueden autenticar una sesión virtual mediante biometría integrada o claves de seguridad FIDO2 en dispositivos que incluyan TPM 2.0 y Windows Hello.

Cuando esta configuración está **permitida**, los usuarios pueden procesar la autenticación FIDO2 mediante las prestaciones del dispositivo de punto final local. De forma predeterminada, esta configuración está **permitida**.

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 120 000 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

Esta configuración habilita o inhabilita lo siguiente:

- Sincronización de la distribución de teclado dinámico
- Editor de métodos de entrada (IME)
- Asignación de distribución de teclado Unicode
- Oculta o muestra el mensaje de notificación del botón para cambiar la distribución del teclado

1. En Web 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 de teclado** para controlar si aparece o no un mensaje y, así, indicar que la distribución del teclado se está sincronizando cuando el usuario cambia la distribución del teclado del cliente. Si no muestra este mensaje, los usuarios tienen que esperar unos momentos antes de escribir para evitar que se introduzcan caracteres incorrectos.

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 del servidor.

Modo tolerante a pérdidas

> **Importante:**
>
> - La función requiere al menos la versión 2002 de la aplicación Citrix Workspace para Windows. Esta versión del VDA lo admite desde que está disponible.
> - El modo tolerante a pérdidas para gráficos se ofrece en Citrix Gateway y en Citrix Gateway Service. Este modo solo está disponible con conexiones directas.

Este parámetro habilita o inhabilita el modo tolerante a pérdidas para gráficos.

De forma predeterminada, el modo tolerante a pérdidas para gráficos está **Permitido**.

Cuando está permitido, se accede a este modo cuando la pérdida de paquetes y la latencia están por encima de un umbral. Puede establecer los umbrales mediante la directiva Umbrales del modo tolerante a la pérdida.

Umbrales de tolerancia a pérdidas

Cuando el modo tolerante a la pérdida está disponible, este parámetro especifica los umbrales de métricas de red en los que la sesión cambia al modo tolerante a pérdidas para gráficos.

Los umbrales predeterminados son:

- Pérdida de paquetes: 5%
- Latencia: 300 ms (RTT)

Para obtener más información, consulte Modo tolerante a pérdidas.

Modo tolerante a pérdidas para audio

Este parámetro habilita o inhabilita el modo tolerante a pérdidas para audio.

Cuando se habilita, el audio se envía a través del modo tolerante a pérdidas.

De forma predeterminada, el modo tolerante a pérdidas para audio está **prohibido**.

Para habilitar la directiva, cambie el Registro de la directiva del modo tolerante a pérdidas para audio a **permitido**.

El transporte EDT es necesario para habilitar el modo tolerante a pérdidas para audio.

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 activa y desactiva en Citrix Cloud y en una configuración de 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. Este parámetro no afecta a las sesiones establecidas directamente entre el cliente y el VDA o a través de un dispositivo Citrix Gateway local.

Para obtener información, consulte Protocolo Rendezvous.

Configuración del proxy de Rendezvous

Este parámetro le permite configurar un proxy explícito para usarlo con el protocolo Rendezvous. Si se utiliza un proxy transparente, esta configuración no necesita estar habilitada.

De forma predeterminada, esta configuración está inhabilitada.

Cuando está inhabilitada, el VDA no redirige el tráfico saliente a través de proxies que no sean transparentes si se intenta establecer una conexión Rendezvous con Gateway Service

Cuando está habilitada, el VDA intenta establecer una conexión Rendezvous con Gateway Service a través del proxy definido en la configuración.

El VDA admite proxies HTTP y SOCKS5 para conexiones Rendezvous. Para configurar el VDA de modo que utilice un proxy para la conexión Rendezvous, debe habilitar esta configuración. Además, especifique la dirección del proxy o la ruta al archivo PAC. Por ejemplo:

- Dirección de proxy: `http://<URL or IP>:<port>` o `socks5://<URL or IP>:<port>`

- Archivo PAC: `http://<URL or IP>/<path>/<filename>.pac`

  La versión 2103 de VDA es la versión mínima admitida para la configuración de proxies con un archivo PAC. Para obtener más información sobre el esquema del archivo PAC para proxies SOCKS5, consulte Configuración de proxy.

> **Nota:**
>
> Solo los proxies SOCKS5 admiten el transporte de datos a través de EDT. Para un proxy HTTP, utilice TCP como el protocolo de transporte para ICA.

Para obtener más 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.

Recopilación de métricas de sesión

Este parámetro permite a Citrix recopilar métricas de sesiones de usuario y máquina entre el VDA y Workspace para mejorar la experiencia del usuario.

Citrix recopila datos como el sistema operativo, el tiempo de actividad, información sobre el sistema informático, detalles del controlador de vídeo, la versión del VDA, el tipo de implementación y el estado de unión al dominio. Además, puede recopilar algunas configuraciones de sesión, junto con datos sobre rendimiento y fiabilidad, para contribuir a la mejora del producto. Para obtener más información sobre nuestro programa Customer Experience Improvement Program, consulte:

- https://more.citrix.com/XD-CEIP
- https://docs.citrix.com/en-us/linux-virtual-delivery-agent/current-release/configure/administration/linux-vda-data-collection-program
- https://docs.citrix.com/en-us/mac-vda/configure/session/supportability-service

De manera predeterminada, esta configuración está habilitada.

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, independientemente del tipo de cliente.

Configuraciones de directiva de Reconexión automática de clientes

August 17, 2024

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 ha caducado. Por ejemplo: puede caducar debido a un retraso en la reconexión o si deben volverse a introducir las credenciales. 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 autorizada, aparece un temporizador de cuenta atrás en el área de notificaciones. Este temporizador indica el tiempo restante

antes de que vuelva a conectarse 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 inhabilitarla, establezca la directiva en **Prohibido**.

Autenticación para reconexión automática de clientes

Esta configuración especifica si se requiere 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.

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.

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. Use esta directiva para establecer el valor del tiempo de espera.

Nivel de transparencia de la interfaz de usuario durante la reconexión

Esta configuración le permite especificar 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%.

Configuraciones de directiva de audio

August 17, 2024

La sección **Audio** contiene las configuraciones que permiten que los dispositivos de usuario reciban y envíen audio en las sesiones, sin disminuir su rendimiento.

Audio adaptable

Esta configuración habilita o inhabilita el audio adaptable. Cuando se habilita esta directiva, los parámetros de calidad de audio se ajustan de manera dinámica para ofrecer una experiencia de usuario óptima. Esta configuración se aplica tanto a las sesiones de SO de sesión única como a las sesiones de SO multisesión de los VDA que utilizan Citrix Virtual Apps and Desktops 2109 o una versión posterior.

Cuando esta configuración está prohibida, se aplica la directiva de calidad de audio. Para obtener más información, consulte Calidad de audio.

De forma predeterminada, la directiva de audio adaptable está habilitada.

Transporte de audio en tiempo real sobre UDP

Esta configuración permite o impide la transmisión y la recepción de audio entre el VDA y el dispositivo del usuario a través de RTP mediante el protocolo UDP. Cuando esta configuración está inhabilitada, el audio se envía y recibe sobre TCP.

De forma predeterminada, el audio sobre UDP está permitido.

Audio Plug and Play

Esta configuración permite o impide el uso de varios dispositivos de audio para grabar y reproducir audio.

De forma predeterminada, el uso de varios dispositivos de audio está permitido.

Esta configuración solo se aplica a máquinas de SO multisesión Windows.

Calidad de audio

Esta configuración especifica el nivel de calidad de audio recibido en las sesiones de usuario.

De forma predeterminada, la calidad de audio está establecida en Alta: audio de alta definición.

Para controlar la calidad del audio, 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 tiene como resultado una reducción significativa de la calidad del sonido. Pero ofrece, al mismo tiempo, un rendimiento razonable en conexiones con poco ancho de banda.
- Seleccione "Media: optimizado para voz"para ofrecer aplicaciones con VoIP. Esta configuración ofrece entrega de aplicaciones multimedia en conexiones de red con poco ancho de banda, inferior a 512 Kbps, o cuando hay congestión de tráfico y pérdida de datos en la red. 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 audio enviado al dispositivo del usuario se comprime hasta 64 Kbps. Esta compresión provoca una ligera reducción en la calidad del audio 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 audio 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 audio. Use esta calidad de audio incluso para la entrega de aplicaciones multimedia en conexiones de red con poco ancho de banda (inferior a 512 Kbps). Asimismo, cuando hay congestión de tráfico y pérdida de datos en la red
- Elija Alta: audio de alta definición para las conexiones en las cuales no hay problemas de ancho de banda y la calidad del audio es importante. Los clientes pueden ejecutar el audio 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 audio 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 **Límite de ancho de banda de redirección de sonido** o **Porcentaje límite de ancho de banda de redirección de sonido**.

Redirección de audio del cliente

Esta configuración especifica si las aplicaciones alojadas en el servidor pueden reproducir sonidos mediante un dispositivo de audio instalado en el dispositivo del usuario. Esta configuración también especifica si los usuarios pueden grabar una entrada de audio.

La redirección del audio 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 audio. Limitar el ancho de banda utilizado para el audio permite mejorar el rendimiento de las aplicaciones, pero también reduce la calidad de audio. El ancho de banda solo se utiliza cuando el audio 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 **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 **Audio Plug and Play** está habilitada para admitir varios dispositivos de audio.

Importante: Cuando la Redirección de audio del cliente está Prohibida, toda la función de audio 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 audio en una sesión.

De forma predeterminada, se permite la redirección de micrófonos.

Por motivos de seguridad, se alerta a los usuarios cuando servidores sin relación de confianza con el dispositivo intentan 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 Audio Plug and Play está habilitada para admitir varios dispositivos de audio.

Si se inhabilita la configuración **Redirección de audio del cliente** en el dispositivo del usuario, esta regla no tiene ningún efecto.

Configuraciones de directiva de Ancho de banda

August 17, 2024

La sección **Ancho de banda** incluye 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 Multisecuencia**. Si se usan las configuraciones de multisecuencia 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 para la reproducción o la grabación de sonido en una sesión de usuario. El ancho de banda máximo permitido se especifica en kilobits por segundo.

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 para la redirección de dispositivos USB hacia y desde el cliente. El ancho de banda máximo permitido se especifica en kilobits por segundo.

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 para la transferencia de datos entre una sesión y el portapapeles local. El ancho de banda máximo permitido se especifica en kilobits por segundo.

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 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 archivos

Esta configuración permite especificar el valor máximo permitido de ancho de banda para el acceso a una unidad del cliente en una sesión de usuario. El ancho de banda máximo permitido se especifica en kilobits por segundo.

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 para entregar por streaming sonido y vídeo mediante la aceleración multimedia HDX MediaStream. El ancho de banda máximo permitido se especifica en kilobits por segundo.

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 para trabajos de impresión mediante un puerto LPT en una sesión de usuario individual. El ancho de banda máximo permitido se especifica en kilobits por segundo.

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 20 Mbps (20 000 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 para el acceso a las impresoras del cliente en una sesión de usuario. El ancho de banda máximo permitido se especifica en kilobits por segundo.

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 de ancho de banda para el control de dispositivos de imágenes TWAIN desde aplicaciones publicadas. El ancho de banda máximo permitido se especifica en kilobits por segundo.

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

August 17, 2024

La sección **Redirección de contenido bidireccional** incluye configuraciones de directiva para habilitar o inhabilitar la redirección de URL entre cliente y VDA y viceversa.

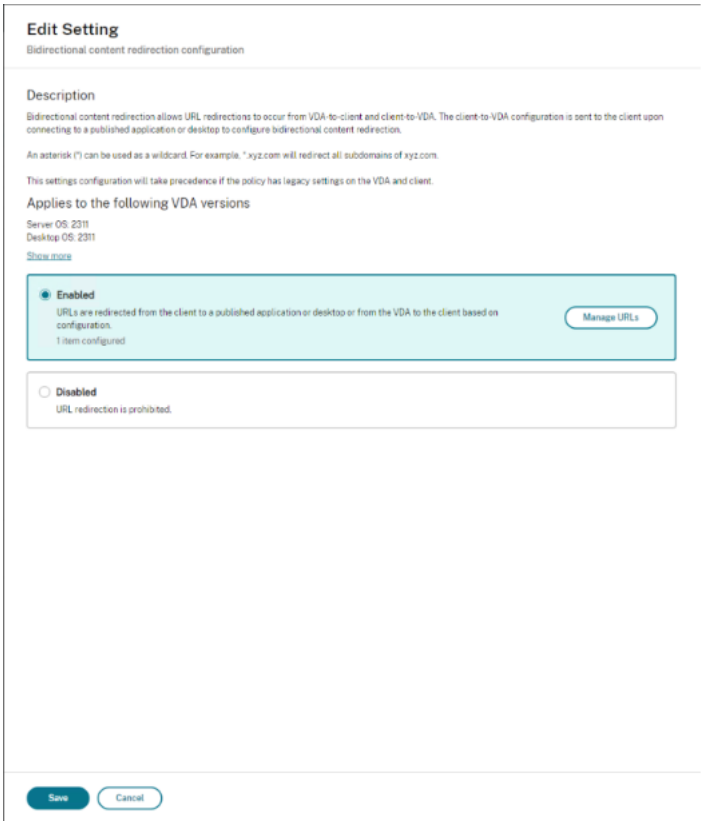
Las directivas de servidor se configuran en Web Studio. A partir de la versión 2311 de la aplicación Citrix Workspace, este parámetro reemplaza los siguientes tres parámetros antiguos de Web Studio retirados:

- Permitir redirección bidireccional de contenido
- Direcciones URL permitidas para redirigir al VDA
- Direcciones URL permitidas para redirigir al cliente

También reemplaza los tres parámetros de objeto de directiva de grupo (GPO) locales siguientes en los clientes Windows:

- Redirección bidireccional de contenido
- Anulaciones de redirección bidireccional de contenido
- Redirección de OAuth

Si está habilitado este parámetro, los parámetros de cliente a VDA se envían al cliente al conectarse a una aplicación o escritorio publicados para configurar la redirección de contenido bidireccional.



Si este parámetro está configurado, prevalece sobre los parámetros anteriores en Web Studio y en el cliente. Citrix recomienda usar solo las nuevas configuraciones de directiva y eliminar las antiguas para evitar comportamientos imprevistos.

No se deben establecer directivas de cliente si el VDA y el DDC ejecutan la versión 2311 o una versión posterior. De lo contrario, las directivas de cliente se configuran en la plantilla administrativa de objetos de directiva de grupo de la aplicación Citrix Workspace.

Citrix ofrece redirección de host a cliente y acceso a aplicaciones locales para la redirección de cliente a URL. Sin embargo, Citrix recomienda utilizar redirección bidireccional de contenido para los clientes de Windows que se unen a un dominio.

Para configurar esta función, Citrix recomienda usar la nueva interfaz de usuario en Web Studio en vez de Desktop Studio.

Redirección con comodines

La redirección bidireccional de contenido admite el uso de comodines al definir las URL que se van a redirigir. Para más información y para configurar la redirección de contenido bidireccional, consulte las instrucciones de configuración.
Para establecer la URL comodín, en Web Studio modifique la cadena JSON como un valor en la clave `url` de la matriz `hostToClientUrls` o la matriz `clientToHostUrls`.

> **Nota:**
>
> - Para evitar bucles infinitos, no establezca la misma URL en `hostToClientUrls` y `clientToHostUrls`.
> - No se admiten los dominios de nivel superior. Por ejemplo: https://www.citrix.* o http://www.citrix.co* no se redirigen.

Configuración de redirección bidireccional de contenido

Establezca esta directiva en `Enabled` para comenzar a configurar la función y haga clic en **Administrar URL**. Establezca las siguientes configuraciones:

- **Redirección del VDA al cliente**
- **Redirección del cliente al VDA**

Redirección del VDA al cliente

Para redirigir las URL del VDA al cliente, introduzca una URL por línea. Se permiten comodines.
La redirección de OAuth le permite usar el explorador del dispositivo de punto final del cliente para realizar la autenticación y enviar el token de vuelta al VDA.

Ventajas:

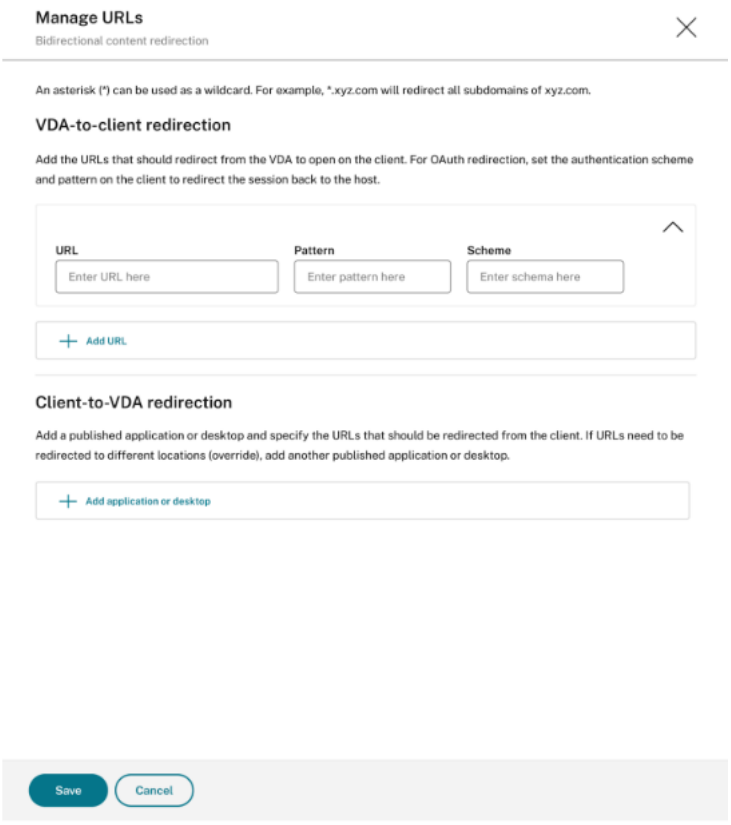
- Puede evitar almacenar estas credenciales en el entorno hospedado.
- Puede usar las funciones biométricas que están disponibles en el dispositivo de punto final y no en el VDA.

Configuraciones:

Para configurar la redirección del VDA al cliente para la URL, especifique lo siguiente:

- **URL** (obligatorio) Agregue la URL que debe redirigirse desde el VDA para que se abra en el cliente. Para la **redirección de OAuth**, defina el esquema y el patrón de autenticación en el cliente para redirigir la sesión de nuevo al host.

- **Patrón**: (Opcional) Expresión regular de URL que, cuando se redirige al cliente mediante la redirección de URL de VDA a cliente, se rastrea como si se hubiera iniciado un flujo de autenticación de OAuth y, cuando el flujo finaliza (lo detecta el esquema resultante o el patrón de URL de redirección que se abre), la URL resultante se redirige de nuevo al VDA host que inició ese flujo.
- **Esquema**: (Opcional) Si se especifica un **esquema**, se espera que la URL de finalización tenga el formato: `<scheme>://<something>`. Considere que el esquema no se ha especificado (vacío). En ese caso, el patrón de URL original resultante se extrae del patrón a través de un grupo de captura mediante una expresión regular (debe especificarse en el patrón) y la URL original se reescribe para usar una URL de redirección que usa `citrix-oauth-redir://`. Cuando se completa el flujo, la URL de redirección original se redirige de nuevo al host (VDA). En este caso, cualquier servidor de autorización OAuth debe configurarse para permitir redireccionar direcciones URL mediante `citrix-oauth-redir://byIndex/1 (2, 3, ... N)`.



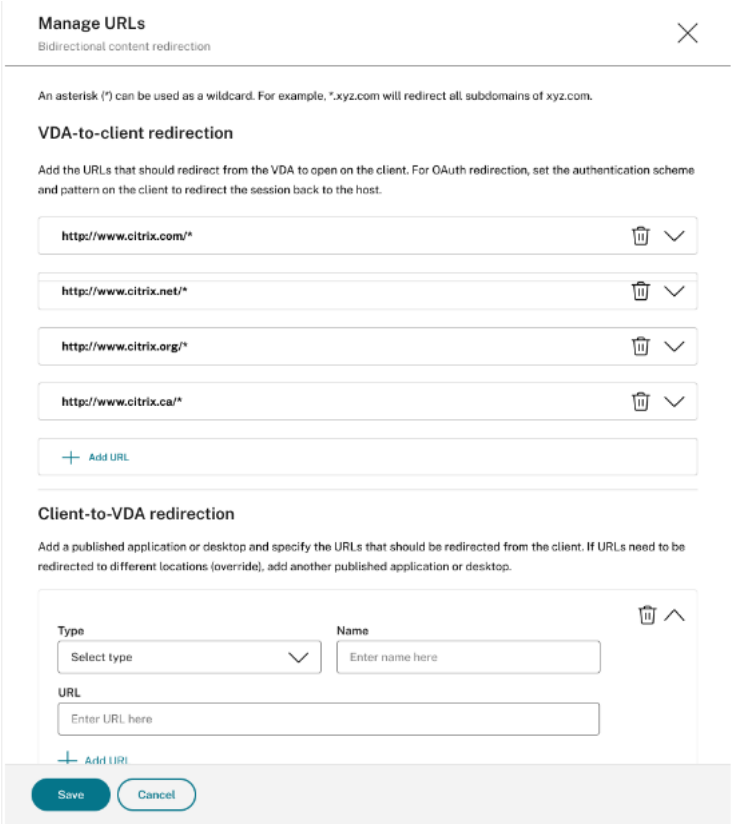
Nota:

Aunque tanto **Patrón** como **Esquema** son opcionales, si se especifica **Patrón**, también debe especificarse **Esquema**.

Redirección del cliente al VDA

Para redirigir las URL del cliente al VDA, siga estos pasos:

1. Configure el destino de las URL del cliente.
2. Seleccione Aplicación publicada o Escritorio publicado.
3. Especifique el nombre de ese recurso.
4. Agregue todas las URL que se deben redirigir a ese recurso.
   Puede supeditar este recurso predeterminado agregando una nueva aplicación o escritorio y, a continuación, especificando las URL que se deben redirigir a ese recurso.



Desktop Studio

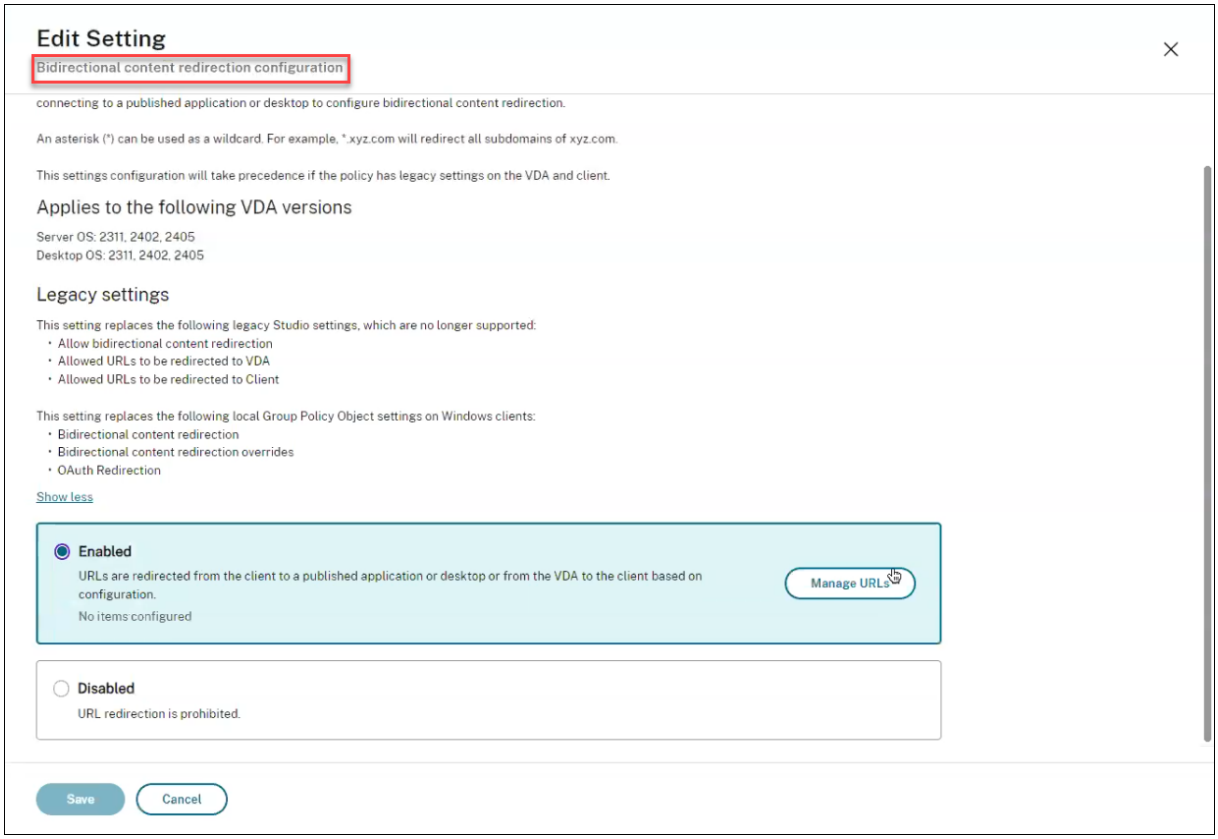
> **Nota:**
>
> Citrix recomienda usar Web Studio para configurar esta función a partir de la versión 2402 de Citrix Virtual Apps and Desktops.

Para configurar la redirección bidireccional de contenido para la versión 2311, cree una cadena JSON con el siguiente formato:

```
1 {
```

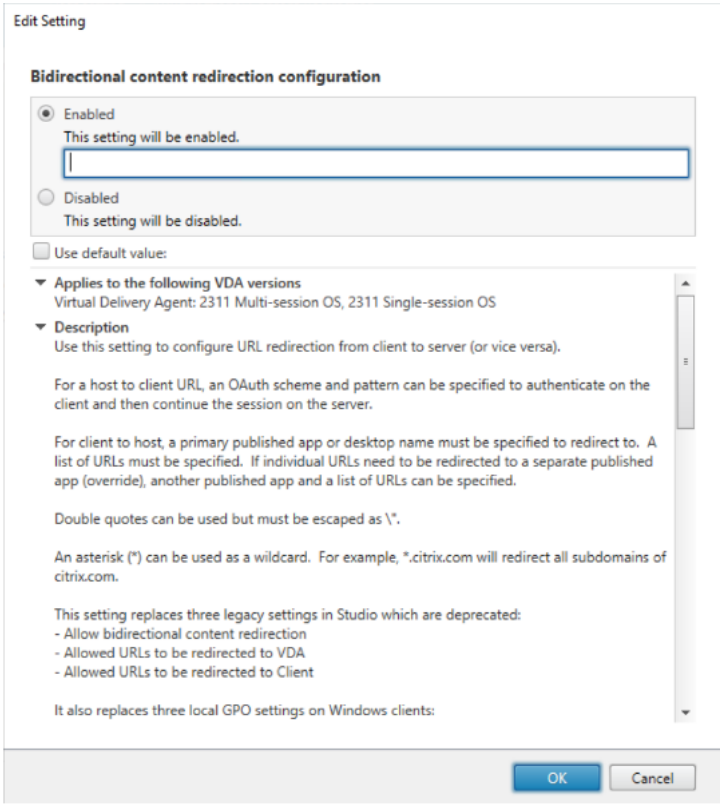


```
 2
 3   "version": 1,
 4   "hostToClientConfig": [
 5     {
 6
 7       "hostToClientUrls": [
 8         {
 9
10           "url": "http://www.citrix.com/*"
11          }
12 ,
13         {
14
15           "url": "www.example.com"
16          }
17 ,
18         {
19
20           "url": "https://login.example.org/*",
21           "oAuthRedirectionPattern": "https://login.example.org/oauth2
                ?.*",
22           "oAuthScheme": "idm.desktop-authentication"
23          }
24
25       ]
26      }
27
28   ],
29   "clientToHostConfig": [
30     {
31
32       "publishedAppOrDesktopNameType": "Desktop",
33       "publishedAppOrDesktopName": "Win11Desktop",
34       "clientToHostUrls": [
35         "https://www.example.net",
36         "https://*.citrix.example"
37       ]
38      }
39 ,
40     {
41
42       "publishedAppOrDesktopNameType": "Application",
43       "publishedAppOrDesktopName": "Chrome",
44       "clientToHostUrls": [
45         "https://tibco.example"
46       ]
47      }
48
49   ]
50 }
```

Se deben establecer los siguientes parámetros:

- **version**: (Obligatorio) Establecida en 1.
- Para la redirección de URL de VDA a cliente, cree una única `hostToClientConfig`.
- **hostToClientUrls**: (Obligatorio) Lista de URL que se redirigirán del host (VDA) al cliente. Se permiten comodines. Si se especifica '*', `clientToHostConfig` debe especificarse con `publishedAppOrDesktopNameType`, un `publishedAppOrDesktopName` vacío y un `clientToHostUrls` vacío.



Redirección de OAuth

La redirección de OAuth le permite usar el explorador del dispositivo de punto final del cliente para realizar la autenticación y enviar el token de vuelta al VDA.

Ventajas:

- Puede evitar almacenar estas credenciales en el entorno hospedado.
- Puede usar las funciones biométricas que están disponibles en el dispositivo de punto final y no en el VDA.

Para configurar la redirección de OAuth para la URL, especifique los siguientes parámetros:

- **oAuthRedirectionPattern**: (Opcional) Expresión regular de URL que, cuando se redirige al cliente mediante la redirección de URL de VDA a cliente, se rastrea como si se hubiera iniciado un flujo de autenticación de OAuth y, cuando el flujo finaliza (lo detecta el esquema resultante o el patrón de URL de redirección que se abre), la URL resultante se redirige de nuevo al VDA host que inició ese flujo.
- **oAuthScheme**: (Opcional) Si se especifica un esquema, se espera que la URL de finalización tenga el formato: `<scheme>://<something>`. Considere que el esquema no se ha especificado (vacío). En ese caso, el patrón de URL original resultante se extrae del patrón a través de un grupo de captura mediante una expresión regular (debe especificarse en el patrón) y la

URL original se reescribe para usar una URL de redirección que usa `citrix-oauth-redir://`. Cuando se completa el flujo, la URL de redirección original se redirige de nuevo al host (VDA). En este caso, cualquier servidor de autorización OAuth debe configurarse para permitir redireccionar direcciones URL mediante `citrix-oauth-redir://byIndex/1 (2, 3, ... N)`.

Para una redirección de cliente a VDA, cree una **clientToHostConfig** para cada recurso que quiera redirigir.
Para cada recurso, incluya los siguientes parámetros:

- **publishedAppOrDesktopNameType**: (Obligatorio) Un escritorio publicado (“Escritorio”) o una aplicación publicada (“Aplicación”) configurados en Web Studio. Si el recurso no es válido, la redirección no funciona correctamente.
- **publishedAppOrDesktopName**: (Obligatorio) Nombre del recurso tal y como está configurado en Web Studio.
- **clientToHostUrls**: (Obligatorio) Lista de URL que se redirigirán del cliente al host (VDA). Se permiten comodines.

Limitación conocida

Al iniciar un explorador mediante PowerShell con un esquema de URL personalizado (no HTTP ni HTTPS), las URL personalizadas no se redirigen al cliente.

Configuración de directiva Redirección de contenido de explorador web

August 17, 2024

La sección “Redirección de contenido de explorador web”incluye 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. No se necesitan directivas de redirección de vídeos HTML5 para que esta característica funcione. Sin embargo, el servicio Citrix HDX HTML5 Video Redirection Service se utiliza para la redirección de contenido del explorador web. Para obtener más información, consulte Redirección de contenido de explorador web.

> **Nota:**
>
> Las configuraciones de directivas disponibles en Web Studio se puede supeditar con claves del Registro en el VDA, pero las claves del 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 sockets de Secure Web 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 del explorador web

De forma predeterminada, la aplicación Citrix Workspace intenta obtener y generar el contenido en el cliente. Se intenta la generación en el lado del servidor cuando la obtención y generación en el cliente fallan. 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 de redirección de contenido del explorador compatible con autenticación de Windows integrada

La redirección de contenido del explorador habilita la superposición que utiliza el esquema Negotiate para la autenticación. Esta mejora proporciona inicio de sesión único (SSO) en un servidor web configurado con Autenticación de Windows integrada (IWA) incluido en el mismo dominio que el VDA.

Cuando se establece en **Permitido**, la superposición de redirección de contenido del explorador obtiene un tíquet Negotiate con las credenciales del VDA del usuario. A continuación, el usuario se autentica en el servidor web con Single Sign-On.

Cuando se establece en **Prohibido**, la superposición de redirección de contenido del explorador web no solicita un tíquet Negotiate del VDA. El usuario se autentica en un servidor web por medio de un

método de autenticación básico. Este método de autenticación requiere que los usuarios introduzcan sus credenciales del VDA cada vez que acceden al servidor web.

De forma predeterminada, este parámetro es Prohibido.

Configuración Autenticación de proxies web de la obtención del servidor de redirección de contenido del explorador

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 incluye 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. Además, se 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, este parámetro es Prohibido.

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 las URL en lista de permitidas 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. Sin embargo, a partir de Citrix Virtual Apps and Desktops 7 2206, el carácter comodín * se permite en la parte de la dirección del subdominio de la URL.

Permitido: `http://www.xyz.com/index.html`, `https://www.xyz.com/*`, `http://www.xyz.com/*videos*`, `http://*.xyz.com/`

No permitido: `http://*.*.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/*`

Para obtener más información, consulte el artículo CTX238236 de Knowledge Center.

> **Nota:**
>
> Puede configurar la lista de control de acceso para permitir que la redirección de contenido del explorador redirija los sitios web al dispositivo de punto final, y los sitios de autenticación se pueden configurar para permitir a los proveedores de identidades (IdP), como Okta y Duo, usar la autenticación de la URL configurada.

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 permitidas 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: un sitio web `www.xyz.com` debe redirigirse al dispositivo de punto final, pero un IdP de terceros, como Okta (`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` en la lista de permitidos. A continuación, utiliza los sitios de autenticación de Redirección de contenido de explorador web para incluir `www.xyz.okta.com` en la lista de permitidos.

Para obtener más información, consulte el artículo CTX238236 de Knowledge Center.

Configuración de lista de bloqueados 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. Tenga en cuenta 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 bloqueados. En este caso, la

configuración de la lista de bloqueados 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 bloqueados 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 se incluye index.html en la lista de bloqueados.

Configuraciones de directiva de redirección de contenido de explorador web

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, este parámetro es Prohibido.

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:

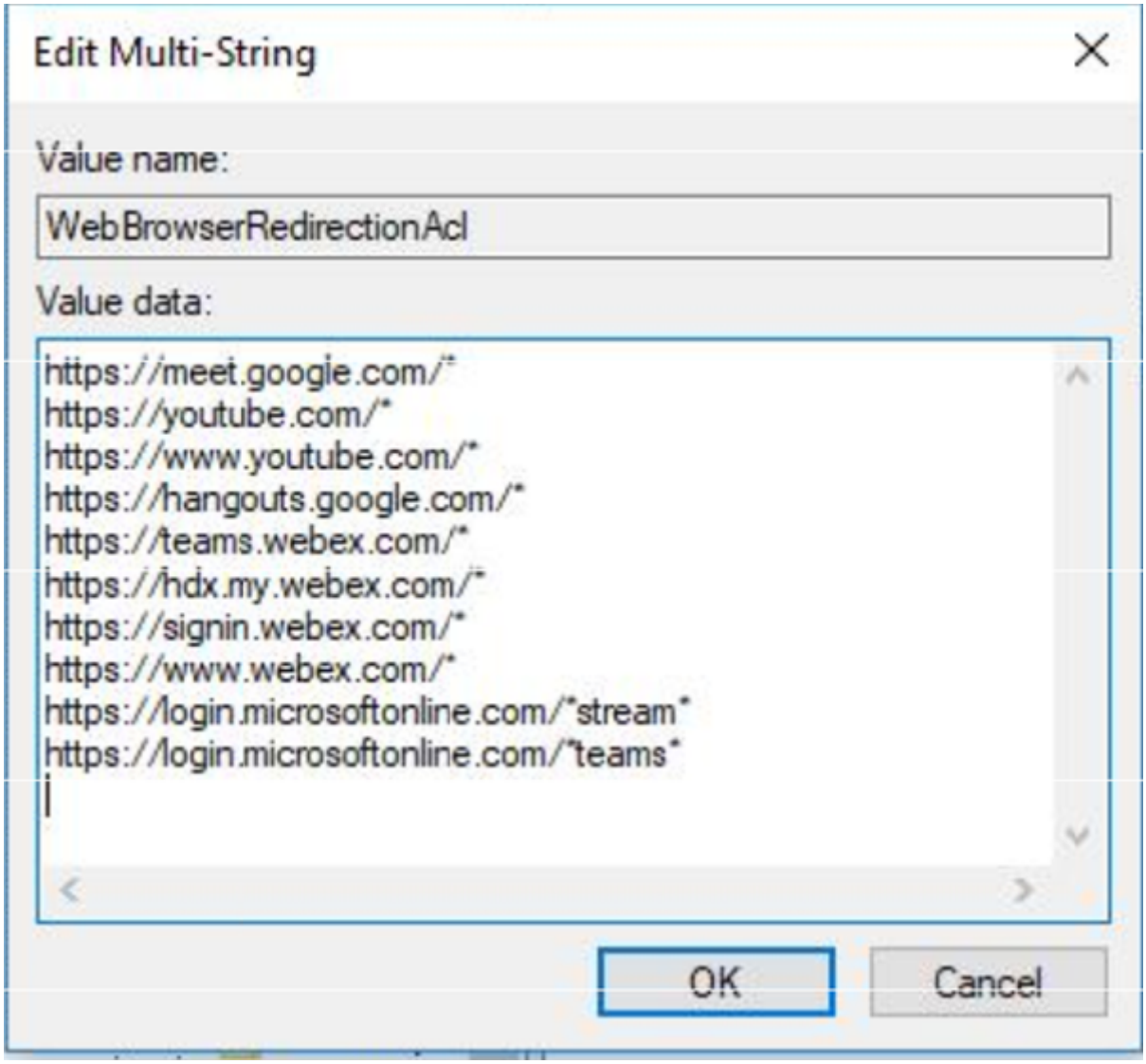
Escriba la palabra **DIRECT** en el cuadro de texto de directiva.

Anulaciones de claves de Registro para la redirección de contenido del explorador web

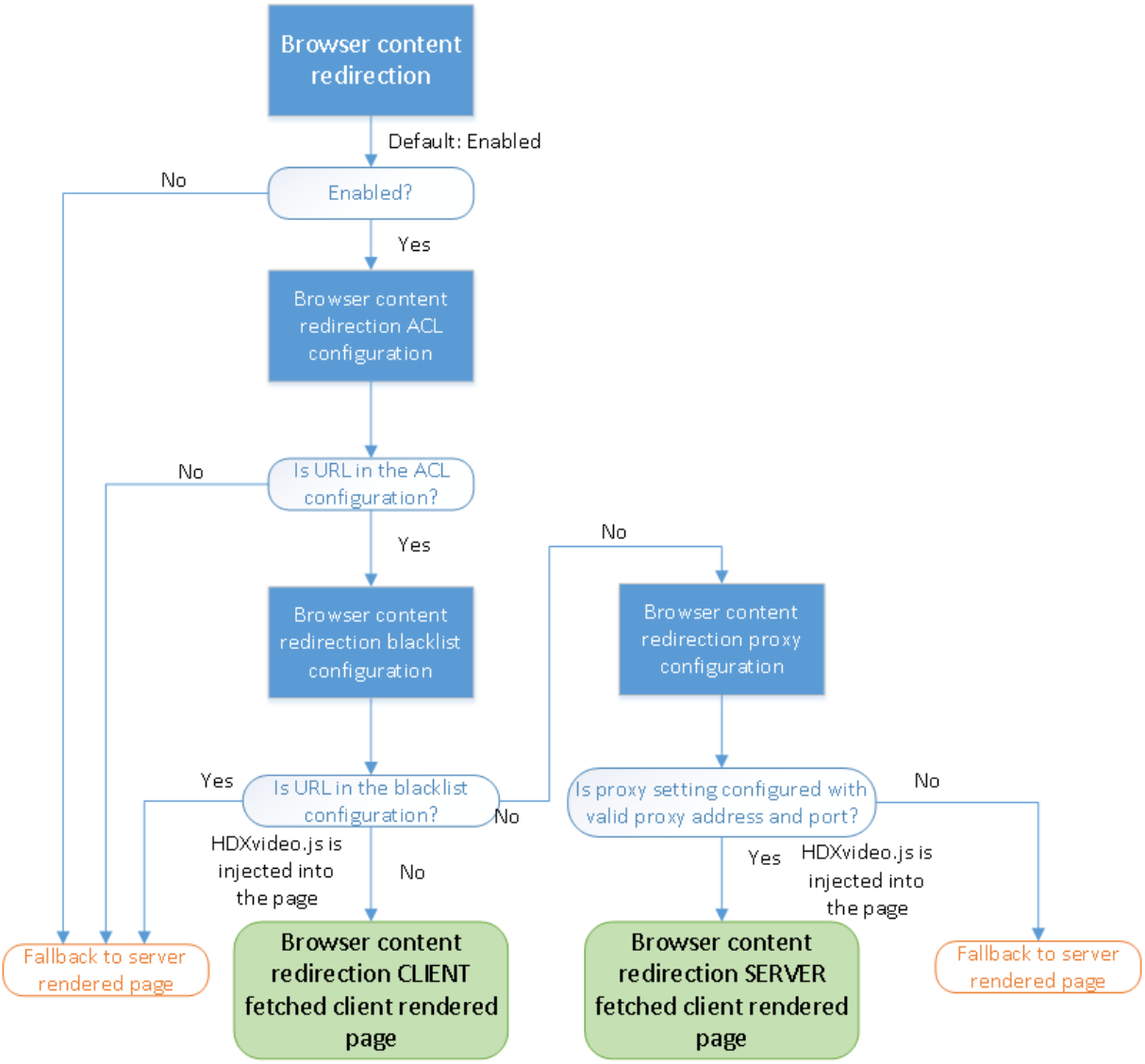
> **Advertencia:**
>
> Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Use el Editor del Registro bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.
>
> Opciones de anulación de los Registros para configuraciones de directiva:

`\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediastream`

Nombre	Tipo	Valor
WebBrowserRedirection	DWORD	1 = Permitido, 0 = Prohibido
WebBrowserRedirectionAcl	REG_MULTI_SZ	
WebBrowserRedirectionAuthenticationSites	REG_MULTI_SZ	
WebBrowserRedirectionProxyAddress	REG_SZ	`http://myproxy.citrix.com:8080` o `http://10.10.10.10:8888`
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 en blanco. 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

August 17, 2024

La sección **Sensores del cliente** incluye 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 peguntan 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 esta manera, se garantiza que los datos obtenidos sean apropi-

ados para los fines de la aplicación. Además, se adapta a 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

August 17, 2024

La sección **Interfaz de usuario de escritorio** incluye configuraciones que controlan los efectos visuales, como el fondo de pantalla de escritorio, las animaciones de menús y las imágenes de arrastrar. Estas configuraciones de directiva ayudan a 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
> - XenDesktop 7.15 LTSR
> - Versiones anteriores de VDA con Windows 7 y Windows 2008 R2.

Redirección de composición del escritorio

Esta configuración especifica si, para la generación de gráficos locales de DirectX a fin de proporcionar a los usuarios una experiencia de escritorio de Windows más fluida, se debe usar la capacidad de procesamiento de:

- La unidad de procesamiento de gráficos (GPU) del dispositivo del usuario
- O bien,
- El procesador de gráficos integrado (IGP) del dispositivo del usuario

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. Tenga en cuenta si configura el escritorio para descartar los cambios cuando finalice la sesión. En este caso, un usuario que haya habilitado las animaciones de menú podría no verlas en sesiones subsiguientes. Si los usuarios requieren animaciones de

> menú, habilite la configuración de Microsoft en la imagen principal del escritorio o asegúrese de 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

August 17, 2024

La sección **Supervisión de usuario final** incluye 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 manera predeterminada, cada iniciación de medición de tiempos de retorno de ICA se demora. Esta demora dura hasta que se detecta algún tráfico que indica 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 manera predeterminada, cada iniciación de medición de tiempos de retorno de ICA se demora. Esta demora dura hasta que se detecta algún tráfico que indica 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

August 17, 2024

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.

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. Considere un usuario con un perfil con el tema Windows 7 que inicia sesión en un escritorio virtual que ejecuta Windows Server 2012. Además, esta directiva no está configurada ni inhabilitada. En este caso, el usuario ve un mensaje de error que indica que no pudo aplicar el tema.

En ambos casos, el problema se resuelve restableciendo el perfil de usuario.

Si inhabilita la directiva en un escritorio virtual con sesiones de usuario activas, la interfaz de esas sesiones no es coherente en los escritorios de Windows 7 y Windows clásico. Para evitar este problema, debe reiniciar el escritorio virtual después de cambiar esta configuración de directiva. A continuación, elimine los perfiles móviles del escritorio virtual. Citrix también recomienda eliminar otros perfiles de usuario del escritorio virtual a fin de evitar inconsistencias entre perfiles.

Considere que está utilizando perfiles de usuario móviles en su entorno. En este caso, 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 los sistemas operativos de cliente y servidor difieren. 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

August 17, 2024

La sección **Redirección de archivos** incluye 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. Cuando está inhabilitada, se impide cualquier redirección de archivos. Esta configuración se aplica, independientemente del estado de las configuraciones individuales de redirección de archivos. Las config-

uraciones individuales de redirección de archivos incluyen 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. Esta configuración es aplicable 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 accedan a, o guarden archivos en, lo siguiente:

- CD-ROM en el dispositivo del usuario
- DVD-ROM en el dispositivo del usuario
- Unidades BD-ROM en el dispositivo del usuario.

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. Esta configuración es aplicable, 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, verifique 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. Esta configuración es aplicable, 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:

- HTTP
- 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 hagan lo siguiente:

- Crear archivos en unidades de cliente asignadas
- Cambiar archivos en unidades de cliente asignadas

- Cambiar carpetas en 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.

Las configuraciones de directiva que impiden que los usuarios accedan a sus discos duros locales o guarden archivos en ellos también impiden que funcione la redirección de carpetas especiales. El motivo es que la redirección de carpetas especiales debe interactuar con el dispositivo del usuario.

Al agregar esta configuración a una directiva, compruebe que la configuración **Unidades fijas del cliente** esté presente y establecida en Permitida.

Directivas de transferencia de archivos

De forma predeterminada, la transferencia de archivos está habilitada. Use Web Studio para cambiar estas directivas, ubicadas en **Configuración de usuario - ICA\Redirección de archivos**. Tenga en cuenta lo siguiente al usar directivas de transferencia de archivos:

- **Transferencia de archivos con la aplicación Citrix Workspace para Chrome OS/HTML5**: Permite o impide que los usuarios transfieran archivos entre una sesión de Citrix Virtual Apps and Desktops y sus dispositivos.

- **Cargar archivo con la aplicación Citrix Workspace para Chrome OS/HTML5**: Permite o impide que los usuarios carguen archivos en una sesión de Citrix Virtual Apps and Desktops desde sus dispositivos.
- **Descargar archivo con la aplicación Citrix Workspace para Chrome OS/HTML5**: Permite o impide que los usuarios descarguen archivos en sus dispositivos desde una sesión de Citrix Virtual Apps and Desktops.

> **Nota:**
>
> Las directivas de transferencia de archivos solo se aplican a la aplicación Citrix Workspace para HTML5 y a la aplicación Citrix Workspace para Chrome OS.

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. Se recomienda, además, 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, verifique 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

August 17, 2024

La sección **Gráficos** incluye 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. Este parámetro 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. Esta herramienta permite al usuario ver información sobre el modo de gráficos activo. La información incluye detalles sobre el códec de vídeo, la codificación de hardware, la calidad de imagen y los monitores en uso durante la sesión. Con el indicador del estado de los gráficos, el usuario también puede habilitar o inhabilitar el modo "Píxel perfecto".

Las versiones de Citrix Virtual Apps and Desktops 2103 y posteriores incluyen un control deslizante para la calidad de imagen que ayuda al usuario a encontrar el equilibrio correcto entre calidad de imagen e interactividad.

Las versiones de Citrix Virtual Apps and Desktops 2109 y posteriores incluyen funcionalidad para configurar un diseño de pantalla virtual a través de una interfaz de usuario que se inicia mediante el indicador del estado de gráficos.

El indicador del estado de gráficos sustituye a la herramienta "indicador de calidad sin pérdida"de versiones anteriores. Esta directiva habilita el indicador de calidad sin pérdida para Citrix Virtual Apps and Desktops versiones 7.16 a 1809.

Uso compartido de pantalla

Esta configuración permite a los usuarios compartir sus sesiones, incluidos el contenido de la pantalla, el teclado y el mouse, con los demás usuarios.

De forma predeterminada, este parámetro está inhabilitado.

El VDA intenta utilizar puertos del rango de puertos TCP para intercambiar datos, empezando por el puerto más bajo y aumentando en cada conexión posterior. El puerto gestiona tanto el tráfico de entrada como el de salida.

De forma predeterminada, el rango de puertos TCP se establece en 52525-52625.

El puerto utilizado para compartir la pantalla debe agregarse a la lista de excepciones de firewall. Esta opción se muestra en forma de casilla de verificación al instalar el VDA. De forma predeterminada, esta opción no está marcada.

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 65,536 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 65,536 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: con una profundidad de color de 32, una resolución vertical de 600 y una resolución horizontal de 800. En este caso, la memoria máxima necesaria es (32/8) x (600) x (800) = 1920000 bytes, lo que equivale a un límite de memoria de presentación de 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.

Cuando se alcanza el límite de memoria para la presentación, esta configuración permite especificar que la profundidad de color o la resolución sean las primeras funciones en degradarse.

De forma predeterminada, se degrada primero la profundidad de color.

Cuando se alcanza el límite de memoria de la sesión, puede reducir la calidad de las imágenes mostradas. Puede reducir esta calidad eligiendo si primero se degrada 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.
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 imágenes en secciones y la recuperación de estas secciones cuando sea necesario hace lo siguiente:

- Desplazamiento más suave en el dispositivo del usuario
- Reduce la cantidad de datos transmitidos a través de la red en el dispositivo del usuario
- Reducción del 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 conexión 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 siguientes sistemas:

- Windows 7
- VDA con Windows Server 2008 R2.

El modo de gráficos antiguo no se admite en los siguientes sistemas:

- Windows 8.x y 10
- 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 es aplicable a VDA que tienen un controlador que no sea Thinwire como controlador de pantalla principal. Estos VDA utilizan un controlador Windows Display Driver Model (WDDM) como 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 Windows multisesión que utilicen un controlador WDDM (como Windows Server 2019), 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 "Códec 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 define 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

August 17, 2024

Esta sección incluye 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 está habilitada la configuración de directiva **Modo de gráficos antiguo**.

Esta configuración almacena los mapas de bits en la memoria caché del disco duro del usuario y, por lo tanto, permite la reutilización de imágenes grandes, utilizadas con frecuencia, de sesiones anteriores.

De manera predeterminada, el valor umbral es de 3000000 bits por segundo.

Este valor representa el umbral por debajo del cual tiene 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

August 17, 2024

> **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** incluye 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 visualización utiliza UDP para 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 que el VDA utiliza para intercambiar datos del canal de presentación Framehawk con el dispositivo de usuario. Los números de puerto tienen el formato *número de puerto más bajo o número de puerto más alto*. 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

August 17, 2024

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.

Mensajes de 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

August 17, 2024

La sección **Acceso a aplicaciones locales** incluye configuraciones de directiva para gestionar las aplicaciones instaladas localmente de los usuarios con aplicaciones alojadas. Estas configuraciones de directiva gestionan la integración 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. Estas configuraciones de directiva gestionan la integración 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 y el estado de la batería de la zona de notificaciones del lado del cliente no aparece en las sesiones de escritorio.

De forma predeterminada, **Permitir 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 estos sitios web:

- Sitios web que requieren información regional, como msn.com o newsgoogle.com
- Sitios web que incluyen 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

August 17, 2024

La sección **Experiencia móvil** incluye 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. Esta configuración permite o prohíbe una interfaz táctil e intuitiva, optimizada para dispositivos de 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

August 17, 2024

La sección **Multimedia** incluye 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. Use el Editor del Registro 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:

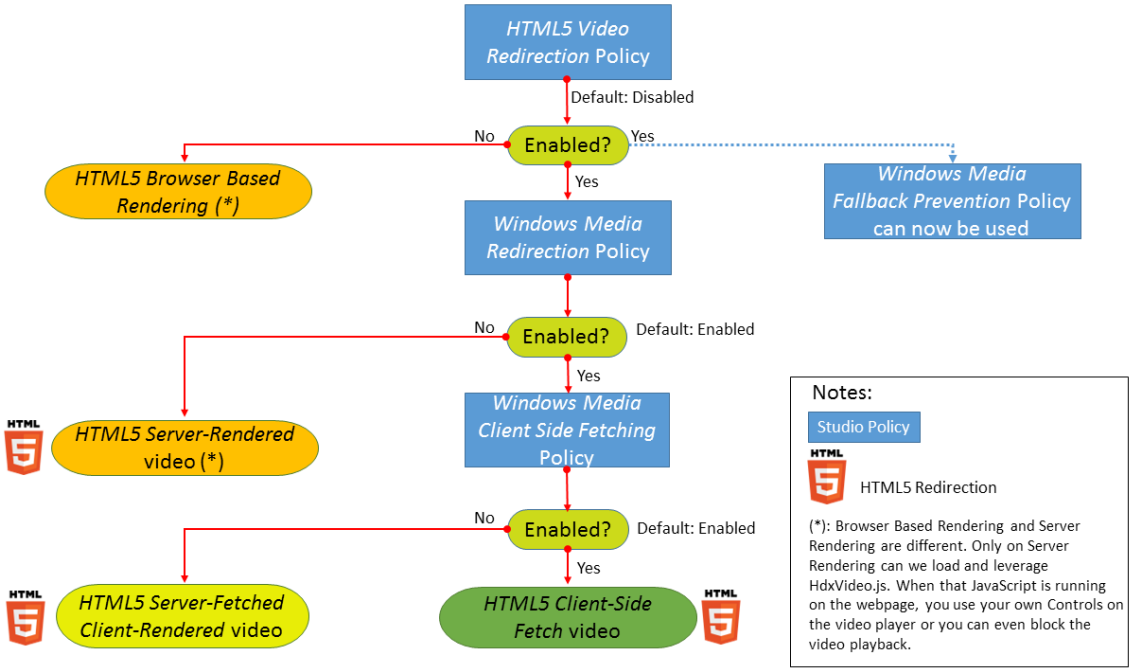
HKEY_LOCAL_MACHINE\Software\Policies\Citrix{User Session ID}\User\MultimediaPolicies

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.

Tenga en cuenta que el JavaScript no se agrega a las páginas web controladas y que el usuario reproduce un vídeo HTML5. En este caso, Citrix Virtual Apps and Desktops recurre de forma predeterminada 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 necesaria para "Obtención del lado del cliente". Obtención del lado del cliente requiere, a su vez, que se permita la *Obtención de contenido de Windows Media en el lado del cliente*.

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.

TLS, la redirección de vídeo HTML5 y la redirección de contenido del explorador web

Puede usar la redirección de vídeo HTML5 para:

- Redirigir vídeos de sitios web HTTPS
- O bien,

- 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. El servicio Citrix HDX HTML5 Video Redirection Service del almacén de certificados del VDA genera dos certificados personalizados para:

- Procesar la redirección de vídeo
- Mantener la integridad TLS de la página web

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.

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:**
>
> Tenga en cuenta si utiliza agentes VDA con la versión 1906.2, o una posterior, con versiones de Controller anteriores, que no tienen la directiva disponible en Web Studio. Un ejemplo de una versión anterior de Controller es 7.15. En este caso, la optimización de HDX está habilitada de forma predeterminada en el VDA. Si la versión de la aplicación Workspace es 1907 o posterior, Microsoft Teams se inicia en modo optimizado. Para obtener información acerca de las advertencias al mezclar controladores LTSR 7.15 y VDA CR, consulte el artículo CTX205549 de Knowledge Center.
>
> En este caso, para inhabilitar la función en usuarios específicos, puede anular el parámetro del Registro. Para anular el parámetro del Registro, utilice 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, verifique que el parámetro **Redirección de Windows Media** esté presente y establecido en **Permitida** (valor predeterminado).

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. La configuración habilita lo siguiente:

- Transcodificación de multimedia en tiempo real
- Permite la entrega de audio y vídeo por streaming a dispositivos móviles en redes de bajo rendimiento
- Mejora la experiencia del usuario al perfeccionar la forma de entregar el contenido de Windows Media a través de una 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. Además, 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, asegúrese de que las siguientes configuraciones estén presentes y configuradas como Permitidas:

- **Redirección de Windows Media**
- **Optimización de la redirección de medios de Windows Media sobre WAN**

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.

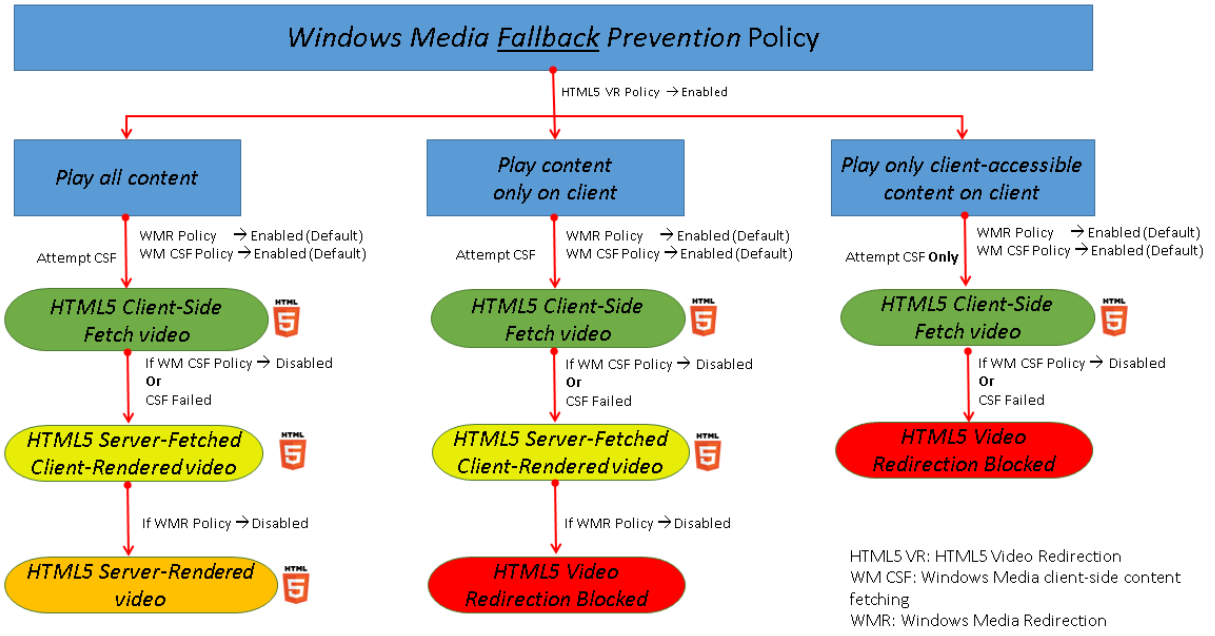
De manera predeterminada, esta configuración no está definida. Cuando la configuración está establecida en No configurada, el comportamiento es el mismo que **Reproducir todo el contenido**.

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 siguiente mensaje de error en la ventana del reproductor (durante un período predeterminado de 5 segundos):

```
"Company has blocked video because of lack of resources"
```



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 bien,

\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**. Permitir esta configuración mejora el uso de la red y la escalabilidad del servidor Esta mejora se logra al transferir el procesamiento de los recursos multimedia 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 solamente 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, la calidad de audio y vídeo que se genera desde el servidor aumenta 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 Founda-

tion. 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 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 multisecuencia

August 17, 2024

La sección **Conexiones de multisecuencia** incluye configuraciones de directiva para gestionar las prioridades de Calidad de servicio (QoS) cuando hay varias conexiones ICA en una sesión.

> **Nota:**
>
> La detección de MTU no está disponible si la directiva Conexiones de multisecuencia está habil-

> itada.

Audio sobre UDP

Esta configuración permite o impide el audio sobre UDP en el servidor.

De forma predeterminada, el audio 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 audio en tiempo real sobre UDP.

Intervalo de puertos UDP de audio

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. Esta especificación sirve de ayuda 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 multisecuencia**.

Configuración de equipo para multisecuencia

Esta configuración habilita o inhabilita la multisecuencia en el servidor.

De forma predeterminada, la multisecuencia está inhabilitada. Defina la directiva Configuración de equipo para multisecuencia si utiliza Citrix SD-WAN o enrutadores de terceros para lograr la calidad de servicio pertinente.

Si la multisecuencia está habilitada, la detección de MTU, una función de Adaptive Transport, no está disponible.

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 multisecuencia

Esta configuración habilita o inhabilita la multisecuencia en el dispositivo del usuario.

De forma predeterminada, la multisecuencia está inhabilitada para todos los usuarios. Defina la directiva Configuración de usuario para multisecuencia 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 multisecuencia**.

> **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 multisecuencia

Este parámetro especifica la secuencia ICA a la que se asignan los canales virtuales cuando se utiliza la multisecuencia.

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 multisecuencia del equipo.

De forma predeterminada, los canales virtuales y sus asignaciones de secuencia son:

- AppFlow: 2
- 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 (**Nota:** Permite arrastrar y colocar archivos entre una sesión de Citrix y un dispositivo de punto final local).
- Plug-in 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

August 17, 2024

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 los utilizan aplicaciones antiguas que envían trabajos de impresión a los puertos LPT. Las aplicaciones antiguas que envían trabajos de impresión a los objetos de impresión del dispositivo del usuario no utilizan estos puertos. 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

August 17, 2024

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 puede instalar el controlador original de una impresora y, en su lugar, se instala 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. Inicie sesión en Web Studio, seleccione **Directivas** en el panel de la izquierda y, a continuación, haga clic en la ficha **Directivas**.
2. Habilite la directiva **Impresoras de sesión**.
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 una impresora de sesión necesita un controlador de impresora nativo, y el controlador de impresora nativo no está instalado en el VDA, es posible que la impresora de la sesión no se cree en la sesión.

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 de Citrix Virtual Apps y el servidor de impresión. Si hace falta, realice una prueba con RDP.

Esperar a que se creen las impresoras

Utilice la directiva del Delivery Controller para habilitar la función en los Citrix Virtual Desktops.

Esperar a que se creen las impresoras (escritorio de servidor):

Este parámetro permite una demora al conectarse a una sesión para que las impresoras redirigidas al cliente se puedan crear automáticamente.

De forma predeterminada, no hay demora en la conexión.

Esperar a que se creen las impresoras (Citrix Virtual Apps):

La ejecución de este cmdlet de PowerShell permite retrasar la conexión con aplicaciones virtuales que se ejecutan en hosts multisesión, de modo que las impresoras redirigidas al cliente se pueden crear automáticamente antes de que se abra la aplicación.

```
Set-BrokerApplication -Name <VirtualAppName> -WaitForPrinterCreation
$true
```

De forma predeterminada, no hay demora en la conexión.

Configuraciones de directiva de Impresoras del cliente

August 17, 2024

La sección **Impresoras del cliente** incluye 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. Esta opción 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 para las sesiones. Estas sesiones incluyen solamente 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.

Configuraciones de directiva relacionadas:

- Uso de controladores de impresión universal
- Preferencia de controlador universal

Crear automáticamente la impresora universal de PDF

Esta configuración habilita o inhabilita la creación automática de Citrix PDF Printer para las sesiones con:

- Aplicación Citrix Workspace para Windows (a partir de VDA 7.19)
- Aplicación Citrix Workspace para HTML5
- 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 antiguas** para utilizar nombres de impresoras cliente antiguas y conservar la compatibilidad con versiones anteriores con los nombres de impresoras antiguas tal y como están presentes en las versiones de XenDesktop del producto. Puede utilizar esta opción con las versiones actuales de Citrix Virtual Apps and Desktops del producto. Un ejemplo de nombre de impresora antiguo es: "Cliente/nombre_cliente#/HPLaserJet 4". Esta opción es menos segura.

Al usar la impresora Citrix PDF Printer en una sesión iniciada desde la aplicación Citrix Workspace para HTML5, establezca la configuración **Nombres de impresora del cliente** como predeterminada o seleccione **Nombres de impresoras estándar**. Si selecciona **Nombres de impresoras antiguos**, la aplicación Citrix Workspace para HTML5 no ofrece la opción Citrix PDF Printer.

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 impresoras del cliente. Aquí, las impresoras del cliente están 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 redirigen 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. Además, 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. Estas reglas permiten a las aplicaciones del servidor acceder a las impresoras cliente que tienen los mismos controladores que el servidor pero distintos nombres de controladores.

Puede realizar lo siguiente:

- Agregar una asignación de controlador
- Modificar una asignación existente
- Supeditar los parámetros personalizados de una asignación
- Quitar una asignación
- Cambiar el orden de las entradas de los controladores 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 quiere reemplazar.

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.
- 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. Esta opción 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 en PDF y lo transfiere 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

August 17, 2024

La sección **Controladores** incluye 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 controladores de impresora desde lo siguiente:

- Conjunto de controladores integrados de Windows
- Paquetes de controladores preparados en el 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 opción de la siguiente tabla:

Opción	Descripción
Usar solo los controladores específicos de la impresora	Indica que la impresora cliente usa solamente los controladores estándar específicos del 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	Utiliza 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

August 17, 2024

La sección **Universal Print Server** incluye 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 se utilizan en 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 [SCHANNEL].

Valor predeterminado: ALL

Esta configuración puede tener los valores: ALL, COM o GOV.

Los conjuntos de cifrado correspondientes a cada valor son los siguientes:

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 Universal Print Client utiliza SSL/TLS para lo siguiente:

- Conexiones de flujo de datos de impresión (CGP)
- Conexiones de 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 ejecuta 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 directiva habilita o inhabilita el uso de Citrix Universal Print Server (UPS). Aplique esta configuración de directiva a las unidades organizativas (OU) que incluyen los escritorios o servidores virtuales que alojan las aplicaciones. Esta configuración de directiva incluye opciones alternativas para permitir las conexiones a los servidores de impresión mediante el servicio de impresión remota nativo de Windows en caso de que el componente UPS de Citrix no esté instalado o no esté disponible en el servidor de impresión solicitado. Los cambios en esta directiva solo se aplicarán después de reiniciar el VDA.

De forma predeterminada, Universal Print Server está inhabilitado.

Al agregar esta configuración a una directiva, seleccione una de las siguientes opciones:

- **Habilitado, con la alternativa de la impresión remota nativa de Windows**: Universal Print Server presta servicio a las conexiones de impresora de red, si es posible. 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 la alternativa de la impresión remota nativa de Windows**: Universal Print Server presta servicio exclusivamente a las conexiones de impresora 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 los datos de impresión. La velocidad de transferencia se calcula para los datos de impresión que se entregan 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 conecta 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 en el servidor, ese servidor se quita del esquema de equilibrio de carga. Además, las conexiones de impresora de ese servidor se redistribuyen entre 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 incluye nombres de servidor duplicados y que todos los servidores tienen un conjunto idéntico de impresoras compartidas instaladas. Es posible que esta operación tarde un poco.

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.

Tiempo de espera de conexión al servicio web de Universal Print Server (HTTP/SOAP)

Esta configuración especifica la cantidad de segundos que Universal Print Client debe esperar hasta que se agote el tiempo de espera de la operación connect() del servicio web de Universal Print Server. Esta configuración puede tener los siguientes valores. Todos estos valores son numéricos y las unidades (de tiempo) son segundos.

- El valor mínimo es 0.
- El valor máximo es 60.
- El valor predeterminado es 10.

Cuando el tiempo de espera oscila entre 1 y 60 (ambos incluidos), Universal Print Client espera el tiempo especificado para que se complete la operación. La operación es una operación de conexión al socket TCP. Los sockets son un recurso del sistema operativo Windows que permite la comunicación entre procesos a través de redes TCP/IP.

Cuando el tiempo de espera es 0, Universal Print Client utiliza el tiempo de espera predeterminado definido por el sistema operativo. Esta configuración era la disponible en las versiones anteriores de Universal Print Client antes de este cambio.

Universal Print Client es el componente de Virtual Delivery Agent (VDA) que comunica con Universal Print Server.

> **Nota:**
>
> Esta configuración de directiva es aplicable a la versión 7.35 y posteriores del VDA.

Tiempo de espera de recepción del servicio web de Universal Print Server (HTTP/SOAP)

Esta configuración especifica la cantidad de segundos que Universal Print Client debe esperar hasta que se agote el tiempo de espera de la operación recv() del servicio web de Universal Print Server. Este parámetro tiene los siguientes valores y todos estos valores son numéricos y las unidades (de tiempo) son segundos.

- El valor mínimo es 0.
- El valor máximo es 60.
- El valor predeterminado es 10.

Cuando el tiempo de espera oscila entre 1 y 60 (ambos incluidos), Universal Print Client espera el tiempo especificado para que se complete la operación. La operación es una operación de recepción de socket TCP. Los sockets son un recurso del sistema operativo Windows que permite la comunicación entre procesos a través de redes TCP/IP.

Cuando el tiempo de espera es 0, Universal Print Client utiliza el tiempo de espera predeterminado definido por el sistema operativo. Esta configuración era la disponible en las versiones anteriores de Universal Print Client antes de este cambio.

Universal Print Client es el componente de Virtual Delivery Agent (VDA) que comunica con Universal Print Server.

> **Nota:**
>
> Esta configuración de directiva es aplicable a la versión 7.35 y posteriores del VDA.

Tiempo de espera de envío del servicio web de Universal Print Server (HTTP/SOAP)

Esta configuración especifica la cantidad de segundos que Universal Print Client debe esperar hasta que se agote el tiempo de espera de la operación send() del servicio web de Universal Print Server. Esta configuración puede tener los siguientes valores. Todos estos valores son numéricos y las unidades (de tiempo) son segundos.

- El valor mínimo es 0.
- El valor máximo es 60.
- El valor predeterminado es 10.

Cuando el tiempo de espera oscila entre 1 y 60 (ambos incluidos), Universal Print Client espera el tiempo especificado para que se complete la operación. La operación es una operación de envío de socket TCP. Los sockets son un recurso del sistema operativo Windows que permite la comunicación entre procesos a través de redes TCP/IP.

Cuando el tiempo de espera es 0, Universal Print Client utiliza el tiempo de espera predeterminado definido por el sistema operativo. Esta configuración era la disponible en las versiones anteriores de Universal Print Client antes de este cambio.

Universal Print Client es el componente del VDA que comunica con Universal Print Server.

> **Nota:**
>
> Esta configuración de directiva es aplicable a la versión 7.35 y posteriores del VDA.

Configuraciones de directiva de Impresión universal

August 17, 2024

La sección **Impresión universal** incluye 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

Este parámetro especifica lo siguiente:

- Máxima calidad disponible para las imágenes impresas con el controlador de impresora universal de Citrix
- Nivel mínimo de compresión disponible 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:

- Tenga en cuenta que el nivel de compresión del parámetro **Límite de compresión de imagen para la impresión universal** es inferior al nivel definido en el parámetro **Valores predeterminados de optimización de impresión universal**. En este caso, las imágenes se comprimen según el nivel definido en el parámetro Límites 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 se almacenan o no en caché las imágenes y fuentes que aparecen varias veces en el flujo de impresión. Esta configuración garantiza que cada imagen o fuente única se envíe a la impresora solo una vez. De forma predeterminada, las fuentes e imágenes incrustadas se almacenan en caché. 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:

- Tenga en cuenta que el nivel de compresión del parámetro **Límite de compresión de imagen para la impresión universal** es inferior al nivel definido en el parámetro **Valores predeterminados de optimización de impresión universal**. En este caso, las imágenes se comprimen según el nivel definido en el parámetro Límites 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 en resolución media (600 ppp), los usuarios pueden imprimir únicamente con una calidad máxima de 600 ppp. Además, el parámetro **Calidad de impresión** de la ficha **Avanzado** del cuadro de diálogo **Impresora universal** muestra los parámetros de resolución solamente hasta la calidad media (600 ppp), incluida también.

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

August 17, 2024

La sección **Seguridad** incluye 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. Pongamos como ejemplo que quiere establecer un nivel de cifrado de mayor prioridad en un servidor o en un dispositivo de usuario. En este caso, la configuración que especifique para los recursos publicados se puede supeditar.

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 esta configuración 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. Estos parámetros se almacenan en el Registro de Windows cuando se instala 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 del usuario y para la transferencia de datos. Además, se utilizan claves de sesión independientes para el tráfico hacia y desde 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

August 17, 2024

La sección **Límites de servidor** incluye la configuración de directiva para controlar las conexiones inactivas.

Intervalo de temporizador de servidor inactivo

Esta configuración determina cuánto tiempo se mantendrá una sesión de usuario ininterrumpida si este no realiza entradas. Los datos se calculan en milisegundos.

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/CTX118618.

Configuraciones de directiva de Límites de sesión

August 17, 2024

La sección **Límites de sesión** incluye configuraciones de directiva para controlar el tiempo que las sesiones pueden permanecer conectadas antes de un cierre forzoso.

Temporizador de sesiones desconectadas

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 esto minutero está habilitado, la sesión desconectada se cierra cuando el minutero expira.

De forma predeterminada, las sesiones desconectadas no se cierran.

Temporizador de sesión desconectada de acceso con Remote PC

Este parámetro habilita o inhabilita un temporizador que cierra una sesión de usuario desconectada una vez agotado el plazo establecido. Si habilita este parámetro, utilice el parámetro **Intervalo de temporizador de sesiones desconectadas** para especificar cuántos minutos permanece bloqueado un escritorio desconectado antes de que se cierre la sesión de usuario.

De forma predeterminada, esta configuración está inhabilitada.

Intervalo de temporizador de sesiones desconectadas

Esta configuración especifica cuánto tiempo, en minutos, permanece 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 sesiones desconectadas: Multisesión

Esta configuración habilita o inhabilita un temporizador que determina cuánto tiempo puede mantenerse una sesión de RDS desconectada antes de que se cierre la sesión. De forma predeterminada, este temporizador está inhabilitado y las sesiones desconectadas no se cierran.

Intervalo del temporizador de sesiones desconectadas: Multisesión

Esta configuración determina cuántos minutos puede mantenerse desconectada una sesión de RDS antes de que se cierre. 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 conexiones de sesión: Multisesión

Esta configuración habilita o inhabilita un temporizador para especificar la duración máxima de una conexión sin interrupciones entre un dispositivo del usuario y un servidor de terminales. De manera predeterminada, este temporizador está inhabilitado.

Intervalo del temporizador de conexiones de sesión: Multisesión

Esta configuración especifica el número máximo de minutos de una conexión sin interrupciones entre un dispositivo del usuario y una sesión de RDS. De forma predeterminada, la duración máxima es 1440 minutos (24 horas).

Temporizador de sesión inactiva

Cuando un usuario no realiza ninguna acción, esta configuración se usa para habilitar o inhabilitar:

- Un temporizador que especifica cuánto tiempo se puede mantener ininterrumpida una conexión entre un dispositivo de usuario y un escritorio.

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

Cuando el usuario no realiza ninguna acción, esta configuración se usa para especificar:

- Los minutos durante los que se mantiene una conexión ininterrumpida entre un dispositivo de usuario y un escritorio.

De forma predeterminada, las conexiones inactivas se mantienen durante 1440 minutos (24 horas).

Temporizador de inactividad de sesiones: Multisesión

Esta configuración habilita o inhabilita un temporizador para determinar la duración máxima de una conexión inactiva entre un dispositivo de usuario y un servidor de terminales. De manera predeterminada, este temporizador está inhabilitado.

Intervalo del temporizador de inactividad de sesiones: Multisesión

Esta configuración especifica la cantidad de minutos de una conexión inactiva entre un dispositivo de usuario y una sesión de RDS. De forma predeterminada, la duración máxima es 1440 minutos (24 horas).

> **Nota:**
>
> Se espera que los valores de temporizador de las máquinas multisesión configuradas mediante directivas de Citrix anulen los valores de temporizador configurados mediante directivas de grupo de Microsoft. Para evitar comportamientos imprevistos, le recomendamos que configure los valores del temporizador con uno de los dos métodos.

Configuraciones de directiva de Fiabilidad de sesiones

August 17, 2024

La sección **Fiabilidad de la sesión** incluye 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.

Los parámetros de Web Studio se aplican en el cliente para:

- La aplicación Citrix Workspace 1808 y versiones posteriores
- Citrix Receiver para Windows 4.7 y versiones posteriores.

La directiva de Web Studio supedita el objeto de directiva de grupo de Citrix Receiver en los clientes. Las actualizaciones de estas directivas en Web 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, configure la directiva en Web Studio.
> - Citrix Receivers para Windows anteriores a 4.7: Configure las directivas en Web Studio. Configure también la plantilla de objetos de directiva de grupo de Citrix Receiver en el cliente para lograr un comportamiento coherente.

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.

Use la fiabilidad de la sesión para mantener la sesión activa en el servidor. Para indicar que se ha perdido la conectividad, la pantalla del usuario se oscurece. Es posible que el usuario vea una sesión bloqueada durante la interrupción del servicio. El usuario puede reanudar la interacción con la aplicación al restaurarse la conexión de la 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 trascurrido 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.

> **Nota:**
>
> Cuando Citrix ADC se está usando, debe seleccionar **Habilitar fiabilidad de la sesión** en Citrix StoreFront > **Administrar dispositivos Citrix Gateway** / **Secure Ticket Authority** en conexiones ICA de proxy.

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.

Tiempo de espera de fiabilidad de la sesión

Este parámetro especifica la duración en segundos. Esta duración es el tiempo que el proxy de la fiabilidad de la sesión espera a que un usuario se conecte de nuevo antes de permitir que la sesión se desconecte.

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).

Configuraciones de directiva de Marca de agua de la sesión

August 17, 2024

La sección **Marca de agua de la sesión** incluye configuraciones de directiva 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, la dirección IP del VDA está inhabilitada.

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, Estilo de la marca de agua de la sesión es Múltiple.

Texto personalizado de la marca de agua

Esta configuración le permite aplicar texto personalizado (por ejemplo, el nombre corporativo) para mostrarlo 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. El texto personalizado de la marca de agua está limitado a 25 caracteres Unicode. Si configura una cadena más larga, se truncará a los 25 caracteres.

No hay texto predeterminado.

A partir de Citrix Virtual Apps and Desktops 7 2206, puede agregar más personalizaciones mediante etiquetas personalizadas en el texto. Como resultado, el máximo de caracteres del texto personalizado aumenta a 1024.

Las etiquetas disponibles para los parámetros de la marca de agua se describen en esta tabla:

Etiqueta	Descripción	Ejemplo
`<font=value>`	Le permite cambiar la fuente del texto de la marca de agua. El valor es el nombre de una fuente disponible en el VDA.	`<font=Courier New>`
`<fontzoom=value>`	Le permite establecer el porcentaje del factor de zoom de la fuente. El valor es 200 para un zoom del 200 % en el texto de la marca de agua.	`<fontzoom=200>`
`<position=value>`	Le permite cambiar la posición del texto de la marca de agua. Los valores son `center`, `topleft`, `topright`, `bottomleft` y `bottomright`. Esta etiqueta solo es aplicable con un solo estilo.	`<position=topright>`
`<rotation=value>`	Le permite girar el texto de la marca de agua. El valor se especifica en grados y el intervalo va de -360 a 360.	`<rotation=45>`
`<style=value>`	Le permite cambiar el estilo de visualización. Esta etiqueta supedita la directiva de estilo de marca de agua de sesión.	`<style=single>`

Están disponibles estos estilos de marca de agua:

- Estilo “single”(único): Aparece una etiqueta de texto de marca de agua única en el centro de la sesión. Puede usar la etiqueta de posición para cambiar la ubicación.
- Estilo “xstyle”(equis) o múltiple: Aparecen 5 etiquetas de marca de agua en la sesión, una en el centro y otra en cada esquina.
- Estilo “tile”(en mosaicos): Aparecen varias etiquetas en la sesión. El texto de la marca de agua se coloca por igual en toda la pantalla.

Las etiquetas disponibles para cambiar el texto de la marca de agua se describen en esta tabla:

Etiqueta	Descripción
<clientip>	La dirección IP del dispositivo de punto final.
<date>	La fecha en que se estableció la sesión.
<domain>	El nombre de dominio de la cuenta del usuario que inició sesión.
<hostname>	El nombre de la máquina del VDA.
<newline>	Crea una línea adicional.
<serverip>	La dirección IP del VDA.
<time>	La hora en que se estableció la sesión.
<username>	El nombre del usuario.

Nota:

- La directiva **Texto personalizado de la marca de agua** solo se aplica cuando la directiva **Habilitar marca de agua de la sesión** está habilitada. De forma predeterminada, está *inhabilitada*.
- Si utiliza las etiquetas para cambiar el texto de la marca de agua, se ignoran todas las demás directivas de marcas de agua de la sesión, excepto **Habilitar marca de agua de la sesión**. Si usa las etiquetas para los parámetros del texto de la marca de agua, puede usar todas las demás directivas de marcas de agua.

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

August 17, 2024

La sección **Control de zona horaria** incluye parámetros de directiva relacionados con la hora local usada para las sesiones.

Calcular hora local para clientes antiguos

Esta configuración habilita o inhabilita la estimación de la zona horaria local de los dispositivos de usuario. Estos dispositivos incluyen los dispositivos de usuario que envían información de zona horaria inexacta 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. Pongamos como ejemplo que quiere usar esta configuración con Citrix Receivers que envían información detallada de la zona horaria al servidor. Por ejemplo: las versiones compatibles de Citrix Receiver para Windows. En este caso, esta configuración no surte efecto.

Restaurar la zona horaria del SO de escritorio al desconectar o al cerrar la sesión

Pongamos como ejemplo que el usuario desconecta una sesión o la cierra. En este caso, esta configuración determina si la configuración de zona horaria de un VDA con SO de sesión única se restaura en la zona horaria original de la máquina. 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 utiliza VDA de sesión única (anteriormente conocidos como VDA de estación de trabajo) en máquinas que ejecutan un SO de servidor, configure el derecho de usuario local **Cambiar zona horaria** a **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 se puede aplicar cuando el servidor es un host de sesión de Escritorio remoto en el VDA con SO multisesión (instalado con el comando `/ServerVDI`). En un SO multisesión, de forma predeterminada y por diseño, los usuarios no tienen el derecho local de cambiar la zona horaria.

Configuraciones de directiva de Dispositivos TWAIN

August 17, 2024

La sección **Dispositivos TWAIN** incluye configuraciones de directivas relacionadas con lo siguiente:

- Asignación de dispositivos cliente TWAIN, como cámaras digitales o escáneres
- Optimización de las transferencias 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

Los dispositivos TWAIN se comunican con aplicaciones de procesamiento de imágenes alojadas en el servidor mediante el protocolo TWAIN.

Esta configuración permite o impide que los usuarios accedan a dispositivos TWAIN del dispositivo del usuario. 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

August 17, 2024

La sección **Dispositivos USB** incluye 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=**03**. Los modos admitidos son: Sin optimización: Valor **01**. Modo interactivo: Valor **02**. Recomendado para dispositivos como tabletas con lápiz y punteros 3D Pro. Modo de captura: Valor **04**. Apropiados 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

Nombre de la etiqueta	Descripción
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 se habilita la compatibilidad con USB. Además, la configuración de preferencias de usuario de USB está definida para conectar automáticamente dispositivos USB.

> **Nota:**
>
> En Receiver para Windows 4.2, los dispositivos USB también se redirigen automáticamente cuando se trabaja en modo Desktop Appliance. Además, la barra de conexión no está presente. En versiones anteriores de Citrix Receiver para Windows, los dispositivos USB también se redirigían automáticamente al trabajar de la siguiente manera:
>
> - Modo Desktop Appliance
> - 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 aparezcan en la lista o se redirijan, utilice DeviceRules en el dispositivo de punto final del cliente o en la directiva de DDC. Consulte las Guías de administración para obtener más detalles.

> **Precaución:**
>
> El uso incorrecto del Editor del Registro del sistema puede causar problemas graves que pueden obligarle 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.

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:

- Al iniciar una sesión, conectar los dispositivos automáticamente
- Cuando se conecta un nuevo dispositivo mientras se ejecuta una sesión, conectar el dispositivo automáticamente.

3. Haga clic en **Aceptar**.

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. Además, 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 operar completamente.

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 la compatibilidad con 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 audio 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 audio simples. Sin embargo, es posible que deba redirigir algunos dispositivos especializados mediante la compatibilidad

con USB. Los datos heurísticos se utilizan para determinar qué dispositivos son dispositivos de audio simples.

Utilice este Registro en el dispositivo de punto final del cliente para establecer si los dispositivos de audio 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 audio 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 lo siguiente:

- Clientes que no son de Windows (por ejemplo, clientes de Linux)
- Clientes en los que el usuario ha restringido (bloqueado) el acceso de los usuarios a las funciones locales del 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. Gracias a una nueva mejora de funciones introducida en Citrix Virtual Apps and Desktops 7 1808, está disponible la redirección de USB genérico de dispositivos de memoria USB con cifrado de hardware en sesiones de VDA con 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. Pongamos como ejemplo un dispositivo que no cumple con las normas o que no se utiliza con la intención original. En este caso, es posible que la redirección de USB genérico sea la única forma de utilizar 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 no siempre coinciden con lo que usted quiere. Ejemplos de dispositivos optimizables de Citrix son impresoras, dispositivos de audio, vídeo o almacenamiento, e imágenes fijas. 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.

Permitir que los dispositivos USB existentes se conecten automáticamente

Esta configuración permite o impide la conexión automática a la sesión remota de los dispositivos USB existentes que están conectados al dispositivo de punto final al comienzo de una sesión.

Al agregar esta configuración a una directiva, seleccione una de las siguientes opciones:

- Preguntar antes de redirigir los dispositivos USB disponibles.
- No redirigir automáticamente los dispositivos USB disponibles.
- Redirigir automáticamente los dispositivos USB disponibles.

De forma predeterminada, está seleccionada la opción **Preguntar antes de redirigir los dispositivos USB disponibles**. Según la directiva seleccionada, se puede anular la opción seleccionada en la sección **Preferencias** > **Dispositivos** del cliente.

> **Nota:**
>
> Actualmente, la directiva **Permitir que los dispositivos USB existentes se conecten automáti-**

> **camente** solo funciona con la aplicación Citrix Workspace para Windows.

Permitir que los dispositivos USB recién llegados se conecten automáticamente

Esta configuración permite o impide la conexión automática a la sesión remota de los dispositivos USB que se insertan en el dispositivo de punto final durante una sesión.

Al agregar esta configuración a una directiva, seleccione una de las siguientes opciones:

- Preguntar antes de redirigir los dispositivos USB disponibles.
- No redirigir automáticamente los dispositivos USB disponibles.
- Redirigir automáticamente los dispositivos USB disponibles.

De forma predeterminada, está seleccionada la opción **Preguntar antes de redirigir los dispositivos USB disponibles**. Según la directiva seleccionada, se puede anular la opción seleccionada en la sección **Preferencias** > **Dispositivos** del cliente.

> **Nota:**
>
> Actualmente, la directiva **Permitir que los dispositivos USB recién llegados se conecten automáticamente** solo funciona con la aplicación Citrix Workspace para Windows.

Reglas de redirección de dispositivos USB del cliente (versión 2)

Esta opción especifica las reglas para filtrar, dividir y conectar automáticamente los dispositivos USB a una sesión remota.

Cuando se selecciona esta opción, el host sustituye las *Reglas de redirección de dispositivos USB del cliente* por las reglas sobre dispositivos configuradas en esta opción.

Para obtener más información, consulte Configurar la redirección de dispositivos USB compuestos.

Configuraciones de la directiva Lista de canales virtuales permitidos

August 20, 2024

La configuración de directiva **Lista de canales virtuales permitidos** permite el uso de una lista que especifica los canales virtuales que pueden abrirse en una sesión ICA.

Al inhabilitarse, se permiten todos los canales virtuales.

Al habilitarse, solo se permiten los canales virtuales de Citrix.

Para utilizar canales virtuales personalizados o de terceros, agregue los canales virtuales a la lista. Para agregar un canal virtual a la lista:

1. Introduzca el nombre del canal virtual seguido de una coma.
2. Introduzca la ruta al proceso que accede al canal virtual.

Se pueden enumerar más rutas ejecutables, y dichas rutas se separan por comas.

Por ejemplo,

```
CTXCVC1,C:\VC1\vchost.exe
```

```
CTXCVC2,C:\VC2\vchost.exe,C:\Program Files\Third Party\vcaccess.exe
```

A partir de Citrix Virtual Apps and Desktops 7 2109, las listas de canales virtuales permitidos están habilitadas de forma predeterminada. Para obtener más información sobre cómo agregar canales virtuales a la lista de permitidos, consulte Agregar canales virtuales a la lista de permitidos.

Si usa HDX RealTime Optimization Pack para Skype Empresarial, agregue el canal virtual a la lista de permitidos. Para obtener más información, consulte la documentación de HDX RealTime Optimization Pack.

> **Importante:**
>
> Las máquinas VDA deben reiniciarse para que la configuración surta efecto.

Para obtener más información sobre los canales virtuales, consulte Canales virtuales ICA.

Registro de la lista de canales virtuales permitidos

Puede usar esta configuración de directiva para configurar el nivel de registro de la lista de permitidos de canales virtuales.

Están disponibles las siguientes opciones:

Opciones	Descripción
Inhabilitado	Inhabilita todos los eventos de registro.
Solo advertencias de registro	Los eventos se registran solo para los canales virtuales personalizados que intentan abrirse y que no forman parte de la lista de permitidos.
Registrar todos los eventos	Se registran todos los eventos

Limitación de registros de la lista de permitidos de canales virtuales

Puede usar esta configuración de directiva para configurar la frecuencia de registro de los eventos de una sesión activa.

Todos los eventos de cada canal virtual se registrarán la primera vez que aparezcan. Los eventos repetidos se suprimirán mientras dure el período de limitación mientras la sesión esté activa. Si se desconecta una sesión, se restablece el período de limitación.

Configuraciones de directiva de Presentación visual

August 17, 2024

La sección **Presentación visual** incluye configuraciones de directiva para controlar la calidad de las imágenes que se envían desde 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. La reducción a 8 o 16 bits por píxel mejora potencialmente la capacidad de respuesta en conexiones con poco ancho de banda. Sin embargo, es posible que esta acción degrade ligeramente la calidad de la 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

August 17, 2024

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 está habilitada la configuración de directiva Modo de gráficos antiguo.

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 está habilitada la configuración de directiva Modo de gráficos antiguo.

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 está habilitada la configuración de directiva Modo de gráficos antiguo.

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.

> **Nota:**
>
> La directiva de Velocidad de fotogramas mínima objetivo ha quedado obsoleta y se ha establecido en 10 fps. Los usuarios finales pueden cambiarlo mediante el control deslizante Calidad del indicador de estado gráfico.

Configuraciones de directiva de Imágenes fijas

August 17, 2024

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 está habilitada la configuración de directiva Modo de gráficos antiguo.

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 está habilitada la configuración de directiva Modo de gráficos antiguo.

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 está habilitada la configuración de directiva Modo de gráficos antiguo.

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 está habilitada la configuración de directiva Modo de gráficos antiguo.

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

August 17, 2024

La sección **WebSockets** incluye 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. La función lo hace 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 WebSockets.

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 directiva de Dispositivos WIA

August 17, 2024

La sección **Dispositivos WIA** incluye configuraciones de directiva para administrar la redirección del escáner mediante Adquisición de imágenes de Windows (WIA).

Redirección WIA

Los dispositivos WIA, como cámaras y escáneres digitales, se comunican con aplicaciones de procesamiento de imágenes alojadas en el servidor a través del marco WIA. Esta configuración permite o

prohíbe que los usuarios accedan a dispositivos WIA del dispositivo del usuario. De forma predeterminada, la redirección WIA está prohibida.

Para obtener información acerca de los dispositivos compatibles con WIA, consulte Dispositivos WIA.

Funciones HDX administradas a través del Registro

August 17, 2024

> **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 usa el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Para abrir el Editor del Registro, ejecute `regedit.exe` en el servidor. A continuación, vaya a la clave de Registro para agregar o modificar la configuración.

Dispositivos

Teclados Bloomberg

Citrix Virtual Apps and Desktops admite el teclado Starboard modelo 4 de Bloomberg y el modelo 3 anterior. De forma predeterminada, el teclado mejorado de Bloomberg está inhabilitado.

Para habilitar la compatibilidad con el teclado Bloomberg, establezca el siguiente valor del Registro en la máquina cliente antes de iniciar una conexión:

- **Clave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB`
- **Nombre del valor**: `EnableBloombergHID`
- **Tipo de valor**: `DWORD`
- **Información del valor**:
  - `0`: Inhabilitar
  - `1`: Habilitar

Para obtener más información, consulte Teclados Bloomberg.

Unidades de cliente asignadas

Como medida de precaución, cuando un usuario inicia sesión en Citrix Virtual Apps and Desktops, de forma predeterminada, el servidor asigna unidades de cliente sin permiso de ejecución del usuario. Para permitir que los usuarios ejecuten archivos ejecutables que hubiera en las unidades de cliente asignadas, modifique el Registro del servidor para cambiar este valor predeterminado.

Para permitir el acceso, modifique la siguiente clave de Registro (cree **CDMSettings** si no existe):

- **Clave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\CDMSettings`
- **Nombre del valor**: `ExecuteFromMappedDrive`
- **Tipo de valor**: `DWORD`
- **Información del valor**:
  - `1` - Autorizar permiso
  - `0` - Denegar permiso en unidades asignadas

El cambio surte efecto para las sesiones que se conecten después de la modificación del Registro.

Citrix Virtual Apps and Desktops 7 2006 es la primera versión que contiene esta ubicación del Registro. Las versiones anteriores de Citrix Virtual Apps and Desktops utilizaban otra ubicación del Registro.

Para obtener más información, consulte Asignación de unidades del cliente.

Lápices para Microsoft Surface Pro y Surface Book

Citrix Virtual Apps and Desktops admite la funcionalidad de lápiz estándar en aplicaciones basadas en Windows Ink. De manera predeterminada, esta función está habilitada.

Para inhabilitar o habilitar esta función, establezca el siguiente valor de Registro:

- **Clave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Citrix Virtual Desktop Agent\PenApi`
- **Nombre del valor**: `DisablePen`
- **Tipo de valor**: `DWORD`
- **Información del valor**:
  - `1`: Inhabilitar
  - `0`: Habilitar

Para obtener más información, consulte Lápices para Microsoft Surface Pro y Surface Book.

Lista de aplicaciones permitidas de Adquisición de imágenes de Windows

Este parámetro le permite controlar qué aplicaciones del VDA pueden acceder a la redirección del escáner de Adquisición de imágenes de Windows (WIA).

De forma predeterminada, ninguna aplicación tiene acceso a Adquisición de imágenes de Windows.

Para ajustar Adquisición de imágenes de Windows para las aplicaciones del VDA, cree el siguiente parámetro de Registro:

- **Clave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`
- **Nombre del valor**: `WIAAllowedProcesses`

  Seleccione y haga clic con el botón secundario en **WIAAllowedProcesses**. Elija **Nuevo > Valor de cadena múltiple** y cambie el nombre del nuevo valor a **AllowProcesses**.
- Información del valor: Introduzca la ruta y nombre del proceso completos para cada aplicación que pueda acceder a Adquisición de imágenes de Windows. Proporcione cada aplicación en una nueva línea.

Los cambios en este parámetro surtirán efecto la próxima vez que se inicie una sesión en el VDA.

General

HDX Reducer

Puede configurar la versión del algoritmo de compresión de HDX (Reducer) que quiere usar en el host de la sesión.

Para habilitar Reducer V4 en un VDA de sesión única, establezca el siguiente valor de Registro:

Clave: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy\Defaults\WDSettings`

Nombre del valor: `ReducerOverrideMask`
Tipo de valor: `DWORD`
Información del valor: 23 (Decimal)

Para habilitar Reducer V4 en un VDA multisesión, establezca el siguiente valor de Registro:

- **Clave**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd`
- **Nombre del valor**: `ReducerOverrideMask`
- **Tipo de valor**: `DWORD`
- **Información del valor**: 23 (Decimal)

Configurar el tiempo de espera de EDT

Puede configurar el tiempo de espera de EDT en cualquier valor comprendido entre 5 y 25 segundos en el VDA. El valor de tiempo de espera de EDT predeterminado es de 25 segundos.

- **Clave**: `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd\Tds\udp\UDPStackParameters`
- **Tipo de valor**: `DWORD`
- **Nombre del valor**: `edtConnectionTimeout`
- **Información del valor**: Tiempo en segundos entre 5 y 25 (decimal)

También puede configurar el tiempo de espera de la aplicación Citrix Workspace para Windows:

- **Clave**: `HKLM\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\EDT`
- **Tipo de valor**: `String / REG_SZ`
- **Nombre del valor**: `edtConnectionTimeout`
- **Información del valor**: Tiempo en segundos entre 5 y 25 (decimal)

Configurar la versión de Rendezvous

Para configurar la versión de Rendezvous que se va a usar, defina el siguiente valor de Registro:

- **Clave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent`
- **Tipo de valor**: `DWORD`
- **Nombre del valor**: `GctRegistration`
- **Información del valor**:
  - `1`: Para habilitar V2
  - `0`: Para habilitar V1

Configurar el inicio de sesión automático en el VDA

Este parámetro le permite habilitar o inhabilitar la configuración de directiva de Microsoft **Siempre solicitar contraseña** en los VDA con SO multisesión y SO de sesión única Windows 10.

Si **Siempre solicitar contraseña** está habilitado, los usuarios deben introducir credenciales en el VDA al iniciar una sesión remota. Si este parámetro está inhabilitado, los usuarios se conectan automáticamente a la sesión remota sin proporcionar credenciales en el VDA.

De forma predeterminada, la configuración de directiva de Microsoft está inhabilitada. Para habilitar o inhabilitar el parámetro **Siempre solicitar contraseña**, establezca el siguiente valor de Registro en el VDA:

- **Clave**: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Portica
- **Nombre del valor**: AutoLogon
- **Tipo de valor**: DWORD
- **Información del valor**:
  - 1: Inhabilita la configuración de directiva de Microsoft y permite a los usuarios iniciar sesión automáticamente en una sesión remota.
  - 0: Habilita la configuración de directiva de Microsoft y pide a los usuarios que proporcionen credenciales cuando inician una sesión remota.

Inhabilitar advertencia de tiempo de espera

De forma predeterminada, los usuarios con sesiones inactivas reciben un mensaje de advertencia dos minutos antes de que su sesión se desconecte automáticamente.

Esta configuración inhabilita y quita el mensaje de advertencia para los usuarios que alcanzan el límite de tiempo de espera en sesión por inactividad en estos casos:

- Windows Server 2004
- Sistema operativo multisesión Windows 10 multisesión 2004 o una versión posterior

Para quitar la advertencia, establezca el siguiente valor de Registro en el VDA:

- **Clave**: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Winstations\ICA-CGP
- **Nombre del valor**: fEnableTimeoutWarning
- **Tipo de valor**: DWORD
- **Información del valor**:
  - 1: Inhabilitar el mensaje de advertencia
  - 0: Habilitar el mensaje de advertencia

Para mostrar el mensaje de advertencia, elimine el valor de Registro o establézcalo en 0.

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.

Esta configuración está habilitada de forma predeterminada. Para inhabilitar la detección de MTU en EDT, configure el siguiente valor del Registro y reinicie el VDA.

- **Clave**: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd
- **Nombre del valor**: MtuDiscovery
- **Tipo de valor**: DWORD
- **Información del valor**: 0

Esta configuración es aplicable a nivel de toda la máquina y afecta a todas las sesiones que se conectan desde un cliente compatible.

Habilitar el modo tolerante a pérdidas

Puede acceder al audio adaptable mediante el modo tolerante a pérdidas con el servicio de audio bidireccional para la aplicación Citrix Workspace para Windows, VDA multiusuario y VDA de escritorio. Este parámetro está inhabilitado de forma predeterminada. Para habilitar el modo tolerante a pérdidas, en función de la máquina que utilice, configure este valor del Registro y reinicie la máquina correspondiente.

Para el cliente de la aplicación Citrix Workspace para Windows:

- **Clave**: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio
- **Nombre del valor**: EdtUnreliableAllowed
- **Tipo de valor**: REG_SZ
- **Información del valor**: 1

Para VDA TS:

- **Clave**: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Audio
- **Nombre del valor**: EdtUnreliableAllowed
- **Tipo de valor**: DWORD
- **Información del valor**: 1

Para VDA WS:

- **Clave**: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Audio
- **Nombre del valor**: EdtUnreliableAllowed
- **Tipo de valor**: DWORD
- **Información del valor**: 1

Redirección de contenido general

Agregar tipos de URL para la redirección del host al cliente

De forma predeterminada, se admite la redirección de los siguientes tipos de URL: HTTP, HTTPS, RTSP, RTSPU, PNM y MMS. Puede agregar tipos de URL a la lista creando las siguientes claves de Registro y valores en el cliente Windows.

- **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://;custometype2://`

Puede agregar tipos de URL solo para clientes Windows. Los clientes que faltan en este parámetro de Registro 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 obtener más información, consulte el artículo Redirección del host al cliente.

Redirección de carpetas de 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. Tenga en cuenta que habilita la redirección de carpetas del cliente en el servidor y el usuario la configura en el dispositivo del usuario. En este caso, se redirige la parte del volumen local especificada por el usuario.

Para habilitar la redirección de carpetas del cliente en el servidor, establezca el siguiente valor de Registro:

- **Clave**: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection`
- **Nombre del valor**: `CFROnlyModeAvailable`
- **Tipo de valor**: `DWORD`
- **Información del valor**: `1`

Para obtener más información, consulte Redirección de carpetas del cliente.

Redirección del host al cliente para un conjunto específico de sitios web

Para habilitar la redirección del host al cliente para un conjunto específico de sitios web, configure el siguiente valor de Registro 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.example.com
```

```
*.example.com
```

Para obtener más información, consulte el artículo Redirección del host al cliente.

Comportamiento de la aplicación local al cerrar sesión y al desconectar

De forma predeterminada, 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. Para configurar el comportamiento de la aplicación local al cerrar sesión y desconectar, establezca el siguiente valor de Registro en el escritorio alojado:

- **Clave**: `HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies`
- **Nombre del valor**: `Session State`
- **Tipo de valor**: `DWORD`
- **Información del valor**:
  - 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 un usuario cierra sesión o se desconecta del escritorio virtual.

Para obtener más información, consulte Acceso a aplicaciones locales y redirección de URL.

Quitar tipos de URL de la lista predeterminada para la redirección del host al cliente

Para quitar tipos de URL de la lista de redirección predeterminada, cree las siguientes claves 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 obtener más información, consulte el artículo Redirección del host al cliente.

Configuración predeterminada del explorador del VDA del servidor

Puede habilitar la redirección del host al cliente para reemplazar cualquier configuración predeterminada del explorador del 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.

- Internet Explorer (predeterminado)
  - **Clave**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **Nombre del valor**: `Default`
  - **Tipo de valor**: `REG_SZ`
  - **Información del valor**: `"c:\program files\internet explorer\iexplore.exe""%1"`
  - **Clave**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`

  - **Nombre del valor**: `Default`
  - **Tipo de valor**: `REG_SZ`
  - **Información del valor**: `"c:\program files\internet explorer\iexplore.exe""%1"`

- Google Chrome
  - **Clave**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **Nombre del valor**: `Default`
  - **Tipo de valor**: `REG_SZ`
  - **Información del valor**: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe""%1"`
  - **Clave**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **Nombre del valor**: `Default`
  - **Tipo de valor**: `REG_SZ`
  - **Información del valor**: `"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe""%1"`

- Microsoft Edge
  - **Clave**: `HKEY_CLASSES_ROOT\http\shell\open\command_backup`
  - **Nombre del valor**: `Default`
  - **Tipo de valor**: `REG_SZ`
  - **Información del valor**: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe""%1"`
  - **Clave**: `HKEY_CLASSES_ROOT\https\shell\open\command_backup`
  - **Nombre del valor**: `Default`
  - **Tipo de valor**: `REG_SZ`
  - **Información del valor**: `"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe""%1"`

Acceso a aplicaciones locales para aplicaciones publicadas

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. Para proporcionar acceso a las aplicaciones publicadas, establezca el siguiente valor de Registro en el servidor:

- **Clave**: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\DesktopStudio
- **Nombre del valor**: ClientHostedAppsEnabled
- **Tipo de valor**: DWORD
- **Información del valor**:
  - 1: Habilitar
  - 0: Inhabilitar

Para obtener más información, consulte Acceso a aplicaciones locales y redirección de URL.

Gráficos

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 el siguiente parámetro de Registro:

- **Clave**: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper
- **Nombre del valor**: CUDA
- **Tipo de valor**: DWORD
- **Información del valor**: 00000001

Para usar las funcionalidades POC de aceleración de OpenCL, habilite el siguiente parámetro de Registro:

- **Clave**: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper
- **Nombre del valor**: OpenCL
- **Tipo de valor**: DWORD
- **Información del valor**: 00000001

Para obtener más información, consulte Aceleración de GPU para SO Windows multisesión

Modo progresivo

El modo progresivo está inhabilitado de forma predeterminada. Puede cambiar el estado del modo progresivo con la siguiente clave de Registro:

- **Clave**: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics

- **Tipo de valor**: `REG_DWORD`
- **Nombre del valor**: `ProgressiveDisplay`
- **Información del valor**:
  - `0` - Siempre desactivado (inhabilita el modo progresivo; este valor es el predeterminado.)
  - `1` - Automático (alternar según las condiciones de la red.)
  - 2 = Siempre activado

Para obtener más información, consulte Modo progresivo.

> **Nota:**
>
> El modo progresivo fue retirado. Thinwire es una opción alternativa que optimiza la entrega de imágenes y mantiene la eficiencia de la caché, a la vez que proporciona casi todos los beneficios del modo progresivo.

Representación de Windows Presentation Foundation (WPF)

HDX 3D Pro permite que las aplicaciones con muchos gráficos que se ejecutan en sesiones con SO Windows multisesión se representen en la unidad de procesamiento de gráficos (GPU) del servidor. Al trasladar la representación de los gráficos de Windows Presentation Foundation (WPF) a la unidad de procesamiento de gráficos (GPU) del servidor, la CPU del servidor no se ralentiza.

Para habilitar las aplicaciones WPF para que representen gráficos mediante la GPU del servidor, cree el siguiente parámetro en el Registro del servidor con SO Windows multisesión:

1. Abra el Editor del Registro en el VDA y vaya a la siguiente clave:

   `HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper`

2. Cree o modifique los siguientes valores de Registro:

   - [REG_DWORD] AdapterHandle = 0x00000001
   - [REG_DWORD] DevicePath = 0x00000001
   - [REG_DWORD] Flag = 0x00000412
   - [REG_DWORD] WPF = 0x00000001

3. Cree una subclave con el nombre ejecutable de su aplicación WPF. Por ejemplo: si su aplicación se llama “mywpfapp.exe”, cree la siguiente clave:

   `HKLM\Software\Citrix\CtxHook\AppInit_DLLs\Graphics Helper\mywpfapp.exe`

4. Reinicie el servidor para que la configuración surta efecto.

Para obtener más información, consulte Aceleración de GPU para SO Windows multisesión y el blog sobre cómo aprovechar al máximo las aplicaciones WPF en un sistema operativo multisesión Windows.

Contenido multimedia

Evitar eco durante conferencias multimedia

Citrix Virtual Apps and Desktops ofrece una opción de eliminación de eco que reduce los ecos al mínimo. Esta función está habilitada de manera predeterminada. Para inhabilitar la eliminación de eco, puede cambiar uno de los siguientes parámetros de Registro:

- **Clave**:
  - 32 bits: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio`
  - 64 bits: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio`
- **Nombre del valor**: `EchoCancellation`
- **Tipo de valor**: `String`/`REG_SZ`
- **Información del valor**: `False`

Para obtener más información, consulte Funciones de audio.

Limitación de audio

Después de instalar un dispositivo de audio en el cliente, habilitar la redirección de audio e iniciar una sesión RDS, es posible que los archivos de audio no se reproduzcan. Como solución alternativa, agregue la siguiente clave al Registro en la máquina RDS y reinícielа:

- **Clave**: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SCMConfig`
- **Nombre del valor**: `EnableSvchostMitigationPolicy`
- **Tipo de valor**: `DWORD`
- **Información del valor**: `0`

Para obtener más información, consulte Funciones de audio.

PPP y redirección de contenido del explorador

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 web redirigido se muestra incorrectamente. Para evitar el problema, inhabilite la aceleración de GPU en la redirección de contenido del explorador para Chrome. Para ello, cree el siguiente valor de registro en la máquina del usuario:

- **Clave**: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxMediaStream

- **Nombre del valor**: GPU
- **Tipo de valor**: DWORD
- **Información del valor**: 0

Para obtener más información, consulte PPP y redirección de contenido del explorador.

Resolución de cámara web de alta definición

Si la negociación del tipo de medios falla, HDX recurre a la resolución VGA predeterminada (640 x 480 píxeles). Puede usar claves de Registro en el cliente para configurar la resolución predeterminada. Antes de configurar las siguientes claves del Registro, asegúrese de que la cámara admite la resolución especificada.

- **Clave**: HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime
- Ancho
  - **Nombre del valor**: DefaultWidth
  - **Tipo de valor**: DWORD
  - **Información del valor**: Anchura deseada en decimal (por ejemplo, 1280)
- Altura
  - **Nombre del valor**: DefaultHeight
  - **Tipo de valor**: DWORD
  - **Información del valor**: Altura deseada en decimal (por ejemplo 720)

Modo de reserva de Microsoft Teams

Si Microsoft Teams no se carga en el modo VDI optimizado (“Citrix HDX no está conectado”en Teams/Acerca de/Versión), el VDA recurre a tecnologías HDX heredadas, como la redirección de la cámara web y la redirección de audio y micrófono del cliente. Si está utilizando un SO de plataforma o versión de la aplicación Workspace que no admite la optimización de Microsoft Teams, no se aplicarán las claves de registro de reserva.

Para controlar el mecanismo de reserva, establezca uno de los siguientes valores de Registro en el VDA:

- **Clave** (solo se necesita una):
  - **Configuración de equipo:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Teams

  - **Configuración de usuario:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Teams

- **Nombre del valor**: DisableFallback
- **Tipo de valor**: DWORD
- Información del valor:
  - 1 - Inhabilitar el modo de reserva
  - 2 - Habilitar solo audio

Si el valor no está presente o está establecido en 0, se habilita el modo de reserva. Esta función requiere Microsoft Teams 1.3.0.13565 o una versión posterior. Para obtener más información, consulte Optimización para Microsoft Teams.

Optimización para Microsoft Teams con Citrix App Layering

Si utiliza Citrix App Layering para administrar instalaciones de VDA y Microsoft Teams en diferentes capas, cree una nueva clave de Registro vacía llamada **PortICA** en Windows antes de instalar Microsoft Teams con el indicador ALLUSER=1 desde la línea de comandos. Deje el nombre, el tipo y los datos del valor predeterminado.

- Clave para la versión de 32 bits del Editor del Registro: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\PortICA
- Clave para la versión de 64 bits del Editor del Registro: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA

Para obtener más información, consulte Optimización para Microsoft Teams.

Single Sign-On con autenticación de Windows integrada para redirección de contenido del explorador web

Esta configuración proporciona inicio de sesión único (SSO) en un servidor web configurado con Autenticación de Windows integrada (IWA) incluido en el mismo dominio que el VDA. Para habilitar Single Sign-On, establezca el siguiente valor de Registro en 1:

- **Clave**:
  - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediastream

  O bien,

  - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\HdxMediastream
- **Nombre del valor**: WebBrowserRedirectionIwaSupport

- **Tipo de valor**: DWORD
- **Información del valor**: 1

Para obtener más información, consulte Single Sign-On con autenticación de Windows integrada (IWA).

Encabezado de solicitud user-agent

El encabezado user-agent ayuda a identificar las solicitudes HTTP enviadas desde la redirección de contenido del explorador web. Este parámetro puede ser útil al configurar reglas de proxy y firewall. Por ejemplo: si el servidor bloquea las solicitudes enviadas desde la redirección de contenido del explorador web, puede crear una regla que contenga el encabezado user-agent para omitir ciertos requisitos. Solo los dispositivos con Windows admiten el encabezado de solicitud user-agent.

De forma predeterminada, la cadena del encabezado de solicitud user-agent está inhabilitada. Para habilitar el encabezado user-agent para el contenido generado en el cliente, utilice el Editor del Registro.

En cada cliente con la aplicación Citrix Workspace para Windows, agregue este parámetro de Registro:

- **Clave**:
  - 32 bits: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStream
  - 64 bits: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\HdxMediaStream
- **Nombre del valor**: EnableCefUserAgentString
- **Tipo de valor**: DWORD
- **Información del valor**: 1

Una vez agregado el valor de Registro, el encabezado user-agent contiene el texto CitrixBCR/2102.1, donde 2102.1 es la versión de la aplicación Citrix Workspace para Windows.

Compresión de software de cámara web

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 los siguientes valores en el cliente:

- **Clave**: HKEY_CURRENT_USER\SOFTWARE\Citrix\HdxRealTime
- **Nombre del valor**: DeepCompress_ForceSWEncode

- **Tipo de valor**: DWORD
- **Información del valor**: 1

Para obtener más información, consulte Compresión de vídeo de cámaras web de HDX.

Compresión de vídeo de cámara web

La compresión de vídeo por cámara web HDX envía el vídeo en H.264 directamente a la aplicación de videoconferencias de la sesión virtual. Para optimizar los recursos de los VDA, la compresión de cámaras web de HDX no codifica, transcodifica ni decodifica el vídeo de las cámaras web. Esta función está habilitada de manera predeterminada.

Para inhabilitar el streaming directo de vídeo del servidor a la aplicación de videoconferencias, establezca el siguiente valor de Registro en el VDA.

- **Clave**: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxRealTime
- **Nombre del valor**: OfferH264ToApp
- **Tipo de valor**: DWORD
- **Información del valor**: 0

Para obtener más información, consulte Compresión de vídeo de cámaras web de HDX.

Velocidad de fotogramas en compresión de vídeo por cámara web

Para ajustar la velocidad de fotogramas de vídeo preferida, modifique el siguiente valor de Registro en el cliente:

- **Clave**: HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXRealTime
- **Nombre del valor**: FramesPerSecond
- **Tipo de valor**: DWORD
- **Información del valor**: 15

Si la cámara web no admite la velocidad de fotogramas especificada, la aplicación utiliza 15 FPS de forma predeterminada.

Para obtener más información, consulte Compresión de vídeo de cámaras web de HDX.

Configuraciones de la directiva Administración de carga

August 17, 2024

La sección **Administración de carga** incluye 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\LogonToleranceIsHardLimit
> 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

> **Nota:**
>
> En los casos en que Workspace Environment Management administra máquinas, el uso de esta configuración junto con la configuración Prioridad de CPU puede tener resultados no deseados. Se recomienda que inhabilite esta configuración si decide utilizar la configuración Prioridad 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. Además, define en MB el uso de memoria por debajo del cual se considera que un servidor tiene carga cero.

De forma predeterminada, este valor está establecido en 768 MB.

Configuraciones de directiva de Profile Management

August 17, 2024

Esta sección contiene configuraciones de directivas para habilitar y configurar Profile Management.

Para obtener más información como la siguiente, consulte Directivas de Profile Management:

- Nombres de la configuración del archivo INI equivalente
- ¿Qué versión de Profile Management se necesita para una configuración de directiva?

Configuraciones avanzadas de directiva

August 17, 2024

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 se configura ni 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 adicionales a las que `Index.dat` no hace referencia. Estas cookies adicionales que permanecen en el sistema de archivos después de múltiples consultas pueden sobrecargar los perfiles. Esta directiva le permite habilitar Profile Management para forzar el procesamiento de Index.dat y quitar las cookies adicionales. Esta directiva prolonga 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 se configura ni 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 directiva le permite acelerar la implementación y simplifica la optimización. No necesita configurar esta directiva. Sin embargo, puede inhabilitar la configuración automática al realizar una de estas acciones:

- Actualizar la versión para conservar los parámetros de versiones anteriores

- Solución de problemas

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	*Inhabilitado* si el disco Personal vDisk se está utilizando; de lo contrario, habilitado.
Guardar siempre en caché	Inhabilitado	*Inhabilitado* si el disco Personal vDisk se está utilizando; de lo contrario, habilitado.
Eliminar perfiles guardados en caché local al cerrar la sesión	Habilitado	*Inhabilitado* en estos casos: 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.

	SO multisesión	SO de sesión única
Streaming de perfiles	Habilitado	*Inhabilitado* 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.

> **Importante:**
>
> Personal vDisk se ha retirado. Para obtener información detallada, consulte Quitar discos PvD, AppDisks y hosts no admitidos.

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). Esta mejora se logra mediante la configuración automática de las siguientes directivas:

- Agregar `Appdata\Local\Microsoft\Windows\Caches` y `Appdata\Local\Packages` a **Carpetas para reflejar**.
- Agregar `Appdata\Local\Microsoft\Windows\UsrClass.Dat*` a **Archivos para sincronizar**.

Si este parámetro no se configura aquí, se utiliza el valor del archivo INI.

Si esta configuración no se define ni aquí ni en el archivo INI, se activa la configuración automática. En este caso, es posible que los parámetros de Profile Management cambien si el entorno cambia.

Cerrar la sesión del usuario si hay algún problema

Le permite especificar si Profile Management cierra la sesión de los usuarios si hay problemas.

Si esta directiva no se inhabilita o no se configura, Profile Management proporciona un perfil temporal a los usuarios si hay problemas. Por ejemplo: el almacén de 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 configura aquí, se utiliza el valor del archivo INI.

Si esta configuración 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 la recopilación de datos de uso y estadísticas anónimas.

Si este parámetro no se configura 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. Esta función espacios adicionales en el almacén de usuarios para guardar los índices de búsqueda de Outlook.

Cierre la sesión y vuelva a iniciarla para que esta directiva surta efecto.

Base de datos del índice de búsqueda de Outlook: Copia de seguridad y restauración

Le permite especificar qué hace Profile Management durante el inicio de sesión cuando la directiva Habilitar itinerancia del índice de búsqueda de Outlook está habilitada.

Si esta directiva está habilitada, 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 no se puede montar la base de datos del índice de búsqueda por una corrupción de la base de datos, Profile Management revierte la base de datos del índice de búsqueda a la última copia correcta conocida.

> 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 almacenamiento de VHDX disponible.

Habilitar las sesiones simultáneas para la itinerancia de datos de búsqueda de Outlook

Permite a Profile Management ofrecer una experiencia de búsqueda nativa de Outlook en sesiones simultáneas del mismo usuario. Utilice esta directiva con la directiva de itinerancia del índice de búsqueda de Outlook.

Con esta directiva habilitada, cada sesión simultánea utiliza un archivo OST de Outlook diferente.

De forma predeterminada, solo se pueden usar dos discos VHDX para almacenar archivos OST de Outlook (un archivo por disco). Si el usuario inicia más sesiones, sus archivos OST de Outlook se almacenan en el perfil de usuario local. Puede especificar el número máximo de discos VHDX para almacenar archivos OST de Outlook.

Habilitar contenedor de OneDrive

Permite que las carpetas de OneDrive se desplacen con los usuarios.

El contenedor de OneDrive es una solución de itinerancia de carpetas basada en VHDX. Profile Management crea un archivo VHDX por usuario en un recurso compartido de archivos y almacena las carpetas de OneDrive de los usuarios en los archivos VHDX. Los archivos VHDX se conectan cuando los usuarios inician sesión y se desconectan cuando los usuarios cierran sesión.

Itinerancia de aplicaciones UWP

Le permite habilitar la itinerancia de las aplicaciones UWP (Plataforma universal de Windows) con los usuarios. De esta forma, los usuarios pueden acceder a las mismas aplicaciones UWP desde diferentes dispositivos.

Con esta directiva habilitada, Profile Management permite que las aplicaciones UWP se muevan con los usuarios al almacenarlas en discos VHDX independientes. Estos discos se adjuntan cuando los usuarios inician sesión y se desconectan cuando los usuarios cierran sesión.

Prioridad de la configuración:

Si este parámetro no se configura aquí, se utiliza el valor del archivo INI.
Si esta configuración no se define ni aquí ni en el archivo INI, la función está inhabilitada.

Habilitar el procesamiento asíncrono para la directiva de grupo de usuarios al iniciar sesión

Windows proporciona dos modos de procesamiento para la directiva de grupo de usuarios: sincrónico y asíncrono. Windows usa un valor de Registro para determinar el modo de procesamiento del siguiente inicio de sesión del usuario. Si el valor de Registro no existe, se aplica el modo sincrónico. El valor de registro es un parámetro en el nivel de máquina que no se desplaza con los usuarios. Por lo tanto, el modo asíncrono no se aplicará como se esperaba si los usuarios:

- Inician sesión en máquinas diferentes.
- Inician sesión en una máquina en la que está habilitada la directiva Eliminar perfiles guardados en caché local al cerrar la sesión.

Con esta directiva habilitada, el valor de Registro se desplaza con los usuarios. Como resultado, se aplica el modo de procesamiento cada vez que los usuarios inician sesión.

Índice de espacio libre para desencadenar la compactación de discos VHD

Se aplica cuando la opción Habilitar la compactación de discos VHD está habilitada. Permite especificar la proporción o índice de espacio libre para desencadenar la compactación de discos VHD. Cuando el índice de espacio libre supera el valor especificado al cerrar la sesión del usuario, se desencadena la compactación del disco.

Índice de espacio libre = (tamaño del archivo VHD actual —tamaño mínimo requerido de archivo VHD*) ÷ tamaño del archivo VHD actual

* Se obtiene mediante el método GetSupportedSize de la clase `MSFT_Partition` del sistema operativo Microsoft Windows.

Cantidad de cierres de sesión para desencadenar la compactación de discos VHD

Se aplica cuando la opción Habilitar la compactación de discos VHD está habilitada. Permite especificar la cantidad de cierres de sesión de usuario necesaria para desencadenar la compactación del disco VHD.

Cuando la cantidad de cierres de sesión desde la última compactación alcanza el valor especificado, la compactación del disco se desencadena de nuevo.

Inhabilitar la desfragmentación para la compactación de discos VHD

Se aplica cuando la opción Habilitar la compactación de discos VHD está habilitada. Permite especificar si inhabilitar o no la desfragmentación de archivos para la compactación de discos VHD.

Cuando la compactación de discos VHD está habilitada, el archivo del disco VHD se desfragmenta primero automáticamente con la herramienta `defrag` integrada de Windows y, a continuación, se compacta. La desfragmentación del disco VHD produce mejores resultados de compactación, mientras que inhabilitarla puede ahorrar recursos del sistema.

Habilitar la reescritura de varias sesiones para contenedores de perfiles

Habilita la reescritura para los contenedores de perfiles en casos con varias sesiones. Si está habilitada, los cambios de todas las sesiones se reescriben en los contenedores de perfiles. De lo contrario, solo se guardan los cambios de la primera sesión, puesto que solo la primera sesión está en modo de lectura/escritura en los contenedores de perfiles. Los contenedores de perfiles de Citrix Profile Management se admiten a partir de Citrix Profile Management 2103. FSLogix Profile Container se admite a partir de Citrix Profile Management 2003.

Para utilizar esta directiva para FSLogix Profile Container, compruebe que se cumplen los siguientes requisitos previos:

- La funcionalidad FSLogix Profile Container está instalada y habilitada.
- El tipo de perfil está establecido en **Try for read-write profile and fallback to read-only** en FSLogix.

Replicar almacenes de usuarios

Le permite replicar el almacén de perfiles de usuario remoto en varias rutas cada vez que se inicia y se cierra sesión. De este modo, Profile Management proporciona redundancia de perfiles para los inicios de sesión de los usuarios.

Habilitar la directiva aumenta la E/S del sistema y puede prolongar los cierres de sesión.

> **Nota:**
>
> Esta función está disponible para soluciones de perfiles basadas en archivos y basadas en contenedores.

Habilitar el acceso basado en credenciales a los almacenes de usuarios

De forma predeterminada, Citrix Profile Management suplantará al usuario actual para acceder al almacén del usuario. Habilite esta función si no quiere que Profile Management suplante al usuario actual al acceder al almacén del usuario. Puede colocar almacenes de usuarios en repositorios de almacenamiento (por ejemplo, Azure Files) a los que el usuario actual no tiene permiso para acceder.

Para asegurarse de que Profile Management pueda acceder a los almacenes de usuarios, guarde las credenciales del servidor de almacenamiento de perfiles en Workspace Environment Management (WEM) o en Administrador de credenciales de Windows. Se recomienda utilizar Workspace Environment Management para no tener que configurar las mismas credenciales en cada máquina en la que se ejecuta Profile Management. Si utiliza el Administrador de credenciales de Windows, utilice la cuenta Sistema local para guardar las credenciales de forma segura.

> **Nota:**
>
> Esta directiva está disponible tanto para los almacenes de usuarios basados en archivos como para aquellos basados en VHDX. Para las versiones de Profile Management anteriores a 2212, esta directiva solo está disponible para almacenes de usuarios basados en VHDX.

Si este parámetro no se configura aquí, se utiliza el valor del archivo INI. Si esta configuración no se define ni aquí ni en el archivo INI, se considera inhabilitado de forma predeterminada.

Personalizar la ruta de almacenamiento de archivos VHDX

Citrix Profile Management ofrece estas directivas basadas en VHDX: Contenedor de perfiles, Itinerancia del índice de búsqueda de Outlook y Acelerar el reflejo de carpetas. De forma predeterminada, los archivos VHDX se almacenan en el almacén de usuarios. Esta directiva le permite especificar una ruta distinta para almacenarlos.

Capacidad predeterminada de contenedores VHD

Le permite especificar la capacidad de almacenamiento predeterminada (en GB) de los contenedores VHD.

Prioridad de la configuración:

1. Si esta directiva no está configurada aquí, se utiliza el valor del archivo INI.
2. Si esta directiva no se configura ni aquí ni en el archivo INI, el valor predeterminado es 50 (GB).

Reconectar discos VHDX automáticamente en las sesiones

Con esta directiva habilitada, Profile Management garantiza un alto nivel de estabilidad de las directivas basadas en VHDX. De manera predeterminada, esta directiva está habilitada.

Cuando esta directiva está habilitada, Profile Management supervisa los discos VHDX que utilizan las directivas basadas en VHDX. Si se desconecta alguno de los discos, Profile Management lo conecta de nuevo automáticamente.

Umbral de expansión automática de contenedores de perfiles

Le permite especificar el porcentaje de utilización de la capacidad de almacenamiento a partir de la cual los contenedores de perfiles activan la expansión automática.

Prioridad de la configuración:

- Si esta directiva no está configurada aquí, se utiliza el valor del archivo INI.
- Si esta directiva no se configura ni aquí ni en el archivo.ini, el valor predeterminado es el 90 (%) de la capacidad de almacenamiento.

Incremento de expansión automática de contenedores de perfiles

Le permite especificar la cantidad de capacidad de almacenamiento (en GB) con la que los contenedores de perfiles se expanden automáticamente cuando se activa la expansión automática.

Prioridad de la configuración:

- Si esta directiva no está configurada aquí, se utiliza el valor del archivo INI.
- Si esta directiva no se configura ni aquí ni en el archivo INI, el valor predeterminado es 10 (GB).

Límite de expansión automática de contenedores de perfiles

Le permite especificar la capacidad de almacenamiento máxima (en GB) a la que los contenedores de perfiles se pueden expandir automáticamente cuando se activa la expansión automática.

Prioridad de la configuración:

- Si esta directiva no está configurada aquí, se utiliza el valor del archivo INI.
- Si esta directiva no se configura ni aquí ni en el archivo INI, el valor predeterminado es 80 (GB).

Habilitar la configuración de directiva a nivel de usuario

Con esta configuración habilitada, las configuraciones de directiva al nivel de la máquina pueden funcionar al nivel del usuario, y las configuraciones al nivel del usuario supeditan las configuraciones al nivel de la máquina.

Prioridad de la configuración:

1. Si esta directiva no está configurada aquí, se utiliza el valor del archivo INI.
2. Si esta directiva no se configura ni aquí ni en el archivo INI, se inhabilita.

Establecer el orden de prioridad para los grupos de usuarios

Le permite especificar el orden de prioridad de los grupos de usuarios. El orden determina qué grupo tiene prioridad cuando un usuario pertenece a varios grupos con diferentes configuraciones de directiva.

Cuando un usuario pertenece a varios grupos con configuraciones de directiva en conflicto, tenga en cuenta lo siguiente:

- Si el usuario pertenece a uno o más grupos definidos en esta directiva, tendrá prioridad el grupo con la prioridad más alta.
- Si el usuario no pertenece a ninguno de los grupos definidos en esta directiva, tendrá prioridad el grupo cuyo SID aparezca primero en orden alfabético.

Método de selección del almacén de usuarios

Permite especificar el método de selección del almacén de usuarios cuando hay varios almacenes de usuarios disponibles. Entre las opciones se incluyen:

- **Orden de configuración.** Profile Management selecciona el almacén configurado más temprano.
- **Rendimiento de acceso.** Profile Management selecciona el almacén con el mejor rendimiento de acceso.

Prioridad de la configuración:

1. Si este parámetro no se configura aquí, se utiliza el valor del archivo .INI.
2. Si este parámetro no está configurado aquí ni en el archivo INI, se usa el **Orden de configuración**.

Habilitar la conmutación por error de contenedores de perfiles durante la sesión entre almacenes de usuarios

De forma predeterminada, cuando se implementan varios almacenes de usuarios, la conmutación por error del contenedor de perfiles solo se produce al iniciar sesión el usuario. Como resultado, la redundancia de perfiles solo está disponible durante el inicio de sesión del usuario. Esta directiva le permite ampliar el alcance de la conmutación por error a toda la sesión, lo que garantiza la redundancia del perfil durante toda la sesión. Con la directiva habilitada, si Profile Management pierde la conexión con el contenedor de perfiles activo durante una sesión, cambia automáticamente a otro disponible.

Prioridad de la configuración:

1. Si esta directiva no está configurada aquí, se utiliza el valor del archivo INI.
2. Si esta directiva no se define ni aquí ni en el archivo INI, el parámetro se inhabilita.

Configuraciones básicas de directiva

August 17, 2024

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 se configura ni 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 configura aquí, se utiliza el valor del archivo INI. Si esta configuración no se define 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. Tenga en cuenta que esta directiva está inhabilitada o no está configurada en sistemas operativos multisesión, como los entornos de Citrix Virtual Apps. En este caso, Profile Management supone que se deben procesar los inicios de sesión de los usuarios del dominio, pero 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 a los usuarios del dominio con derechos de administrador local, normalmente usuarios de Citrix Virtual Desktops con escritorios virtuales asignados, hacer lo siguiente:

- Omitir cualquier procesamiento
- Iniciar sesión
- Solucionar problemas de escritorio con Profile Management

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 se configura ni 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.
- Inhabilitado 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 esta directiva se expanda 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\U

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 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 se configura ni 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
- 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 configura aquí, se utiliza el valor del archivo INI.

Si esta configuración no se define 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 se configura ni 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 localmente. Además, al final se sincronizan con el almacén de usuarios cuando se restablece 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 configura 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.

Reescritura activa al bloquear y al desconectar sesiones

Con esta directiva y la directiva **Reescritura activa** habilitadas, los archivos y carpetas del perfil solo se reescribirán cuando una sesión esté bloqueada o desconectada.

Con esta directiva y las directivas **Registro de reescritura activa** y **Reescritura activa** habilitadas, las entradas del Registro solo se reescriben cuando una sesión está bloqueada o desconectada.

Compatibilidad con perfiles sin conexión

Habilita la función de perfiles sin conexión. Esta función está diseñada para equipos que normalmente se desconectan de las redes. Por ejemplo: portátiles o dispositivos móviles, no servidores ni equipos de escritorio.

Si este parámetro no se configura aquí, se utiliza el valor del archivo INI.

Si esta configuración no se define ni aquí ni en el archivo INI, se inhabilita la funcionalidad de perfiles sin conexión.

Configuraciones de directiva de Multiplataforma

August 17, 2024

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 se configura ni 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 se configura ni 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 se configura ni 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. Tenga en cuenta que el almacén de configuración multiplataforma contiene un archivo de definición sin datos o que los datos almacenados en la caché en un perfil de plataforma única son más recientes que los datos de la definición que hay en el almacén. En este caso, Profile Management migra los datos del perfil de plataforma única al almacén a menos que 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

August 17, 2024

Esta sección contiene directivas que establecen lo siguiente:

- Qué archivos de un perfil de usuario se sincronizan entre el sistema en el que está instalado el perfil y el almacén de usuarios
- Qué directorios de un perfil de usuario se sincronizan entre el sistema en el que está instalado el perfil y el almacén de usuarios

Configuraciones de directiva de Exclusiones

August 17, 2024

En esta sección, se describen 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%). Los comodines se admiten en los nombres de archivos y carpetas, pero solo los comodines de los nombres de archivos se aplican de forma recursiva.

Ejemplos:

- `Desktop\Desktop.ini` ignora el archivo `Desktop.ini` de la carpeta `Desktop`
- `%USERPROFILE%\*.tmp` ignora todos los archivos con la extensión `.tmp` en todo el perfil
- `AppData\Roaming\MyApp\*.tmp` ignora todos los archivos con la extensión `.tmp` en una parte del perfil
- `Downloads\*\a.txt` ignora `a.txt` en cualquier subcarpeta inmediata de la carpeta `Downloads`.

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 se configura ni aquí ni en el archivo INI, no se excluirá ningún archivo.

Habilitar lista de exclusión predeterminada: 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 se configura ni 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%). Se admiten los comodines en los nombres de carpetas, pero no se aplican de forma recursiva.

Ejemplo:

- `Desktop` ignora la carpeta `Desktop` en el perfil de 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. La configuración de directiva y las acciones correspondientes posibles se muestran en esta tabla:

Configuración de directiva	Acción
La configuración está inhabilitada o el valor de "Sincronizar carpetas o archivos excluidos al iniciar sesión"tiene su valor predeterminado La configuración se establece en "Omitir carpetas o archivos excluidos al iniciar sesión"	Profile Management sincroniza carpetas o archivos excluidos del almacén de usuarios al perfil local cuando un usuario inicia sesión. Profile Management omite las carpetas o archivos excluidos del almacén de usuarios cuando un usuario inicia sesión.

Configuración de directiva	Acción
La configuración se establece en "Eliminar carpetas o archivos excluidos al iniciar sesión"	Profile Management elimina las carpetas o archivos excluidos del almacén de usuarios cuando un usuario inicia sesión.
La configuración no está definida en Web Studio	Se utiliza el valor del archivo INI
La configuración no está definida en Web Studio ni en el archivo INI	Los archivos y carpetas excluidos se sincronizan del almacén de usuarios a un 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, Profile Management crea un enlace simbólico en lugar de copiar archivos de 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.

No se puede acceder a esos archivos simultáneamente desde varias sesiones.

Configuraciones de directiva de Sincronización

August 17, 2024

La sección **Sincronización** describe 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

De forma predeterminada, Profile Management sincroniza el perfil de usuario entre el sistema en el que está instalado y el almacén de usuarios. Si excluye una carpeta de la sincronización, esta directiva le permite incluir las subcarpetas de la carpeta excluida en la sincronización.

Las rutas de la lista deben ser relativas al perfil de usuario. Se admiten los comodines en los nombres de carpetas, pero no se aplican de forma recursiva.

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

De forma predeterminada, Profile Management sincroniza el perfil de usuario entre el sistema en el que está instalado y el almacén de usuarios. Si excluye una carpeta de la sincronización, esta directiva le permite volver a incluir los archivos de la carpeta excluida en la sincronización.

Las rutas de la lista deben ser relativas al perfil de usuario. Los comodines se admiten en los nombres de archivos y carpetas, pero solo los comodines de los nombres de archivos se aplican de forma recursiva. Los comodines no se pueden anidar.

Ejemplos:

- `AppData\Local\Microsoft\Office\Access.qat` especifica un archivo de una carpeta que está excluida en la configuración predeterminada
- `AppData\Local\MyApp\*.cfg` especifica todos los archivos con la extensión `.cfg` en la carpeta de perfil `AppData\Local\MyApp` 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 que reflejar

Esta directiva permite solucionar problemas relacionados con las carpetas transaccionales (también conocidas como carpetas de referencia). Estas carpetas contienen archivos interdependientes, donde un archivo hace referencia al otro.

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: en esta tabla se describe cómo Index.dat hace referencia a las cookies mientras un usuario navega por Internet:

Caso	Cómo hace referencia Index.dat a las cookies
—	—
Un usuario tiene dos sesiones de Internet Explorer, cada una en un servidor diferente, y visita diferentes sitios en cada sesión.|Las cookies de cada sitio se agregan al servidor correspondiente.| Las cookies de cada sitio se agregan al servidor correspondiente.
El usuario cierra la primera sesión o se desconecta en medio de una sesión (si la función de reescritura activa está configurada)	Las cookies de la segunda sesión deben reemplazar a las cookies de la primera sesión.
La primera y la segunda sesión se fusionan, y las referencias a las cookies en Index.dat quedan desactualizadas	Si se sigue navegando en nuevas sesiones, se producen fusiones repetidas, y la carpeta de cookies se sobrecarga

El reflejo de la carpeta de cookies resuelve el problema. En este caso, las cookies se sobrescriben con las cookies de la última sesión cada vez que el usuario cierra la sesión. De esta manera, Index.dat permanece 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.

Acelerar el reflejo de carpetas

Con esta directiva y la directiva **Carpetas para reflejar** habilitadas, **Profile Management almacena las carpetas reflejadas** en un disco virtual basado en VHDX. Además, conecta el disco virtual durante los inicios de sesión y lo desconecta durante los cierres de sesión. Al habilitar esta directiva, se elimina la necesidad de copiar las carpetas entre el almacén de usuarios y los perfiles locales y se acelera el reflejo de carpetas.

Configuraciones de directiva de Redirección de carpetas

August 17, 2024

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 permite incluir la variable de entorno `%userdomain%` como parte de la ruta UNC. Esta ruta UNC se especifica para las carpetas redirigidas.

De forma predeterminada, esta configuración está inhabilitada. Y la variable de entorno `%userdomain%` no se incluye como parte de la ruta UNC que se especifica para las carpetas redirigidas.

Configuraciones de directiva de AppData(Roaming)

August 17, 2024

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. Para obtener más información, consulte la sección Ruta al almacén de usuarios.

Si esta configuración no está definida aquí, Profile Management no redirige la carpeta especificada.

Configuraciones de directiva de Contactos

August 17, 2024

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

August 17, 2024

Esta sección contiene configuraciones de directiva para redirigir el contenido de la carpeta `Desktop` 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

August 17, 2024

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

August 17, 2024

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

August 17, 2024

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

August 17, 2024

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

August 17, 2024

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

August 17, 2024

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

August 17, 2024

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

August 17, 2024

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

August 17, 2024

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

August 17, 2024

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

August 17, 2024

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 esta configuración no está definida en Web Studio, se usa el valor del archivo INI.

Si esta configuración no se define ni en Web Studio ni en el archivo INI, se registra lo siguiente:

- Errores
- 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 configura aquí, se utiliza el valor del archivo INI.

Si esta configuración no se define ni en Web Studio ni en el archivo INI, se registra lo siguiente:

- Errores
- 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 configura aquí, se utiliza el valor del archivo INI.

Si esta configuración no se define ni en Web Studio ni en el archivo INI, se registra lo siguiente:

- Errores
- 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 configura 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 configura aquí, se utiliza el valor del archivo INI.

Si esta configuración no se define ni en Web Studio ni en el archivo INI, se registra lo siguiente:

- Errores
- 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 configura aquí, se utiliza el valor del archivo INI.

Si esta configuración no se define ni en Web Studio ni en el archivo INI, se registra lo siguiente:

- Errores
- 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 configura aquí, se utiliza el valor del archivo INI.

Si esta configuración no se define ni en Web Studio ni en el archivo INI, se registra lo siguiente:

- Errores
- 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 configura aquí, se utiliza el valor del archivo INI.

Si esta configuración no se define ni en Web Studio ni en el archivo INI, se registra lo siguiente:

- Errores
- Información general

Tamaño máximo del archivo de registros

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 registros supera el tamaño máximo:

- Se elimina una copia de seguridad existente del archivo (.bak)
- El nombre del archivo de registros cambia a .bak
- Se crea otro archivo de registros

El archivo de registros se crea en %SystemRoot%\System32\Logfiles\UserProfileManager.

Si este parámetro no se configura 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 registros

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. Este parámetro garantiza que los archivos de registros se conserven cuando la máquina se reinicia. Para máquinas virtuales sin disco duro persistente, definir una ruta UNC permite conservar los archivos de registros. Sin embargo, la cuenta de sistema de las máquinas debe tener acceso de escritura en el recurso 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 registros, Citrix recomienda aplicar una lista de control de acceso a la carpeta de los archivos de registros. Esta configuración garantiza que solo las cuentas autorizadas de usuarios o equipos puedan acceder a los archivos almacenados.

Si este parámetro no se configura 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 configura aquí, se utiliza el valor del archivo INI.

Si esta configuración no se define ni en Web Studio ni en el archivo INI, se registra lo siguiente:

- Errores
- 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 configura aquí, se utiliza el valor del archivo INI.

Si esta configuración no se define ni en Web Studio ni en el archivo INI, se registra lo siguiente:

- Errores
- 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 configura aquí, se utiliza el valor del archivo INI.

Si esta configuración no se define ni en Web Studio ni en el archivo INI, se registra lo siguiente:

- Errores
- 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 configura aquí, se utiliza el valor del archivo INI.

Si esta configuración no se define ni en Web Studio ni en el archivo INI, se registra lo siguiente:

- Errores
- Información general

Configuraciones de directiva de Gestión de perfiles

August 17, 2024

Esta sección incluye 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. Como resultado, un valor de 60 garantiza que los perfiles se eliminen entre uno y dos minutos después de que los usuarios hayan cerrado la sesión. Esta acción depende de cuándo se realizó 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, este proceso 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 configura 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 configura 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 cómo se comporta Profile Management si existe un perfil de usuario en estos dos casos:

- Almacén de usuarios
- Perfil de usuario local de Windows (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 configura aquí, se utiliza el valor del archivo INI.

Si esta configuración 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. Después de eso, Profile Management utiliza el perfil del almacén de usuarios en estos dos casos:

- Sesión actual
- 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 configura aquí, se utiliza el valor del archivo INI.

Si esta configuración 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 ubicar los perfiles de aplicación existentes.

Si este parámetro no se configura aquí, se utiliza el valor del archivo INI.

Si esta configuración no se define ni aquí ni en el archivo INI, se considera inhabilitado de forma predeterminada.

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\ntuse 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 configura 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.

Imagine un usuario que no tiene un perfil de usuario de Citrix, pero sí un perfil de usuario de Windows local. En este caso, de forma predeterminada, el perfil local se usa y se migra al almacén de usuarios, si este valor está habilitado. 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 configura 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.

Imagine un usuario que no tiene un perfil de usuario de Citrix, pero sí un perfil de usuario de Windows móvil. En este caso, de forma predeterminada, el perfil móvil se usa y se migra al almacén de usuarios, si este valor está habilitado. 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 configura 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 configura 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

August 17, 2024

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 se configura ni 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 si se daña el archivo.

Si esta directiva no está configurada aquí, Profile Management usa el valor del archivo INI. Si esta directiva no se configura ni 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

August 17, 2024

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 configura aquí, se utiliza el valor del archivo INI.

Si esta configuración no se define ni aquí ni en el archivo INI, está 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, el 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 configura aquí, se utiliza el valor del archivo INI.

Si esta configuración no se define ni aquí ni en el archivo INI, está inhabilitado.

Streaming de perfiles

Esta configuración habilita o inhabilita la función de streaming de perfiles de usuario de Citrix. Cuando está habilitada, los archivos y carpetas del perfil se obtienen del almacén de usuarios y se envían al equipo local solo cuando los usuarios acceden a ellos después de iniciar 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 configura aquí, se utiliza el valor del archivo INI.

Si esta configuración no se define ni aquí ni en el archivo INI, está 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 configura 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.

Habilitar la exclusión de streaming de perfiles

Cuando se habilita la exclusión de streaming de perfiles:

- Profile Management no envía por streaming carpetas de la lista de exclusiones
- Todas las carpetas se obtienen inmediatamente del 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. Este comportamiento evita la saturación en el área de archivos pendientes y garantiza que el almacén de usuarios contenga siempre los archivos más actualizados.

De forma predeterminada, este parámetro está establecido en 1 (un) día.

Si este parámetro no se configura 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.

Habilitar el streaming de perfiles para el área pendiente

Le permite habilitar la función de streaming de perfiles para los archivos y las carpetas del área pendiente.

El área pendiente se utiliza para garantizar la coherencia de los perfiles mientras el streaming de perfiles está habilitado. En ella se almacenan temporalmente los archivos y las carpetas de perfiles que han cambiado en sesiones simultáneas.

De forma predeterminada, esta directiva está inhabilitada y todos los archivos y carpetas del área pendiente se obtienen en el perfil local al iniciar sesión. Con esta directiva habilitada, los archivos del área pendiente solo se obtienen en el perfil local cuando se solicitan. Utilice esta directiva con la directiva de streaming de perfiles para garantizar una experiencia de inicio de sesión óptima en situaciones de sesiones simultáneas.

La directiva se aplica a las carpetas del área pendiente cuando está habilitada la directiva Habilitar el streaming de perfiles para carpetas.

Configuraciones de la directiva Capa de personalización de usuarios

August 17, 2024

Para habilitar el montaje de capas de usuarios dentro de Virtual Delivery Agents, use 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 la capa de usuarios en GB: El tamaño predeterminado de la capa de usuarios es de 10 GB, el mínimo que recomienda Citrix. Una capa de usuarios es un disco aprovisionado ligero que se expande al tamaño establecido a medida que se utiliza el espacio. Las capas de usuarios nunca disminuyen de tamaño.

> **Nota:**
>
> Aumentar el tamaño de la capa de usuarios afecta a las nuevas capas de usuarios y expande las existentes. Disminuir el tamaño de la capa solo afecta a las nuevas capas de usuarios. Las capas de usuarios existentes nunca disminuyen de tamaño.

Para obtener más información, consulte Capa de personalización de usuarios.

Configuraciones de directiva de Virtual Delivery Agent

August 17, 2024

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 subred 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 registran los VDA. Los VDA se registran 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 Controllers** está inhabilitada.

Esta configuración especifica el número de puerto TCP/IP que los VDA utilizan para registrarse en 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 Controllers** 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. Esta configuración es opcional y 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 Controllers** 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 configuración es opcional y se puede usar con la configuración **SID 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 obtener información sobre el Controller. El Controller envía listas actualizadas a sus VDA registrados si se produce una de estas situaciones:

- Se ha agregado o quitado un Controller desde la última comprobación
- Se ha producido un cambio de directiva

El VDA acepta conexiones de todos los Controllers de la lista más reciente que haya 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 forma predeterminada, esta configuración está inhabilitada.

GUID del sitio

Use esta configuración solamente si **Habilitar actualización automática de Controllers** está inhabilitada.

Esta configuración especifica el identificador único global (GUID) del sitio que utiliza el 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

August 17, 2024

La sección HDX 3D Pro incluye configuraciones de directiva para habilitar y definir los parámetros de la herramienta de configuración de la calidad de imagen para los usuarios. Esta herramienta permite

a los usuarios optimizar el uso del ancho de banda disponible. Para esta optimización, el equilibrio entre la calidad de la imagen y la capacidad de respuesta se ajusta en tiempo real.

Habilitar sin pérdida

Esta configuración especifica si los usuarios pueden 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.

Imagine un usuario que habilita la compresión sin pérdida. En este caso, la calidad de la imagen se establece automáticamente en el valor máximo disponible en la herramienta de configuración de imágenes. 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 disponibles para los usuarios en la herramienta de configuración de la calidad de la imágenes. Con estos valores, los usuarios pueden definir el intervalo de ajuste de la calidad de imagen en la herramienta de configuración de la calidad de las imágenes.

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

August 17, 2024

La sección **Supervisión** incluye configuraciones de directiva para la supervisión de procesos, recursos y errores de aplicaciones.

El ámbito de estas directivas se puede definir en función de lo siguiente:

- Sitio
- Grupo de entrega
- Tipo de grupo de entrega
- Unidad organizativa
- 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. Imagine que no quiere supervisar ni los datos de recursos ni los datos de procesamiento para un ámbito específico. Por ejemplo: un grupo de entrega o una unidad organizativa específicos. En este caso, 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 transmiten desde cada VDA a la base de datos en intervalos de 5 minutos. Los datos de procesos (si la opción está habilitada) se transmiten 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
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 la configuración de retención de datos, se necesitan aproximadamente 276 KB de espacio en disco para almacenar lo siguiente para un VDA durante un período de un año:

- CPU
- Memoria
- E/S por segundo
- Datos de latencia de disco

Cantidad de máquinas	Almacenamiento aproximado requerido
1	276 KB
1K	270 MB
40K	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
1K	1,5 GB	3 GB

> **Nota:**
>
> Las cifras proporcionadas anteriormente no incluyen el espacio Índice. Además, todos los 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, esta configuración 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.

Directiva de recopilación de datos para Analytics

Recopilación de datos de VDA para Analytics

Utilice la directiva para habilitar o inhabilitar el servicio Supervisar para recopilar métricas relacionadas con el rendimiento y la seguridad de los VDA para Performance y Security Analytics. De forma predeterminada, la directiva está **Permitida**. Establezca la directiva en **Prohibida** para detener la recopilación de datos de los VDA.

Recopilación de metadatos del Portapapeles para la supervisión de la seguridad

Utilice la directiva para habilitar o inhabilitar la recopilación de metadatos del Portapapeles por parte del servicio intermediario para la supervisión, la auditoría y el cumplimiento de la seguridad. De manera predeterminada, la directiva está **habilitada**. **Inhabilite** la directiva para detener la recopilación de datos de los VDA.

Recopilación de datos de diagnóstico para la supervisión del rendimiento

Use esta directiva para permitir que el servicio de supervisión recopile datos de diagnóstico, como la información de la sesión, los estados del servicio UPM/EUEM, la optimización de Microsoft Teams y los protocolos de conexión. De manera predeterminada, la directiva está **habilitada**. **Inhabilite** la directiva para detener la recopilación de datos de los VDA.

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 Crear 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

August 17, 2024

> **Importante:**
>
> - La multisesión de Windows 10 Enterprise no incluye la función de virtualización de IP de Escritorio remoto (IP virtual) y nosotros no incluimos la función de Virtualización de IP de Escritorio remoto ni bucle invertido virtual en multisesión con Windows 10 Enterprise.
> - La virtualización de IP de escritorio remoto (IP virtual) no es compatible con las máquinas alojadas en la nube. Para obtener más información, consulte la documentación de Microsoft.

La sección **IP virtual** incluye 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 solo el nombre del ejecutable. No es necesario especificar la ruta completa.

De forma predeterminada, no hay archivos ejecutables especificados.

Exclusión de puerto de bucle invertido de IP virtual

Cuando una aplicación llama a la dirección de bucle invertido en cualquier puerto especificado en este parámetro, el bucle invertido virtual no cambia la llamada a la dirección de bucle invertido específica de la sesión

Configurar la redirección de puertos COM y puertos LPT mediante el Registro

August 17, 2024

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 Web 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: 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 usa 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

August 17, 2024

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 Web 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.

Warning frequency interval (Intervalo de frecuencia de las advertencias)

Este parámetro define el intervalo 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 intervalo de 0 a 999.
- hh son las horas, con un intervalo de 0 a 23.
- mm son los minutos, con un intervalo de 0 a 59.
- ss son los segundos, con un intervalo de 0 a 59.

De forma predeterminada, el valor del intervalo es de 1 hora (01:00:00).

Warning message box body text (Texto del mensaje de advertencia)

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} Save your work. The server will go offline for maintenance in {TIMELEFT}.

Warning message box title (Título del mensaje de advertencia)

Este parámetro contiene el texto modificable del título del mensaje de advertencia dirigido a los usuarios.

De manera predeterminada, el título es Upcoming Maintenance.

Warning time period (Periodo de advertencia)

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 intervalo de 0 a 999.
- hh son las horas, con un intervalo de 0 a 23.
- mm son los minutos, con un intervalo de 0 a 59.
- ss son los segundos, con un intervalo 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 forzado.

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 forzado.

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 forzado 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 intervalo de 0 a 999.
- hh son las horas, con un intervalo de 0 a 23.
- mm son los minutos, con un intervalo de 0 a 59.
- ss son los segundos, con un intervalo de 0 a 59.

De manera predeterminada, el período de gracia para el cierre de sesión forzado es de 5 minutos (00:05:00).

Texto del mensaje de cierre de sesión forzado

Esta configuración 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} 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 Web 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 intervalo de 0 a 999.
- hh son las horas, con un intervalo de 0 a 23.
- mm son los minutos, con un intervalo de 0 a 59.
- ss son los segundos, con un intervalo de 0 a 59.

De forma predeterminada, el parámetro del intervalo regular es de 5 minutos (00:05:00).

Cambios en directivas

August 17, 2024

La siguiente tabla muestra los cambios realizados en la documentación de las directivas de Citrix Virtual Apps and Desktops 7 2407.

Tabla de contenido modificado en Directivas:

Configuración de directiva	Changes	Fecha
Profile Management > Parámetros avanzados > Habilitar la conmutación por error del contenedor de directivas durante la sesión entre almacenes de usuarios	Nueva directiva de conmutación por error de contenedores de perfiles durante la sesión entre almacenes de usuarios. Más información.	31 Jul 2024
Profile Management > Registro > Lista de inclusión	La compatibilidad con exclusión e inclusión del Registro se extendió a la solución de perfiles basada en contenedores. Más información.	31 Jul 2024
Profile Management > Registro > Lista de exclusión		31 Jul 2024
Profile Management > Redirección de carpetas	Mejoras en las directivas de redirección de carpetas. Más información.	31 Jul 2024
Recopilación de métricas de sesión	Para obtener más información, consulte Configuraciones de directiva de ICA.	31 Jul 2024

Tabla de contenido obsoleto en Directivas:

Configuración de directiva	Elementos retirados	Fecha
Publicación de Citrix Virtual Apps and Desktops 7 2407.	Ninguno	31 Jul 2024

Administrar

August 17, 2024

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 u otro servicio para alojar máquinas que entregan aplicaciones y escritorios a los usuarios, cree la primera conexión a ese hipervisor o servicio 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 más 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 para utilizar una dirección de bucle invertido virtual exclusiva en el intervalo de host local.

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 ayude a entregar aplicaciones y escritorios, antes 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 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/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 implementaciones. 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 utiliza esta solución de perfiles, consulte este artículo para obtener información general. Consulte la documentación de Profile Management para obtener información detallada.

Recopilar rastreos de Citrix Diagnostic Facility (CDF)

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.

Citrix Insight Services

Citrix Insight Services (CIS) es una plataforma de Citrix para instrumentación, telemetría y generación de información empresarial.

Citrix Scout

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.

Aplicaciones

August 17, 2024

> **Nota:**
>
> Puede administrar la implementación de Citrix Virtual Apps and Desktops mediante dos consolas de administración: Web Studio (basada en la web) y Citrix Studio (basada en Windows). Este artículo se refiere únicamente a Web Studio. Para obtener información sobre Citrix Studio, consulte el artículo equivalente en Citrix Virtual Apps and Desktops 7 2212 o versiones anteriores.

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 Agregar aplicaciones, seleccione al menos un grupo de entrega o al menos un grupo 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, puede haber un problema de visibilidad si no dispone de permisos suficientes para ver la aplicación en todos esos grupos. En tales casos, consúltelo con un administrador que tenga 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 de grupos diferentes) para los mismos usuarios, cambie la propiedad `Application name (for user)` en Web Studio. De lo contrario, los usuarios ven 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. Estos procedimientos se detallan en 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.
- No se pueden quitar aplicaciones de grupos de entrega o grupos de aplicaciones mediante el asistente Agregar aplicaciones. Se trata de dos operaciones diferentes.

Para agregar una o varias aplicaciones:

1. Seleccione **Aplicaciones** en el panel de la izquierda y, a continuación, seleccione **Agregar aplicaciones** en la barra de 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**. 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 la izquierda de Web Studio, seleccione un grupo de entrega en el panel central y, por último, seleccione **Agregar aplicaciones** en la barra de 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 la izquierda de Web Studio, seleccione un Grupo de aplicaciones en el panel central y, por último, seleccione la entrada **Agregar aplicaciones** bajo el nombre del grupo de aplicaciones en la barra de acciones. El asistente no mostrará la página **Grupos**.

Página Grupos

Esta página contiene una lista de todos los grupos de entrega del 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 está disponible) como mínimo. Cada aplicación debe estar siempre asociada a un grupo como mínimo.

Página Aplicaciones

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 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.
- **Manualmente:** Se trata de aplicaciones que se encuentran en un VDA del grupo de entrega o en otro lugar de la red. Al seleccionar este origen, se abre una nueva página en la que se especifica una aplicación para agregarla de las siguientes maneras:

  - Especifique la ruta al archivo ejecutable, el directorio de trabajo, los argumentos opcionales de línea de comandos y los nombres simplificados de los administradores y los usuarios.
  - Seleccione una aplicación de un VDA del grupo de entrega. Para ello, haga clic en **Examinar**, introduzca las credenciales de acceso al VDA, espere a que se conecte al VDA y, a continuación, seleccione una aplicación del VDA. Los campos de la página se rellenan automáticamente con las propiedades de la aplicación seleccionada.

- **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 Implementar y entregar aplicaciones de App-V.

  Este origen no se puede seleccionar si App-V no se configuró 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 verificación 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.

Puede cambiar las propiedades de una aplicación (parámetros) en esta página, o más tarde.

De forma predeterminada, las aplicaciones 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 carpeta, se le pedirá cambiar el nombre de la aplicación que va

a agregar. 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 **Aplicaciones** y usted intenta agregar otra aplicación denominada también `app` a esa carpeta, se le sugerirá el nombre `app_1`.

Página 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 a los que está asociada.

Puede arrastrar una aplicación a un grupo adicional. Esta es una alternativa al uso de comandos en la barra de 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 `Edit delivery group`. El tipo de grupo de entrega se convierte automáticamente a `desktops and applications` cuando se confirma el cuadro de diálogo de propiedades.

1. Inicie sesión en Web Studio, seleccione **Aplicaciones** en el panel de la izquierda y, a continuación, seleccione la aplicación.
2. Seleccione **Propiedades** en la barra de acciones.
3. Seleccione la página **Grupos**.

    - Para agregar un grupo, haga clic en **Agregar** y seleccione **Grupos de aplicaciones** o **Grupos de entrega** (si aún no ha creado ningún grupo de aplicaciones, la única entrada que verá es **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.

- 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 queda asociada a ningún grupo, se le alertará de que la aplicación será eliminada.
- 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**.

4. 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).
- **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 cambiar el nombre de 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 la izquierda.
2. Seleccione una o más aplicaciones en el panel central y, a continuación, seleccione la tarea correspondiente en la barra de acciones.
3. Confirme la acción, cuando se le solicite.

Quitar aplicaciones de un grupo de entrega

La aplicación debe estar asociada (pertenecer) a un grupo de entrega o un grupo de aplicaciones como mínimo. Quitar una aplicación de un grupo de entrega la desasocia de cualquier grupo de entrega o

grupo de aplicaciones. Por eso, se le notifica que se quitará la aplicación si continúa. 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 la izquierda.
2. Seleccione un grupo de entrega. En el panel inferior central, seleccione la aplicación que quiere quitar en la ficha **Aplicaciones**.
3. Seleccione **Quitar aplicación** en la barra de acciones.
4. Confirme la eliminación.

Quitar aplicaciones de un grupo de aplicaciones

Una aplicación debe pertenecer al menos a un grupo de entrega o un grupo de aplicaciones. Al quitar una aplicación de un grupo de aplicaciones dejará de pertenecer a ningún grupo. Por eso se le notifica que se quitará la aplicación si continúa. En estos casos, si quiere poder entregar la aplicación, debe volver a agregarla desde un origen válido.

1. Seleccione **Aplicaciones** en el panel de la izquierda.
2. Seleccione el grupo de aplicaciones en el panel central y, a continuación, seleccione una o más aplicaciones.
3. Seleccione **Quitar del grupo de aplicaciones** en la barra de 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 la izquierda.
2. Seleccione una aplicación y, a continuación, seleccione **Modificar propiedades de aplicación** en el panel de 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 hecho y deje la ventana abierta, o 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

Propiedad	Página
Argumentos de línea de comandos; consulte Transferir parámetros a aplicaciones publicadas	Location
Grupos de entrega y grupos de aplicaciones donde la aplicación está disponible	Grupos
Descripción	Identificación
Extensiones de nombre de archivo y asociación de tipos de archivo: Qué extensiones abre automáticamente la aplicación	Asociación de tipos de archivos
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	Location
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 puede abrir). Para que no esté disponible e invisible, agréguelo a otro grupo.	Limitar visibilidad
Directorio de trabajo	Location

Es posible que los cambios a 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. Ese límite 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 interrupción.

De forma predeterminada, no hay ningún límite en la cantidad de instancias de aplicación que pueden ejecutarse al mismo tiempo. Existen varias configuraciones para limitar 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 `Alpha`. 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 `Alpha`, se generará un mensaje de error y `Alpha` 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 ese mismo día, 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 10 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 10 usuarios actuales de `Delta` 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 `Charlie` tiene requisitos de licencia y rendimiento que estipulan cuántas instancias se pueden ejecutar al mismo tiempo en un servidor específico. Esos requisitos también dictan cuántas instancias se pueden ejecutar 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 `Charlie`, 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 la aplicación `Charlie` 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 solo a determinadas máquinas dentro de un grupo de entrega (además de limitar las instancias en todas las máquinas del sitio):

  - Utilice la funcionalidad de etiquetado para esas máquinas.
  - Configure el máximo de instancias por límite de máquina para esa aplicación.

Si se inician aplicaciones sin Controller como intermediario (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. Las instancias que superaron el límite no se cierran de forma forzada. Se les permitirá continuar hasta que sus usuarios las cierren.

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 sobre la itinerancia, consulte Sesiones.

Para configurar el límite máximo de instancias por grupo de entrega y el límite de una instancia por usuario:

1. Seleccione **Aplicaciones** en el panel de la izquierda y, a continuación, seleccione una aplicación.
2. Seleccione **Modificar propiedades de aplicación** en la barra de 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.

- Especificar la cantidad máxima de instancias que pueden ejecutarse simultáneamente por máquina
- 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 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 a 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""%*"
```

> **Nota:**
>
> El máximo de caracteres, incluidos los argumentos, en la línea de comandos para iniciar aplica-

> ciones publicadas es de 203.

Solución de problemas de cierre de sesión con aplicaciones publicadas

Al publicar aplicaciones, solo se especifica el archivo ejecutable principal de la aplicación publicada. Sin embargo, algunas aplicaciones pueden generar procesos adicionales (secundarios) que se ejecutan en segundo plano y el archivo ejecutable principal correspondiente no los cierra cuando se cierra la aplicación principal publicada. También se pueden crear procesos adicionales, a partir de scripts que se ejecutan o a partir de claves de registro específicas, como `Run` y `RunOnceKey`. Estas aplicaciones pueden impedir un cierre de sesión correcto, lo que provoca que las sesiones se prolonguen indebidamente o bloqueen y que la sesión no se cierre y que el usuario se quede fuera.

En este caso, debe restablecer o cerrar estas sesiones mediante Citrix Director.

Para ayudar a identificar y solucionar problemas en las sesiones que no se cierran correctamente, Citrix ha puesto a disposición tres entradas de registro. La identificación y solución de problemas de una sesión que no se cierra correctamente debido a estos problemas es un proceso de tres pasos:

1. Identificar qué sesiones con aplicaciones publicadas están obstruyendo un cierre de sesión correcto
2. Identificar si esas aplicaciones publicadas generan algún proceso adicional (secundario)
3. Agregar estos procesos a una entrada de registro específica para evitar que obstruyan el cierre de sesión

Paso 2: Identificar si esas aplicaciones publicadas generan algún proceso adicional (secundario)

Una vez que se identifica una aplicación publicada impide un cierre de sesión correcto, el siguiente paso es determinar si esta aplicación genera procesos adicionales cuando se ejecuta.

Puede leer `HKCU\Software\CitrixVolatile\Seamless\Sessions\[ID]\LogoffCheckerBlock` para determinar si algún proceso bloquea el cierre de sesión correcto cuando se cierra una aplicación publicada.

En el ejemplo siguiente, la clave `LogoffCheckerBlockingProcess` contiene las siguientes entradas:

```
PhoneExperienceHost.exe
SkypeApp.exe
SkypeBackgroundHost.exe
```

Estos procesos han obstruido el cierre de sesión correcto.

> **Nota:**
>
> Sustituya el [ID] por el ID de sesión correcto para la sesión que quiere comprobar.

Paso 3: Agregar estos procesos a una entrada de registro específica para evitar que obstruyan el cierre de sesión

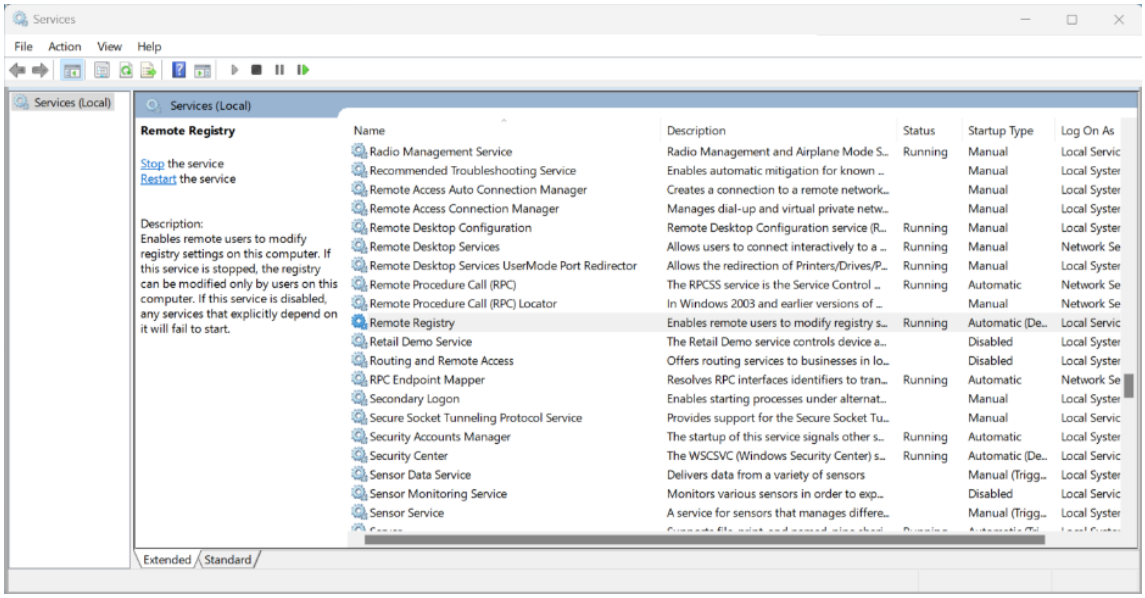
Puede agregar estos procesos a las siguientes claves de Registro para evitar que obstruyan el cierre de sesión en sesiones futuras:

```
Add the process file name to the following registry key:
Caution! Refer to the Disclaimer at the end of this article before
   using the Registry Editor.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI
Value Name:LogoffCheckSysModules
Type:REG_SZ
String:MyAppName.exe
```

Para obtener más información sobre `LogoffCheckSysModules`, consulte Graceful logoff from a published application renders the session in an active state.

Guía paso a paso para la resolución de problemas

1. Inicie el servicio Registro remoto en el VDA que se está probando:
    a) En el Panel de control, seleccione **Herramientas administrativas > Servicios**.
    b) Haga clic con el botón secundario en el **servicio Registro remoto** y seleccione **Propiedades**.
    c) En **Tipo de inicio**, seleccione **Automático** en el menú desplegable.



2. Desactive el firewall de Windows en el VDA que se está probando o cree una regla de firewall de entrada para habilitar el puerto 455:

    a) En el Panel de control, seleccione **Firewall de Windows Defender > Configuración avanzada**.

    b) Haga clic con el botón secundario en **Reglas de entrada** y seleccione **Nueva regla**.

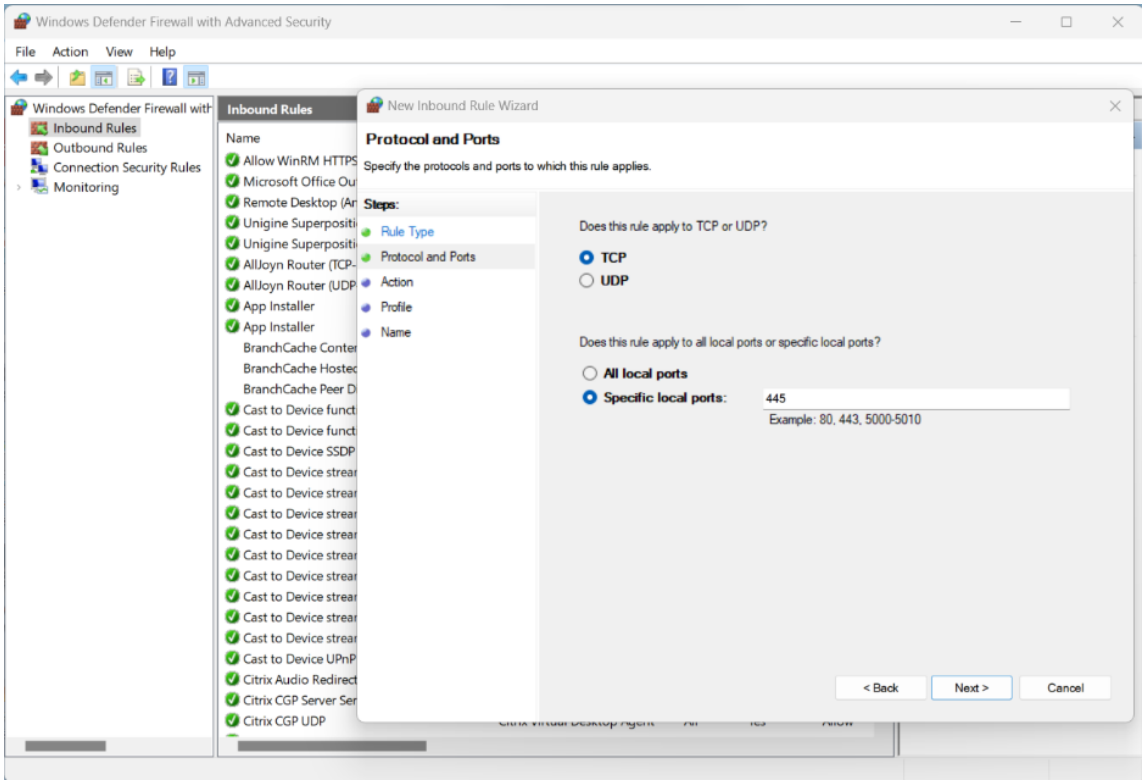
    c) En el **Asistente para nuevas reglas de entrada**, seleccione **Puerto**.

    d) En la página **Protocolos y puertos**, seleccione **TCP y Puertos locales específicos**. Introduzca 445 como puerto local.

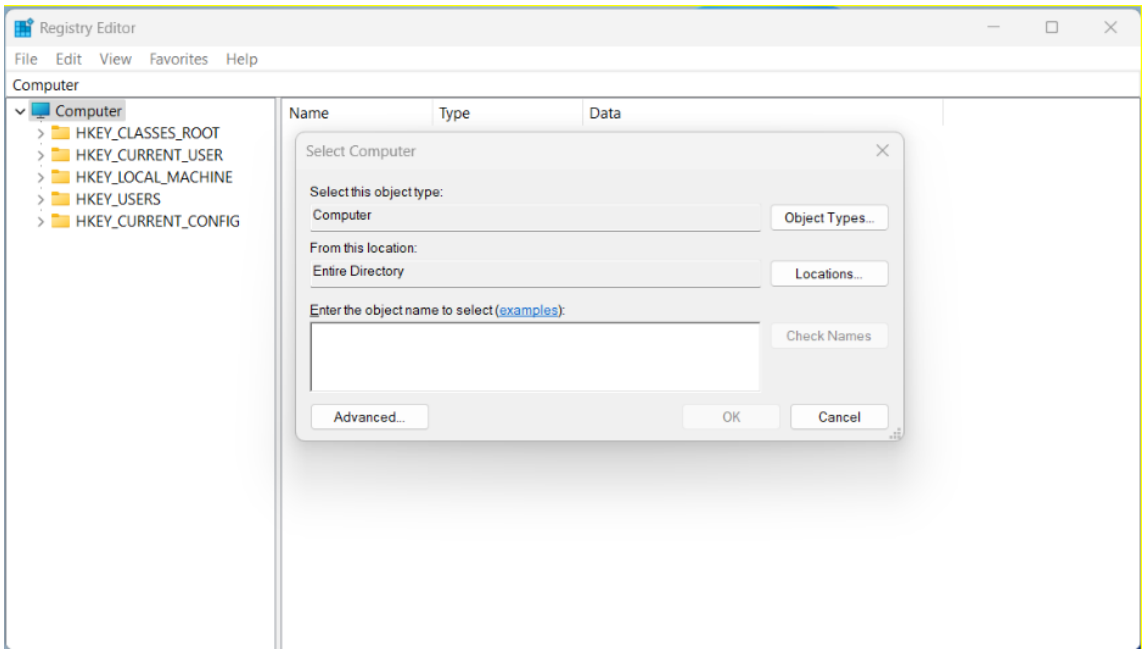
    e) En la página **Acción**, seleccione **Permitir la conexión**.

    f) Seleccione los perfiles de firewall a los que quiere aplicar la nueva regla de entrada.

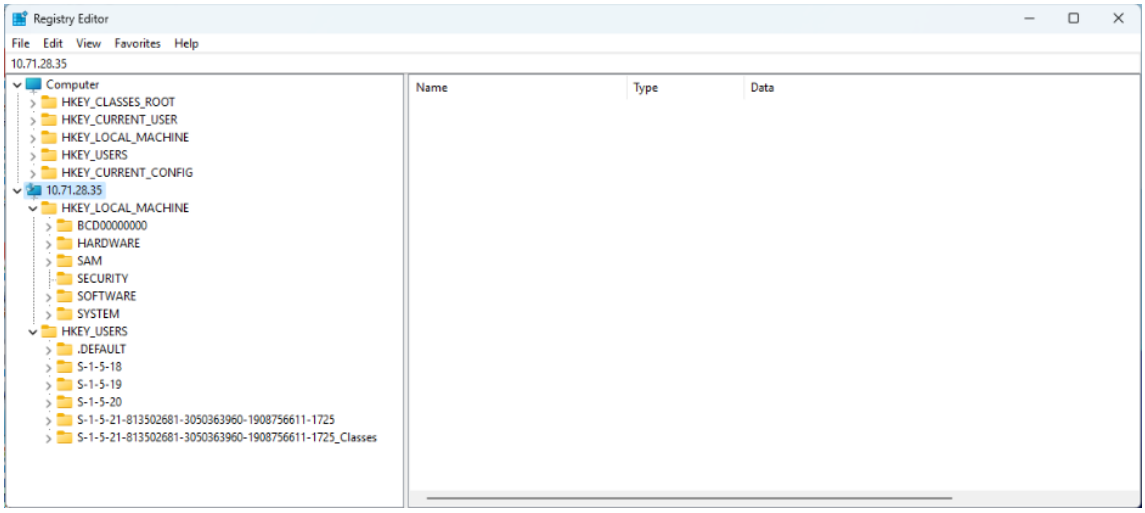
    g) Asigne un nombre a la regla de firewall y seleccione **Finalizar** para salir del **Asistente para nuevas reglas de entrada**.



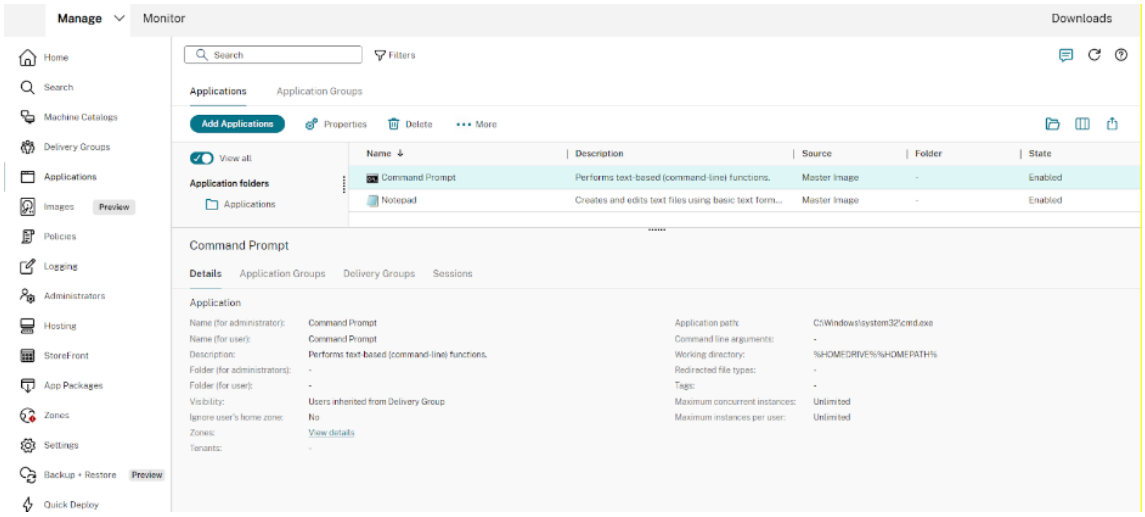
3. Desde otra máquina virtual del mismo dominio (puede ser DC, DDC u otro VDA), ejecute `Regedit` y conéctese a un registro remoto.



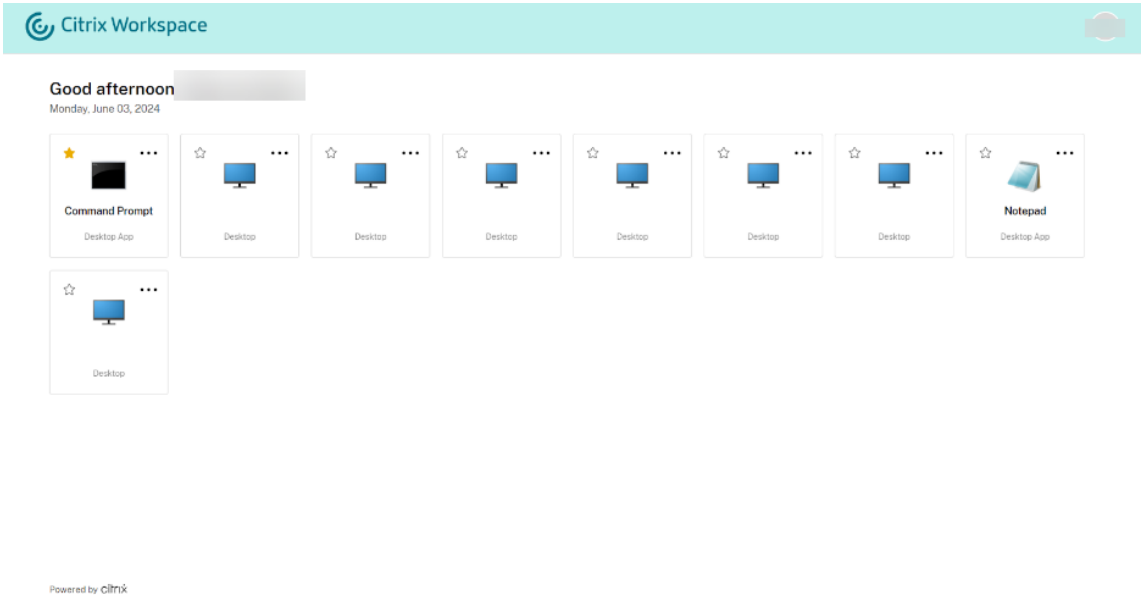
4. Introduzca la dirección IP del VDA que se está probando y haga clic en **Aceptar**. El árbol `regedit` debe mostrar las ramas del VDA que se está probando.



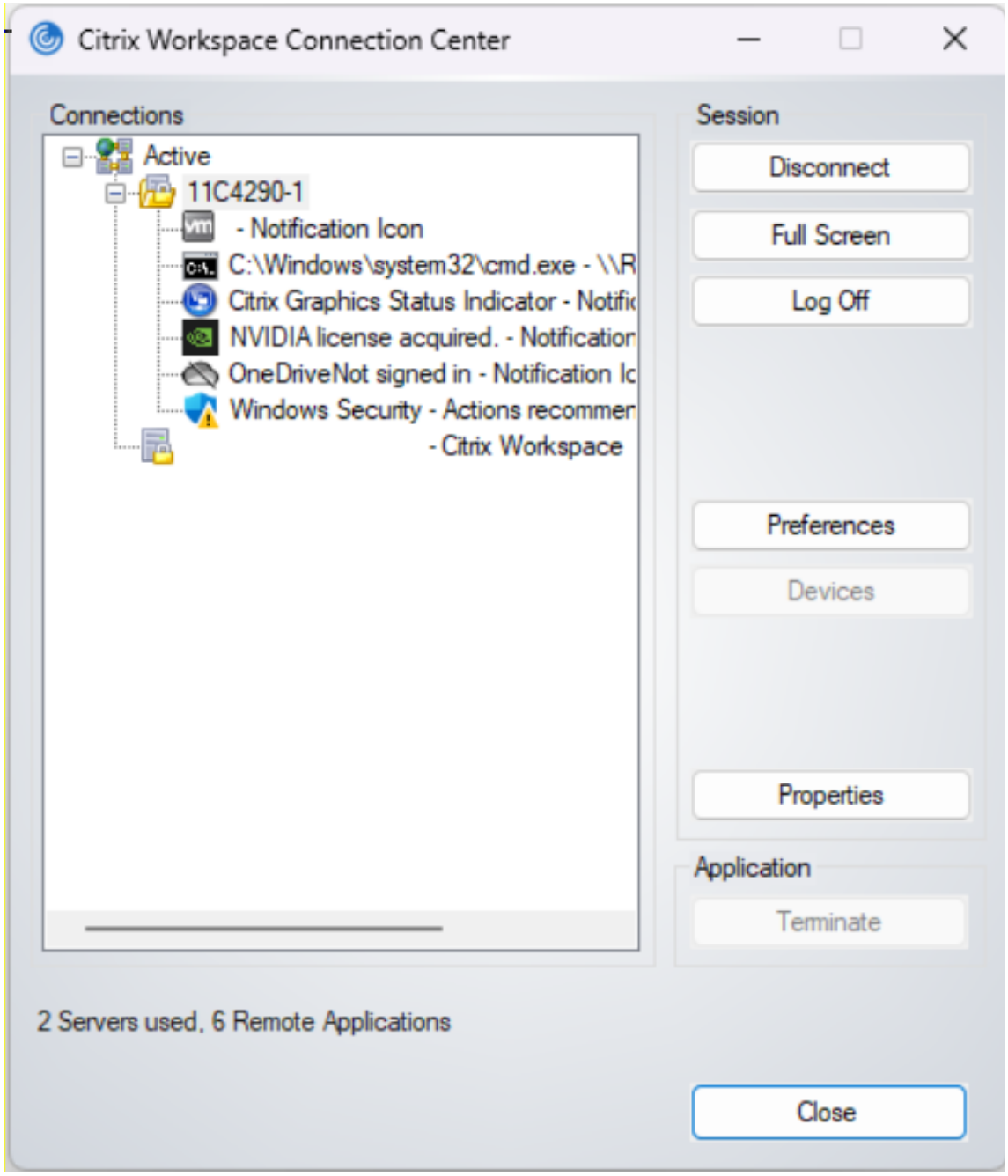
5. Abra la aplicación publicada **Símbolo del sistema**.



La aplicación **Símbolo del sistema** se muestra en Citrix Workspace.



6. Abra **Central de conexiones** en el cliente. Se usa para supervisar cuándo se cierra una sesión, después de cerrar una aplicación integrada abierta. Podemos ver en la siguiente imagen que el proceso de Símbolo del sistema `c:\Windows\system32\cmd.exe` está activo en la VDI remota.



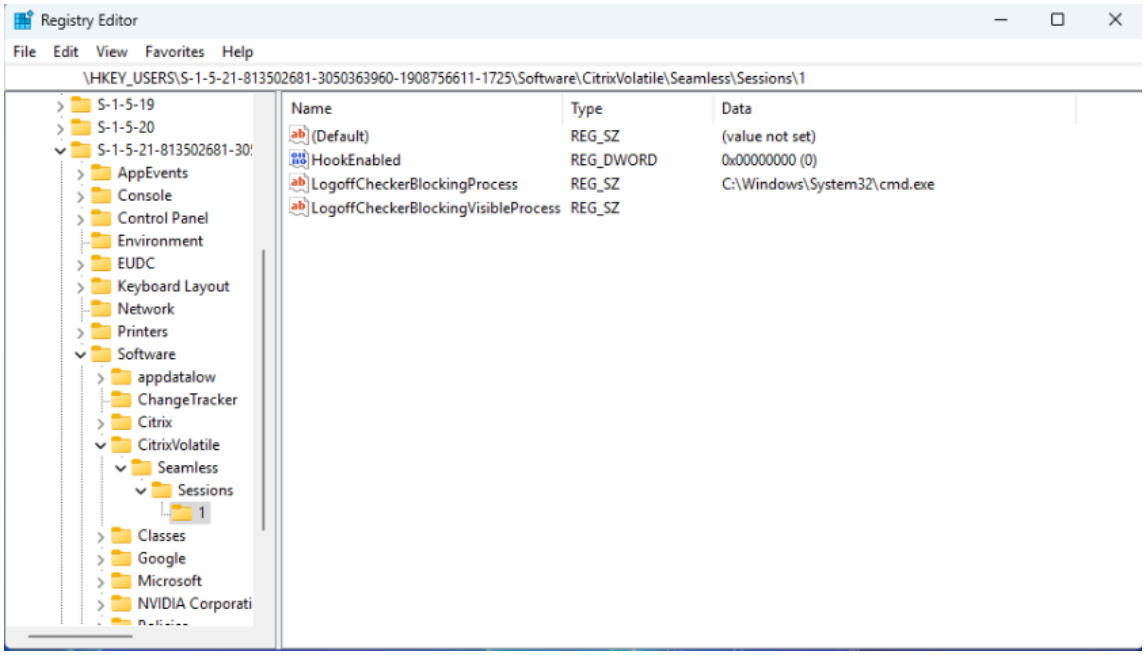
7. Desde el VDA en el que se ejecuta **regedit**, vaya a la siguiente ubicación IP remota: `HKEY_USERS\S-1-X-XX-XXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-XXXX\SOFTWARE\CitrixVolatile\Seamless\Sessions\X\`

   > **Note:**
   >
   > This path changes every time you open a new session.

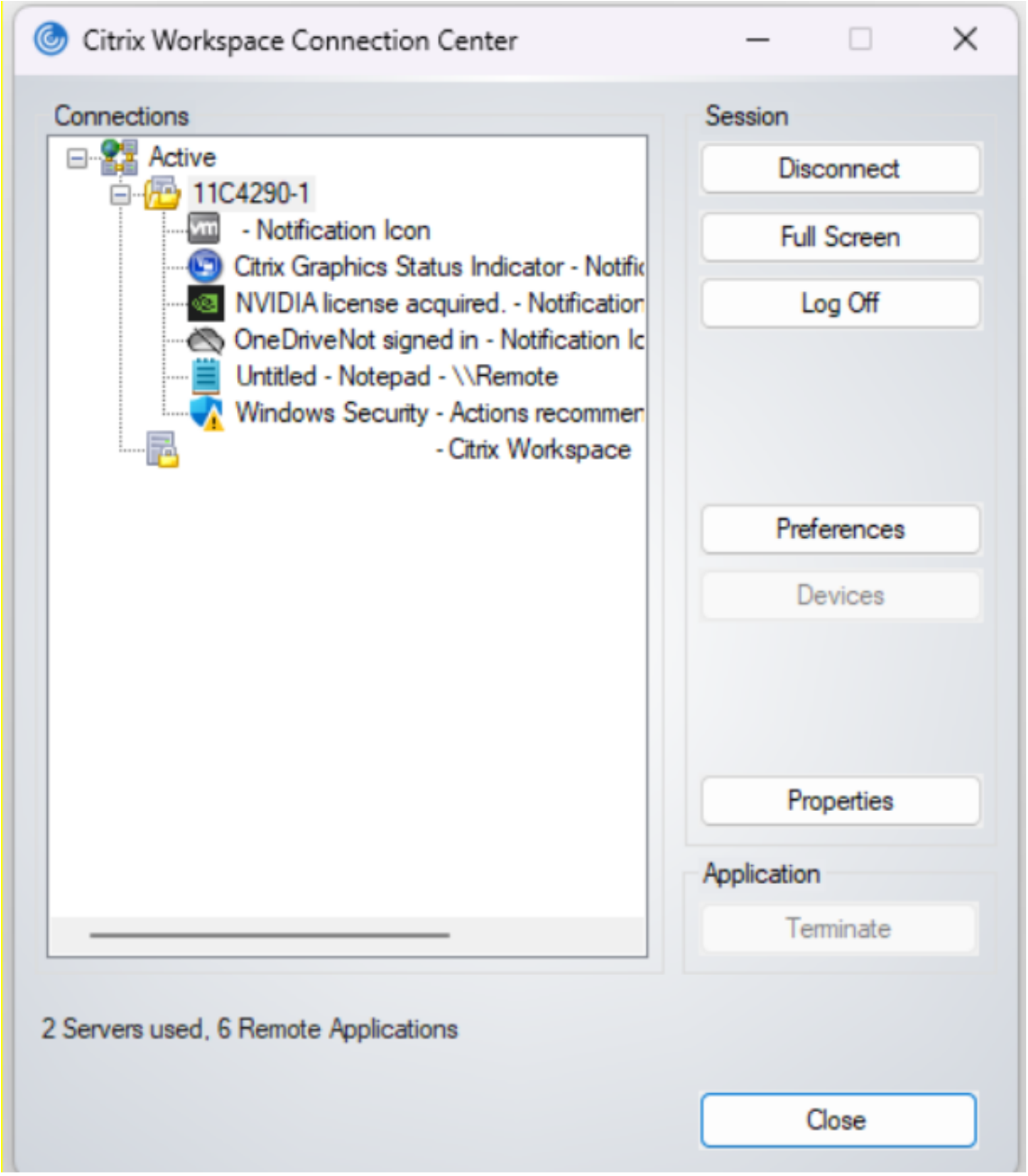
8. Hay dos claves para leer aquí (no las cambie aquí): **LogoffCheckBlockingProcess** y **LogoffCheckerBlockingVisibleProcess**. Estas claves muestran los programas que bloquean el

cierre de sesión. La primera debe mostrar `C:\Windows\System32\cmd.exe` ya que estaba abierto y aún no se ha cerrado.

> **Nota:**
>
> **LogoffCheckBlockingProcess** y **LogoffCheckerBlockingVisibleProcess** no se deben modificar manualmente. La modificación manual de estos valores de Registro podría dar lugar a sesiones inestables.

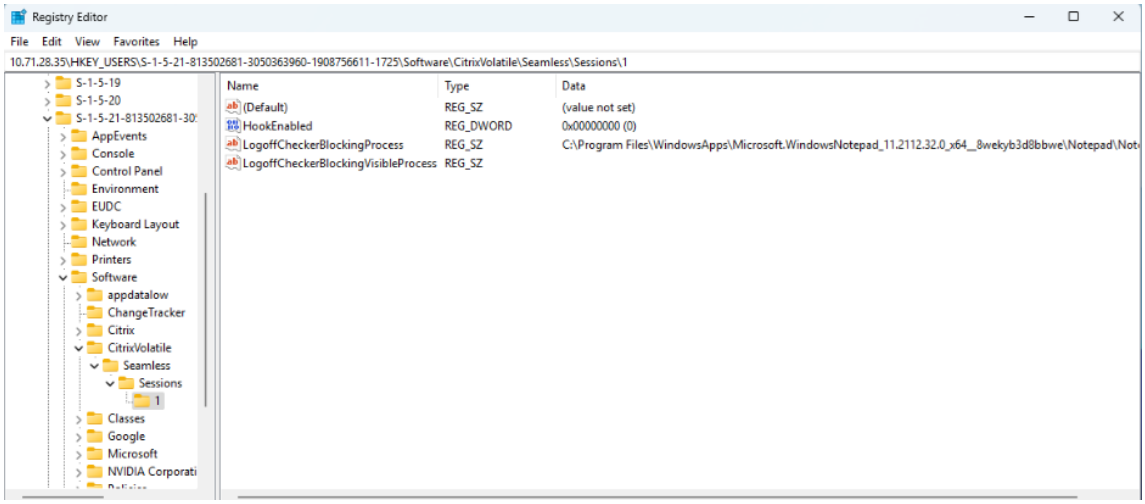


9. Haga clic en la **X** en la esquina superior derecha para salir de **Seamless CMD**.
10. Compruebe en Central de conexiones si la sesión se cierra. El cierre puede tardar hasta 30 segundos. Si se cierra, no ha habido ninguna aplicación o proceso que haya impedido cerrar sesión correctamente.



11. Si la sesión no se cerró, actualice la salida de **regedit** con F5.
12. Compruebe de nuevo el contenido de **LogoffCheckBlockingProcess** y **LogoffCheckerBlockingVisibleProcess**. CMD ya no debe estar presente, pero debería haber otro proceso en la lista. Cualquier proceso que esté bloqueando actualmente el cierre de sesión debe mostrarse aquí.

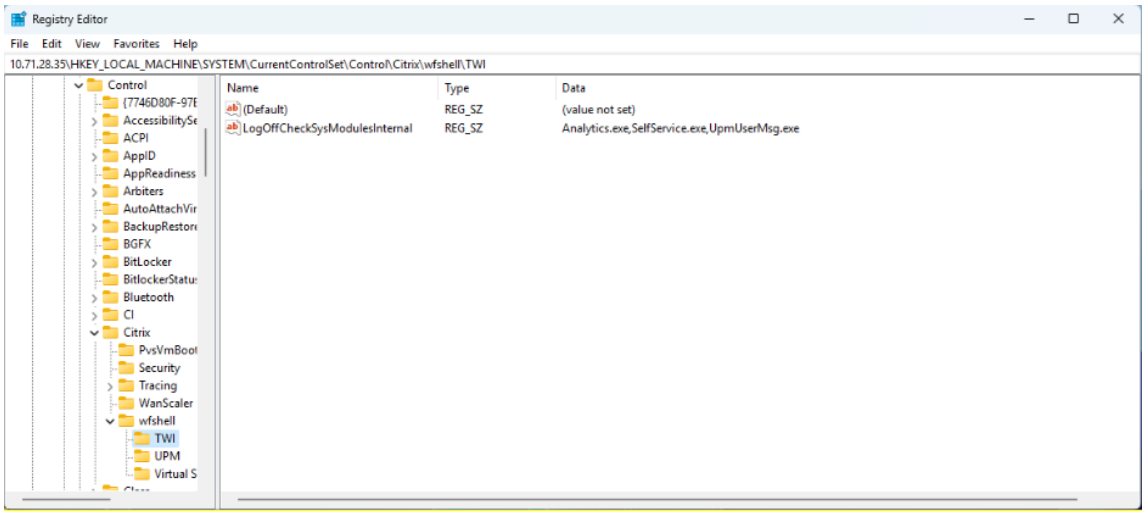
    En este caso, **Notepad.exe** está abierto desde el símbolo del sistema publicado antes de que se cerrara el símbolo del sistema, y este proceso de Notepada remoto está obstruyendo el cierre de sesión correcto.



13. Anote la ruta de acceso a este ejecutable y la clave en la que aparece e introdúzcala en la siguiente clave de Registro, en el árbol remoto:

    - Si aparece en **LogoffCheckBlockingProcess**: `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckSysModulesInternal`
    - Si aparece en **LogoffCheckerBlockingVisibleProcess**: `HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWILogoffCheckVisibleSysModules`

    > **Nota:**
    >
    > Si ya hay una o más entradas en la clave, agregue una coma al final y coloque la nueva entrada después de la coma.



14. Cierre la sesión desde Central de conexiones del cliente y abra de nuevo la aplicación remota.
15. Repita los pasos 9 a 16 hasta que la sesión se cierre automáticamente en un plazo de 30 segundos del cierre de la aplicación remota.

> **Nota:**
>
> Tras la solución de problemas, revierta los cambios temporales del firewall para permitir el acceso remoto al Registro si es necesario.

Cómo modificar LogonUI para ver el mensaje de renuncia de responsabilidades de Windows a tamaño completo al abrir aplicaciones publicadas

La escala de la ventana de **LogonUI** se ha mejorado para los casos en los que no tiene lugar la autenticación PassThrough. La ventana de **LogonUI** se escala en función de la resolución del monitor y la configuración de PPP usada, lo que garantiza que toda la ventana de **LogonUI** sea visible sin ningún recorte.

El tamaño de la ventana en píxeles también se puede configurar manualmente en el Registro.

1. Abra el **Editor del Registro** con `regedit` en el comando **Ejecutar**.
2. Vaya a `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\`.
3. Cree dos nuevas claves DWORD: **LogonUIWidth** y **LogonUIHeight**.
4. Establezca el valor de las claves en el ancho y el alto requeridos en píxeles para la ventana de **LogonUI**.

   Al configurar manualmente el tamaño de las ventanas de **LogonUI**, la escala automática está inhabilitada.

> **Nota:**
>
> Estas rutas de Registro han cambiado desde la versión 2407. Los valores de Registro antiguos son obsoletos y se ignoran.

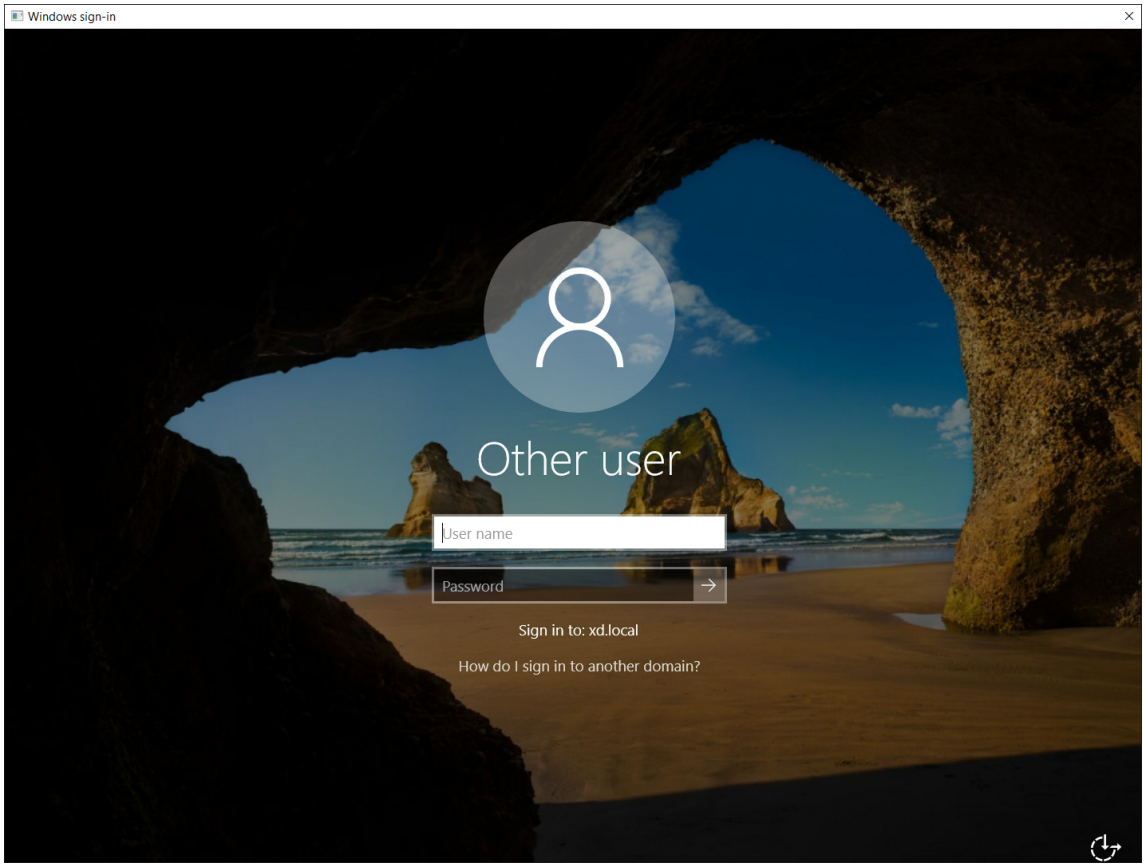
De forma predeterminada, la ventana de **LogonUI** incluye una barra de título con un botón de cierre que permite al usuario final desconectarse de la sesión si es necesario.

Inhabilitar una barra de mosaicos

Puede inhabilitar la barra de mosaicos en la ventana **LogonUI** con la siguiente clave de registro:

1. Abra el Editor del Registro con `regedit` en el comando **Ejecutar**.
2. Vaya a `HKEY_LOCAL_MACHINE\Software\Citrix\CtxHook\AppInit_DLLS\Seamless Hook\`.

3. Cree nuevas claves DWORD: **LogonUICaption** y establezca el valor de la clave en `0`.



Administrar carpetas de aplicaciones

De forma predeterminada, las aplicaciones nuevas agregadas a los grupos de entrega se colocan en una carpeta denominada **Aplicaciones**. Puede indicar otra carpeta 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 Web 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 `View Applications`. Para quitar, cambiar el nombre o eliminar una carpeta que contenga aplicaciones, debe tener el permiso de `Edit Application Properties` para todas las aplicaciones que contenga dicha carpeta.
- La mayoría de los procedimientos siguientes requieren acciones mediante la barra de acciones de Web Studio. También puede utilizar los menús contextuales o arrastrar el elemento. 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 la izquierda. 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 la barra de acciones. Escriba un nombre.
- **Para cambiar una carpeta:** Seleccione esa carpeta y, a continuación, seleccione **Mover carpeta** en la barra de 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).
- **Para cambiar el nombre de una carpeta:** Seleccione esa carpeta y, a continuación, seleccione **Cambiar nombre de carpeta** en la barra de acciones. Escriba un nombre.
- **Para eliminar una carpeta:** Seleccione esa carpeta y, a continuación, seleccione **Eliminar carpeta** en la barra de 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 esta 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 la barra de acciones. Seleccione la carpeta.

También puede colocar las aplicaciones que agrega en una carpeta en la página **Aplicación** al crear un grupo de entrega o un grupo de aplicaciones. De forma predeterminada, las aplicaciones 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 la aplicación `New-Broker` 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 Web Studio.
- Esta opción requiere, como mínimo: StoreFront 3.14, Citrix Receiver para Windows 4.11 y Delivery Controller 7.17.

Paquetes de aplicaciones

August 17, 2024

> **Nota:**
>
> Puede administrar la implementación de Citrix Virtual Apps and Desktops mediante dos consolas de administración: Web Studio (basada en la web) y Citrix Studio (basada en Windows). Este artículo se refiere únicamente a Web Studio. Para obtener información sobre Citrix Studio, consulte el artículo equivalente en Citrix Virtual Apps and Desktops 7 2212 o versiones anteriores.

Microsoft ofrece tres tecnologías de empaquetado para entregar aplicaciones a los usuarios: App-V, MSIX y conexión de aplicaciones MSIX. En este artículo se explica cómo implementar y entregar estas aplicaciones empaquetadas mediante **Web Studio > Paquetes de aplicaciones**:

- Implementar y entregar aplicaciones de App-V
- Implementar y entregar aplicaciones en formato MSIX y de conexión de aplicaciones MSIX

Implementar y entregar aplicaciones de App-V

En esta sección se incluye la siguiente información:

- Descripción general. Describe los métodos de administración para entregar y administrar los paquetes de App-V.
- Procedimientos. Muestra procedimientos para implementar y entregar estos paquetes.

Información general

En esta sección se describen los métodos de administración para entregar y administrar los paquetes de App-V. Para obtener más información sobre los componentes y conceptos con los que se interactúa al entregar aplicaciones empaquetadas de App-V, consulte la documentación de Microsoft: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-for-windows.

Puede utilizar estos métodos para entregar y administrar paquetes de App-V:

- **Administración dual**. Los paquetes de aplicaciones se configuran y se administran en servidores de App-V. Los servidores de Citrix Virtual Apps and Desktops y de App-V colaboran para entregar y administrar paquetes.

  Este método requiere que Citrix Virtual Apps and Desktops actualice periódicamente la vista de instantáneas del estado del servidor de App-V. Esto provoca una sobrecarga de hardware, infraestructura y administración. Los servidores de Citrix Virtual Apps and Desktops y de App-V deben permanecer sincronizados, especialmente para los permisos de usuario.

  La administración dual funciona mejor en implementaciones en las que App-V y su entorno están estrechamente unidos:

  - **Servidor de administración de App-V**. Publica y administra el ciclo de vida de paquetes de App-V y los archivos de configuración dinámica.
  - **Componente Citrix Personalization** instalado en máquinas VDA. Administre el registro del servidor de publicación de App-V adecuado que se necesite para el inicio de aplicaciones.

  Este método garantiza que, en un momento dado, el servidor de publicación de App-V esté sincronizado para el usuario. El servidor de publicación mantiene otros aspectos del ciclo de vida de los paquetes, como, por ejemplo, la actualización en inicios de sesión y grupos de conexión.

- **Administración única**. Los paquetes de aplicaciones se almacenan en recursos compartidos de red. Citrix Virtual Apps and Desktops entrega y administra paquetes de forma independiente.

  Este método reduce la sobrecarga porque los servidores de App-V y la infraestructura de bases de datos no son necesarios en la implementación.

En este método, se almacenan paquetes de App-V en un recurso compartido de red y se cargan sus metadatos desde esa ubicación en su entorno. A continuación, el componente Citrix Personalization instalado en las máquinas VDA administra y entrega las aplicaciones de la siguiente manera:

- Procesan los archivos de configuración de implementación y los archivos de configuración de usuario cuando se inicie una aplicación.
- Gestionan todos los aspectos de los ciclos de vida de los paquetes en la máquina host.

Puede usar los dos 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 presentes en servidores de App-V o en recursos compartidos 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).

Procedimientos

Para poder entregar aplicaciones de App-V, debe instalar el componente Citrix Personalization en las máquinas VDA. Consulte Instalar el componente Citrix Personalization en máquinas VDA para obtener información detallada.

Para entregar aplicaciones empaquetadas de App-V a sus usuarios, siga estos pasos:

1. Almacenar paquetes de aplicaciones en recursos compartidos de red.
2. Cargue paquetes de aplicaciones en su entorno.
3. Agregar aplicaciones a grupos de entrega.
4. Para habilitar la entrega automática de paquetes de App-V interdependientes, cree grupos de aislamiento.

Para que Citrix Virtual Apps and Desktops reconozca y aplique los archivos de configuración dinámica de App-V con el método de administración única, consulte este blog de Citrix.

Implementar y entregar aplicaciones en formato MSIX y de conexión de aplicaciones MSIX

En esta sección se incluye la siguiente información:

- Descripción general. Describe cómo se entregan y se administran los paquetes en formato MSIX y de conexiones de aplicaciones MSIX.
- Procedimientos. Muestra procedimientos para implementar y entregar estos paquetes.

Información general

Citrix Virtual Apps and Desktops entrega las aplicaciones en formato MSIX y de conexión de aplicaciones MSIX a los usuarios a través del componente Citrix Personalization instalado en las máquinas VDA. Este componente gestiona todos los aspectos de los ciclos de vida de los paquetes en la máquina host.

Para obtener más información sobre el formato MSIX y de conexión de aplicaciones MSIX, consulte la documentación de Microsoft: https://docs.microsoft.com/en-us/windows/msix/ y https://docs.microsoft.com/en-us/azure/virtual-desktop/what-is-app-attach, respectivamente.

Procedimientos

Para permitir la entrega de paquetes en formato MSIX y de conexión de aplicaciones MSIX debe instalar el componente Citrix Personalization en las máquinas VDA. Consulte Instalar el componente Citrix Personalization en máquinas VDA para obtener información detallada.

Para entregar aplicaciones en formato MSIX y de conexión de aplicaciones MSIX a sus usuarios, siga estos pasos:

1. Almacenar paquetes de aplicaciones en recursos compartidos de red.
2. Cargue paquetes de aplicaciones en su entorno.
3. Agregar aplicaciones a grupos de entrega.

Instalar el componente Citrix Personalization en máquinas VDA

El componente Citrix Personalization administra el proceso de publicación de los paquetes de aplicaciones en formato App-V, MSIX y de conexión de aplicaciones MSIX. Este componente no se instala de forma predeterminada cuando se instala un VDA. Puede instalar el componente durante o después de la instalación del VDA.

Para instalarlo durante la instalación del VDA, use una de estas opciones:

- En el asistente de instalación, vaya a la página **Componentes adicionales** y, a continuación, marque la casilla **Citrix Personalization para App-V: VDA**.
- En la interfaz de línea de comandos, use la opción **/includeadditional "Citrix Personalization para App-V: VDA"**.

Para instalar el componente después de la instalación del VDA, siga estos pasos:

1. En la máquina VDA, vaya a **Panel de control > Programas > Programas y funciones**, haga clic con el botón secundario en **Citrix Virtual Delivery Agent** y, a continuación, seleccione **Cambiar**.

2. En el asistente que aparece, vaya a la página **Componentes adicionales** y, a continuación, marque la casilla **Citrix Personalization para App-V: VDA**.

> **Nota:**
>
> El cliente de escritorio de Microsoft App-V es el componente que ejecuta aplicaciones virtuales de paquetes App-V en dispositivos de usuario. Windows 10 (1607 o una versión posterior) y Windows Server 2019 ya incluyen este software cliente de App-V. Solo tiene que habilitarlo en máquinas VDA. Para obtener más información, consulte este artículo de la documentación de Microsoft: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-enable-the-app-v-desktop-client.

Almacenar paquetes de aplicaciones en recursos compartidos de red

Después de configurar la infraestructura, genere los paquetes de aplicaciones y guárdelos en una ubicación de red, como un recurso compartido de red UNC o SMB, o en un recurso compartido de archivos de Azure.

Estos son los pasos detallados:

1. Genere paquetes de aplicaciones. Consulte la documentación de Microsoft para obtener más detalles.
2. Almacene paquetes de aplicaciones en una ubicación de red:
    - Para la **administración única de App-V**: Almacene los paquetes y los archivos de configuración dinámica (App-V) correspondientes en un recurso compartido de red UNC o SMB, o en un recurso compartido de archivos de Azure.
    - Para la **administración dual de App-V**: 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.)
    - Para el **formato MSIX o de conexión de aplicaciones MSIX**: Almacene los paquetes en un recurso compartido de red UNC o SMB o en un recurso compartido de archivos de Azure.
3. Asegúrese de que el VDA tenga permiso de lectura en la ruta de almacenamiento de paquetes:
    - Si almacena paquetes en un recurso compartido de red UNC o SMB en su dominio de AD, conceda permiso de lectura a la máquina VDA para leer la ruta de almacenamiento. Para hacerlo, puede conceder el permiso de lectura de la cuenta de AD de la máquina al recurso compartido de forma explícita o incluir la cuenta en un grupo de AD que tenga ese permiso.
    - Si almacena paquetes en un recurso compartido de archivos de Azure, primero conceda permiso de lectura a una cuenta de usuario para leer la ruta de almacenamiento en Azure.

A continuación, configure el servicio `ctxAppVService` que se ejecuta en la máquina VDA para que use esa cuenta de usuario para acceder a la ruta de almacenamiento de paquetes. Consulte la siguiente sección para conocer los pasos detallados.

Cambiar la cuenta de inicio de sesión del usuario

El VDA llama a `ctxAppVService` para acceder a las rutas de almacenamiento de paquetes. De forma predeterminada, `ctxAppVService` accede a las rutas de almacenamiento de paquetes mediante la **cuenta del sistema local** de la máquina. Este tipo de autenticación de máquina funciona en los dominios de AD. Sin embargo, no funciona en los casos de integración de AD y Azure AD, los cuales requieren autenticación basada en cuentas de usuario.

Si almacena paquetes en un recurso compartido de archivos de Azure, cambie la cuenta de inicio de sesión de `ctxAppVService` a una cuenta de usuario que tenga permiso de lectura en la ruta de almacenamiento de paquetes. Estos son los pasos detallados:

1. Inicie **Servicios**, haga clic con el botón secundario en **ctxAppVService** y seleccione **Propiedades**.
2. En la ficha **Iniciar sesión**, seleccione **Esta cuenta**, introduzca una cuenta de usuario que tenga permiso de lectura para la ruta de almacenamiento de paquetes y, a continuación, introduzca la contraseña del usuario dos veces.
3. Haga clic en **Aceptar**.

Cargar paquetes de aplicaciones en su entorno

Después de almacenar los paquetes de aplicaciones en una ubicación de red según sea necesario, cárguelos en su entorno para su entrega. Utilice uno de estos métodos según sea necesario:

- Carga en bloque
- Cargar uno a uno

Preparativos

Citrix Virtual Apps and Desktops usa una máquina VDA para establecer la conexión con la ubicación de red para la detección de paquetes. Por lo tanto, cree un grupo de entrega de antemano y asegúrese de que al menos un VDA del grupo cumpla con estos requisitos:

- Versión de VDA:
  - Para detectar paquetes de App-V: 2203 o versiones posteriores

  - Para detectar paquetes en formato MSIX y de conexión de aplicaciones MSIX: 2209 o posterior

- Componente de Citrix Personalization para App-V: Instalado
- Permiso en la ubicación del paquete: Lectura (consulte el paso 2: Almacenar paquetes de aplicaciones en recursos compartidos de red para obtener más información).
- Encendido
- Estado: Registrado

Cargar paquetes de aplicaciones en bloque

Cargue paquetes de una ubicación de red en su entorno. Asegúrate de tener estos elementos listos antes de cargarlos:

- Un grupo de entrega que cumpla con los requisitos indicados en Preparación
- La ruta de la ubicación de red

Para cargar paquetes en bloque, sigue estos pasos:

1. En el panel de la izquierda, seleccione **Paquetes de aplicaciones**.
2. En la ficha **Orígenes**, haga clic en el botón **Agregar origen**. Aparecerá la página **Agregar origen**.
3. En el campo **Nombre**, introduzca un nombre descriptivo del origen del paquete.
4. En el campo **Grupo de entrega**, haga clic en **Seleccione un grupo de entrega**. A continuación, seleccione un grupo de entrega que cumpla los requisitos establecidos en Preparación y, a continuación, haga clic en **Aceptar**.
5. En el campo **Tipo de ubicación**, seleccione **Servidor de Microsoft App-V** o **Recurso compartido de red** según el lugar en el que almacene los paquetes y, a continuación, complete los parámetros correspondientes:

   - Si selecciona **Servidor de Microsoft App-V**, introduzca esta información:
     - URL del servidor de administración. Ejemplo:`http://appv-server.example.com`
     - Credenciales de inicio de sesión del administrador del servidor de administración.
     - URL y número de puerto del servidor de publicación. Ejemplo:`http://appv-server.example.com:3330`
   - Si seleccionó **Recurso compartido de red**, especifique esta información:
     - Introduzca la ruta UNC del recurso compartido de red. Ejemplo:`\\PackageServer\apps\`
     - Seleccione los tipos de paquetes que quiere cargar. Las opciones incluyen App-V, MSIX y conexión de aplicaciones MSIX.

- Especifique si quiere buscar paquetes en las subcarpetas.

6. Haga clic en **Agregar origen**.

   La página Agregar origen se cierra y el origen recién agregado aparece en la lista de orígenes. Citrix Virtual Apps and Desktops carga los paquetes en su entorno mediante un VDA del grupo de entrega. Una vez completada la carga, el campo Estado muestra *Importación correcta*. Los paquetes correspondientes aparecen en la ficha **Paquetes**.

   > **Nota:**
   >
   > Para comprobar si hay actualizaciones de paquetes en la ubicación de un origen e importarlas en su entorno, seleccione la ubicación en la lista de orígenes y haga clic en **Buscar actualizaciones de paquetes**.

Cargar paquetes de aplicaciones uno a uno

Cargue un paquete de aplicaciones desde un recurso compartido de red en su entorno. Antes de cargarlo, asegúrate de tener estos elementos listos:

- Un grupo de entrega que cumpla con los requisitos establecidos en Preparación
- La ruta de la ubicación de red.

Para cargar un paquete en su entorno, siga estos pasos:

1. En el panel de la izquierda, seleccione **Paquetes de aplicaciones**.
2. En la ficha **Paquetes**, haga clic en el botón **Agregar paquete**. Aparecerá la página **Agregar paquete**.
3. En el campo **Grupo de entrega**, haga clic en **Seleccione un grupo de entrega**. A continuación, seleccione un grupo de entrega que cumpla los requisitos establecidos en Preparación y, a continuación, haga clic en **Aceptar**.
4. En el campo **Ruta completa del paquete**, introduzca una ruta según sea necesario:

   - Para cargar varios paquetes a la vez, introduzca sus rutas completas, separadas por punto y coma (`;`). Ejemplo:`\\Package-Server\apps\office365.appv;\\Package-Server\apps\skype.msix;\\Package-Server\apps\slack.vhd`
   - Para cargar todos los paquetes presentes en un recurso compartido de red, introduzca la ruta de almacenamiento. Ejemplo: \servidor-paquetes\aplicaciones\

5. Haga clic en **Agregar paquete**.

   El paquete de aplicaciones aparece en la ficha **Paquetes**.

Agregar aplicaciones a grupos de entrega

Una vez que se haya cargado por completo un paquete de aplicaciones, agregue sus aplicaciones a uno o más grupos de entrega según sea necesario. Como resultado, los usuarios asociados a esos grupos de entrega pueden acceder a las aplicaciones.

Para agregar una o más aplicaciones de un paquete a varios grupos de entrega, siga estos pasos:

1. En el panel de la izquierda, seleccione **Paquetes de aplicaciones**.
2. En la ficha **Paquetes**, seleccione el paquete que necesite.
3. En la barra de acciones, haga clic en **Agregar grupos de entrega**. Aparecerá la página Agregar grupos de entrega.
4. Seleccione una o más aplicaciones del paquete en función de sus necesidades y, a continuación, haga clic en **Siguiente**.
5. En la lista de grupos de entrega, seleccione los grupos a los que quiere asignar las aplicaciones y, a continuación, haga clic en **Siguiente**.
   Nota: Si seleccionó un paquete en formato MSIX o de conexión de aplicaciones MSIX, solo se mostrarán en la lista los grupos de entrega cuyo nivel funcional sea 2106 o posterior.
6. Haga clic en **Finalizar**.

También puede agregar aplicaciones empaquetadas a un grupo de entrega cuando:

- Se crea un grupo de entrega. Para obtener más información, consulte Crear grupos de entrega.
- Se modifica n grupos de entrega o grupos de aplicaciones existentes. Para obtener más información, consulte Agregar aplicaciones.

(Opcional) Crear grupos de aislamiento para paquetes de App-V

Puede crear grupos de aislamiento para habilitar la entrega automática de paquetes de App-V interdependientes.

> **Nota:**
>
> Los grupos de aislamiento son compatibles con el método de administración única de App-V. Si usa el método de administración dual de App-V, puede lograr el mismo objetivo mediante la creación de *grupos de conexiones* en la infraestructura de Microsoft App-V. Para obtener más información, consulte este artículo de la documentación de Microsoft: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-connection-group-file.

Acerca de los grupos de aislamiento

Un grupo de aislamiento es una colección de paquetes de aplicaciones interdependientes que deben ejecutarse en el mismo espacio aislado de Windows para crear un entorno virtual. Los grupos de

aislamiento de App-V de Citrix son similares, pero no idénticos, a los grupos de conexión de App-V. Un grupo de aislamiento incluye dos tipos de paquetes:

- Paquetes de aplicaciones **explícitas**. Aplicaciones con requisitos específicos de licencia. Puede restringir esas aplicaciones a un grupo específico de usuarios al agregarlas a grupos de entrega.
- Paquetes de aplicaciones **automáticas**. Aplicaciones que están siempre disponibles para todos los usuarios, independientemente de si se agregan a grupos de entrega.

Por ejemplo: la aplicación app−a requiere JRE 1.7 para ejecutarse. Puede crear un grupo de aislamiento que contenga app-a (marcada como *Explícita*) y JRE 1.7 (marcada como *Automática*). A continuación, agregue el paquete de App-V de app−a a uno o más grupos de entrega. Cuando un usuario inicie la aplicación A, JRE 1.7 se implementará automáticamente con ella.

Cuando un usuario inicia una aplicación de App-V marcada como *Explícita* en un grupo de aislamiento, Citrix Virtual Apps and Desktops comprueba los permisos de acceso del usuario a la aplicación en los grupos de entrega. Si el usuario tiene permiso para acceder a la aplicación, todos los paquetes de aplicaciones *automáticas* del mismo grupo de aislamiento estarán disponibles para el usuario.

No es necesario agregar los paquetes *automáticos* a ningún grupo de entrega. Si hay otro paquete de aplicaciones *explícitas* en el grupo de aislamiento, ese paquete estará disponible para el usuario solo si está en el mismo grupo de entrega.

Para obtener más información sobre los grupos de aislamiento, consulte este blog de Citrix.

Crear un grupo de aislamiento de App-V Cree un grupo de aislamiento y agréguele paquetes de aplicaciones interdependientes. Estos son los pasos detallados:

1. En la ficha **Grupos de aislamiento**, haga clic en **Agregar grupo de aislamiento**.
2. Introduzca un nombre y una descripción para el grupo de aislamiento. Todos los paquetes de aplicaciones de su entorno aparecen en la lista **Paquetes disponibles**.
3. En la lista **Paquetes disponibles**, seleccione la aplicación que necesite y, a continuación, haga clic en la flecha de la derecha. Las aplicaciones seleccionadas aparecen en la lista **Paquetes en grupo de aislamiento**.
4. En el campo **Implementación**, seleccione **Explícita** o **Automática** para la aplicación.
5. Repita los pasos 2 y 3 para agregar más paquetes.
6. Para ajustar el orden de los paquetes de la lista, haga clic en la flecha hacia arriba o hacia abajo.
7. Haga clic en **Guardar**.

> **Nota:**
>
> Las configuraciones de grupos de aislamiento resultan en la creación de grupos de conexiones de App-V en el VDA. Los casos de implementación pueden volverse complejos, y el cliente de App-V admite paquetes que solo están en un grupo de conexiones activo a la vez. Le recomendamos

> no agregar el mismo paquete a dos grupos de aislamiento diferentes que se hayan agregado al mismo grupo de entrega.

Publicar aplicaciones empaquetadas en VDA de escritorio compartido o de sesión única

Ahora puede entregar paquetes adjuntos de aplicaciones de App-V, MSIX y MSIX a sus sesiones de VDA de escritorio compartido o de sesión única directamente a través de grupos de entrega. Puede acceder a las aplicaciones empaquetadas de su VDA de escritorio al iniciar sesión en función de los permisos de accesibilidad establecidos en las aplicaciones.

Ventajas

- Las aplicaciones están disponibles en el VDA al iniciar sesión y no se pueden organizar bajo demanda a través de Workspace o StoreFront.
- Mejora del tiempo de inicio al acceder a las aplicaciones empaquetadas.
- Facilita el mantenimiento de las aplicaciones empaquetadas de forma independiente, separada de la imagen base del VDA.

Consideraciones

- Esta opción solo está disponible para VDA de sesión única a través del SDK de PowerShell apropiado. No está disponible actualmente en el flujo de trabajo de Web Studio. La publicación en escritorios compartidos se puede realizar con el SDK de PowerShell o de la forma existente a través del flujo de trabajo de Web Studio. Para obtener más información sobre el procedimiento actual, consulte Agregar aplicaciones a los grupos de entrega.
- Las solicitudes deben formar parte de un grupo de entrega.

Antes de comenzar

- Asegúrese de que las aplicaciones empaquetadas estén firmadas y disponibles en la ubicación de archivos compartidos o UNC. Para obtener más información, consulte Almacenar paquetes de aplicaciones en recursos compartidos de red.
- Instalar el componente Citrix Personalization en máquinas VDA.

Procedimiento

Para entregar aplicaciones empaquetadas a los VDA de escritorio, siga estos pasos:

1. Importe paquetes de aplicaciones a Web Studio.
2. Publique la BrokerApplication empaquetada.
3. Limite la visibilidad de las aplicaciones en Web Studio.

Importar paquetes de aplicaciones a Web Studio

1. Abra un explorador web. Escriba `https://<address of the server hosting Web Studio>/Citrix/Studio`.
2. Cree un grupo de entrega. Para obtener más información, consulte Crear grupos de entrega.
3. Importe los paquetes de aplicaciones a Web Studio. Para obtener más información, consulte Cargar paquetes de aplicaciones de forma masiva.

Publicar la aplicación empaquetada en BrokerApplication

Si está publicando en un VDA multisesión (compartido) o en un VDA de aplicaciones de sesión única, el procedimiento de publicación es el mismo. Para obtener más información, consulte Agregar aplicaciones a los grupos de entrega.
Si va a publicar en un VDA de escritorio de sesión única, haga lo siguiente:

Ejecute los siguientes comandos de PowerShell en el Delivery Controller:

1. Para recuperar los comandos presentes en el paquete:

   ```
   Import-Module "D:\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.v1.psm1"
   ```

   > **Nota:**
   >
   > La versión del `App-V package discovery module` que tiene disponible esta funcionalidad se encuentra en la ISO de Citrix Virtual Apps and Desktops (2311 o versiones superiores) en la ruta anterior.

2. Para obtener los ID de los grupos de entrega y los ID de las aplicaciones empaquetadas pertinentes:

   ```
   Get-BrokerDesktopGroup | Format-Table Uid, Name
   Get-AppLibAppVApplication | Format-Table Uid, Name
   ```

3. Para publicar los paquetes y crear las configuraciones de BrokerMachine adecuadas:

   ```
   Publish-PackagedApplication -AppLibararyApplicationUid <AppLibararyApplica
   .Uid > -DesktopGroupUid <DesktopGroup.Uid>
   ```

4. Para sincronizar las configuraciones del Broker, que luego se envían al agente del Broker en el VDA:


```
Update-DesktopGroupMachineConfigurations -DesktopGroupUid <
DesktopGroup.Uid>
```

> **Nota:**
>
> Asegúrese de ejecutar el comando PowerShell `Update-DesktopGroupMachineConfigurations` después de publicar o quitar aplicaciones empaquetadas de un VDA.

Limite la visibilidad de las aplicaciones en Web Studio

De forma predeterminada, los usuarios tienen todas las aplicaciones empaquetadas asignadas al grupo de entrega que sirva a su VDA disponibles en su sesión de escritorio. Puede controlar la visibilidad de las aplicaciones empaquetadas en los VDA de escritorio configurando la visibilidad de las aplicaciones para usuarios o grupos específicos en Web Studio. Para administrar la visibilidad de las aplicaciones empaquetadas, consulte Cambiar las propiedades de la aplicación.

Aplicaciones de la Plataforma universal de Windows

August 17, 2024

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.

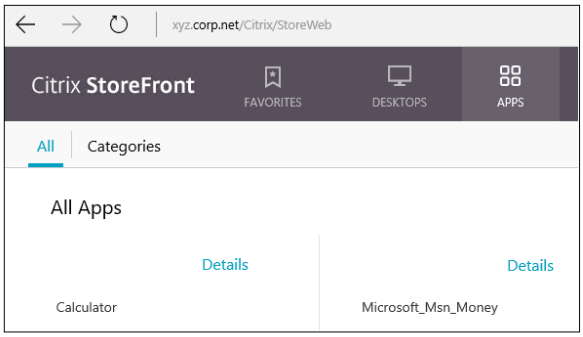
Durante la carga lateral, la aplicación UWP se instala en la máquina y empieza a estar disponible para otros usuarios. Cuando otro usuario inicia la aplicación, esta se instala, y el sistema operativo actualiza su base de datos de AppX para indicar que ese usuario la ha instalado.

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.

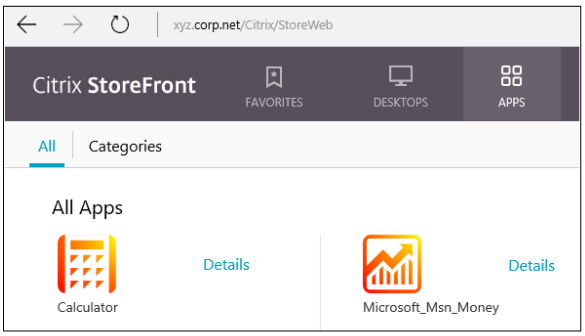
Es posible que los nombres principales y las descripciones de las aplicaciones UWP no sean correctos. Modifique y corrija esas propiedades al agregar las aplicaciones a un grupo de entrega.

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 con 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.



Before



After

En Windows Server 2016 y versiones posteriores, es posible que el Administrador del servidor también se inicie cuando se inicie una aplicación UWP. Para evitar que esto ocurra, puede impedir que el Administrador del servidor se inicie automáticamente durante el inicio de sesión con la clave de Registro `HKLM\Software\Microsoft\ServerManager\DoNotOpenServerManagerAtLogon`. Para obtener información detallada, consulte https://blogs.technet.microsoft.com/rmilne/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 inhabilitar el uso de aplicaciones universales 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.

Autoscale

August 17, 2024

> **Nota:**
>
> Puede administrar la implementación de Citrix Virtual Apps and Desktops mediante dos consolas de administración: Web Studio (basada en la web) y Citrix Studio (basada en Windows). Esta función solo está disponible en Web Studio.

Autoscale es una función que ofrece una solución robusta y de alto rendimiento para administrar de forma proactiva la energía de sus máquinas. Su objetivo es equilibrar los costes y la experiencia de usuario.

Autoscale permite administrar de forma proactiva la energía de todas las máquinas con SO de sesión única y de SO multisesión registradas en un grupo de entrega.

Las funciones de Autoscale incluyen:

- Parámetros basados en la programación y en la carga
- Tiempos de espera de sesión dinámicos
- Autoscale de máquinas etiquetadas (ampliación en la nube)
- Notificaciones de cierre de sesión del usuario

Plataformas compatibles de alojamiento de VDA

Autoscale es compatible con todas las plataformas compatibles con Citrix Virtual Apps and Desktops. Esto incluye varias plataformas de infraestructura en la nube, como XenServer, Amazon Web Services, Google Cloud Platform, Microsoft Azure Resource Manager, VMware vSphere y muchas más. Para

obtener una lista completa de las plataformas compatibles, consulte los requisitos del sistema para Citrix Virtual Apps and Desktops.

> **Nota:**
>
> Al agregar conexiones de host de nube pública a una implementación, necesita una licencia de derechos híbridos. Para obtener información sobre la licencia de derechos híbridos, consulte Transición e intercambios (TTU) con derechos híbridos. Para obtener información sobre cómo agregar una licencia, consulte Crear un sitio.

Cargas de trabajo admitidas

Autoscale admite grupos de entrega tanto de SO multisesión como de SO de sesión única. Hay tres interfaces de usuario a tener en cuenta:

- Interfaz de usuario de Autoscale para grupos de entrega de SO multisesión (antes denominados grupos de entrega de RDS)
- Interfaz de usuario de Autoscale para grupos de entrega aleatorios (agrupados) de SO de sesión única (antes denominados grupos de entrega de VDI agrupados)
- Interfaz de usuario de Autoscale para grupos de entrega estáticos de SO de sesión única (antes denominados grupos de entrega de VDI estáticos)

Para obtener más información sobre las interfaces de usuario para diferentes grupos de entrega, consulte Interfaces de usuario de Autoscale.

Ventajas

La función Autoscale ofrece las siguientes ventajas:

- Ofrezca un mecanismo único y coherente para administrar la energía de las máquinas de un grupo de entrega.
- Garantice la disponibilidad y el control de los costes con administración de energía de máquinas por carga o por programación, o una combinación de ambas.
- Para supervisar métricas como el ahorro de costes y la utilización de capacidades, y para habilitar las notificaciones, use Director.

Vídeo de 2 minutos

Este vídeo ofrece un recorrido rápido por Autoscale.

Esto es un vídeo incrustado. Haga clic en el enlace para ver el vídeo.

Introducción a Autoscale

August 17, 2024

Autoscale funciona a nivel de grupos de entrega. Administra de forma proactiva la energía de las máquinas de un grupo de entrega en función de los horarios que usted establezca.

Autoscale se aplica a todos los tipos de grupos de entrega:

- SO estático de sesión única
- SO aleatorio de sesión única
- SO aleatorio multisesión

En este artículo se describen los conceptos básicos relacionados con Autoscale y se proporcionan instrucciones sobre cómo habilitar y configurar Autoscale para un grupo de entrega.

Conceptos básicos

Antes de empezar, obtenga información sobre estos conceptos básicos en Autoscale:

- Horarios
- Búfer de capacidad
- Índice de carga

Horarios

Autoscale enciende y apaga máquinas de un grupo de entrega según el horario que usted establezca.

Los horarios incluyen la cantidad de máquinas activas para cada franja horaria, con las horas punta y las horas de actividad normal definidas.

Los parámetros de los horarios varían según el tipo de grupo de entrega. Para obtener más información, consulte:

- Grupos de entrega de SO multisesión
- Grupos de entrega aleatorios de SO de sesión única
- Grupos de entrega estáticos de SO de sesión única

Búfer de capacidad

El búfer de capacidad se utiliza para agregar capacidad de reserva a la demanda actual y, así, tener en cuenta los aumentos de carga dinámica. Existen dos casos a tener en cuenta:

- Para los grupos de entrega de SO multisesión, el búfer de capacidad se define como un porcentaje de la capacidad total del grupo de entrega en términos de índice de carga.
- Para los grupos de entrega de SO de sesión única, el búfer de capacidad se define como un porcentaje del total de máquinas del grupo de entrega.

Índice de carga

> **IMPORTANTE:**
>
> El índice de carga se aplica solamente a grupos de entrega multisesión.

La métrica del índice de carga determina la probabilidad de que una máquina reciba solicitudes de inicio de sesión de los usuarios. Se calcula mediante la configuración de directiva de **administración de carga de Citrix** definida para el uso simultáneo de inicios de sesión, sesiones, CPU, discos y memoria.

El índice de carga oscila entre 0 y 10 000. De forma predeterminada, una máquina se considera a carga completa cuando aloja 250 sesiones.

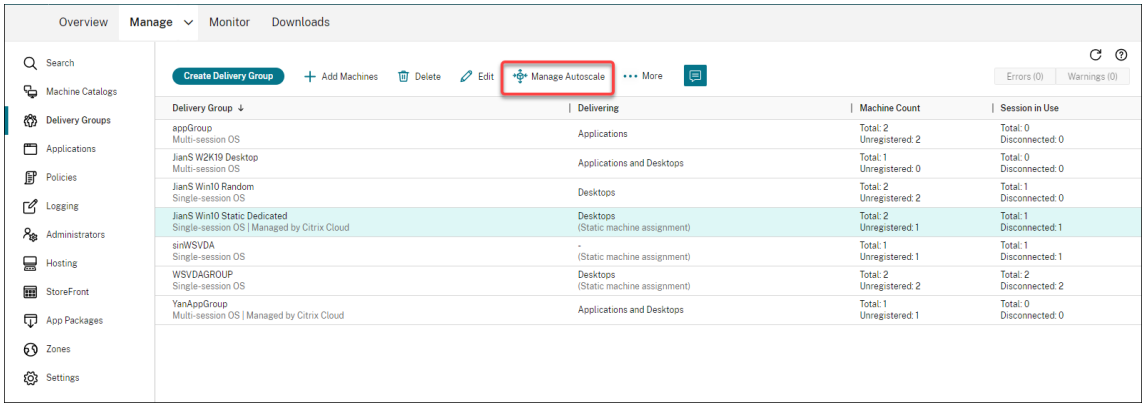
- La cifra "0"indica una máquina descargada. Una máquina con un valor 0 de índice de carga se halla en una carga base.
- La cifra "10 000"indica una máquina completamente cargada que no puede ejecutar más sesiones.

Habilitar Autoscale para un grupo de entrega

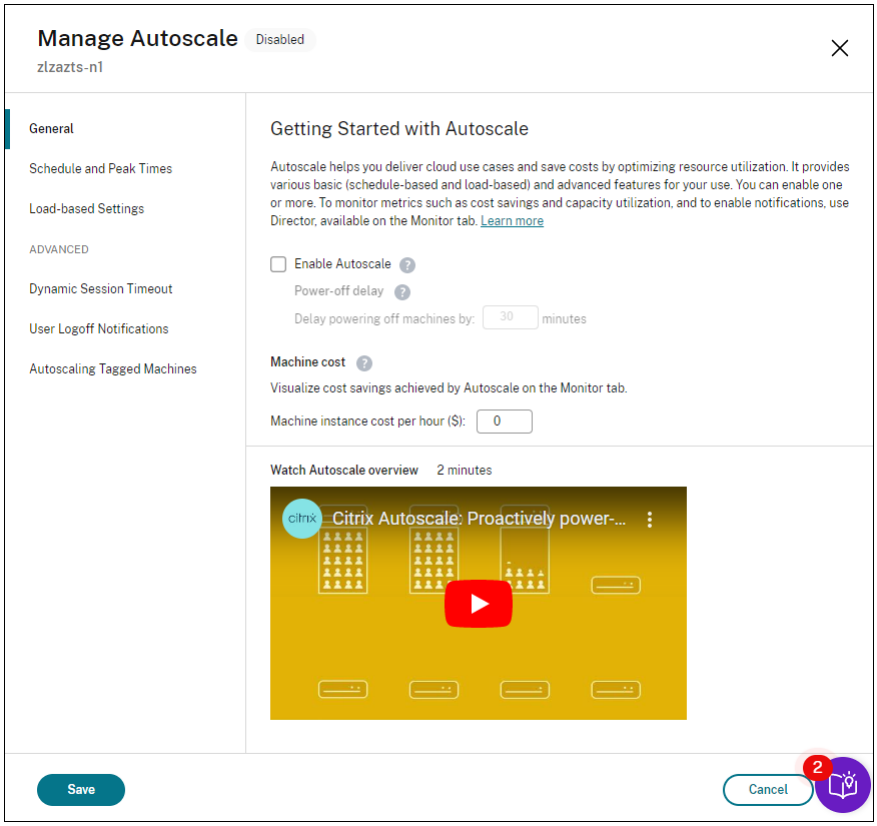
De forma predeterminada, Autoscale está inhabilitado al crear grupos de entrega. Para habilitar y configurar Autoscale para un grupo de entrega mediante Web Studio, siga estos pasos:

También puede usar comandos de PowerShell para habilitar y configurar Autoscale para un grupo de entrega. Para obtener más información, consulte Comandos del SDK de Broker PowerShell.

1. Seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione el grupo de entrega que quiere administrar y, a continuación, haga clic en **Administrar Autoscale**.



3. En la página **Administrar Autoscale**, marque la casilla **Habilitar Autoscale** para activar la función. Después de habilitar Autoscale, se habilitan las opciones de la página.



4. Para cambiar los parámetros predeterminados en función de las necesidades de su organización, complete estos parámetros:

   - Configurar horarios
   - Para apagar máquinas inactivas de manera más eficiente, utilice Tiempos de espera de sesión dinámicos y Notificaciones de cierre de sesión.
   - Para administrar la energía de un subconjunto de máquinas del grupo de entrega, utilice Autoscale de máquinas etiquetadas.

Para inhabilitar Autoscale, desmarque la casilla **Autoscale**. Las opciones de la página quedan atenuadas para indicar que Autoscale no está habilitado en el grupo de entrega seleccionado.

> **Importante:**
>
> - Si inhabilita Autoscale, todas las máquinas administradas por Autoscale permanecen en el estado en que se encuentren al inhabilitarse.
> - Después de inhabilitar Autoscale, las máquinas en estado de purga salen de dicho estado. Para obtener más información sobre el estado de purga, consulte Estado de purga.

Supervisar métricas

Tras habilitar Autoscale para un grupo de entrega, puede supervisar estas métricas de las máquinas administradas por Autoscale desde Director.

- Uso de máquinas
- Ahorro estimado
- Notificaciones de alerta para máquinas y sesiones
- Estado de la máquina
- Tendencias de los patrones de carga

> **Nota:**
>
> Al habilitar inicialmente Autoscale en un grupo de entrega, puede tardar unos instantes en mostrar los datos de supervisión de ese grupo de entrega.
> Los datos de supervisión siguen estando disponibles si Autoscale está habilitado y, a continuación, se inhabilita en el grupo de entrega. Autoscale recopila datos de supervisión en intervalos de 5 minutos.

Para obtener más información sobre las métricas, consulte Supervisar máquinas administradas con Autoscale.

Información útil

Autoscale funciona a nivel de grupos de entrega. Se configura por grupo de entrega. Administrará la energía solamente de las máquinas que haya en el grupo de entrega seleccionado.

Capacidad y registro de máquinas

Autoscale solo incluye máquinas registradas en el sitio al determinar la capacidad. Las máquinas encendidas que no están registradas no pueden aceptar solicitudes de sesión. Como consecuencia,

no se incluyen en la capacidad general del grupo de entrega.

Escalado en varios catálogos de máquinas

En algunos sitios, es posible que varios catálogos de máquinas estén asociados a un único grupo de entrega. Autoscale enciende de forma aleatoria máquinas de cada catálogo para cumplir con los requisitos de programación o de demanda de sesiones.

Por ejemplo, un grupo de entrega tiene dos catálogos de máquinas: el catálogo A tiene tres máquinas encendidas, y el catálogo B, una. Si Autoscale necesita encender una máquina adicional, es posible que la encienda desde el catálogo A o el catálogo B.

Aprovisionamiento de máquinas y demanda de sesiones

El catálogo de máquinas asociado al grupo de entrega debe tener suficientes máquinas para encender y apagar a medida que la demanda aumente o disminuya. Si la demanda de sesiones supera la cantidad total de máquinas registradas en el grupo de entrega, Autoscale garantiza el encendido de todas las máquinas registradas. No obstante, **Autoscale no proporciona máquinas adicionales**.

Consideraciones sobre el tamaño de las instancias

Puede optimizar los costes si tiene el tamaño adecuado de sus instancias en nubes públicas. Recomendamos aprovisionar instancias más pequeñas siempre que coincidan con los requisitos de capacidad y rendimiento de la carga de trabajo.

Las instancias más pequeñas alojan menos sesiones de usuario que las de mayor tamaño. Por lo tanto, Autoscale pone a las máquinas en estado de purga mucho más rápido porque tarda menos tiempo en cerrar la última sesión de usuario. Como resultado, Autoscale apaga antes las instancias más pequeñas, lo que reduce los costes.

Estado de purga

Autoscale intenta reducir la cantidad de máquinas encendidas en el grupo de entrega para equipararla al búfer de capacidad y al tamaño del grupo configurados.

Para lograr este objetivo, Autoscale pone en "estado de purga"las máquinas sobrantes con la menor cantidad de sesiones y las apaga cuando se cierran todas las sesiones. Este comportamiento se da cuando la demanda de sesiones disminuye y la programación requiere menos máquinas de las que están encendidas.

Autoscale pone el exceso de máquinas en "estado de purga"una por una.

- Si dos o más máquinas tienen la misma cantidad de sesiones activas, Autoscale purga la máquina que se ha encendido durante un tiempo equivalente a la demora de apagado especificada.

  Al hacerlo, se evita poner máquinas encendidas recientemente en estado de purga porque es más probable que esas máquinas tengan menos sesiones.

- Si se han encendido dos o más máquinas durante un tiempo equivalente a la demora de apagado especificada, Autoscale purga esas máquinas una por una al azar.

Las máquinas en estado de purga ya no alojan nuevos inicios de sesión y esperan a que se cierren las sesiones existentes. Una máquina se convierte en candidata para apagarse únicamente cuando todas las sesiones se cierran. Sin embargo, si no hay máquinas disponibles inmediatamente para iniciar sesión, Autoscale prefiere dirigir los inicios de sesión a una máquina en estado de purga en vez de tener que encender una máquina.

Una máquina sale del estado de purga cuando se cumple una de las siguientes condiciones:

- La máquina se apaga.
- Autoscale se inhabilita para el grupo de entrega al que pertenece la máquina.
- Autoscale utiliza la máquina para cumplir con los requisitos de demanda de carga o programación. Este caso se produce cuando la programación (escalado por programación) o la demanda actual (escalado por carga) requiere más máquinas de la cantidad de máquinas que están actualmente encendidas.

> **Importante:**
>
> Si no hay máquinas disponibles inmediatamente para iniciar sesión, Autoscale prefiere dirigir inicios de sesión a una máquina en estado de purga en vez de tener que encender una máquina. Una máquina en estado de purga que aloja un inicio de sesión permanece en estado de purga.

Para averiguar qué máquinas están en estado de purga, utilice el comando de PowerShell `Get-BrokerMachine`. Por ejemplo: `Get-BrokerMachine -DrainingUntilShutdown $true`. Como alternativa, puede utilizar la consola Administrar. Consulte, Mostrar máquinas en estado de purga.

Mostrar máquinas en estado de purga

> **Nota:**
>
> Esta función solo se aplica a máquinas multisesión.

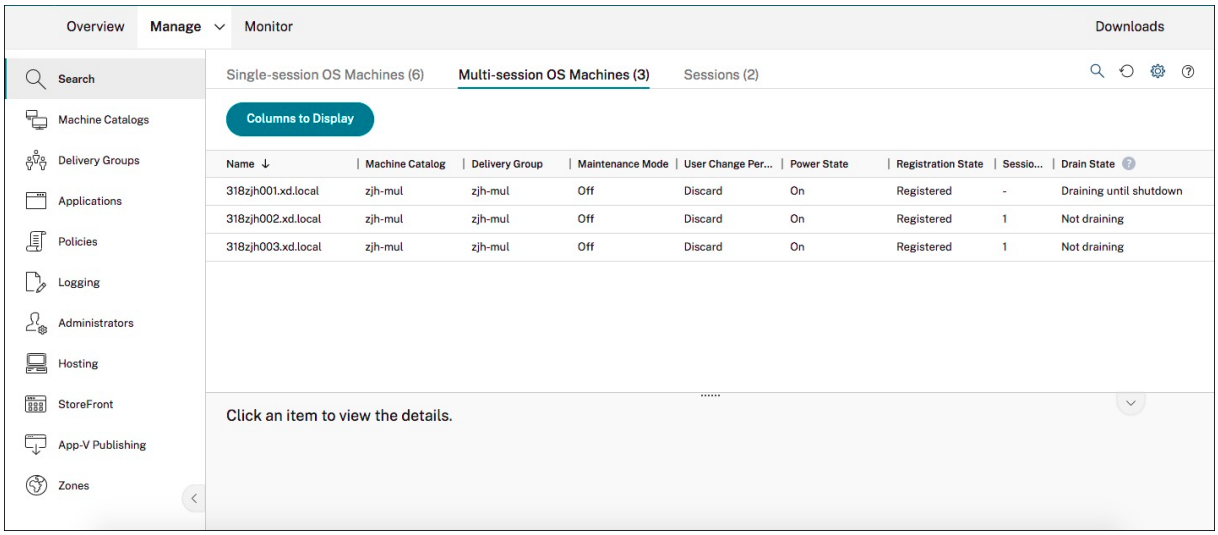
En Web Studio, puede mostrar máquinas que están en estado de purga, lo que le permite saber qué máquinas están a punto de apagarse. Siga estos pasos:

1. Vaya al nodo **Buscar** y, a continuación, haga clic en **Columnas que mostrar**.

2. En la ventana **Columnas que mostrar**, marque la casilla situada junto a **Estado de la purga**.
3. Haga clic en **Guardar** para salir de la ventana **Columnas que mostrar**.

La columna **Estado de la purga** puede mostrar esta información:

- **Purga hasta el apagado.** Aparece cuando las máquinas se hallan en estado de purga hasta que se apagan.
- **Sin purga.** Aparece cuando las máquinas aún no se hallan en estado de purga.



Más información

Para obtener más información sobre Autoscale, consulte Citrix Autoscale en Tech Zone.

Parámetros basados en la programación y en la carga

August 17, 2024

Cómo administra Autoscale la energía de las máquinas

Autoscale enciende y apaga las máquinas en función de la programación seleccionada. Autoscale permite establecer varias programaciones que incluyen días específicos de la semana y ajustar la cantidad de máquinas disponibles durante esos días. Si espera que un conjunto de usuarios consuma los recursos de las máquinas a una hora específica en días específicos, Autoscale ayuda a proporcionar una experiencia optimizada. Tenga en cuenta que esas máquinas se encenderán durante la programación, independientemente de si hay sesiones activas en ellas.

> **Nota:**
>
> Autoscale admite cualquier máquina con administración de energía.

La programación se basa en la **zona horaria** del grupo de entrega. Para cambiar la zona horaria, puede cambiar la configuración del usuario en un grupo de entrega. Para obtener más información, consulte Administrar de grupos de entrega.

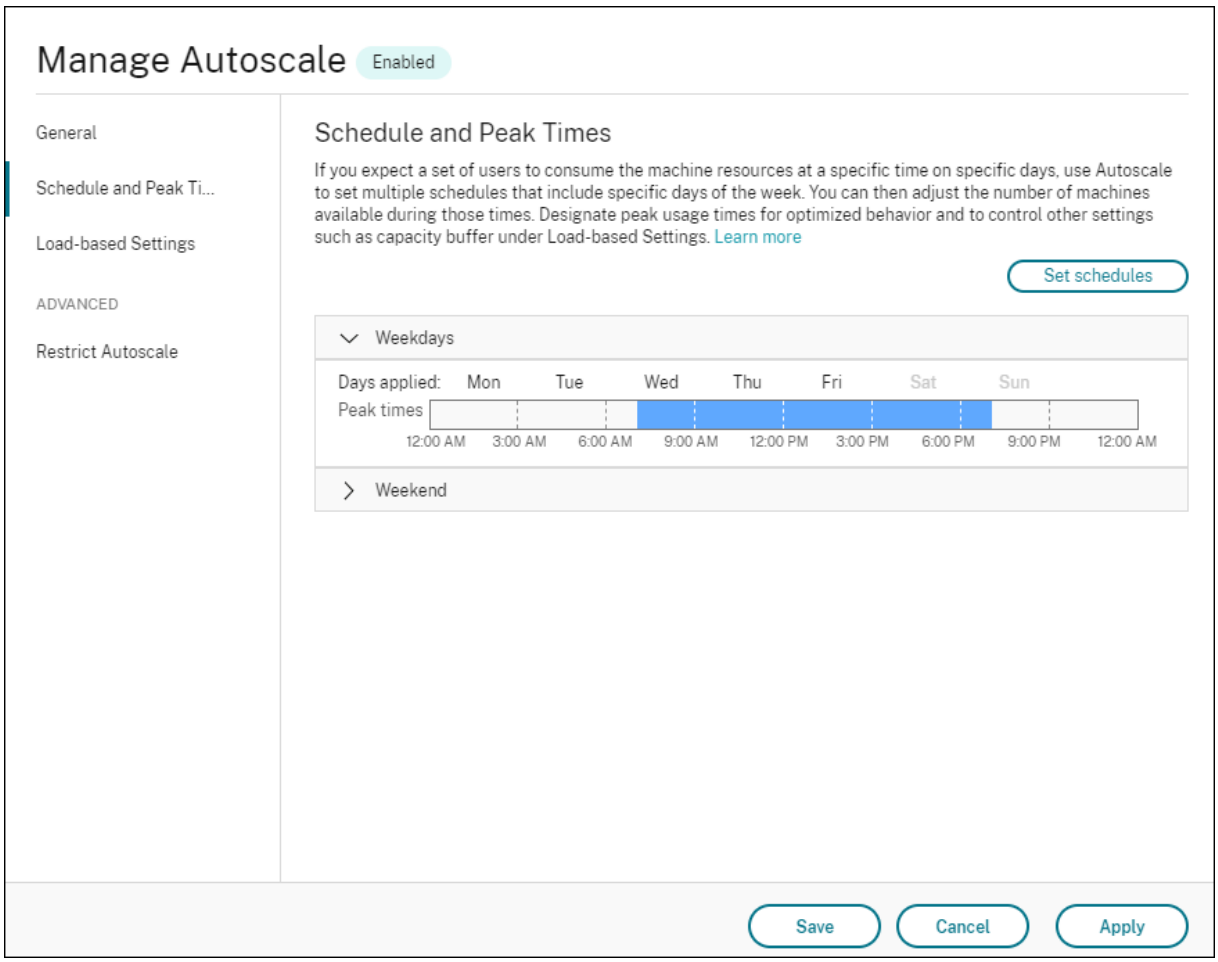
Autoscale tiene dos horarios: *días laborables* (de lunes a viernes) y *fin de semana* (sábado y domingo). De forma predeterminada, la programación de **días laborables** mantiene una máquina encendida entre las 7:00 y las 18:30 durante las horas punta y ninguna durante las horas normales. El búfer de capacidad predeterminado se establece en 10% durante las horas punta y las horas normales De forma predeterminada, la programación de **fin de semana** no mantiene ninguna máquina encendida.

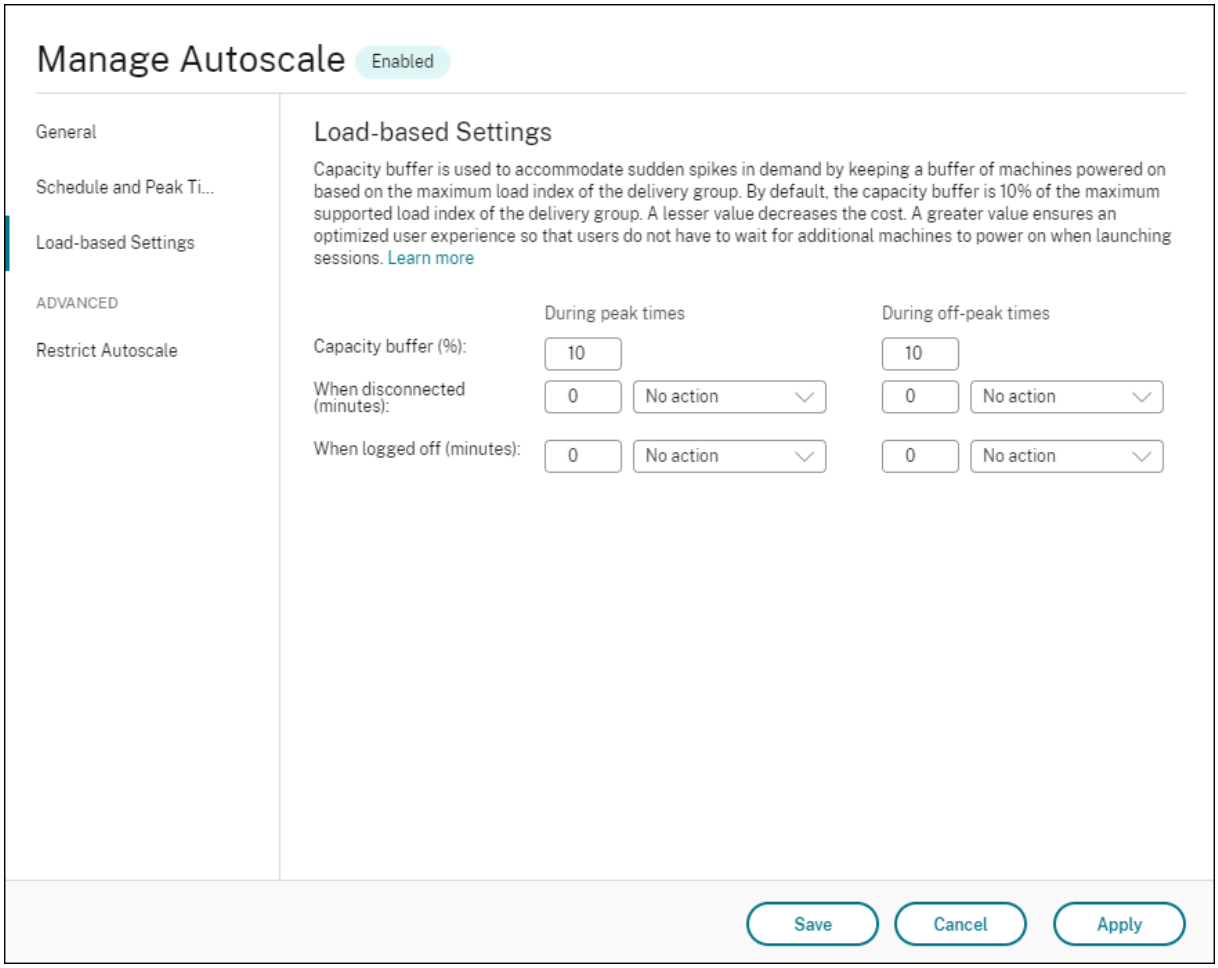
> **Nota:**
>
> Autoscale trata solamente aquellas máquinas que estén registradas en el sitio como parte de la capacidad disponible en los cálculos que realiza. "Registrado"significa que la máquina puede utilizarse o que ya se está utilizando. Esto asegura que solamente las máquinas que pueden aceptar sesiones de usuario se incluyan en la capacidad del grupo de entrega.

Interfaces de usuario

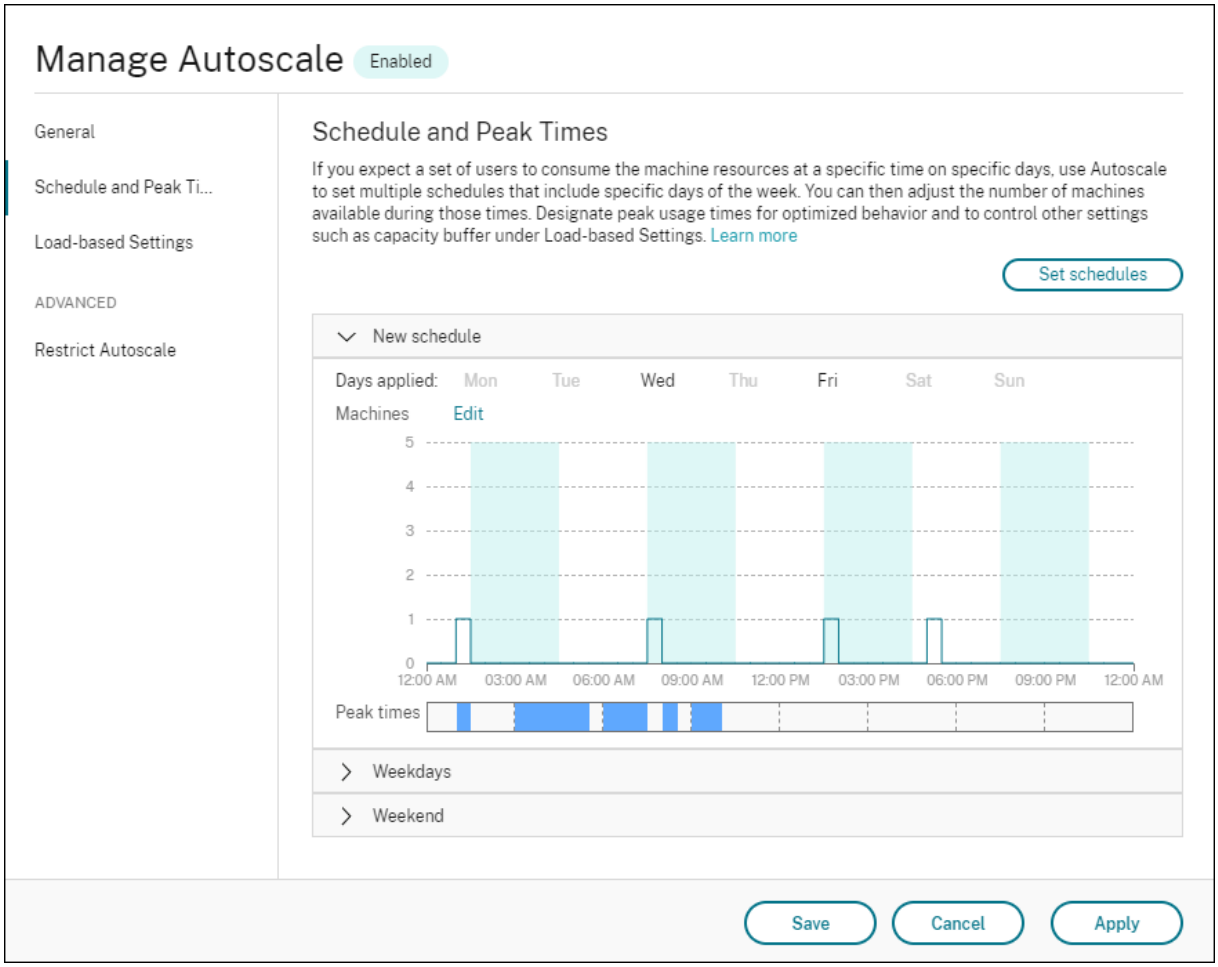
Hay tres tipos de interfaces de usuario a tener en cuenta.

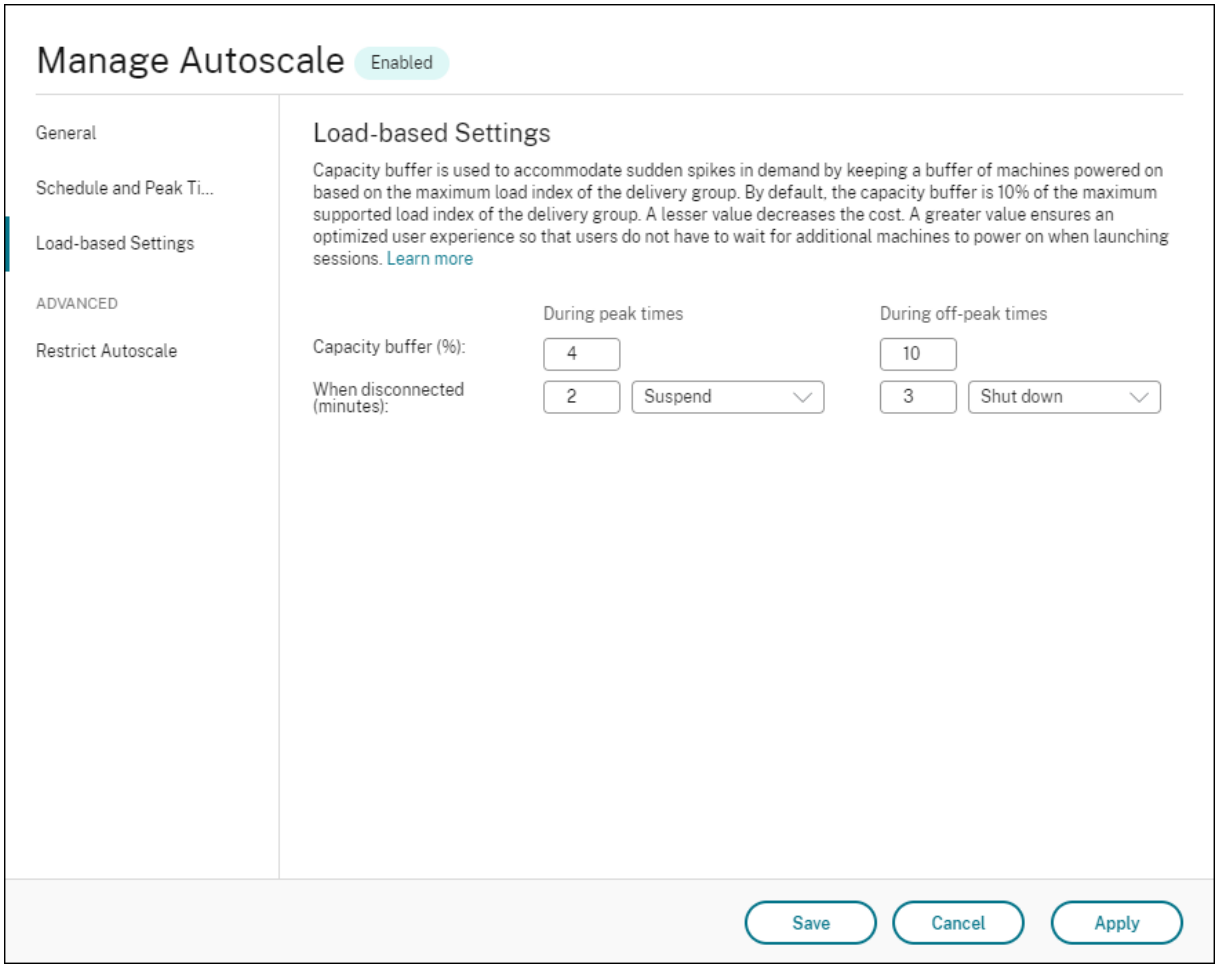
Interfaz de usuario para *grupos de entrega estáticos de SO de sesión única*:



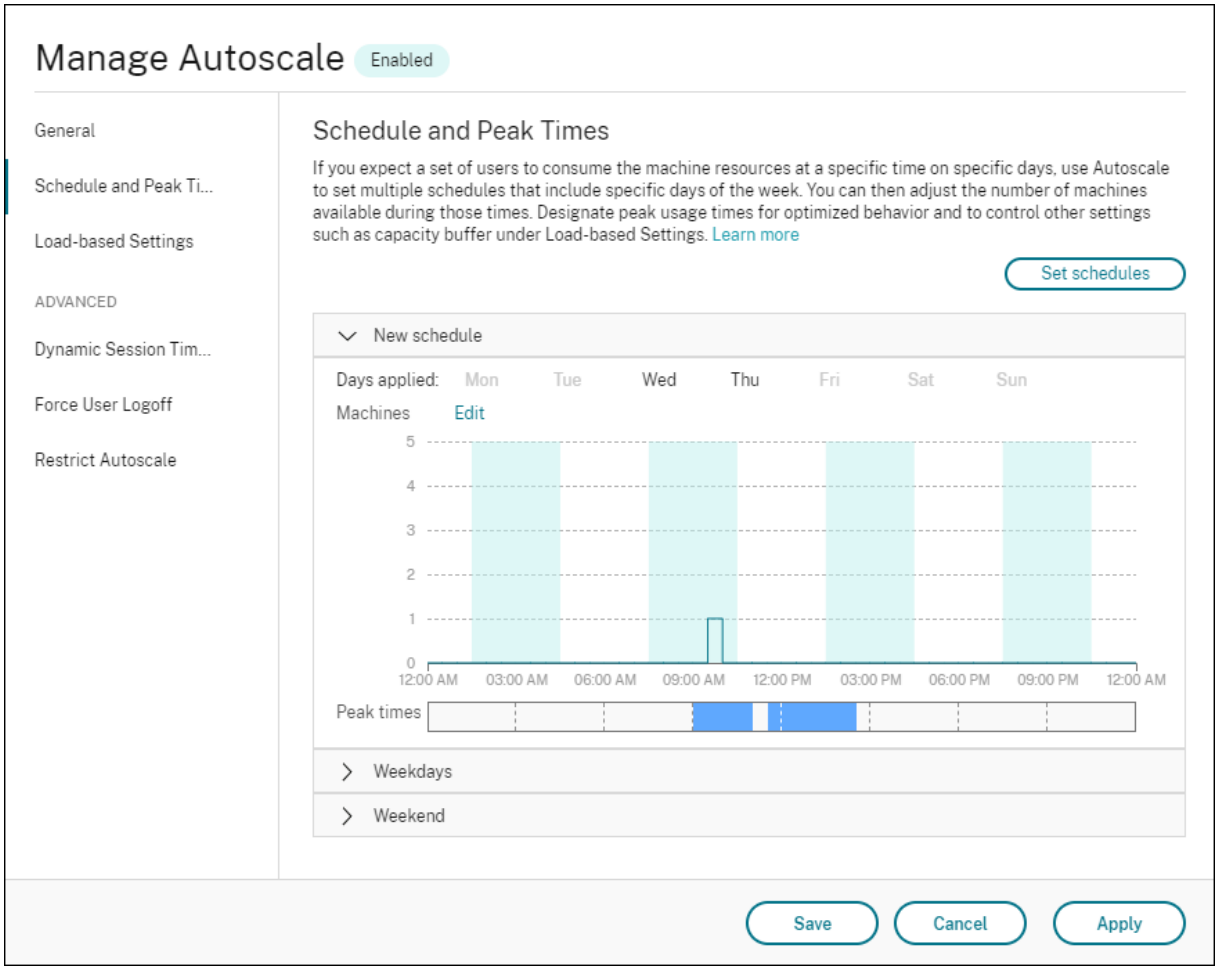


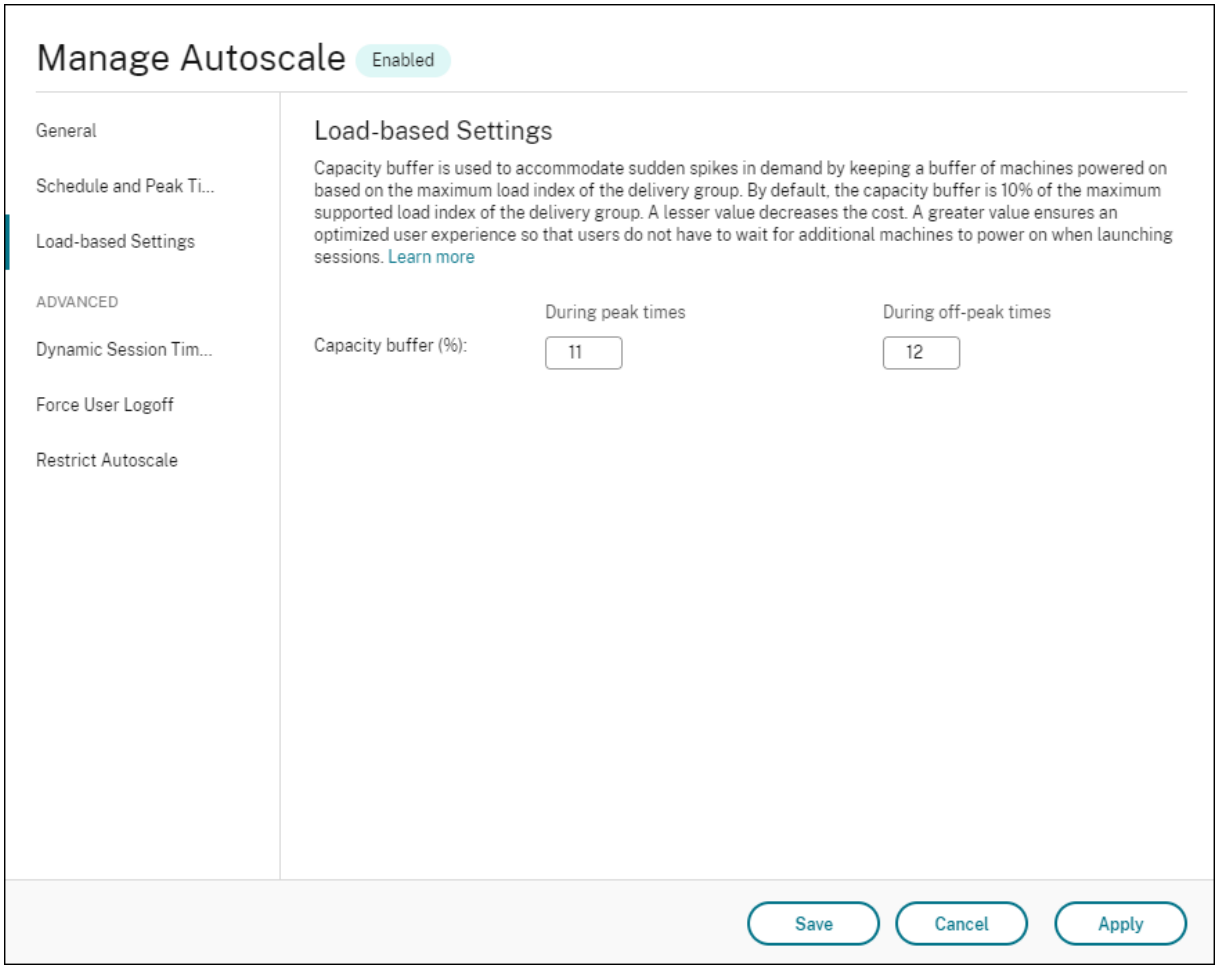
Interfaz de usuario de Autoscale para *grupos de entrega aleatorios de SO de sesión única*:





Interfaz de usuario de Autoscale para *grupos de entrega de SO multisesión*:





Configuración basada en la programación

Programación de Autoscale. Permite agregar, modificar, seleccionar y eliminar programaciones.

Días aplicados. Resalta los días aplicados a la programación seleccionada. Los días restantes quedan atenuados.

Modificar. Permite asignar las máquinas en cada hora o cada media hora. Puede asignar las máquinas por cantidad y por porcentaje.

> **Nota:**
>
> - Esta opción solo está disponible en las interfaces de usuario de Autoscale para grupos de entrega aleatorios de SO multisesión y SO de sesión única.
> - El histograma situado junto a **Modificar** muestra la cantidad o el porcentaje de máquinas activas en diferentes intervalos de tiempo.
> - Puede **asignar máquinas** en cada intervalo de tiempo a través de la opción **Modificar** situada encima de **Horas punta**. Según la opción que haya seleccionado en el menú de la ven-

> tana **Máquinas para iniciar**, puede asignar las máquinas por cantidad o por porcentaje.
> - Para los grupos de entrega de SO multisesión, puede establecer por separado la cantidad mínima de máquinas activas en incrementos granulares de 30 minutos durante cada día. Para los grupos de entrega aleatorios de SO de sesión única, puede establecer por separado la cantidad mínima de máquinas activas en incrementos granulares de 60 minutos durante cada día.

Para definir sus propias programaciones, siga estos pasos:

1. En la página **Programación y horas punta** de la ventana **Administrar Autoscale**, haga clic en **Establecer programaciones**.
2. En la ventana **Modificar programaciones de Autoscale**, seleccione los días que quiere aplicar a cada programación. También puede suprimir programaciones cuando corresponda.
3. Haga clic en **Listo** para guardar las programaciones y volver a la página **Programación y horas punta**.
4. Seleccione la programación correspondiente y configúrela según sea necesario.
5. Haga clic en **Aplicar** para salir de la ventana **Administrar Autoscale** o configurar los parámetros en otras páginas.

> **Importante:**
>
> - Autoscale no permite que el mismo día coincida en diferentes programaciones. Por ejemplo, si selecciona Lunes en la programación2 después de seleccionar Lunes en la programación1, el lunes se borra automáticamente en la programación1.
> - El nombre de las programaciones no distingue entre mayúsculas y minúsculas.
> - El nombre de las programaciones no debe estar vacío ni contener solamente espacios.
> - Autoscale permite espacios vacíos entre caracteres.
> - Los nombres de las programaciones no deben contener estos caracteres: \ / ; : # . * ? = < > | [ ] ( ) { } ‘“‘
> - Autoscale no admite nombres duplicados para las programaciones. Introduzca un nombre distinto para cada programa.
> - Autoscale no admite programaciones vacías. Esto significa que las programaciones sin días seleccionados no se guardan.
>
> **Nota:**
>
> Los días incluidos en la programación seleccionada quedan resaltados, mientras que los no incluidos aparecen atenuados.

Configuración basada en la carga

Horas punta. Permite definir las horas punta de los días aplicados en la programación seleccionada. Para ello, haga clic con el botón secundario en el gráfico de barras horizontales. Tras definir las horas punta, las horas restantes y sin definir son, de manera predeterminada, horas normales. **De forma predeterminada**, el intervalo horario de 7:00 a 19:00 se define como horas punta en los días incluidos en la programación seleccionada.

> **Importante:**
>
> - Para los grupos de entrega de SO multisesión, el gráfico de barras de las horas punta se utiliza para el búfer de capacidad.
> - Para los grupos de entrega de SO de sesión única, el gráfico de barras de las horas punta se utiliza para el búfer de capacidad y controla las acciones que se desencadenarán después de una desconexión o un cierre de sesión.
> - Se pueden definir las horas punta que tendrán los días incluidos en una programación con una precisión de 30 minutos tanto para los grupos de entrega de SO multisesión como para los de SO de sesión única. También puede usar el comando `New-BrokerPowerTimeScheme PowerShell`. Para obtener más información, consulte Comandos del SDK de Broker PowerShell.

Búfer de capacidad. Le permite mantener un búfer de máquinas encendidas. Un valor menor disminuye el coste. Un valor mayor garantiza una experiencia de usuario optimizada para que, al iniciar sesiones, los usuarios no tengan que esperar a que se enciendan máquinas adicionales. De forma predeterminada, el búfer de capacidad es del 10% para las horas punta y las horas normales. Si establece el búfer de capacidad en 0 (cero), es posible que los usuarios tengan que esperar a que se enciendan máquinas adicionales al iniciar las sesiones. Autoscale permite determinar el búfer de capacidad por separado para las horas punta y las horas normales.

Otros parámetros

> **Sugerencia:**
>
> - Puede configurar las opciones diversas mediante el SDK de Broker PowerShell. Para obtener más información, consulte Comandos del SDK de Broker PowerShell.
> - Para entender los comandos del SDK asociados a la configuración de cuando se desconecta y cuando se cierra la sesión, consulte https://citrix.github.io/delivery-controller-sdk/Broker/about_Broker_PowerManagement/#power-policy.

Cuando está desconectado. Le permite especificar el tiempo que una máquina desconectada y bloqueada permanece encendida después de la desconexión de una sesión antes de que la máquina se suspenda o se apague. Si se especifica un valor de tiempo, la máquina se suspende o se apaga cuando

haya transcurrido el tiempo de desconexión especificado según la acción que haya configurado. De forma predeterminada, no se asigna ninguna acción a las máquinas desconectadas. Puede definir acciones por separado para las horas punta y las horas normales. Para ello, haga clic en la flecha hacia abajo y, a continuación, seleccione una de las siguientes opciones en el menú:

- **Ninguna acción**. Si se selecciona, la máquina, después de que la sesión se haya desconectado, permanece encendida. Autoscale no interviene.
- **Suspender**. Si se selecciona, Autoscale pausa la máquina sin apagarla una vez transcurrido el tiempo de desconexión especificado. La siguiente opción está disponible después de seleccionar **Suspender**.
  - **Al no reconectarse en (minutos)**. Las máquinas suspendidas permanecen disponibles para los usuarios desconectados cuando se vuelven a conectar, pero no están disponibles para nuevos usuarios. Para que las máquinas estén disponibles de nuevo para manejar todas las cargas de trabajo, apáguelas. Especifique el tiempo de espera, en minutos, tras el cual Autoscale las apaga.
- **Apagar**. Si se selecciona, Autoscale apaga la máquina una vez transcurrido el tiempo de desconexión especificado.

> **Nota:**
>
> Esta opción solo está disponible en las interfaces de usuario de Autoscale para grupos de entrega aleatorios y estáticos de SO de sesión única.

Al cerrar la sesión. Permite especificar el tiempo que una máquina permanece encendida después de cerrar sesión antes de que la máquina se suspenda o se apague. Si se especifica un valor de tiempo, la máquina se suspende o se apaga cuando haya transcurrido el tiempo de cierre de sesión especificado según las acciones que haya configurado. De forma predeterminada, no se asigna ninguna acción a las máquinas cuya sesión se haya cerrado. Puede definir acciones por separado para las horas punta y las horas normales. Para ello, haga clic en la flecha hacia abajo y, a continuación, seleccione una de las siguientes opciones en el menú:

- **Ninguna acción**. Si se selecciona, la máquina, después de que la sesión se haya cerrado, permanece encendida. Autoscale no interviene.
- **Suspender**. Si se selecciona, Autoscale pausa la máquina sin apagarla una vez transcurrido el tiempo de cierre de sesión especificado.
- **Apagar**. Si se selecciona, Autoscale apaga la máquina una vez transcurrido el tiempo de cierre de sesión especificado.

> **Nota:**
>
> Esta opción solo está disponible en las interfaces de usuario de Autoscale para grupos de entrega

> estáticos de SO de sesión única.

Administrar la energía de máquinas con SO de sesión única que pasan a otro período de tiempo con sesiones desconectadas

> **Importante:**
>
> - Esta mejora solo se aplica a máquinas con SO de sesión única y sesiones desconectadas. No se aplica a máquinas con SO de sesión única y sesiones cerradas.
> - Para que esta mejora surta efecto, debe habilitar Autoscale para el grupo de entrega correspondiente. De lo contrario, las acciones de directiva de energía para desconexiones no se activan al cambiar de período.

En versiones anteriores, las máquinas con SO de sesión única 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 esta versión, Autoscale suspende o apaga las máquinas 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 estas directivas de energía para un grupo de entrega de SO de sesión única:

- Establezca `PeakDisconnectAction` en “Nada”
- Establezca `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 y https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/.

En versiones anteriores, una máquina con SO de sesión única y una sesión desconectada durante horas punta permanecía encendida cuando pasaba del período de horas punta al de horas normales. A partir de esta versión, las acciones de directiva `OffPeakDisconnectAction` y `OffPeakDisconnectTimeout` se aplican a la máquina con SO de sesión única 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 SO de 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.

Cómo funciona el búfer de capacidad

El búfer de capacidad se utiliza para agregar capacidad de reserva a la demanda actual y, así, tener en cuenta los aumentos de carga dinámica. Existen dos casos a tener en cuenta:

- Para los grupos de entrega de SO multisesión, el búfer de capacidad se define como un porcentaje de la capacidad total del grupo de entrega en términos de índice de carga. Para obtener más información acerca del índice de carga, consulte Índice de carga.
- Para los grupos de entrega de SO de sesión única, el búfer de capacidad se define como un porcentaje de la capacidad total del grupo de entrega en términos de cantidad de máquinas.

> **Nota:**
>
> En situaciones en las que se restringe Autoscale a las máquinas etiquetadas, el búfer de capacidad se define como un porcentaje de la capacidad total de las máquinas etiquetadas del grupo de entrega en términos de índice de carga.

Autoscale le permite establecer el búfer de capacidad por separado para las horas punta y las horas normales. Un valor menor en el campo de búfer de capacidad disminuye el coste porque Autoscale utiliza energía de una capacidad de reserva menor. Un valor mayor garantiza una experiencia de usuario

optimizada para que los usuarios no tengan que esperar a que se enciendan máquinas adicionales al iniciar sesiones. De forma predeterminada, el búfer de capacidad es del 10%.

> **Importante:**
>
> El búfer de capacidad provoca que las máquinas se enciendan cuando la capacidad total de reserva cae por debajo de un "X"por ciento de la capacidad total del grupo de entrega. Esto reserva el porcentaje requerido de la capacidad de reserva.

Grupos de entrega de SO multisesión

¿Cuándo se encienden las máquinas?

> **Importante:**
>
> Si se selecciona una programación, Autoscale enciende todas las máquinas configuradas para encenderse en la programación. Autoscale mantiene encendida esta cantidad especificada de máquinas durante la programación, independientemente de la carga.

Cuando la cantidad de máquinas encendidas en el grupo de entrega ya no satisface la demanda deseada para respetar la capacidad del búfer en términos de índice de carga, Autoscale enciende máquinas adicionales. Por ejemplo, un grupo de entrega tiene 20 máquinas, y 3 están programadas para encenderse como parte del escalado programado con un búfer de capacidad del 20 %. Al final, 4 máquinas se encenderán cuando no haya carga. Esto se debe a que se necesita un índice de carga de 4 x 10 k como búfer; por lo tanto, al menos 4 máquinas deben encenderse. Es posible que esto se produzca durante horas punta, un aumento de la carga en las máquinas, el inicio de nuevas sesiones y al agregar nuevas máquinas al grupo de entrega. Tenga en cuenta que Autoscale solo enciende las máquinas que cumplen los siguientes criterios:

- Las máquinas no se hallan en modo de mantenimiento.
- El hipervisor en el que se ejecutan las máquinas no está en modo de mantenimiento.
- Las máquinas están actualmente apagadas.
- Las máquinas no tienen ninguna acción de energía pendiente.

¿Cuándo se apagan las máquinas?

> **Importante:**
>
> - Si se selecciona una programación, Autoscale apaga las máquinas en función de la programación.
> - Autoscale no apaga las máquinas configuradas en la programación para encenderse du-

> rante la programación.

Cuando hay más máquinas de las suficientes para admitir la cantidad deseada de máquinas encendidas (búfer incluido) en el grupo de entrega, Autoscale apaga las máquinas adicionales. Es posible que esto se produzca durante horas de actividad normal, una disminución de la carga en las máquinas, el cierre de sesiones y al quitar máquinas del grupo de entrega. Autoscale apaga solamente las máquinas que cumplen los siguientes criterios:

- Las máquinas y el hipervisor en el que estas se ejecutan no están en modo de mantenimiento.
- Las máquinas están actualmente encendidas.
- Las máquinas están registradas como disponibles o a la espera de registrarse después de la puesta en marcha.
- Las máquinas no tienen sesiones activas.
- Las máquinas no tienen ninguna acción de energía pendiente.
- Las máquinas satisfacen la demora de apagado especificada. Esto significa que las máquinas se encendieron durante al menos "X"minutos, donde "X"es la demora de apagado especificada para el grupo de entrega.

Caso de ejemplo

Supongamos que tiene ante usted este caso:

- **Configuración del grupo de entrega**. El grupo de entrega al que quiere aplicar Autoscale para administrar la energía contiene 10 máquinas (de M1 a M10).
- **Configuración de Autoscale**
  - El búfer de capacidad es del 10%.
  - No se incluye ninguna máquina en la programación seleccionada.

El escenario se desarrolla de la siguiente manera:

1. Ningún usuario inicia sesión.
2. Las sesiones de usuario aumentan.
3. Se inician más sesiones de usuario.
4. La carga por sesión de usuario disminuye por la finalización de sesiones.
5. La carga de sesiones de usuario disminuye aún más hasta que la carga de sesiones se controla solamente mediante recursos locales.

Consulte lo que hay a continuación para obtener información detallada sobre cómo funciona Autoscale en este escenario.

- Sin carga de usuarios (estado inicial)
  - Se enciende una máquina (por ejemplo, M1). La máquina se enciende debido al búfer de capacidad configurado. En este caso, 10 (cantidad de máquinas) x 10 000 (índice de carga) x 10% (búfer de capacidad configurado) equivale a 10 000. Por lo tanto, se enciende una máquina.
  - El valor del índice de carga de la máquina encendida (M1) se halla en una carga base (el índice de carga es igual a 0).
- El primer usuario inicia sesión
  - La sesión se dirige para alojarse en la máquina M1.
  - El índice de carga de la máquina encendida M1 aumenta y la máquina M1 deja de estar en una carga base.
  - Autoscale comienza a encender una máquina adicional (M2) para satisfacer la demanda debido al búfer de capacidad configurado.
  - El valor del índice de carga de la máquina M2 se halla en una carga base.
- Los usuarios aumentan la carga
  - Se equilibra la carga de las sesiones entre las máquinas M1 y M2. Como resultado, aumenta el índice de carga de las máquinas encendidas (M1 y M2).
  - La capacidad total de reserva sigue estando por encima de 10 000 en términos de índice de carga.
  - El valor del índice de carga de la máquina M2 deja de estar en una carga base.
- Se inician más sesiones de usuario
  - Se equilibra la carga de las sesiones entre las máquinas (M1 y M2). Como resultado, aumenta todavía más el índice de carga de las máquinas encendidas (M1 y M2).
  - Cuando la capacidad total de reserva cae por debajo de 10 000 en términos de índice de carga, Autoscale comienza a encender una máquina adicional (M3) para satisfacer la demanda debido al búfer de capacidad configurado.
  - El valor del índice de carga de la máquina M3 se halla en una carga base.
- Se inician todavía más sesiones de usuario
  - Se equilibra la carga de las sesiones entre las máquinas (M1 y M3). Como resultado, aumenta el índice de carga de las máquinas encendidas (M1 y M3).
  - La capacidad total de reserva está por encima de 10 000 en términos de índice de carga.
  - El valor del índice de carga de la máquina M3 deja de estar en una carga base.
- La carga de las sesiones de usuario disminuye debido a la finalización de sesiones

  - Después de que los usuarios hayan cerrado sus sesiones o tras agotarse el tiempo de espera de las sesiones inactivas, la capacidad liberada de las máquinas M1 a M3 se reutiliza para alojar sesiones iniciadas por otros usuarios.
  - Cuando la capacidad total de reserva está por encima de 10 000 en términos de índice de carga, Autoscale pone una de las máquinas (por ejemplo, M3) en estado de purga. Como resultado, las sesiones iniciadas por otros usuarios ya no se dirigen a esa máquina, a no ser que ocurran nuevos cambios. Por ejemplo, la carga del usuario final aumenta de nuevo u otras máquinas tienen menor carga.

- La carga de las sesiones de usuario continúa disminuyendo
  - Una vez finalizadas todas las sesiones de la máquina M3 y transcurrida la demora de apagado especificada, Autoscale apaga la máquina M3.
  - Una vez que más usuarios hayan finalizado sus sesiones, la capacidad liberada en máquinas encendidas (M1 y M2) se reutiliza para alojar sesiones iniciadas por otros usuarios.
  - Cuando la capacidad total de reserva está por encima de 10 000 en términos de índice de carga, Autoscale pone una de las máquinas (por ejemplo, M2) en estado de purga. Como resultado, las sesiones iniciadas por otros usuarios ya no se dirigen a esa máquina.
- La carga de las sesiones de usuario continúa disminuyendo hasta que no queden sesiones
  - Una vez finalizadas todas las sesiones de la máquina M2 y transcurrida la demora de apagado especificada, Autoscale apaga la máquina M2.
  - El valor del índice de carga de la máquina encendida (M1) se halla en una carga base. Autoscale no pone la máquina M1 en estado de purga debido al búfer de capacidad configurado.

> **Nota:**
>
> Para los grupos de entrega de SO multisesión, todos los cambios en el escritorio se pierden cuando los usuarios cierran la sesión. Sin embargo, si se configuran, los parámetros específicos del usuario se mueven junto con el perfil de usuario.

Grupos de entrega aleatorios de SO de sesión única

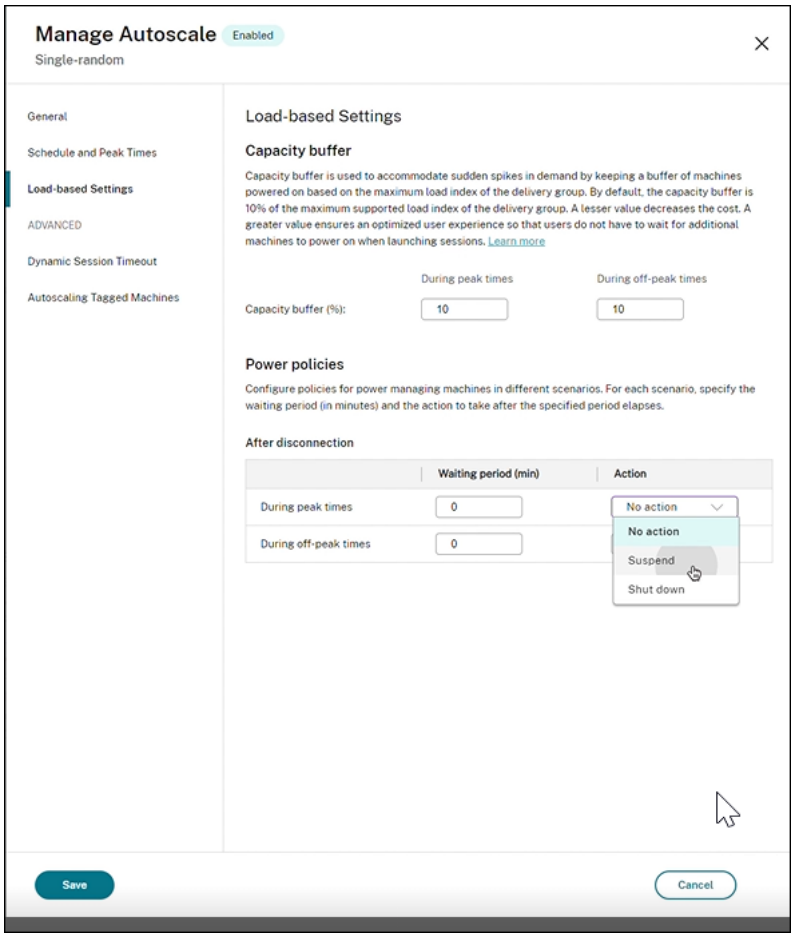
El búfer de capacidad se utiliza para adaptarse a picos repentinos de demanda y, al mismo tiempo, mantener un búfer de máquinas encendidas en función de la cantidad total de máquinas del grupo de entrega. De forma predeterminada, el búfer de capacidad es el 10 % de la cantidad total de máquinas del grupo de entrega.

Si la cantidad de máquinas (búfer de capacidad incluido) supera la cantidad total de máquinas encendidas en un momento dado, se encienden máquinas adicionales para satisfacer la demanda. Si

la cantidad de máquinas (búfer de capacidad incluido) es inferior a la cantidad total de máquinas encendidas en un momento dado, las máquinas sobrantes se apagarán o se suspenderán, según las acciones que usted haya configurado.

Directivas de energía

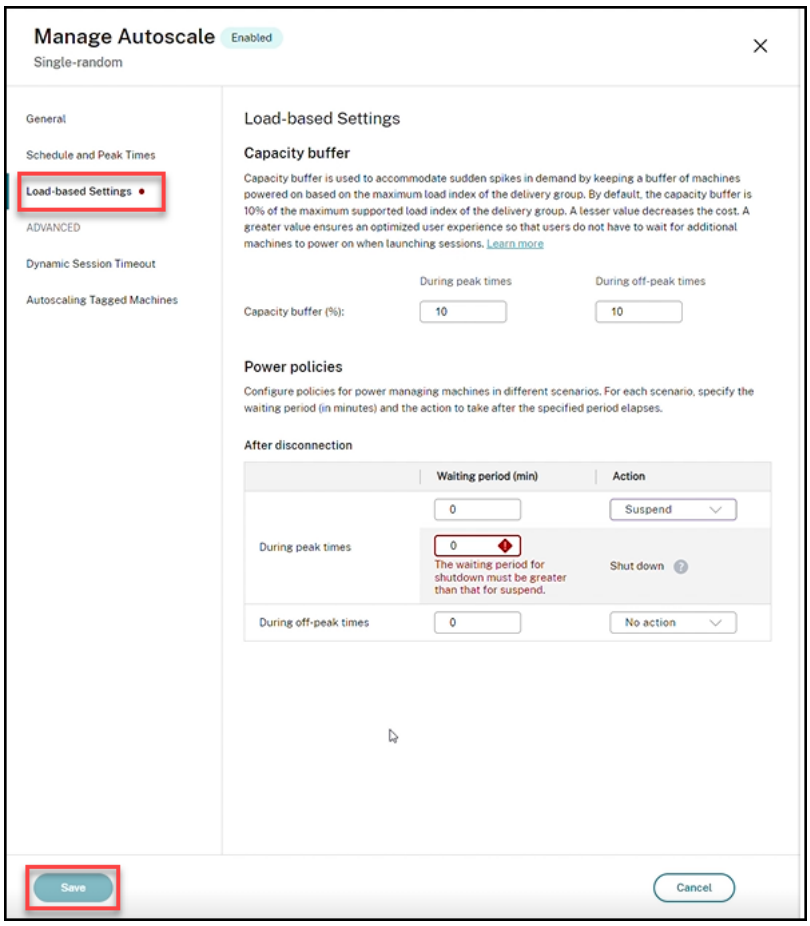
Configure directivas para administrar la energía de las máquinas en diferentes supuestos. Para cada supuesto, puede especificar el tiempo de espera (en minutos) y la acción prevista una vez finalizado el tiempo especificado. Las directivas de energía se aplican a los grupos de entrega aleatorios de SO de sesión única y a los grupos de entrega estáticos de SO de sesión única.



Tras la desconexión, se aplicarán los siguientes parámetros tanto durante las horas pico como fuera de ellas:

- Puede configurar el tiempo de espera en minutos y acciones como ninguna acción, suspender o cerrar desde el menú desplegable.
- Si selecciona la acción suspender, configure un tiempo de espera adicional para apagar la máquina.

> **Nota:**
>
> - Durante las horas punta y fuera de ellas, el tiempo de espera para la acción de apagado debe ser mayor que el tiempo de espera para suspensión.
> - Las máquinas suspendidas solo son accesibles para los usuarios desconectados cuando se vuelven a conectar. Para que las máquinas suspendidas estén disponibles para nuevos usuarios, apáguelas.
> - Si los parámetros de tiempo se configuran incorrectamente para los campos de suspensión y apagado, la opción **Guardar** está desactivada y aparece también un punto rojo junto a los elementos de navegación que indica los errores de configuración.



Por ejemplo

- Si establece el tiempo de espera en 12 minutos y elige que la primera acción sea no realizar ninguna acción, una vez transcurridos 12 minutos, la máquina seguirá encendida.
- Si establece el tiempo de espera en 15 minutos y elige que la primera acción sea suspender y el segundo tiempo de espera sea de 20 minutos, una vez transcurridos los 15 minutos, la máquina se suspende. Una vez transcurrido el segundo tiempo de espera, la máquina se apagará.

- Si establece el tiempo de espera en 18 minutos y elige que la primera acción sea apagar, transcurridos 18 minutos, la máquina se apagará.

Caso de ejemplo

Supongamos que tiene ante usted este caso:

- **Configuración del grupo de entrega**. El grupo de entrega al que quiere aplicar Autoscale para administrar la energía contiene 10 máquinas (de M1 a M10).
- **Configuración de Autoscale**
  - El búfer de capacidad es del 10%.
  - No se incluye ninguna máquina en la programación seleccionada.

El escenario se desarrolla de la siguiente manera:

1. Ningún usuario inicia sesión.
2. Las sesiones de usuario aumentan.
3. Se inician más sesiones de usuario.
4. La carga por sesión de usuario disminuye por la finalización de sesiones.
5. La carga de sesiones de usuario disminuye aún más hasta que la carga de sesiones se controla solamente mediante recursos locales.

Consulte lo que hay a continuación para obtener información detallada sobre cómo funciona Autoscale en este escenario.

- Sin carga de usuarios (estado inicial)
  - Se enciende una máquina (M1). La máquina se enciende debido al búfer de capacidad configurado. En este caso, 10 (cantidad de máquinas) x 10% (búfer de capacidad configurado) es igual a 1. Por lo tanto, se enciende una máquina.
- Un primer usuario inicia sesión
  - La primera vez que un usuario inicia sesión para utilizar un escritorio, se le asigna un escritorio de un grupo de escritorios alojado en máquinas encendidas. En este caso, al usuario se le asigna un escritorio de la máquina M1.
  - Autoscale comienza a encender una máquina adicional (M2) para satisfacer la demanda debido al búfer de capacidad configurado.
- Un segundo usuario inicia sesión
  - Al usuario se le asigna un escritorio de la máquina M2.

  - Autoscale comienza a encender una máquina adicional (M3) para satisfacer la demanda debido al búfer de capacidad configurado.

- Un tercer usuario inicia sesión
  - Al usuario se le asigna un escritorio de la máquina M3.
  - Autoscale comienza a encender una máquina adicional (M4) para satisfacer la demanda debido al búfer de capacidad configurado.
- Un usuario cierra la sesión
  - Después de que un usuario haya cerrado la sesión o se haya agotado el tiempo de espera del escritorio del usuario, la capacidad liberada (por ejemplo, M3) queda disponible como búfer. Como resultado, Autoscale comienza a apagar la máquina M4 porque el búfer de capacidad está configurado al 10%.
- Más usuarios cierran la sesión hasta que no quedan usuarios
  - Después de que más usuarios hayan cerrado la sesión, Autoscale apaga las máquinas (por ejemplo, M2 o M3).
  - Aunque no queden usuarios, Autoscale no apaga la máquina restante (por ejemplo, M1) porque esa máquina queda reservada como capacidad de reserva.

> **Nota:**
>
> Para los grupos de entrega aleatorios de SO de sesión única, todos los cambios en el escritorio se pierden cuando los usuarios cierran la sesión. Sin embargo, si se configuran, los parámetros específicos del usuario se mueven junto con el perfil de usuario.

Grupos de entrega estáticos de SO de sesión única

El búfer de capacidad se utiliza para adaptarse a picos repentinos de demanda y, al mismo tiempo, mantener un búfer de máquinas encendidas sin asignar en función de la cantidad total de máquinas sin asignar del grupo de entrega. De forma predeterminada, el búfer de capacidad es el 10 % de la cantidad total de máquinas sin asignar del grupo de entrega.

> **Importante:**
>
> Una vez asignadas todas las máquinas del grupo de entrega, el búfer de capacidad no desempeña ningún papel en el encendido ni en el apagado de las máquinas.

Si la cantidad de máquinas (búfer de capacidad incluido) supera la cantidad total de máquinas encendidas en un momento dado, se encienden máquinas adicionales sin asignar para satisfacer la demanda. Si la cantidad de máquinas (búfer de capacidad incluido) es inferior a la cantidad total de

máquinas encendidas en un momento dado, el exceso de máquinas se apagarán o se suspenderán, según las acciones que usted haya configurado.

Para grupos de entrega estáticos de SO de sesión única, Autoscale:

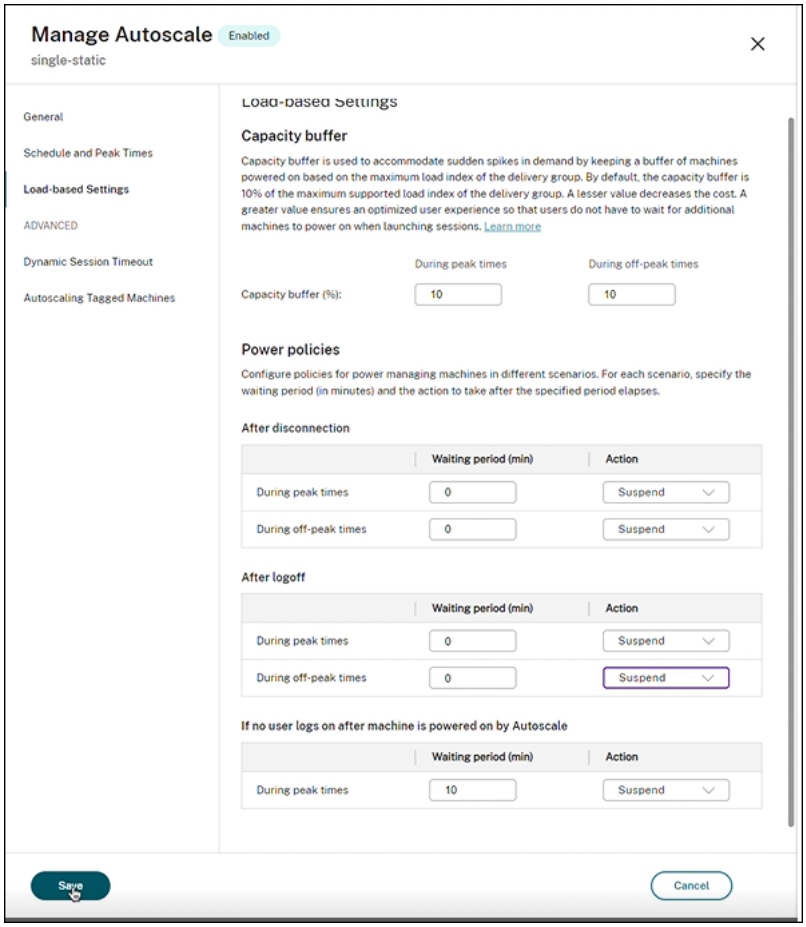
- Enciende las máquinas asignadas durante las horas punta y las apaga durante las horas de actividad normal solo cuando la propiedad `AutomaticPowerOnForAssigned` del grupo de entrega de SO de sesión única aplicable está establecida en true.
- Enciende automáticamente una máquina durante las horas punta si está apagada, y la propiedad `AutomaticPowerOnForAssignedDuringPeak` del grupo de entrega al que pertenece está establecida en true.

Para entender cómo funciona el búfer de capacidad con las máquinas asignadas, tenga en cuenta lo siguiente:

- El búfer de capacidad solo funciona cuando el grupo de entrega tiene una o más máquinas sin asignar.
- Si el grupo de entrega no tiene máquinas sin asignar (todas las máquinas del grupo de entrega están asignadas), el búfer de capacidad no desempeña ningún papel en el encendido o apagado de las máquinas.
- La propiedad `AutomaticPowerOnForAssignedDuringPeak` determina si las máquinas asignadas se encienden durante las horas punta. Si se establece en true, Autoscale mantiene las máquinas encendidas durante las horas punta. Autoscale también las encenderá, incluso si están apagadas.

Directivas de energía

Configure directivas para administrar la energía de las máquinas en diferentes supuestos. Para cada supuesto, puede especificar el tiempo de espera (en minutos) y la acción prevista una vez finalizado el tiempo especificado. Las directivas de energía se aplican a los grupos de entrega aleatorios de SO de sesión única y a los grupos de entrega estáticos de SO de sesión única.



Para **Tras la desconexión** y **Tras el cierre de sesión**, se aplican los siguientes parámetros tanto en las horas punta como fuera de ellas: Puede establecer el tiempo de espera en minutos y acciones como no realizar ninguna acción, suspender o cerrar desde el menú desplegable.

Si ningún usuario inicia sesión después de encenderse la máquina con Autoscale, los siguientes parámetros solo se aplican durante las horas punta: Puede establecer el tiempo de espera en minutos y acciones como no realizar ninguna acción, suspender o apagar desde el menú desplegable durante las horas punta.

Caso de ejemplo

Supongamos que tiene ante usted este caso:

- **Configuración del grupo de entrega**. El grupo de entrega al que quiere aplicar Autoscale para administrar la energía contiene 10 máquinas (de M1 a M10).
- **Configuración de Autoscale**
  - Las máquinas que van de la M1 a la M3 se asignan, y las máquinas que van de la M4 a la M10, no.

  - El búfer de capacidad se establece en 10% para las horas punta y las horas normales.
  - Según la programación seleccionada, Autoscale administra la energía de las máquinas entre las 9:00 y las 18:00.

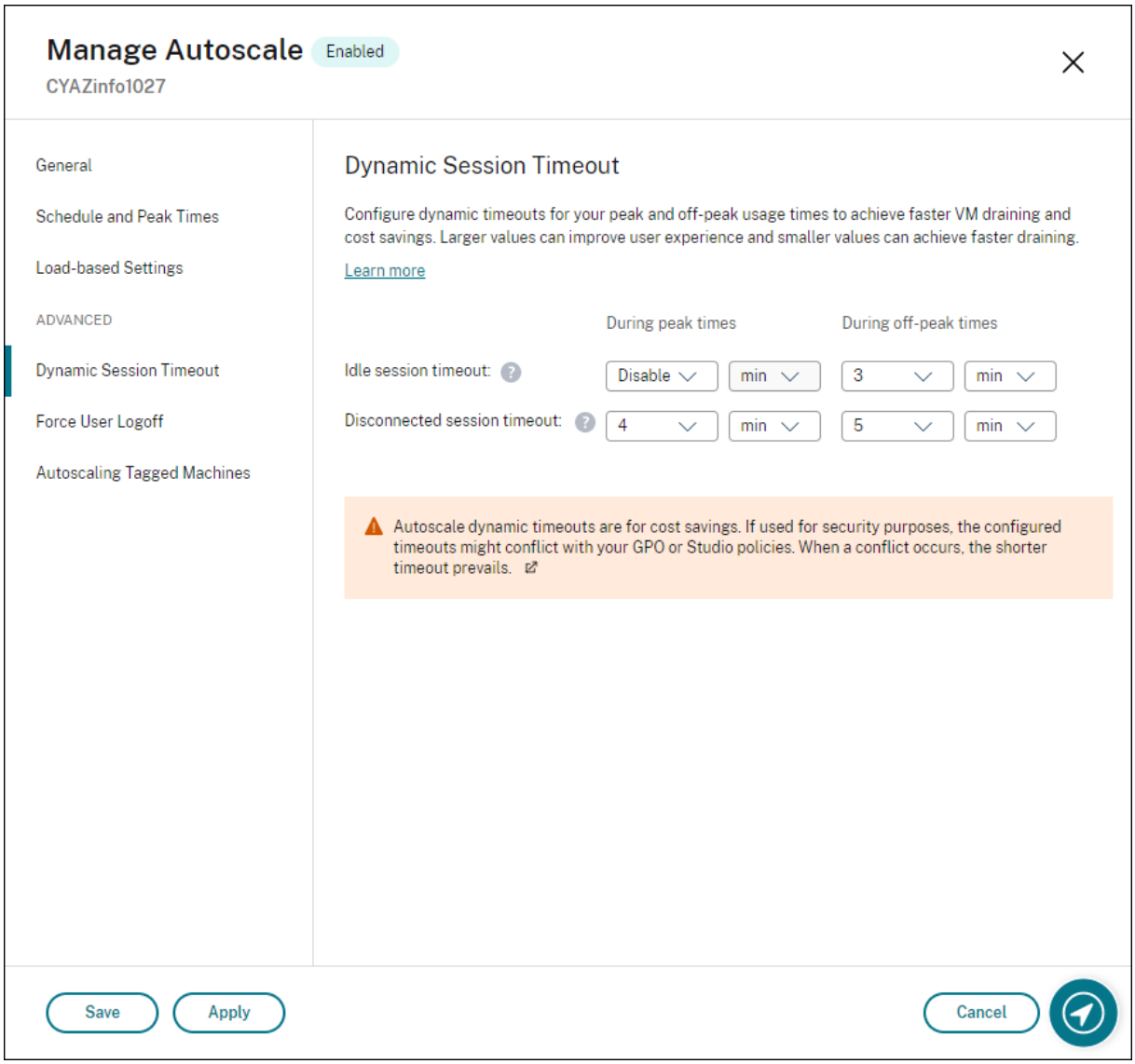
Consulte lo que hay a continuación para obtener información detallada sobre cómo funciona Autoscale en este escenario.

- Inicio de la programación: 9:00
  - Autoscale enciende las máquinas que van de la M1 a la M3.
  - Autoscale enciende una máquina adicional (por ejemplo, M4) debido al búfer de capacidad configurado. La máquina M4 no está asignada.
- Un primer usuario inicia sesión
  - La primera vez que un usuario inicia sesión para utilizar un escritorio, se le asigna un escritorio de un grupo de escritorios alojado en máquinas encendidas sin asignar. En este caso, al usuario se le asigna un escritorio de la máquina M4. Las siguientes conexiones del usuario se establecen con el mismo escritorio que se asignó la primera vez.
  - Autoscale comienza a encender una máquina adicional (por ejemplo, M5) para satisfacer la demanda debido al búfer de capacidad configurado.
- Un segundo usuario inicia sesión
  - Al usuario se le asigna un escritorio de las máquinas encendidas sin asignar. En este caso, al usuario se le asigna un escritorio de la máquina M5. Las siguientes conexiones del usuario se establecen con el mismo escritorio que se asignó la primera vez.
  - Autoscale comienza a encender una máquina adicional (por ejemplo, M6) para satisfacer la demanda debido al búfer de capacidad configurado.
- Los usuarios cierran la sesión
  - A medida que los usuarios cierran la sesión de sus máquinas de escritorio o transcurren los tiempos de espera de estas, Autoscale mantiene encendidas de la máquina M1 a la M5 entre las 9:00 y las 18:00. La próxima vez que esos usuarios inician sesión, se conectan al mismo escritorio que se asignó la primera vez.
  - La máquina sin asignar M6 está esperando para publicar un escritorio para un usuario entrante y sin asignar.
- Fin de la programación: 18:00
  - A las 18:00, Autoscale apaga de la máquina M1 a la M5.
  - Autoscale mantiene encendida la máquina M6 sin asignar debido al búfer de capacidad configurado. Esa máquina está esperando para publicar un escritorio para un usuario entrante y sin asignar.
  - En el grupo de entrega, las máquinas que van de la M6 a la M10 son máquinas sin asignar.

Tiempos de espera de sesión dinámicos

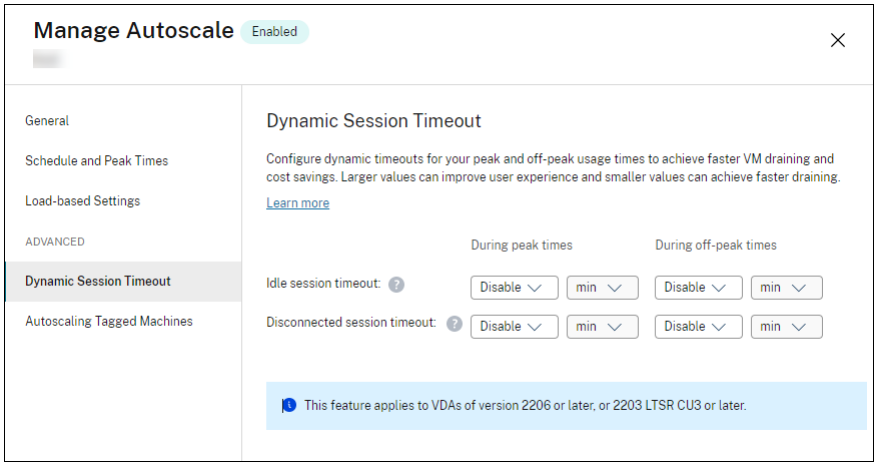
August 17, 2024

Esta función le permite configurar los tiempos de espera de sesión por desconexión y por inactividad para los tiempos de uso de horas punta y horas normales con el fin de lograr una purga más rápida de las máquinas y ahorrar costes. Esta función se aplica a máquinas con SO de sesión única y multi-sesión. Un VDA registra tiempos de inactividad de las sesiones que han estado inactivas durante más de 10 minutos, por lo que los tiempos de espera dinámicos de las sesiones no podrán desconectar las sesiones inactivas durante esos 10 minutos de inactividad. Un valor menor elimina las sesiones persistentes antes, lo que reduce los costes.



Nota:

- Esta función siempre está disponible para grupos de entrega con SO multisesión.
- Para los grupos de entrega con SO de sesión única, esta función se aplica a los VDA con la versión 2206 CR o una posterior, o con la 2203 LTSR CU3 o una posterior. Asegúrese de que dichos VDA se hayan registrado en Citrix Cloud al menos una vez. Cuando no está disponible, aparece esta interfaz de usuario:



- Los tiempos de espera dinámicos de Autoscale son para ahorrar costes. Si se utilizan por motivos de seguridad, es posible que los tiempos de espera configurados entren en conflicto con sus directivas de GPO o de la consola Administrar. Cuando se produce un conflicto, prevalece el menor tiempo de espera.

Tiempo de espera de sesión por inactividad. Habilita o inhabilita un temporizador que especifica cuánto tiempo se mantiene una conexión de usuario ininterrumpida si no hay ninguna acción por parte del usuario. Cuando se agota el tiempo de este temporizador, la sesión pasa al estado desconectado y se aplica el **Tiempo de espera de sesión por desconexión**. Si el **Tiempo de espera de sesión por desconexión** está inhabilitado, la sesión no se cierra.

Importante:

- Si especifica un valor inferior o igual a 10 minutos (600 segundos), Autoscale desconecta las sesiones correspondientes después de que hayan estado inactivas durante 10 minutos. Esto se debe a que Autoscale se basa en los tiempos de inactividad de las sesiones que registran los VDA. Los VDA registran tiempos de inactividad solo para las sesiones que hayan estado inactivas durante más de 10 minutos.
- Una sesión inactiva seguirá pasando al estado desconectado si el usuario interactúa con ella dentro de los 5 últimos minutos de alcanzar el tiempo de espera de la sesión inactiva.

Tiempo de espera de sesión por desconexión. Habilita o inhabilita un temporizador para determinar cuánto tiempo permanece desconectado un escritorio antes de que se cierre la sesión. Si se

habilita, la sesión desconectada se cierra cuando se agota el tiempo del temporizador.

Autoscale de máquinas etiquetadas (ampliación en la nube)

August 17, 2024

> **Nota:**
>
> Esta función se denominaba anteriormente Restringir Autoscale.

Introducción

Autoscale proporciona la flexibilidad necesaria para administrar la energía solo en un subconjunto de máquinas de un grupo de entrega. Para hacer esto, aplique una etiqueta a una o varias máquinas y, a continuación, configure Autoscale para que administre solo las máquinas etiquetadas.

Esta función puede ser útil en casos de uso de "cloud bursting"(ampliación en la nube), en los que quiera utilizar los recursos locales (o instancias reservadas de nube pública) para gestionar las cargas de trabajo antes de usar los basados en la nube para hacer frente a la demanda adicional (es decir, cargas de trabajo en ráfagas). Para que las máquinas locales (o las instancias reservadas) se encarguen de las cargas de trabajo primero, debe usar la restricción por etiquetas junto con la preferencia de zonas.

La restricción por etiquetas especifica qué máquinas se administrarán con Autoscale. La preferencia de zona especifica qué máquinas de la zona preferida gestionarán las solicitudes de inicio del usuario. Para obtener más información, consulte Etiquetas y Preferencias de zona.

Para administrar con Autoscale determinadas máquinas etiquetadas, puede usar la consola Administrar o PowerShell.

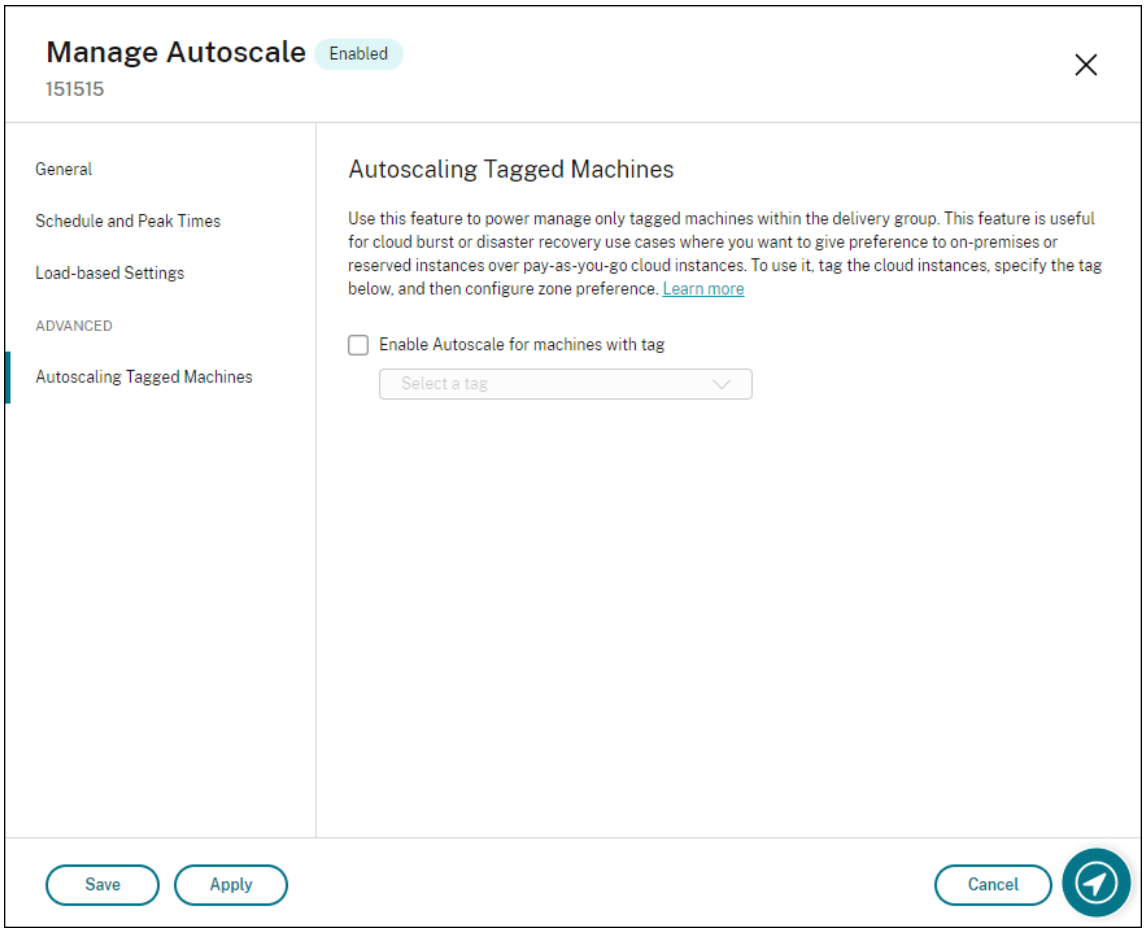
Usar la consola Administrar para administrar con Autoscale determinadas máquinas etiquetadas

Para administrar con Autoscale ciertas máquinas etiquetadas, complete los siguientes pasos:

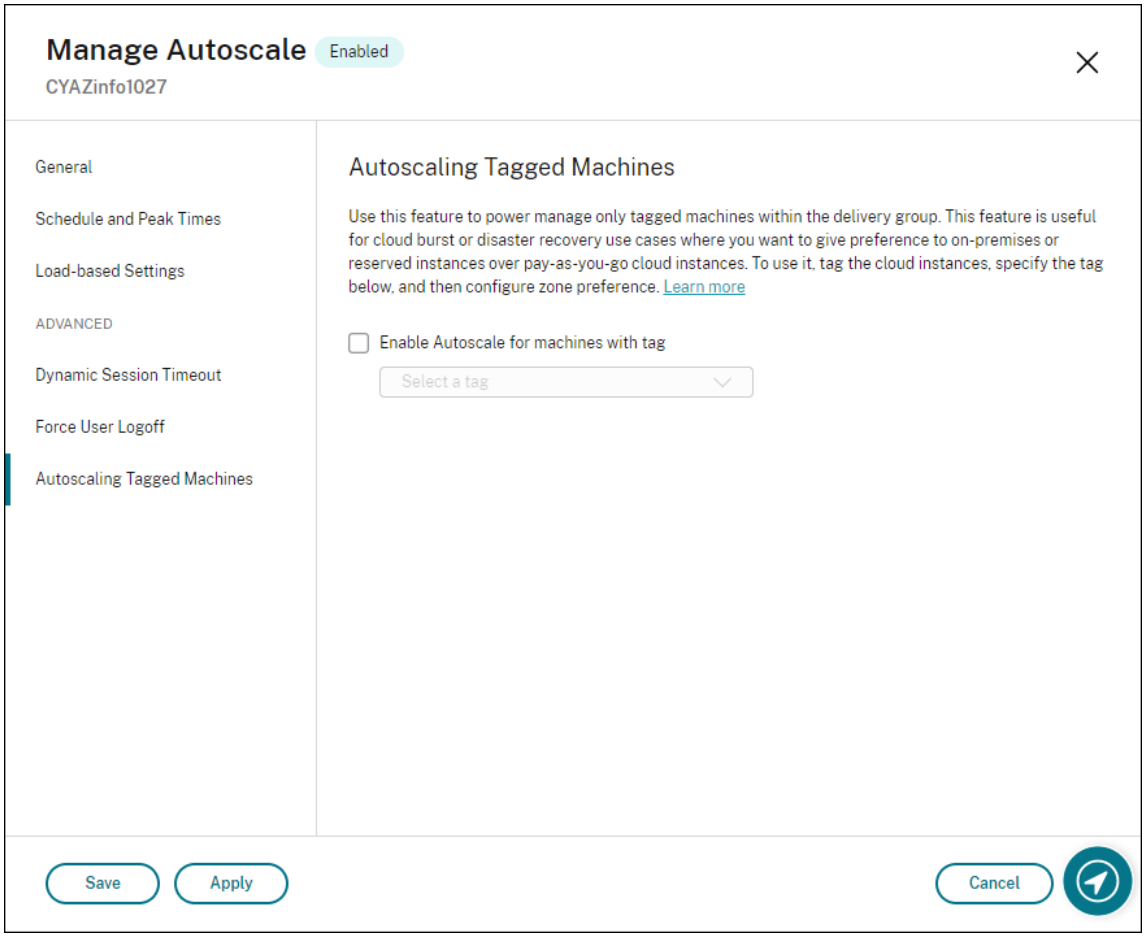
1. Cree una etiqueta y aplíquela a las máquinas correspondientes del grupo de entrega. Para obtener más información, consulte Administrar etiquetas y restricciones por etiqueta.
2. Seleccione el grupo de entrega y, a continuación, abra el asistente **Administrar Autoscale**.

3. En la página **Autoscale de máquinas etiquetadas**, seleccione **Habilitar Autoscale para máquinas con etiquetas**, seleccione una etiqueta de la lista y, a continuación, haga clic en **Aplica** para guardar los cambios.

   Interfaz de usuario para grupos de entrega *estáticos* y *aleatorios* de SO de sesión única:



   Interfaz de usuario para *grupos de entrega de SO multisesión*:



Advertencia:

- Es posible que, al usar Autoscale en máquinas con una etiqueta específica, el histograma se actualice automáticamente para reflejar la cantidad de máquinas para la etiqueta. En la página **Programación y horas punta**, puede asignar máquinas manualmente en cada intervalo de tiempo si fuera necesario.
- No puede eliminar una etiqueta que se esté utilizando en máquinas. Para eliminarla, primero debe eliminar la restricción de las etiquetas en cuestión.

Después de aplicar la restricción por etiquetas, es posible que quiera quitarla del grupo de entrega más tarde. Para eso, vaya a la página **Administrar Autoscale > Autoscale de máquinas etiquetadas** y desactive **Habilitar Autoscale para máquinas con etiquetas**.

Advertencia:

- Si quita la etiqueta de las máquinas correspondientes sin desmarcar **Habilitar Autoscale para máquinas con etiquetas**, es posible que reciba una advertencia al abrir el asistente **Administrar Autoscale**. Al quitar la etiqueta de las máquinas, es posible que no queden

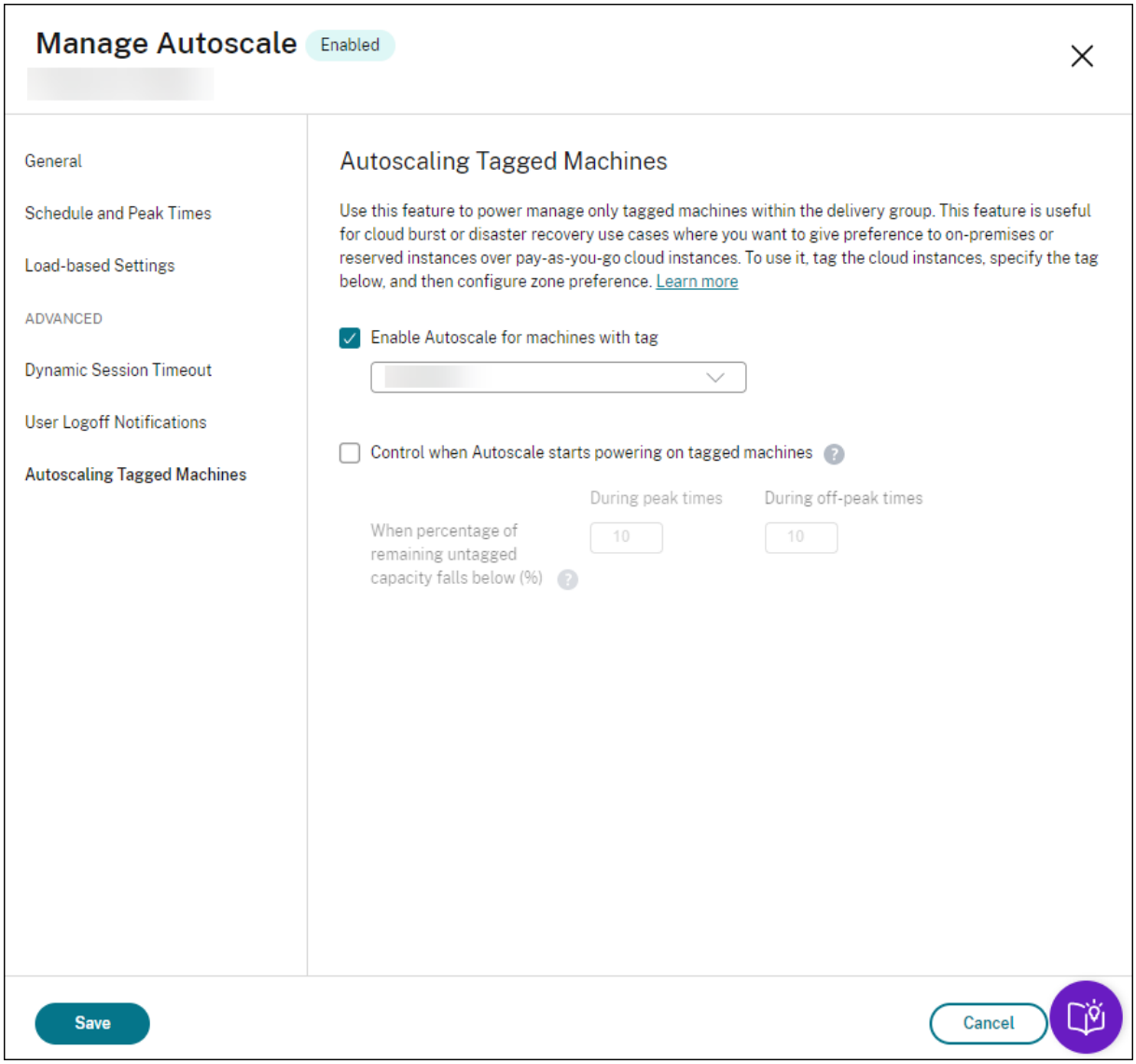
> máquinas por administrar para Autoscale porque la etiqueta especificada en Autoscale no es válida. Para resolver esto, vaya a la página **Autoscale de máquinas etiquetadas**, quite la etiqueta no válida y, a continuación, haga clic en **Aplicar** para guardar los cambios.

Controlar cuándo Autoscale enciende los recursos

También puede controlar cuándo Autoscale comienza a encender máquinas etiquetadas en función del uso de máquinas sin etiquetar. De esta forma, puede optimizar aún más el consumo de sus cargas de trabajo de nube pública o etiquetadas.

Para eso, complete los pasos siguientes:

1. En la página **Autoscale de máquinas etiquetadas**, seleccione **Controle cuándo Autoscale comienza a encender máquinas etiquetadas**.
2. Introduzca la cantidad porcentual de uso de máquinas sin etiquetar que desea alcanzar tanto para las horas punta como para las horas no punta y, a continuación, haga clic en **Aplicar**. Valores admitidos: 0—100.



Sugerencia:

El porcentaje controla el momento en que AutoScale comienza a encender las máquinas etiquetadas. Cuando el porcentaje cae por debajo del umbral (el valor predeterminado es 10%), Autoscale comienza a encender las máquinas etiquetadas. Cuando el porcentaje supera el umbral, Autoscale pasa al modo de apagado. Al introducir el porcentaje, considere dos situaciones:

- Para grupos de entrega con SO de sesión única: El valor se define como un porcentaje de la cantidad total de máquinas sin etiquetar en estado inactivo. Ejemplo: Tiene 10 máquinas con sistema operativo de sesión única sin etiquetar. Cuando solo queda una sin sesión, AutoScale comienza a encender una máquina etiquetada.
- Para grupos de entrega con SO multisesión: El valor se define como un porcentaje de la capacidad total (en términos de índice de carga) de las máquinas sin etiquetar disponibles.

> Ejemplo: Tiene 10 máquinas con sistema operativo multisesión sin etiquetar. Cuando están cargadas al 90%, AutoScale comienza a encender una máquina etiquetada.

Usar PowerShell para administrar con Autoscale determinadas máquinas etiquetadas

Para usar el SDK de PowerShell directamente, siga estos pasos:

1. **Cree una etiqueta.** Utilice el comando New-Brokertag de PowerShell para crear una etiqueta.
   - Por ejemplo: `$managed = New-BrokerTag Managed`. En este caso, la etiqueta se denomina "Managed". Para obtener más información acerca del comando New-Brokertag de PowerShell, consulte https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/New-BrokerTag/.
2. **Aplique la etiqueta a máquinas**. Utilice el comando Get-Brokermachine de PowerShell para aplicar la etiqueta a las máquinas de un catálogo en las que quiere que Autoscale administre la energía.
   - Por ejemplo: `Get-BrokerMachine -CatalogName "cloud" | Add-BrokerTag $managed.Name`. En este caso, el catálogo se denomina "cloud".
   - Para obtener más información acerca del comando Get-Brokermachine de PowerShell, consulte https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerMachine/.

   > **Nota:**
   >
   > Puede agregar nuevas máquinas al catálogo después de aplicar la etiqueta. La etiqueta *NO* se aplica automáticamente a esas nuevas máquinas.

3. **Agregue máquinas etiquetadas al grupo de entrega en el que quiere que Autoscale administre la energía.** Utilice el comando Get-BrokerDesktopGroup de PowerShell para agregar una restricción por etiqueta al grupo de entrega que contiene las máquinas (es decir, "restringir el inicio a las máquinas con la etiqueta X").
   - Por ejemplo: `Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagUid $managed.Uid`. En este caso, el UID del grupo de entrega es 1.
   - Para obtener más información acerca del comando Get-BrokerDesktopGroup de PowerShell, consulte https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/.

Después de aplicar la restricción por etiquetas, es posible que quiera quitarla del grupo de entrega más tarde. Para eso, utilice el comando Get-BrokerDesktopGroup de PowerShell.

Ejemplo: `Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscal $null`. En este caso, el UID del grupo de entrega es 1.

> **Nota:**
>
> Las máquinas sin etiquetar se reinician automáticamente después de que los usuarios las apaguen. Este sistema garantiza que estén disponibles para gestionar las cargas de trabajo antes. Esto se puede habilitar o inhabilitar por grupo de escritorios a través de la propiedad `AutomaticRestartForUntaggedMachines` de `Set-BrokerDesktopGroup`. Para obtener más información, consulte https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/.

Caso de ejemplo

Supongamos que tiene ante usted este caso:

- **Configuración del catálogo de máquinas**. Hay dos catálogos de máquinas (C1 y C2).
  - El catálogo C1 contiene 5 máquinas (M1 a M5) que son locales en implementaciones locales.
  - El catálogo C2 contiene 5 máquinas (M6 a M10) que son remotas en implementaciones en la nube.
- **Restricción por etiquetas**. Se crea una etiqueta denominada "Cloud", la cual se aplica a las máquinas M6 a M10 del catálogo C2.
- **Configuración de zonas**. Se crean dos zonas (Z1 y Z2).
  - La zona Z1 que contiene el catálogo C1 corresponde a las implementaciones locales.
  - La zona Z2 que contiene el catálogo C2 corresponde a las implementaciones en la nube.
- **Configuración del grupo de entrega**
  - El grupo de entrega contiene 10 máquinas (de M1 a M10), 5 máquinas del catálogo C1 (de M1 a M5) y 5 del catálogo C2 (de M6 a M10).
  - Las máquinas M1 a M5 se encienden manualmente y permanecen encendidas durante toda la programación.
- **Configuración de Autoscale**
  - El búfer de capacidad es del 10%.
  - AutoScale administra solo la energía de las máquinas que tienen la etiqueta "Cloud". En este caso, Autoscale administra la energía de las máquinas M6 a M10 en la nube.

- **Configuración de escritorios o aplicaciones publicados**. Las preferencias de zona se configuran para los escritorios publicados (por ejemplo), donde hay preferencia de la Zona Z1 sobre la Zona Z2 para las solicitudes de inicio del usuario.
  - La zona Z1 se configura como la zona preferida (zona particular) para los escritorios publicados.

El escenario se desarrolla de la siguiente manera:

1. Ningún usuario inicia sesión.
2. Las sesiones de usuario aumentan.
3. Las sesiones de usuario aumentan hasta que se consumen todas las máquinas locales disponibles.
4. Se inician más sesiones de usuario.
5. Las sesiones de usuario disminuyen por la finalización de sesiones.
6. Las sesiones de usuario disminuyen aún más hasta que la carga de sesiones se controla solamente mediante máquinas locales.

Consulte lo que hay a continuación para obtener información detallada sobre cómo funciona Autoscale en este escenario.

- Sin carga de usuarios (estado inicial)
  - Todas las máquinas locales, M1 a M5, están encendidas.
  - Una máquina en la nube (por ejemplo, M6) está encendida. La máquina se enciende debido al búfer de capacidad configurado. En este caso, 10 (cantidad de máquinas) x 10 000 (índice de carga) x 10% (búfer de capacidad configurado) equivale a 10 000. Por lo tanto, se enciende una máquina.
  - El valor del índice de carga de las máquinas encendidas (M1 a M6) se halla en una carga base (el índice de carga es igual a 0).
- Los usuarios inician sesión
  - Las sesiones se dirigen para alojamiento en las máquinas M1 a M5, según la preferencia de zona configurada y existe un equilibrio de carga entre estas máquinas locales.
  - El valor del índice de carga de las máquinas encendidas (M1 a M5) aumenta.
  - El valor del índice de carga de la máquina encendida (M6) se halla en una carga base.
- Los usuarios aumentan la carga y se consumen todos los recursos locales
  - Las sesiones se dirigen para alojamiento en las máquinas M1 a M5, según la preferencia de zona configurada y existe un equilibrio de carga entre estas máquinas locales.
  - El índice de carga de todas las máquinas encendidas (M1 a M5) ha alcanzado el valor 10 000.
  - El valor del índice de carga de la máquina encendida (M6) permanece en una carga base.

- Un usuario más inicia sesión
  - La sesión desborda la preferencia de zona y se dirige para alojamiento en la máquina M6 en la nube.
  - El índice de carga de todas las máquinas encendidas (M1 a M5) ha alcanzado el valor 10 000.
  - El valor del índice de carga de la máquina encendida (M6) aumenta y deja de estar en una carga base. Cuando la capacidad total de reserva cae por debajo de 10 000 en términos de índice de carga, Autoscale comienza a encender una máquina adicional (M7) para satisfacer la demanda debido al búfer de capacidad configurado. La máquina M7 podría tardar un tiempo en encenderse. Por tanto, podría haber una demora hasta que la máquina M7 esté lista.
- Más usuarios inician sesión
  - Las sesiones se dirigen para alojamiento en la máquina M6.
  - El índice de carga de todas las máquinas encendidas (M1 a M5) ha alcanzado el valor 10 000.
  - El valor del índice de carga de la máquina M6 encendida sigue aumentando, pero la capacidad total de reserva está por encima de 10 000 en términos del índice de carga.
  - El valor del índice de carga de la máquina encendida (M7) permanece en una carga base.
- Aún más usuarios inician sesión
  - Una vez que la máquina M7 está lista, las sesiones se dirigen para alojamiento en las máquinas M6 y M7 y la carga se equilibra entre estas máquinas.
  - El índice de carga de todas las máquinas encendidas (M1 a M5) ha alcanzado el valor 10 000.
  - El valor del índice de carga de la máquina M7 deja de estar en una carga base.
  - El valor del índice de carga de las máquinas encendidas (M6 y M7) aumenta.
  - La capacidad total de reserva sigue estando por encima de 10 000 en términos de índice de carga.
- La carga de las sesiones de usuario disminuye debido a la finalización de sesiones
  - Después de que los usuarios hayan cerrado sus sesiones o tras agotarse el tiempo de espera de las sesiones inactivas, la capacidad liberada de las máquinas M1 a M7 se reutiliza para alojar sesiones iniciadas por otros usuarios.
  - Cuando la capacidad total de reserva está por encima de 10 000 en términos de índice de carga, Autoscale pone una de las máquinas (M6 a M7) en estado de purga. Como resultado, las sesiones iniciadas por otros usuarios ya no se dirigen a esa máquina (por ejemplo, M7), a menos que se produzcan nuevos cambios; por ejemplo, la carga del usuario final aumenta de nuevo o las demás máquinas en la nube se cargan menos.

- La carga de la sesión de usuario disminuye aún más hasta que ya no se necesitan uno o más máquinas en la nube
  - Una vez finalizadas todas las sesiones de la máquina M7 y transcurrida la demora de apagado especificada, Autoscale apaga la máquina M7.
  - El valor del índice de carga de todas las máquinas encendidas (M1 a M5) podría caer a un nivel inferior a 10 000.
  - El valor del índice de carga de la máquina encendida (M6) aumenta.
- Las sesiones de usuario disminuyen, hasta un nivel en que no se necesitan máquinas en la nube.
  - Aunque no hay sesiones de usuario en la máquina M6, Autoscale no la apaga, porque esa máquina queda reservada como capacidad de reserva.
  - Autoscale mantiene encendida la máquina M6 en la nube, debido al búfer de capacidad configurado. Esa máquina está esperando para publicar un escritorio para un usuario entrante.
  - Las sesiones no se dirigen para alojarse en la máquina M6 siempre que las máquinas locales tengan capacidad disponible.

Notificaciones de cierre de sesión del usuario (antes denominado "forzar el cierre de sesión del usuario")

August 17, 2024

> **Importante:**
>
> Esta funcionalidad solo está disponible en la interfaz de usuario de Autoscale para grupos de entrega multisesión basados en aplicaciones.

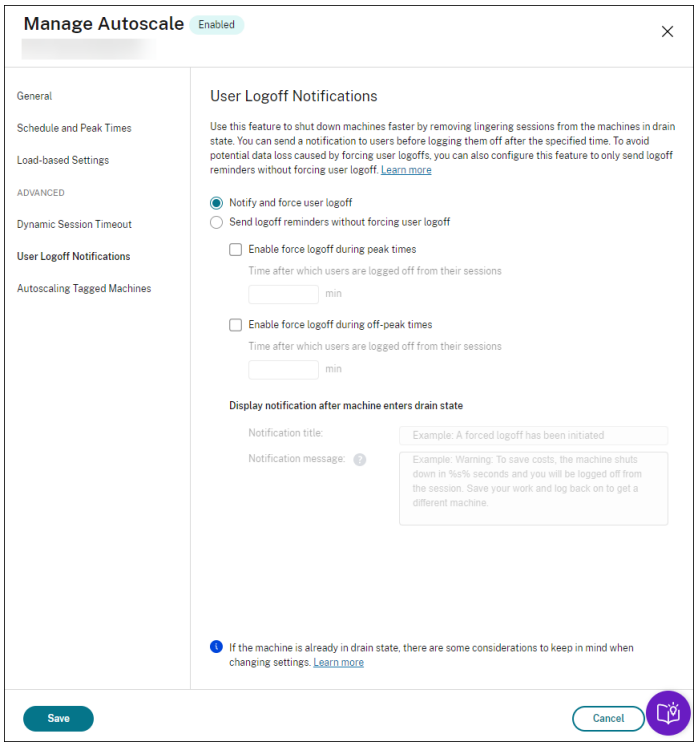
Para ahorrar más costes, Autoscale le permite forzar la cierre de sesión de las sesiones persistentes. Para ello, le permite enviar una notificación personalizada a los usuarios y especificar un período de gracia tras el cual se fuerza el cierre de sesión de las sesiones. Esto se hace solo para máquinas en el estado de purga y no para todas las máquinas encendidas. Para evitar la posible pérdida de datos causada por el cierre de sesión forzado, puede configurar esta función para que solo envíe recordatorios de cierre de sesión sin forzar el cierre de sesión del usuario.

Dispone de estas dos opciones:

- **Notificar y forzar al usuario a cerrar la sesión**
- **Enviar recordatorios de cierre de sesión sin forzar al usuario a cerrar sesión**

Notificar y forzar al usuario a cerrar la sesión

Si se selecciona, Autoscale cierra la sesión de los usuarios después de las horas especificadas a continuación.



Habilitar cierre de sesión forzado durante horas punta. Si se selecciona, Autoscale cerrará la sesión de esos usuarios durante las horas punta cuando transcurra el tiempo indicado.

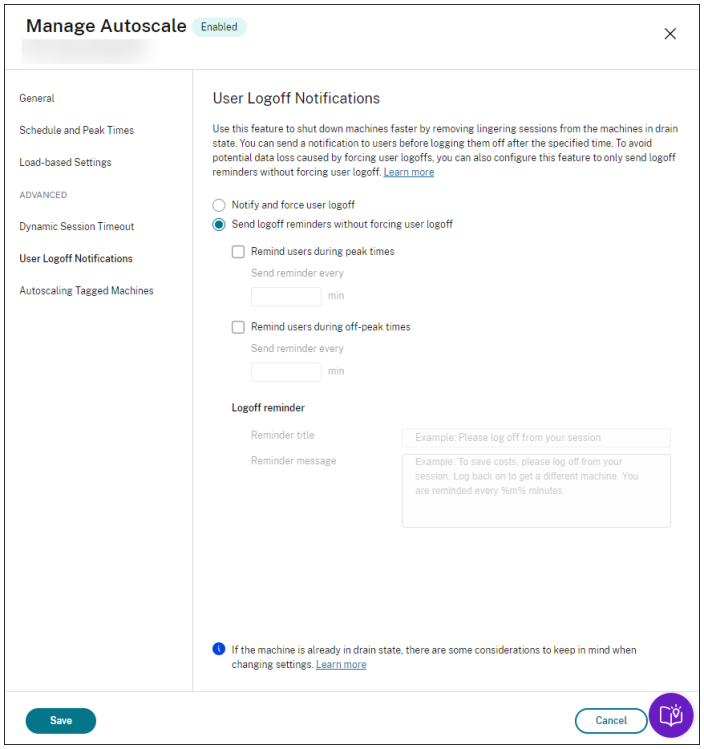
Habilitar cierre de sesión forzado durante horas normales. Si se selecciona, Autoscale cerrará la sesión de esos usuarios durante las horas de baja actividad cuando transcurra el tiempo indicado.

Mostrar una notificación cuando la máquina entra en estado de purga. Le permite enviar notificaciones a los usuarios después de que su máquina haya entrado en estado de purga.

- **Título de la notificación**. Permite especificar un título de la notificación que se enviará a los usuarios. Ejemplo:`A forced logoff has been initiated`.
- **Mensaje de notificación**. Permite especificar el contenido de la notificación que se enviará a los usuarios. Puede utilizar %s% o %m% como variables para indicar la hora especificada en el mensaje. Para expresar el tiempo en segundos, utilice %s%. Para expresar el tiempo en minutos, utilice %m%. Ejemplo: `Warning: To save costs, the machine shuts down in %s% seconds and you will be logged off from the session. Save your work and log back on to get a different machine`.

Enviar recordatorios de cierre de sesión sin forzar al usuario a cerrar sesión

Si se selecciona, los usuarios recibirán un recordatorio para cerrar la sesión de sus máquinas después de que estas hayan entrado en estado de purga. Este recordatorio se puede configurar para que se envíe en el intervalo especificado a continuación.



Enviar un recordatorio a los usuarios durante las horas punta. Si se selecciona, los usuarios reciben un recordatorio para que cierren sus sesiones durante las horas punta cada X minutos (X indica el tiempo especificado).

Enviar un recordatorio a los usuarios durante las horas normales. Si se selecciona, los usuarios reciben un recordatorio para que cierren sus sesiones durante las horas de menor actividad cada X minutos (X indica el tiempo especificado).

Recordatorio de cierre de sesión. Le permite configurar el recordatorio que se envía a los usuarios después de que su máquina haya entrado en estado de purga.

- **Título del recordatorio**. Le permite especificar un título para que el recordatorio se envíe a los usuarios. Ejemplo: `Please log off from your session`.
- **Mensaje del recordatorio**. Le permite especificar un mensaje que se enviará a los usuarios. Ejemplo: `Please log off from your session and log back on to save costs`.

Consideraciones

Si la máquina ya se halla en estado de purga, tenga en cuenta lo siguiente al cambiar parámetros:

- Si cambia el parámetro de **Enviar recordatorios de cierre de sesión sin forzar al usuario a cerrar sesión** a **Notificar y forzar al usuario a cerrar sesión**, el nuevo parámetro se aplica de inmediato.
- Si cambia el parámetro de **Notificar y forzar al usuario a cerrar sesión** a **Enviar recordatorios de cierre de sesión sin forzar al usuario a cerrar sesión**, el nuevo parámetro no se aplicará hasta la próxima vez que la máquina entre en estado de purga. Se sigue forzando al usuario a cerrar la sesión.

Comandos del SDK de Broker PowerShell

August 17, 2024

Puede configurar Autoscale para grupos de entrega mediante el SDK de Broker PowerShell. Para configurar Autoscale con comandos de PowerShell, debe utilizar la versión 7.21.0.12 del SDK de PowerShell o una posterior. Para obtener más información sobre los SDK de PowerShell, consulte SDK y API.

Set-BrokerDesktopGroup

Inhabilita o habilita un grupo BrokerDesktopGroup o altera su configuración. Para obtener más información sobre este cmdlet, consulte https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/.

Ejemplos

Consulte los ejemplos siguientes para obtener información detallada sobre cómo utilizar los cmdlets de PowerShell.

Habilitar Autoscale

- Supongamos que quiere habilitar Autoscale para el grupo de entrega “MyDesktop”. Utilice el comando `Set-BrokerDesktopGroup` de PowerShell. Por ejemplo:

  ```
  - PS C:\> Set-BrokerDesktopGroup "MyDesktop"-AutoscalingEnabled
    $true
  ```


Configurar el búfer de capacidad por separado para las horas punta y las horas normales

- Supongamos que quiere establecer el búfer de capacidad en un 20 % para las horas punta y un 10 % para las horas de actividad normal en el grupo de entrega "MyDesktop". Utilice el comando `Set-BrokerDesktopGroup` de PowerShell. Por ejemplo:

  ```
  PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakBufferSizePercent
  20 -OffPeakBufferSizePercent 10
  ```

Configurar el parámetro del **tiempo de espera cuando se desconecta**

- Supongamos que quiere establecer el valor del **tiempo de espera cuando se desconecta** en 60 minutos para las horas punta y 30 minutos para las horas de actividad normal para un grupo de entrega llamado "MyDesktop". Utilice el comando `Set-BrokerDesktopGroup` de PowerShell. Por ejemplo:

  ```
  PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakDisconnectTimeout
  60 -OffPeakDisconnectTimeout 30
  ```

Configurar el parámetro del **tiempo de espera cuando se cierra la sesión**

- Supongamos que quiere establecer el valor del **tiempo de espera cuando se cierra la sesión** en 60 minutos para las horas punta y 30 minutos para las horas de actividad normal para un grupo de entrega llamado "MyDesktop". Utilice el comando `Set-BrokerDesktopGroup` de PowerShell. Por ejemplo:

  ```
  PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakLogOffTimeout
  60 -OffPeakLogOffTimeout 30
  ```

Configurar el parámetro de **demora de apagado**

- Supongamos que quiere establecer la demora de apagado en 15 minutos para el grupo de entrega "MyDesktop". Utilice el comando `Set-BrokerDesktopGroup` de PowerShell. Por ejemplo:

  ```
  PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PowerOffDelay 15
  ```

Configurar un período de tiempo durante el cual la demora del apagado no se produzca

- Supongamos que quiere que la demora del apagado no se produzca hasta que hayan transcurrido 30 minutos para el grupo de entrega "MyDesktop". Utilice el comando `Set-BrokerDesktopGroup` de PowerShell. Por ejemplo:

  ```
  C:\PS> Set-BrokerDesktopGroup "MyDesktop"-SettlementPeriodBeforeAutoSh
  30.
  ```

Configurar el parámetro del **coste de instancia de máquina**

- Supongamos que quiere establecer el coste de instancia de máquina por hora en 0,2 USD para el grupo de entrega "MyDesktop". Utilice el comando `Set-BrokerDesktopGroup` de PowerShell. Por ejemplo:

  ```
  - PS C:\> Set-BrokerDesktopGroup "MyDesktop"-MachineCost 0.2
  ```

New-BrokerPowerTimeScheme

Crea un esquema BrokerPowerTimeScheme para un grupo de entrega. Para obtener más información, consulte https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerPowerTimeScheme/.

Ejemplo

Supongamos que quiere crear un esquema de tiempo de energía para un grupo de entrega cuyo valor UID es 3. El nuevo esquema cubre el fin de semana, el lunes y el martes. La franja horaria de 8:00 a 18:30 se define como horas punta en los días incluidos en el esquema. Para las horas punta, el tamaño del grupo (la cantidad de máquinas que se mantienen encendidas) es 20. Para las horas normales, es 5. Puede utilizar el comando `Set-BrokerDesktopGroup` de PowerShell. Por ejemplo:

- `PS C:\> $ps48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37){ 5 } else { 20 } } )`
- `PS C:\> $pt48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37){ $false } else { $true } } )`
- `PS C:\> New-BrokerPowerTimeScheme -Name 'First Half Week'-DaysOfWeek Weekend,Monday,Tuesday -DesktopGroupUid 3 -PeakHalfHours $pt48 -PoolSize $ps48`

Parámetros para los tiempos de espera dinámicos de las sesiones

Estos cmdlets del SDK de Broker PowerShell se han ampliado para permitir tiempos de espera de sesión dinámicos gracias a varios parámetros nuevos:

- Get-BrokerDesktopGroup
- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup

Estos parámetros incluyen:

- **DisconnectPeakIdleSessionAfterSeconds**: Representa el tiempo en segundos tras el cual se desconecta una sesión inactiva durante las horas punta. Esta propiedad tiene un valor predeterminado de 0, que indica la inhabilitación de su comportamiento asociado durante las horas

punta. Un valor superior a 0 habilita su comportamiento para el grupo de entrega solamente durante las horas punta.

- **DisconnectOffPeakIdleSessionAfterSeconds**: Representa el tiempo en segundos tras el cual se desconecta una sesión inactiva durante las horas de actividad normal. El valor predeterminado de esta propiedad es 0, lo que indica la inhabilitación de su comportamiento asociado durante las horas de actividad normal. Un valor superior a 0 habilita su comportamiento asociado para el grupo de entrega solamente durante las horas de actividad normal.
- **LogoffPeakDisconnectedSessionAfterSeconds**: Representa el tiempo en segundos tras el cual finaliza una sesión desconectada durante las horas punta. El valor predeterminado de esta propiedad es 0, lo que indica la inhabilitación de su comportamiento asociado durante las horas punta. Un valor superior a 0 habilita su comportamiento asociado para el grupo de entrega solamente durante las horas punta.
- **LogoffOffPeakDisconnectedSessionAfterSeconds**: Representa el tiempo en segundos tras el cual finaliza una sesión desconectada durante las horas de actividad normal. El valor predeterminado de esta propiedad es 0, lo que indica la inhabilitación de su comportamiento asociado durante las horas de actividad normal. Un valor superior a 0 habilita su comportamiento asociado para el grupo de entrega solamente durante las horas de actividad normal.

Ejemplo

Supongamos que quiere establecer el tiempo de espera de sesión inactiva en 3600 segundos durante las horas punta de un grupo de entrega cuyo nombre es "MyDesktop". Utilice el comando `Set-BrokerDesktopGroup` de PowerShell. Por ejemplo:

- `C:\PS> Set-BrokerDesktopGroup "MyDesktop"-DisconnectOffPeakIdleSessionAfte`
  `3600`

Al hacerlo, se desconectan las sesiones que hayan estado inactivas durante más de 1 hora en horas normales para el grupo de escritorios denominado "MyDesktop".

Citrix Insight Services

August 17, 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:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name
    SendExperienceMetrics -PropertyType DWORD -Value 0
```

- 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 **Parámetros** en el panel de la izquierda de Web Studio y desactive el parámetro **Citrix Customer Experience Improvement Program**.

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
```

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
  ```

  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
        -UploadFrequency {
  3  Daily|Weekly }
  ```

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.


```
$timespan – New-TimeSpan –Hours 22 –Minutes 20
Set-CitrixCallHomeSchedule –TimeOfDay $timespan -UploadFrequency Daily
```

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.

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20
Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek Wed -
    UploadFrequency Weekly
```

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.

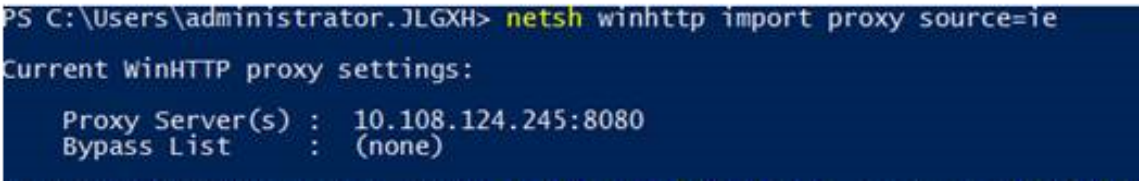
```
Enable-CitrixTrace -Listen'{ "trace":{ "enabled":false,"persistDirectory
":"C:\Users\Public","maxSizeBytes":1000000, "sliceDurationSeconds
":300 } } '
```

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`.



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.

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:

```
Start-CitrixCallHomeUpload [-Credential] PSCredential [-InputPath
    string] [-Description string] [-IncidentTime string] [-SRNumber
    string] [-Name string] [-UploadHeader string] [-AppendHeaders string
    ] [-Collect string] [<CommonParameters>]
```

Recopilar datos para guardarlos localmente:

```
Start-CitrixCallHomeUpload -OutputPath <String> [-InputPath string] [-
    Description string] [-IncidentTime string] [-SRNumber string] [-Name
     string] [-UploaderHeader string] [-AppendHeaders string] [-Collect
    strings] [<CommonParameters>]
```


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 <PSCredentia\> -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.

```
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 "{
 'wmi':{
 'enabled':false }
  }
 " -UploadHeader "{
 'key1':'value1' }
 " -AppendHeaders "{
 'key2':'value2' }
 "
```

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.

```
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
```

El cmdlet siguiente carga el paquete de los datos que guardó previamente.

```
$cred=Get-Credential
C:\PS>Send-CitrixCallHomeBundle  – Credential $cred -Path \mynetwork\
    myshare\mydata.zip
```

Citrix Scout

August 17, 2024

Introducción

Citrix Scout recopila diagnósticos y realiza comprobaciones de estado. Puede utilizar los resultados para el mantenimiento 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, Virtual Delivery Agents (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.

> **Nota:**
>
> Los procedimientos **Rastrear y reproducir**, **Programar** y **Comprobación de estado** no están disponibles por ahora para Linux VDA.

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 que use Citrix DaaS (antes, Citrix Virtual Apps and Desktops Service), 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 %PROGRAMDATA%\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.

Configuración de Scout

Scout se puede configurar para que funcione en Linux VDA. Para obtener más información sobre Linux VDA y telemetría, consulte Integración con Citrix Telemetry Service

Es posible que Linux VDA cambie automáticamente el puerto del socket `ctxtelemetry` o el puerto del servicio de telemetría. Si eso ocurre, debe configurar el puerto manualmente.

1. Vaya a C:\Archivos de programa\Citrix\Telemetry Service
2. Abra el archivo ScoutUI.exe.config.
3. Cambie el valor de LinuxVDATelemetryServicePort o LinuxVDATelemetryWakeupPort a lo que se configuró en Linux VDA:

- `<add key="LinuxVDATelemetryServicePort"value="7502"/>`
- `<add key="LinuxVDATelemetryWakeupPort"value="7503"/>`

1. Guarde los cambios y cierre el archivo.
2. Abra Scout de nuevo para asegurarse de que carga la configuración más reciente.

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 sesiones 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
- Parámetros de Registro para el inicio de sesiones

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

Para Profile Management en VDA, Scout comprueba lo siguiente:

- Detección de hipervisor
- Detección de aprovisionamiento
- Citrix Virtual Apps and Desktops
- Configuración de disco Personal vDisk
- Almacén de usuarios
- Detección de estado de Profile Management Service
- Prueba de enlazado de Winlogon.exe

Para ejecutar comprobaciones en Profile Management, debe instalar y habilitar Profile Management en el VDA. Para obtener más información sobre las comprobaciones de configuración de Profile Management, consulte el artículo CTX132805 de Knowledge Center

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, no se detecta el servidor de licencias.

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. Haga clic en **Buscar máquina** para detectar 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 servidores StoreFront y máquinas VDA), consulte Agregar máquinas manualmente e Importar máquinas VDA. 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). Las comprobaciones de estado no se ejecutan 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 realizan 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

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.
  - Establezca la directiva de ejecución de scripts en, al menos, `RemoteSigned` para permitir que se ejecuten los scripts. Por ejemplo: `Set-ExecutionPolicy RemoteSigned`. **Nota:** Otros privilegios de ejecución de scripts también pueden funcionar.
- Use **Ejecutar como administrador** al iniciar Citrix Scout.

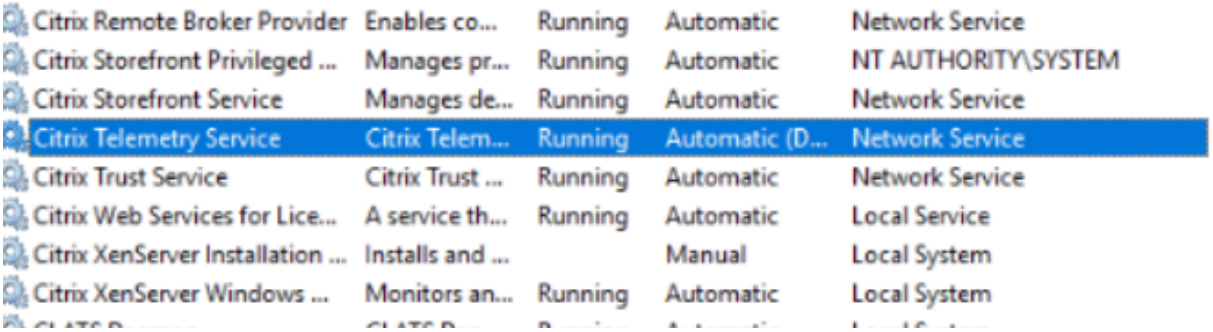
Para cada máquina desde la que recopile diagnósticos o realice comprobaciones de estado:

- 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.

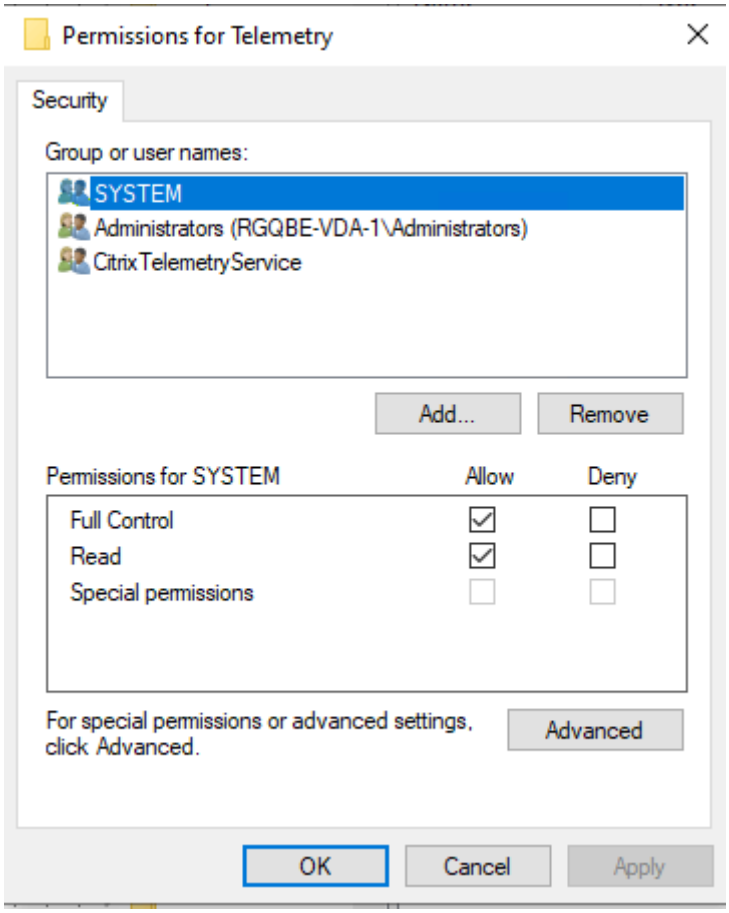
Scout ejecuta pruebas de verificación en las máquinas que seleccione para garantizar que se cumplen estos requisitos.

El servicio de telemetría para Windows se ejecuta en el Servicio de red.

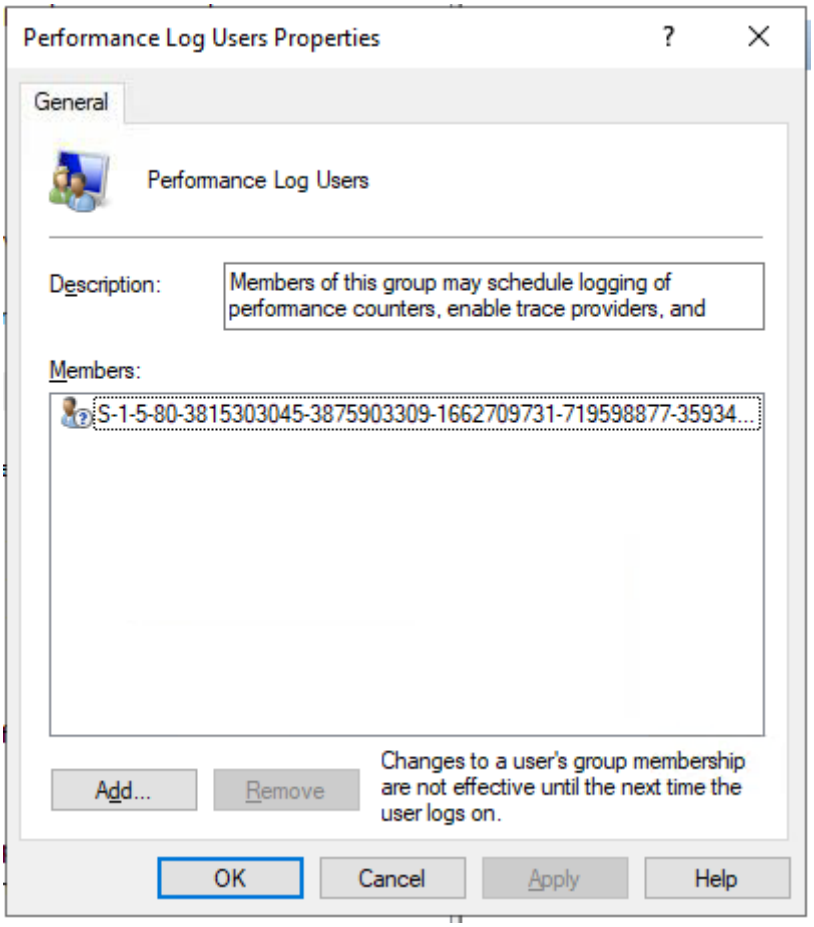


La carpeta de seguimiento AOT se guarda en `C:\ProgramData\Citrix\TelemetryService\CitrixAOT`.

Solo los usuarios del grupo Administrador, Sistema y SID del servicio de telemetría tienen permiso para acceder al Registro `HKEYLOCALMACHINE:SOFTWARE\Citrix\Telemetry`.



El SID del servicio de telemetría permanece en el grupo de usuarios del registro de rendimiento después de desinstalar el servicio de telemetría, pero puede quitarlo manualmente.



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 se incluye en las acciones **Recopilar** ni **Rastrear y reproducir**.
- **Scout no puede conectarse al socket systemd de esta máquina**. Compruebe lo siguiente:
  - El puerto 7503 debe estar abierto. Verifique que `systemd ctxtelemetry.socket` esté escuchando en el puerto 7503 de la máquina. Es posible que el puerto sea diferente si se ha cambiado el puerto de `ctxtelemetry.socket`. Para ajustar los puertos, consulte Configuración de Scout.
  - La conexión de red funciona correctamente (es posible que esto implique verificar que el firewall está configurado correctamente).
- **Linux VDA Telemetry Service no está activo en esta máquina** . Compruebe lo siguiente:
  - El puerto 7502 debe estar abierto. Verifique que Linux VDA Telemetry Service esté instalado y activo en la máquina. Es posible que el puerto sea diferente si se ha cambiado el puerto del servicio de telemetría. Para ajustar los puertos, consulte Configuración de Scout.
  - La conexión de red funciona correctamente (es posible que esto implique verificar que el firewall está configurado correctamente).

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 y 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	7.1–7.13	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)

Función	Scout 2.23	Scout 3.0
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 la versión de Telemetry Service en esa máquina, no se incluye 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 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 autorizar de nuevo 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.

Buscar máquina

Para los procedimientos **Recopilar**, **Rastrear y reproducir** y **Programar**, Scout enumera los Controllers y los VDA que detecta automáticamente.

Cuando ejecute Comprobación del estado de Scout desde el Delivery Controller, haga clic en **Buscar máquina** para detectar máquinas, incluidos los controladores de entrega, los agentes VDA, los servidores de licencias y los servidores StoreFront.

Cuando se ejecuta la comprobación del estado de Scout desde una máquina unida a un dominio que no es Delivery Controller, Scout no puede detectar máquinas automáticamente. Deberá agregar máquinas manualmente o importar máquinas VDA.

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.

Importar máquinas VDA

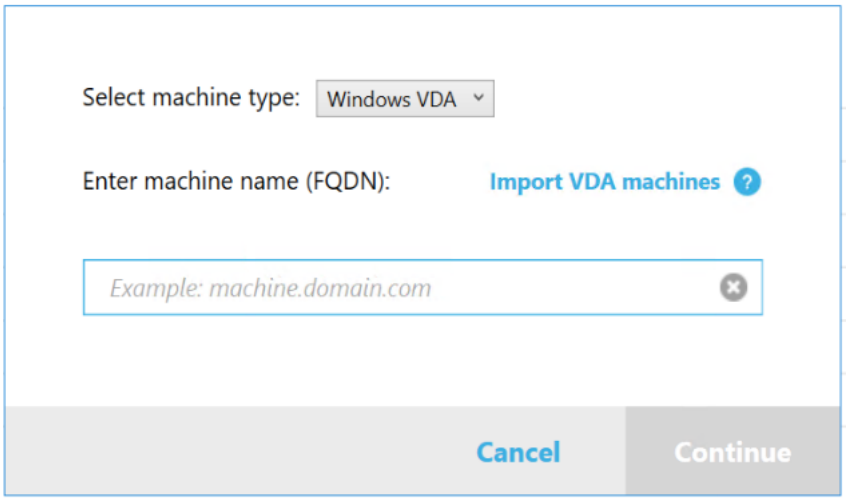
Puede importar máquinas VDA en la implementación al realizar comprobaciones de estado.

1. En Delivery Controller o Connector, genere el archivo de lista de máquinas con el comando de PowerShell. En Connector, debe introducir credenciales de Citrix y seleccionar al cliente en el cuadro de diálogo emergente.

   ```
   Get-BrokerMachine| foreach { $_.DnsName } | out-file C:\machineList
   .txt
   ```

2. Copie el archivo machineList.txt a la máquina unida al dominio donde quiere iniciar la comprobación del estado de Scout.
3. En la página Comprobaciones de estado de Citrix Scout, haga clic en **Agregar máquina**.
4. Seleccione el tipo de máquina **Windows VDA**.
5. Haga clic en **Importar máquinas VDA**.
6. Seleccione el archivo machineList.txt.
7. Haga clic en **Abrir**.

Las máquinas VDA importadas se enumeran en la página Comprobaciones de estado de Citrix Scout.



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.

   - En un Controller, 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. Para agregar manualmente otras máquinas, por ejemplo, servidores Citrix Provisioning o StoreFront, consulte Agregar máquinas manualmente.
   - En otros componentes (como servidores VDA), la página **Seleccionar máquinas** muestra solo la máquina local. No se admite la agregación manual de máquinas.

   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**.

   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 recopilan 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. Autentíquese 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 recopilan datos de rastreo ni diagnóstico 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 recopilan 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. Autentíquese 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.

Habilitar la recopilación de registros adicionales

La función **Enable additional log collection** le permite usar la función de rastreo y reproducción con más herramientas, como perfmon, Netsh, DebugView y Wireshark.

A partir de la versión 2407, cuando habilita otra recopilación de registros, Scout detecta automáticamente las herramientas relacionadas con CDC instaladas en su máquina y recopila automáticamente los registros de seguimiento relacionados con las herramientas de CDC en el paquete ZIP. Puede personalizar este archivo ZIP y adjuntarlo a Scout. Con esta automatización, puede usar Citrix Scout de manera más eficaz y esto le ayuda a diagnosticar los problemas rápidamente.

> **Nota:**
>
> Esto solo se aplica a las máquinas locales.

Para configurar una recopilación de registros adicionales:

1. Inicie Citrix Scout.
2. Haga clic en el engranaje de **Settings**.
3. Haga clic en **Enable additional log collection with more tools**.
4. Haga clic en **Guardar**.

Para recopilar registros adicionales:

1. En la página principal de Scout, haga clic en **Trace & Reproduce**.
2. En la página **Select machines**, haga clic en el engranaje a la derecha de la máquina local.
3. Siga las instrucciones de Rastrear y reproducir.
4. Cuando haya terminado, revise los registros del archivo ZIP. Los registros se comprimen en la carpeta *CDCLogs*.

> **Nota:**
>
> Si se selecciona la herramienta Procmon para el rastreo, los registros de Process Monitor pueden crecer rápidamente. Asegúrese de seleccionar solo las herramientas necesarias. También puede controlar el tamaño de los registros en *%temp%\Scout-CDC-Log*.

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 recopilan 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 aplican 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. Autentíquese 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.

Enmascaramiento de datos

Tal vez la información de diagnóstico recopilada mediante Citrix Scout contenga información confidencial sobre seguridad. La función de enmascaramiento de datos de Citrix Scout le permite ocultar información confidencial en archivos de diagnóstico antes de cargarlos en Citrix.

El enmascaramiento de datos de Scout está configurado para ocultar la dirección IP, los nombres de las máquinas, los nombres de los dominios, los nombres de los usuarios, los nombres de los hipervisores, los nombres de los grupos de entrega, los nombres de los catálogos, los nombres de las aplicaciones y los SID.

> **Nota:**
>
> Los rastros CDF están cifrados y no se pueden enmascarar.
>
> Los registros de Linux VDA se comprimen en el formato `.tar.gz2` y no se pueden enmascarar.

Recopilar nuevos diagnósticos y enmascarar datos

Para utilizar la función de enmascaramiento de datos de Citrix Scout, inicie Scout desde la línea de comandos.

1. En Windows, abra el símbolo del sistema como administrador.
2. Vaya al directorio donde está instalado Scout: `cd C:\Program Files\Citrix\Telemetry Service`.
3. Inicie Scout: `ScoutUI.exe datamasking`.

4. Haga clic en **Recopilar** o **Rastrear y reproducir** para recopilar los diagnósticos.
5. Una vez completada la recopilación, seleccione **Habilitar enmascaramiento de datos** para continuar. Esta opción está habilitada de forma predeterminada.
6. Configure la máscara de datos. Puede utilizar las reglas predeterminadas o personalizarlas.
7. Seleccione si desea cargar o guardar la colección de diagnósticos.

    - Si selecciona **Cargue en Citrix los diagnósticos recopilados**, los archivos de diagnóstico enmascarados se cargan en Citrix.
    - Si selecciona **Guarde los diagnósticos recopilados en su máquina local**, se guardan tanto los diagnósticos originales como los enmascarados en la ubicación especificada.

Enmascarar datos en diagnósticos existentes

1. En Windows, abra el símbolo del sistema como administrador.
2. Vaya al directorio donde está instalado Scout: `cd C:\Program Files\Citrix\Telemetry Service`.
3. Inicie Scout directamente en el modo de enmascaramiento de datos: `ScoutUI.exe datamasking filePath`.
4. Seleccione "Habilitar enmascaramiento de datos"para continuar. Esta opción está habilitada de forma predeterminada.
5. Configure la máscara de datos. Puede ejecutar el enmascaramiento de datos con las reglas predeterminadas o con reglas personalizadas.
6. Seleccione si desea cargar o guardar la colección de diagnósticos.

    - Si selecciona **Cargue en Citrix los diagnósticos recopilados**, los archivos de diagnóstico enmascarados se cargan en Citrix.
    - Si selecciona **Guarde los diagnósticos recopilados en su máquina local**, se guardan tanto los diagnósticos originales como los enmascarados en la ubicación especificada.

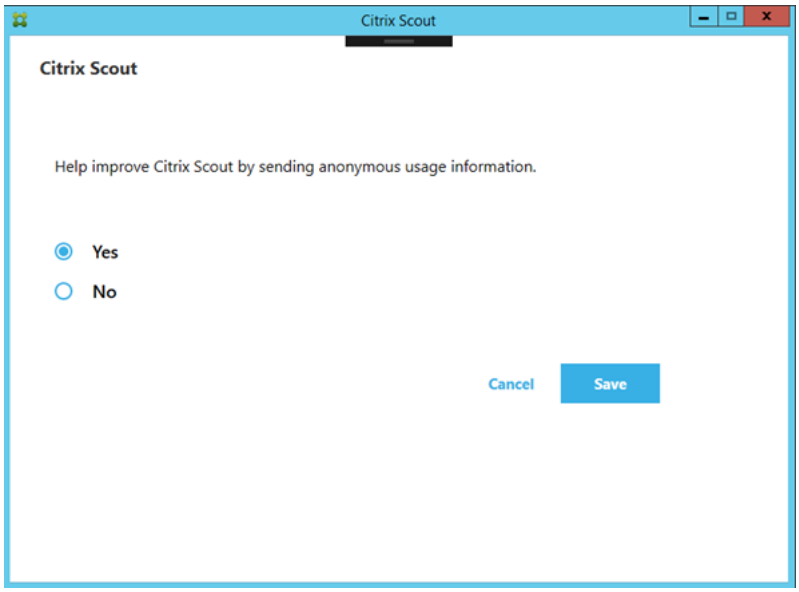
Ubicación del archivo de asignación y del archivo de datos enmascarados

Después de cargar o guardar la colección de diagnósticos, haga clic en el enlace para abrir los diagnósticos originales y enmascarados, y abra el archivo de información de asignación.

Recopilación de datos de uso

Al utilizar Scout, Citrix emplea Google Analytics para recopilar datos de uso anónimos que se usarán para futuras funciones y mejoras del producto. La recopilación de datos se habilita de forma predeterminada.

Para cambiar la recopilación y carga de datos de uso, haga clic en el icono con forma de engranaje **Parámetros** en la interfaz de usuario de Scout. A continuación, puede elegir si enviar la información. Para ello, seleccione **Sí** o **No** y, a continuación, haga clic en **Guardar**.



Recopilar rastreos de Citrix Diagnostic Facility (CDF) durante el inicio del sistema

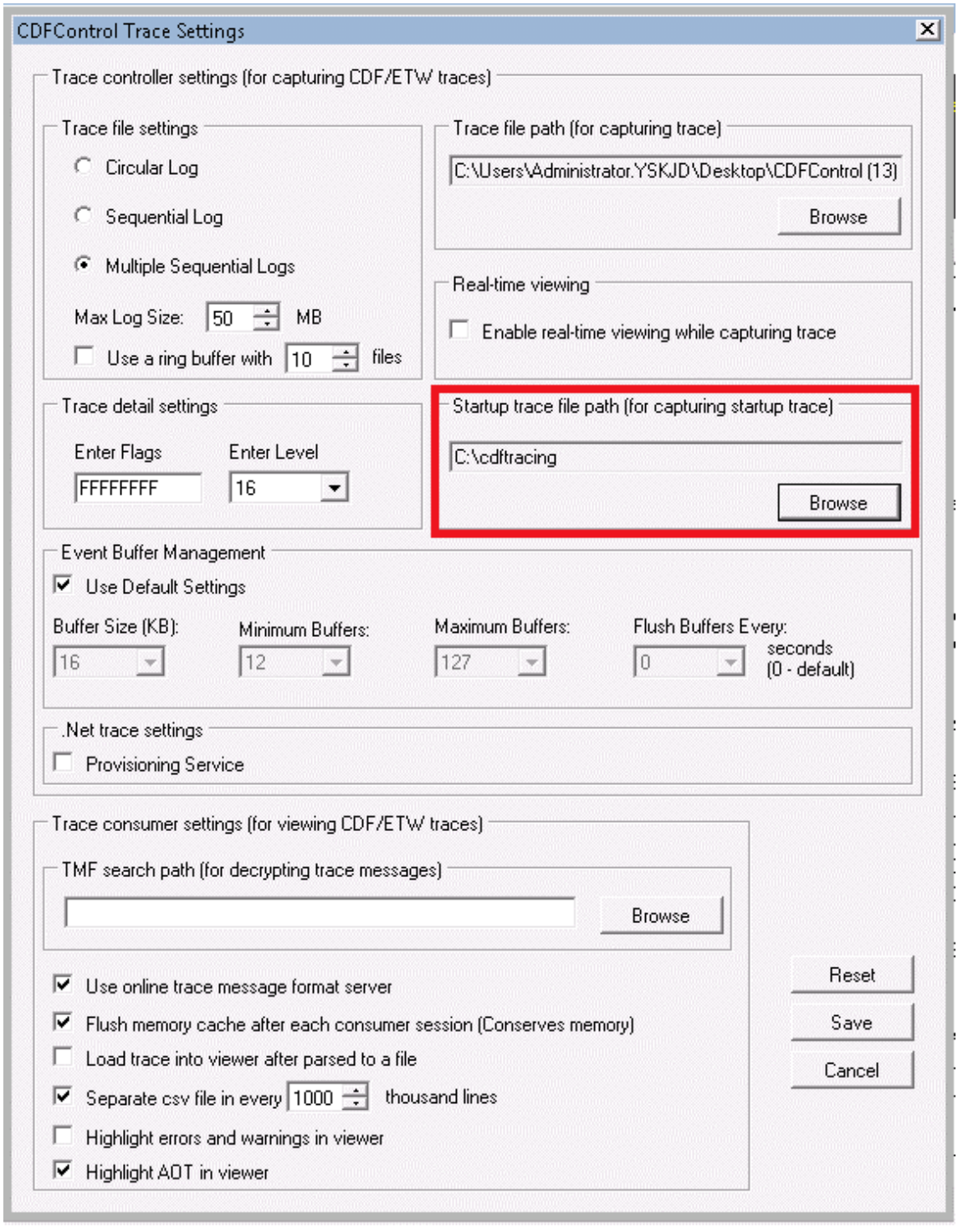
August 17, 2024

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.

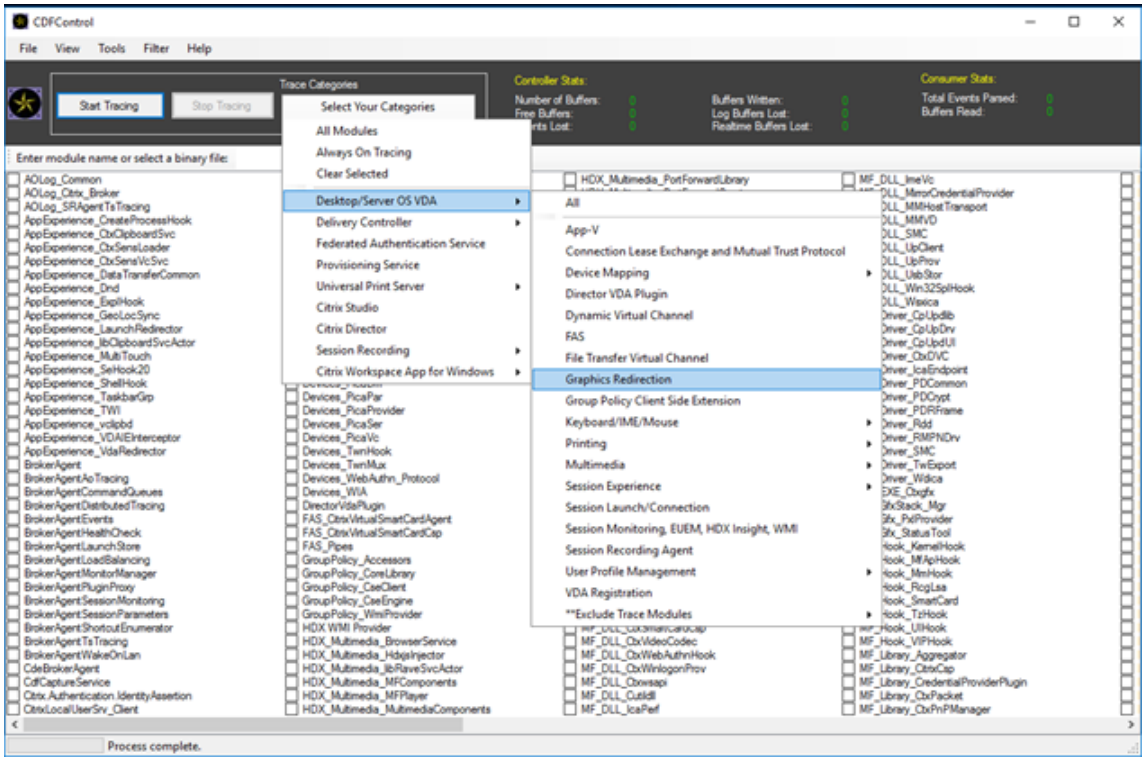
Recopilar un rastreo al iniciar el sistema

Utilice este procedimiento para recopilar un rastro CDF en el inicio del sistema. Necesita privilegios de administrador.

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 de Citrix Support. (En el siguiente ejemplo, está seleccionada la **redirección de gráficos**. esa selección es solo un ejemplo, por lo que le recomendamos habilitar los proveedores para el problema específico que quiera solucionar).



4. Seleccione **Startup Tracing** y **Enable** en el menú **Tools**.

   Después de seleccionar **Enable**, la barra animada comienza a desplazarse. Esto no afecta al procedimiento. Continúe con el siguiente paso.

5. Una vez habilitado **Startup Tracing**, cierre la **utilidad CDFControl** y reinicie el sistema.
6. Inicie la utilidad **CDFControl**. Una vez reiniciado el sistema y aparecido el error, inhabilite el rastreo de inicio; para ello, seleccione **Startup Tracing** en el menú **Tools** y haga clic en **Disable**.
7. Vaya a la ruta del archivo de rastreo especificado en el paso 2 y recopile el archivo de registros de rastreo (.etl) para analizarlo.

Administración delegada

August 17, 2024

> **Nota:**
>
> Puede administrar la implementación de Citrix Virtual Apps and Desktops mediante dos consolas de administración: Web Studio (basada en la web) y Citrix Studio (basada en Windows). Este artículo se refiere únicamente a Web Studio. Para obtener información sobre Citrix Studio, consulte el artículo equivalente en Citrix Virtual Apps and Desktops 7 2212 o versiones anteriores.

El modelo de administración delegada ofrece la flexibilidad necesaria para adaptarse al modo en que la organización desee delegar las 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).

Rol	Permisos
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.
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	Todo
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 específicas (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 crear y administrar administradores, siga estos pasos:

1. Inicie sesión en Web Studio, haga clic en **Administradores** en el panel de la izquierda y, a continuación, en la ficha **Administradores**.
2. Siga las instrucciones correspondientes a la tarea que quiere completar:

    - **Crear un administrador:** Haga clic en **Crear administrador** en la barra de acciones. Escriba o vaya al nombre de la cuenta de usuario, seleccione o cree un ámbito y, a continuación, seleccione un rol. El nuevo administrador se habilita de forma predeterminada, aunque puede modificar este valor.
    - **Copiar un administrador:** Seleccione el administrador y, a continuación, haga clic en **Copiar administrador** en la barra de 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 y, a continuación, haga clic en **Modificar administrador** en la barra de acciones. Puede modificar o eliminar los pares de rol y ámbito, así como agregar otros nuevos.
    - **Eliminar un administrador:** Seleccione el administrador y, a continuación, haga clic en **Eliminar administrador** en la barra de 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

> **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 la barra de acciones, haga clic en **Modificar administrador**.

2. En la ventana **Nombre y detalles del administrador**, seleccione el par de rol y ámbito y, a continuación, haga clic en **Eliminar**.
3. Haga clic en **Guardar** para salir.

- Elimine al administrador.

1. En la barra de acciones, haga clic en **Eliminar administrador**.
2. En la ventana de confirmación, 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 la barra de acciones.

Para crear y administrar roles, siga estos pasos:

1. Inicie sesión en Web Studio, haga clic en **Administradores** en el panel de la izquierda y, a continuación, en la ficha **Funciones**.
2. Siga las instrucciones correspondientes a la tarea que quiere completar:

   - **Ver detalles del rol:** Seleccione el rol. La parte inferior muestra los tipos de objetos y los permisos asociados al 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 rol** en el panel de acciones. Escriba un nombre y una descripción. Seleccione los tipos de objeto y los permisos pertinentes.
   - **Copiar un rol:** Seleccione el rol y, a continuación, haga clic en **Copiar rol** en la barra de acciones. Cambie el nombre, la descripción, los tipos de objeto y los permisos, según sea necesario.

- **Modificar un rol personalizado:** Seleccione el rol y, a continuación, haga clic en **Modificar rol** en la barra de acciones. Cambie el nombre, la descripción, los tipos de objeto y los permisos, según sea necesario.
- **Eliminar un rol personalizado:** Seleccione el rol y, a continuación, haga clic en **Eliminar rol** en la barra de 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.

Reglas para crear y gestionar ámbitos:

- 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 de los ámbitos 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 crear y administrar ámbitos, siga estos pasos:

1. Inicie sesión en Web Studio, haga clic en **Administradores** en el panel de la izquierda y, a continuación, en la ficha **Ámbitos**.
2. Siga las instrucciones correspondientes a la tarea que quiere completar:

- **Crear un ámbito:** Haga clic en **Crear ámbito** en la barra de 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).
- **Copiar un ámbito:** Seleccione el ámbito y, a continuación, haga clic en **Copiar ámbito** en la barra de acciones. Escriba un nombre y una descripción. Cambie los objetos y los tipos de objeto, según sea necesario.
- **Modificar un ámbito:** Seleccione un ámbito y, a continuación, haga clic en **Modificar ámbito** en la barra de acciones. Cambie el nombre, la descripción, los tipos de objeto y los objetos, según sea necesario.
- **Eliminar un ámbito:** Seleccione un ámbito y, a continuación, haga clic en **Eliminar ámbito** en la barra de acciones. Cuando se le solicite, confirme la eliminación.

Configurar la administración de arrendatarios

Configure la administración de arrendatarios para crear particiones de administración en un único sitio de Citrix Virtual Apps and Desktops. Cada arrendatario tiene recursos y configuraciones segregados, como catálogos de máquinas y grupos de entrega. Los administradores con acceso a un arrendatario específico solo pueden administrar los recursos y las configuraciones asociados a ese arrendatario. Entre los ejemplos de casos de uso se incluyen:

- Empresas con diferentes silos empresariales (divisiones independientes o equipos de administración de TI separados) en un solo sitio.
- Citrix Service Providers que configuran y administran implementaciones para varios clientes en un solo sitio.

En un nivel superior, el flujo de trabajo para configurar la administración de arrendatarios incluye:

1. Crear arrendatarios
2. Agregar administradores para arrendatarios

Crear arrendatarios

Para crear un arrendatario, cree un ámbito de arrendatario. Estos son los pasos detallados:

1. Inicie sesión en Web Studio, haga clic en **Administradores** en el panel de la izquierda y, a continuación, en la ficha **Ámbitos**.
2. Haga clic en *Crear ámbito** para iniciar la creación del arrendatario.
3. Introduzca los siguientes detalles para el ámbito del arrendatario:

a) Escriba un nombre descriptivo para el ámbito. Este nombre también sirve como identificador del arrendatario.
b) (Opcional) Introduzca una descripción breve.
c) Seleccione **Ámbito del arrendatario**.
d) Si es necesario, seleccione los objetos asociados al arrendatario. También puede agregar objetos a los ámbitos de arrendatario al crear o administrar objetos.
e) Haga clic en **Aceptar** para completar la creación.

Una vez completado el proceso, puede ver:

- El registro del nuevo ámbito de arrendatario aparece en la lista de ámbitos, identificado como **Arrendatario** en la columna **Tipo**.
- El nombre del ámbito se muestra en la lista desplegable **Todos los arrendatarios** situada en la esquina superior derecha de Web Studio.

Cuando trabaje con un ámbito de arrendatario, tenga en cuenta estas consideraciones:

- La propiedad de arrendatario sigue un orden de asignación jerárquico: Alojamiento > Catálogos de máquinas > Grupos de entrega > Aplicaciones. Los objetos de nivel inferior heredan la propiedad de arrendatario de los objetos de nivel superior. Por ejemplo, al seleccionar un grupo de entrega para un ámbito de arrendatario, seleccione también el alojamiento y el catálogo de máquinas asociados. De lo contrario, el grupo de entrega no puede heredar la propiedad de arrendatario.
- Después de crear un ámbito de arrendatario, puede modificar los objetos para modificar las asignaciones de arrendatario. Cuando se modifica una asignación de arrendatario, sigue sujeta a la restricción de que debe asignarse a los mismos arrendatarios o a un subconjunto de estos. Sin embargo, los objetos de nivel inferior no se vuelven a evaluar cuando cambian las asignaciones de arrendatario. Asegúrese de que los objetos estén restringidos correctamente cuando cambie las asignaciones de arrendatario. Por ejemplo, si hay un catálogo de máquinas disponible para `TenantA` y `TenantB`, puede crear un grupo de entrega para `TenantA` y otro para `TenantB`. (`TenantA` y `TenantB` están asociados a ese catálogo de máquinas). A continuación, puede cambiar el catálogo de máquinas para que se asocie solo a `TenantA`. Como resultado, el grupo de entrega asociado a `TenantB` deja de ser válido.

Agregar administradores para arrendatarios

Para agregar administradores para arrendatarios, asigne cuentas de usuario con roles de administrador y arrendatarios.

Para agregar un administrador para un arrendatario, siga estos pasos:

1. Inicie sesión en Web Studio, haga clic en **Administradores** en el panel de la izquierda y, a continuación, en la ficha **Administradores**.

2. Haga clic en **Agregar administrador** y siga estos pasos para completar el proceso:

    a) Escriba o busque el nombre de la cuenta de usuario y haga clic en **Siguiente**.
    b) Seleccione **Acceso personalizado** y, a continuación, seleccione uno o más roles (por ejemplo, administrador de catálogos de máquinas) según sea necesario.
    c) Haga clic en **Modificar ámbitos** junto a cada rol, cambie el ámbito de **Todos** al ámbito de arrendatario deseado y, a continuación, haga clic en **Guardar**.

3. Haga clic en **Siguiente**.
4. En la página **Revisar y confirmar**, haga clic en **Enviar invitación**.

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 Web Studio.

  Para crear este informe, sigue estos pasos:

  1. Inicie sesión en Web Studio, haga clic en **Administradores** en el panel de la izquierda.
  2. Seleccione un administrador y, a continuación, haga clic en **Crear informe** en la barra de 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
`-Help`	Muestra la ayuda del script.
`-Csv`	Especifica el archivo CSV resultante. Valor predeterminado = HTML

Parámetro	Descripción
`-Path string`	Destino de escritura de los resultados. Valor predeterminado = stdout
`-AdminAddress string`	La dirección IP o el nombre de host del Delivery Controller con el que hay que establecer conexión. Predeterminado = localhost
`-Show`	(Válido solamente cuando el parámetro `-Path` también se especifica) Cuando se escribe el resultado en un archivo, `-Show` hace que dicho archivo se abra con el programa adecuado como, por ejemplo, un explorador web.
CommonParameters	`Verbose`, `Debug`, `ErrorAction`, `ErrorVariable`, `WarningAction`, `WarningVariable`, `OutBuffer` y `OutVariable`. 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.

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
-Path Roles.html  – Show
```

El siguiente ejemplo escribe una tabla CSV en un archivo denominado Roles.csv. La tabla no se muestra.

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
 – CSV -Path Roles.csv
```

En una ventana de símbolo de sistema de Windows, el comando para el ejemplo anterior es:

```
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'
-CSV -Path Roles.csv"
```

Delivery Controllers

August 17, 2024

> **Nota:**
>
> Puede administrar la implementación de Citrix Virtual Apps and Desktops mediante dos consolas de administración: Web Studio (basada en la web) y Citrix Studio (basada en Windows). Este artículo se refiere únicamente a Web Studio. Para obtener información sobre Citrix Studio, consulte el artículo equivalente en Citrix Virtual Apps and Desktops 7 2212 o versiones anteriores.

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. Los Controllers adicionales permiten 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.

Cuando agregue un Delivery Controller a un sitio, debe agregar credenciales de inicio de sesión en esa máquina a todos los servidores SQL replicados que utilice para la alta disponibilidad.

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 comprobar las imágenes reflejadas después de agregar, quitar o mover un Controller, ejecute el cmdlet `Get-configdbconnection` de PowerShell. Ese cmdlet garantiza que el servidor de conmutación por error se ha establecido en la cadena de conexión al reflejado.

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 un sitio, ejecute Citrix Site Manager en este Controller para crear un sitio. La dirección IP de este controlador se agrega automáticamente al nuevo sitio.

   Si va a generar scripts para inicializar bases de datos, agregue los Controllers antes de generarlos.
3. Si ya creó un sitio, siga estos pasos:

   a) Ejecute Citrix Site Manager en este Controller, haga clic en **Unirse a un sitio existente** y escriba la dirección de un Controller en el sitio al que quiere unirse.
   b) Ejecute la herramienta de configuración de Studio para agregar el Controller al Web Studio.

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 para 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 Web 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`.

Después de quitar un Controller:

- Los VDA que utilizan la actualización automática se registran de nuevo con otros Controllers disponibles. Este nuevo registro solo se produce si el mecanismo de actualización automática está habilitado y los VDA pueden contactar con otros Controllers (en la misma zona secundaria que el Controller quitado o en la zona principal para implementaciones locales).
- Actualice la información del Controller en Citrix StoreFront. Para obtener más información, consulte Administrar Controllers.
- En Citrix StoreFront, actualice las URL de Secure Ticket Authority (STA) para el acceso remoto mediante Citrix Gateway. Para obtener más información, consulte Administrar Secure Ticket Authorities.
- En Citrix Gateway, actualice todas las URL de STA de servidores virtuales. Para obtener más información, consulte Citrix Gateway.

> **Importante:**
>
> No quite el Controller de Active Directory hasta que lo haya quitado del sitio.

1. Asegúrese de que el Controller está ejecutándose de forma que Web Studio se cargue en menos de una hora. Una vez que Web Studio haya cargado el Controller que quiere quitar, asegúrese de que todos los servicios del Controller estén ejecutándose y que el Controller esté apagado.
2. Inicie sesión en Web Studio y seleccione **Parámetros** en el panel de la izquierda.
3. Busque el icono del **Delivery Controller** y haga clic en **Modificar**.
4. En la página **Administrar Delivery Controller**, seleccione el Controller que quiera quitar.
5. Seleccione **Quitar Controller**. Si no dispone de los roles y permisos adecuados para la base de datos, se le ofrece la opción de generar un script que permite al administrador de bases de datos quitar el Controller por usted.

Web Studio realiza una comprobación previa antes de quitar un Controller. Es seguro quitar un Controller si está apagado y no se encuentra en el siguiente estado de servicio:

- Desconocido
- Fallo pendiente
- Versión anterior
- Versión más reciente
- Cambio de versión en curso
- Faltan funciones obligatorias

Si el Controller no está apagado y se encuentra en alguno de los estados de servicio mencionados, Web Studio le pedirá que apague el Controller.

6. Debe quitar la cuenta de la máquina del Controller del servidor de la base de datos. Antes de quitarla, compruebe que no hay ningún otro servicio que esté utilizando la cuenta.

Después de usar Web 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 Zonas para obtener información sobre cómo puede este traslado afectar al registro de VDA y otras operaciones.

1. Seleccione **Zona** en el panel de la izquierda.
2. Seleccione una zona en el panel central y, a continuación, seleccione un Controller.
3. Seleccione **Mover elementos** en la barra de acciones.
4. En la página **Mover elementos** que aparece, seleccione la zona a la que quiere mover el Controller.
5. Haga clic en **Guardar**.

Mover un VDA a otro sitio

Si un VDA se aprovisionó mediante Citrix Provisioning o es una imagen existente, puede transferir el VDA a otro sitio (del sitio 1 al sitio 2) al actualizar, o al mover una imagen de VDA que fue creada en un sitio de prueba a un sitio de producción. Los VDA aprovisionados con Machine Creation Services (MCS)

no se pueden mover de un sitio a otro. MCS no admite el cambio de la lista de Desktop Delivery Controllers (ListOfDDC) que un VDA consulta para registrarse con un Controller. Los VDA aprovisionados con MCS siempre consultan la lista ListOfDDC asociada al sitio donde se crearon.

Hay dos formas de mover un VDA a otro sitio: con el instalador o con 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.
    - Controllers: 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) y selecciona uno de los Controllers especificados en la directiva, la cual especifica una lista de 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. 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. Por lo tanto, el VDA vuelve a registrarse, eligiendo entre los Controllers de la lista del sitio 2. A partir de entonces, el VDA se actualiza automáticamente con la información del sitio 2.

Para obtener información sobre cómo usar el Editor de directivas de grupo, consulte la documentación de las Directivas de Citrix.

Compatibilidad con IPv4/IPv6

August 17, 2024

Esta versión es compatible con solo IPv4, con solo IPv6, así como con implementaciones de doble pila que usan redes IPv4 e IPv6 superpuestas.

Los siguientes componentes solo admiten IPv4. Todos los demás son compatibles con IPv4 e IPv6.

- XenServer
- Los Virtual Delivery Agents (VDA) no controlados por la configuración de directiva **Usar solo registro de Controller con IPv6**

Las comunicaciones de IPv6 se controlan con dos configuraciones de directiva de Citrix relacionadas con las conexiones del Virtual Delivery Agent (VDA).

- **Configuración principal que aplica el uso de IPv6:** Usar solo registro de Controller con IPv6.

  Esta configuración de directiva controla el tipo de dirección que usa el VDA para registrarse en el Delivery Controller.

  Cuando está habilitada, el VDA se registra y se comunica con el Controller a través de 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. Este es el valor predeterminado.

  Si un equipo de personas utiliza con frecuencia una red IPv6, publique los escritorios y las aplicaciones de esos usuarios basándose en una imagen o unidad organizativa (OU) que tenga habilitada la configuración de directiva **Usar solo registro de Controller con IPv6**.

  Si un equipo de personas utiliza con frecuencia una red IPv4, publique los escritorios y las aplicaciones de esos usuarios en función de una imagen u unidad organizativa que tenga inhabilitada la configuración de directiva **Usar solo registro de Controller con IPv6**.

- **Configuración dependiente que define una máscara de red IPv6:** Máscara de red IPv6 para registro de Controller.

  Una máquina puede tener varias direcciones IPv6. Esta configuración de directiva permite que los administradores puedan restringir el VDA a una sola subred preferida, en lugar de una dirección IP global, si está registrada. Esta configuración especifica la red en la que se registra el VDA. El VDA se registra solo en la primera dirección que coincida con la máscara de red especificada.

  Esta configuración solo es válida cuando la configuración de **directiva Usar solo registro de Controller con IPv6** está habilitada. Valor predeterminado = Cadena vacía

Consideraciones sobre la implementación

Si el entorno contiene redes IPv4 e IPv6, cree configuraciones diferentes de grupos de entrega, una para los clientes que solo pueden acceder a IPv4 y otra para los clientes que pueden acceder a la red IPv6. Considere la posibilidad de usar nombres, asignaciones manuales de grupos 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 que solo tiene acceso a IPv4.

NOTA: Estas consideraciones no se aplican si tiene habilitada la resolución de DNS.

Licencias de Citrix Virtual Apps and Desktops con Web Studio

August 17, 2024

> **Nota:**
>
> Puede administrar la implementación de Citrix Virtual Apps and Desktops mediante dos consolas de administración: Web Studio (basada en la web) y Citrix Studio (basada en Windows). Este artículo se refiere únicamente a Web Studio. Para obtener información sobre Citrix Studio, consulte el artículo equivalente en Citrix Virtual Apps and Desktops 7 2212 o versiones anteriores.

Puede usar Web Studio para administrar y realizar un rastreo de las licencias, siempre y cuando el servidor de licencias esté en el mismo dominio que Web Studio o en un dominio de confianza. Para obtener información sobre las tareas relacionadas con las licencias, consulte la documentación sobre el sistema de licencias y Licencias de varios tipos.

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, consulte Licencia simultánea y Licencia de usuario/dispositivo.

Versiones Current Release (CR) y Long Term Service Release (LTSR) compatibles

Esta tabla muestra la **versión mínima de LS compatible** para Citrix Virtual Apps and Desktops, XenApp y XenDesktop. Para obtener más información sobre las fechas de ciclo de vida útil de los productos Citrix, consulte la Tabla de productos.

> **Importante:**
>
> La información de esta tabla se proporciona únicamente para mostrar la compatibilidad de los productos. Citrix recomienda encarecidamente que utilice siempre la versión más reciente

> disponible de Citrix License Server para beneficiarse de las mejoras funcionales o de seguridad que pueda incluir.
>
> **Nota:**
>
> 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.

Versión actual	Versión mínima de LS compatible
2305	11.17.2.0, compilación 35000
2303	11.17.2.0, compilación 35000
2212	11.17.2.0, compilación 35000
2209	11.17.2.0, compilación 35000
2206	11.17.2.0, compilación 35000
2203	11.17.2.0, compilación 35000
2112	11.17.2.0, compilación 35000
2109	11.17.2.0, compilación 35000
2106	11.17.2.0, compilación 35000
2103	11.16.3.0, compilación 28000

Long Term Service Release	Versión mínima de LS compatible
2203 LTSR	11.17.2.0, compilación 35000
1912 LTSR	11.16.3.0, compilación 28000
7.15 LTSR	11.15.0.0, compilación 24100
7.6 LTSR	11.14.0.1, compilación 21103

Para obtener información sobre los productos y versiones antiguas, consulte Legacy Product Matrix.

Debe ser un administrador total de licencias para llevar a cabo las siguientes tareas. Para ver la información de licencias en Web 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 ese permiso.

Descargar e instalar una licencia de Citrix con Web Studio

1. Inicie sesión en Web Studio y seleccione **Licencias** en el panel de la izquierda.
2. Seleccione **Asignar licencias** en la barra de acciones.
3. Introduzca el código de acceso de licencias suministrado por Citrix en un mensaje de correo electrónico tras la compra o renovación de las licencias correspondientes.
4. Seleccione un producto y elija **Asignar licencias**. 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 reutilizar ese código. Para realizar otras transacciones con el mismo código, inicie sesión en Mi cuenta.

Agregar licencias almacenadas en el equipo local o en la red

1. Inicie sesión en Web Studio y seleccione **Licencias** en el panel de la izquierda.
2. Seleccione **Agregar licencias** en la barra de acciones.
3. Vaya a un archivo de licencias y agréguelo al servidor de licencias.

Cambiar el servidor de licencias

1. Inicie sesión en Web Studio y seleccione **Licencias** en el panel de la izquierda.
2. Seleccione **Cambiar servidor de licencias** en la barra de 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).

Seleccionar el tipo de licencia que se va a utilizar

- Al configurar el sitio, después de especificar el servidor de licencias, se le pide 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.

Cambiar la edición y el modelo de licencia del producto

1. Inicie sesión en Web Studio y seleccione **Licencias** en el panel de la izquierda.
2. Seleccione **Modificar edición de producto** en la barra de acciones.
3. Actualice las opciones pertinentes.

Para acceder a la consola License Administration Console, en la barra de 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.

> **Nota:**
>
> Cuando cambia de licencia en Web Studio, el cambio puede tardar hasta 5 minutos en aparecer en Citrix Director. Por ejemplo: si cambia entre Advanced y Premium o viceversa.

Agregar un administrador de licencias

1. Inicie sesión en Web Studio y seleccione **Licencias** en el panel de la izquierda.
2. Seleccione la ficha **Administradores de licencias**.
3. Seleccione **Agregar administrador de licencias** en la barra de acciones.
4. Vaya al usuario que quiere agregar como administrador y elija los permisos correspondientes.

Modificar los permisos de un administrador de licencias o eliminarlo

1. Inicie sesión en Web Studio y seleccione **Licencias** en el panel de la izquierda.
2. Seleccione la ficha **Administradores de licencias** y, a continuación, seleccione el administrador en cuestión.
3. Seleccione **Modificar administrador de licencias** o **Eliminar administrador de licencias** en la barra de acciones.

Agregar un grupo de administradores de licencias

1. Inicie sesión en Web Studio y seleccione **Licencias** en el panel de la izquierda.
2. Seleccione la ficha **Administradores de licencias**.
3. Seleccione **Agregar grupo de administradores de licencias** en la barra de 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.

Modificar los permisos de un grupo de administradores de licencias o eliminar el grupo

1. Inicie sesión en Web Studio y seleccione **Licencias** en el panel de la izquierda.
2. Seleccione la ficha **Administradores de licencias** 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 la barra de acciones.

Ver información de licencias

Inicie sesión en Web Studio y seleccione **Licencias** en el panel de la izquierda. 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.

Ver alertas de caducidad de licencias

Web Studio realiza consultas para obtener las fechas de caducidad del archivo de licencias desde Citrix License Server. Web Studio avisa a los administradores de la ficha Resumen si los archivos de licencias están a punto de caducar o ya han caducado.

Enlaces relacionados

- Consulte Suscripción local de Citrix para licencias Retail anuales y temporales.
- Consulte Transición e intercambios (TTU) con derechos híbridos.

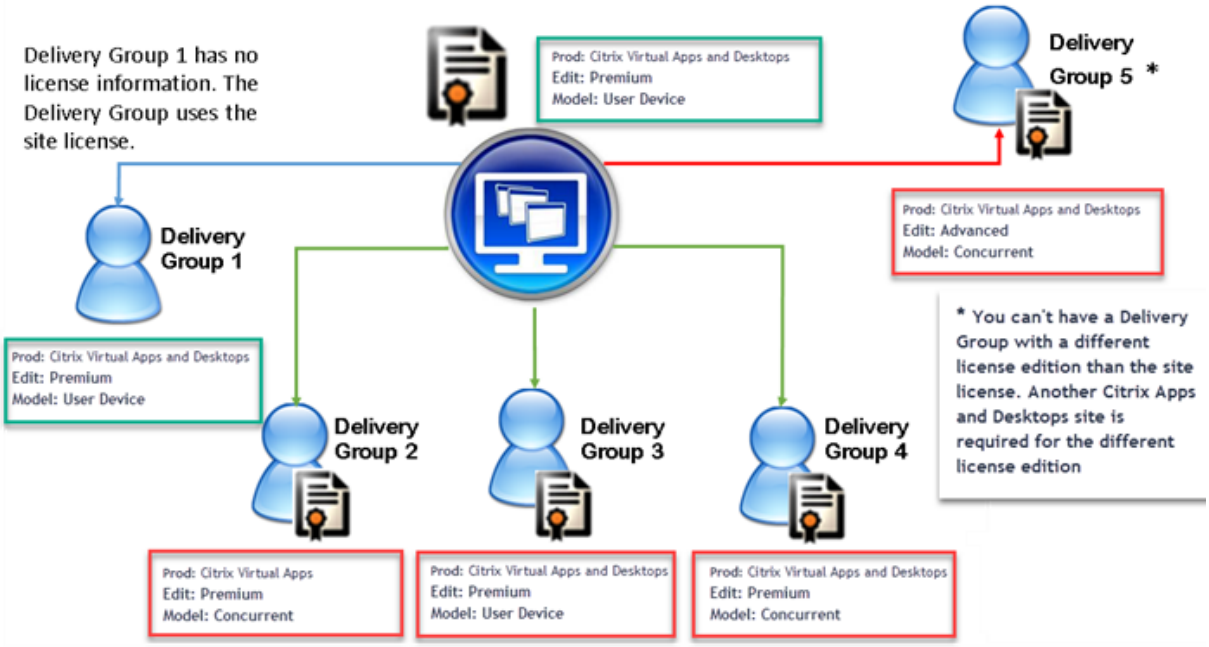
Licencias de varios tipos

August 17, 2024

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
- citrix.com

Las fechas de Customer Success Services 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 Customer Success Services entre sí.

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 revierten 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 está disponible con las licencias de Citrix Virtual Apps Standard y Citrix Virtual Desktops Standard.

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. CCU y CCS son licencias simultáneas y UD son licencias de usuario/dispositivo.

Old Name	New Name	Feature	Multi-type licensing compatibility			
			STD	ADV	ENT	PLT
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
Citrix XenDesktop VDI Edition (XDT-U)	Citrix Virtual Desktops Standard- Per User/Device	XDT_STD_UD	X			
Citrix XenDesktop VDI Edition (XDT-C)	Citrix Virtual Desktops Standard - 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/

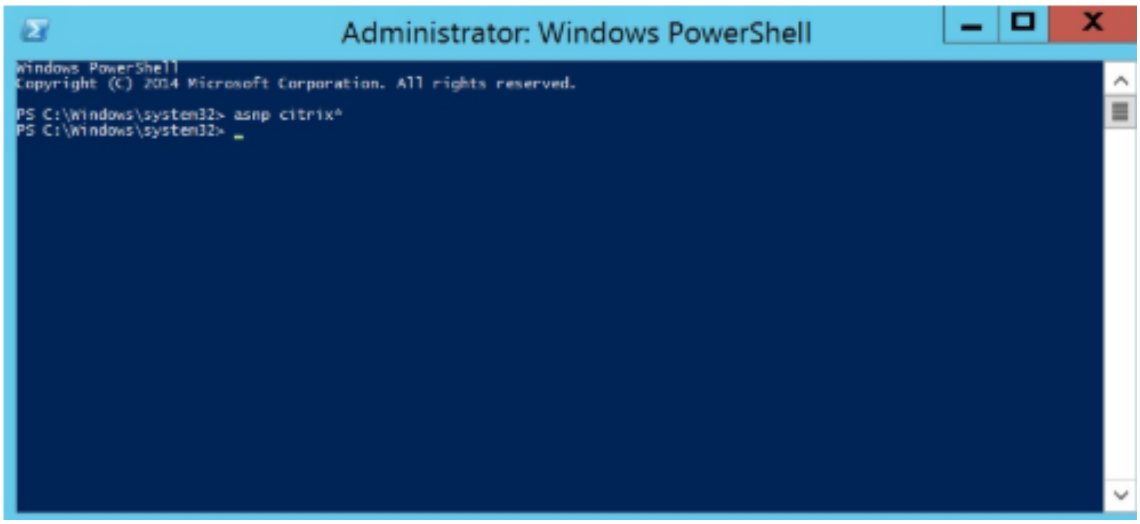
Get-BrokerDesktopGroup

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

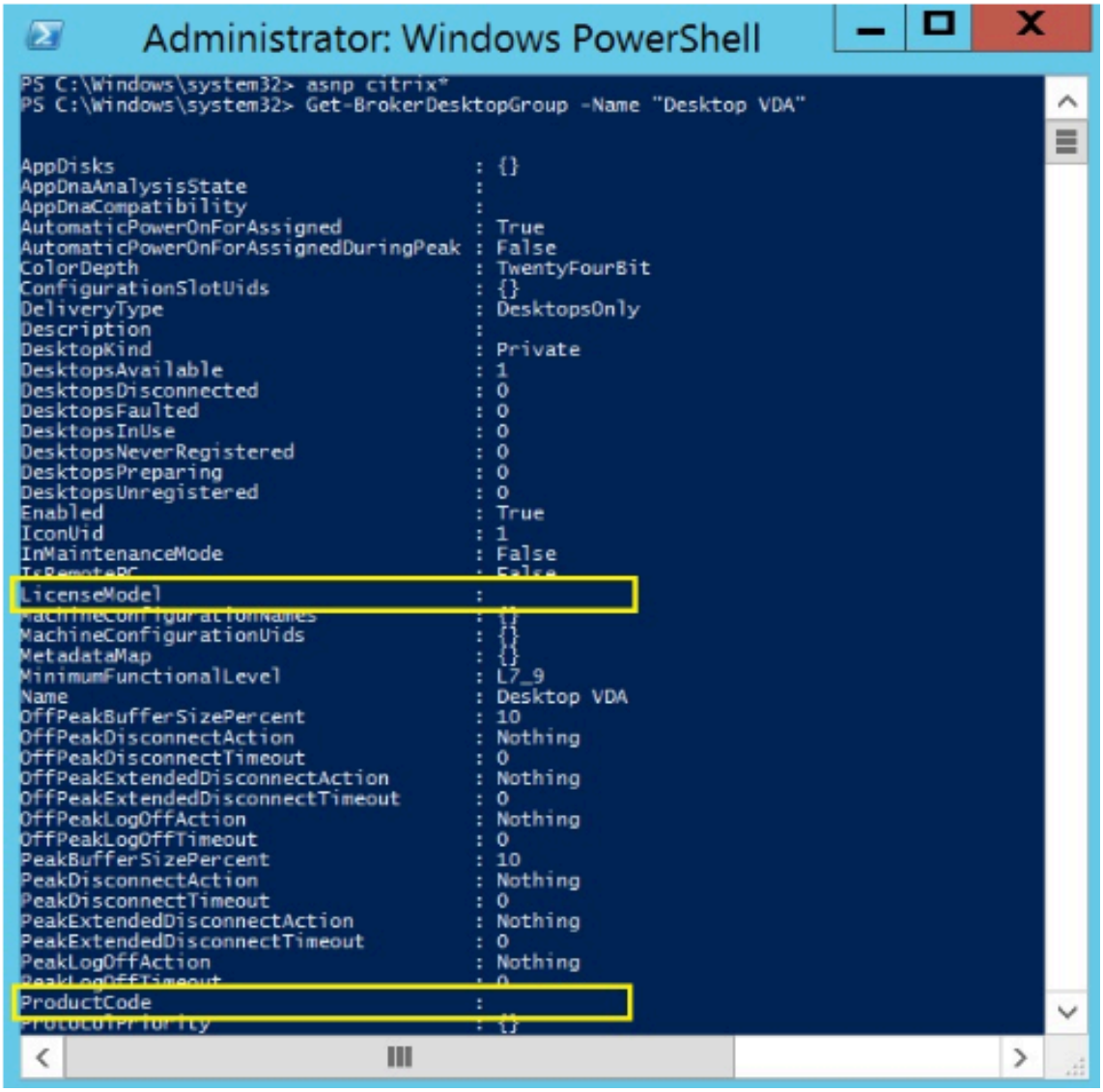
> **Nota:**
>
> No puede configurar dos o más tipos diferentes de productos, ediciones o modelos de licencia configurados en un solo grupo de entrega. En caso de que tenga diferentes tipos de productos, ediciones o modelos de licencia, configúrelos en grupos de entrega independientes.

1. Abra PowerShell con derechos de administrador y agregue el complemento de Citrix.

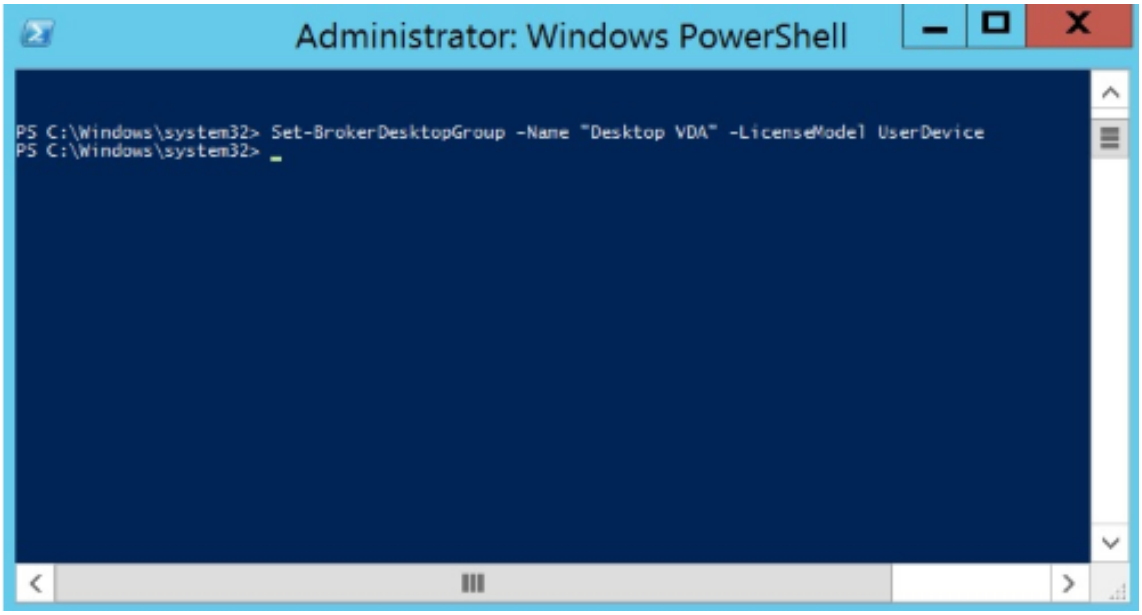


2. Ejecute el comando **Get-BrokerDesktopGroup** –**Name "DeliveryGroupName"** para ver la configuración de licencias actual. Busque los parámetros **LicenseModel** y **ProductCode**. Si no ha configurado estos parámetros antes, es posible que estén vacíos.

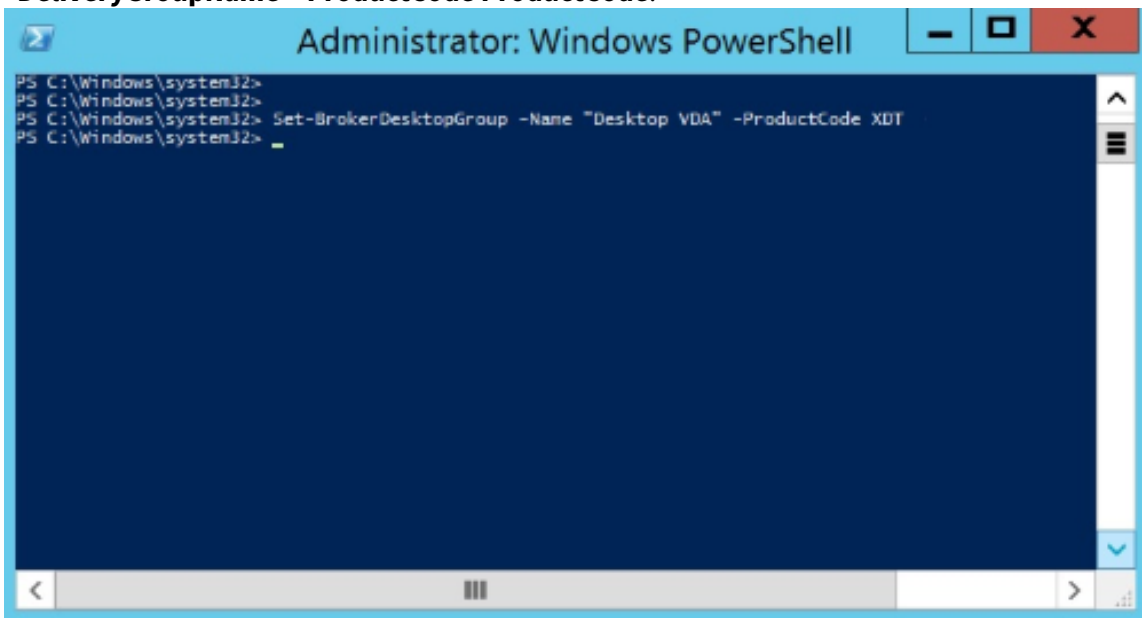
   > **Nota:**
   >
   > Si un grupo de entrega no tiene una información de licencias establecida, se utiliza de manera predeterminada la directiva **Site level Site license**.



3. Para cambiar el modelo de licencia, ejecute el comando **Set-BrokerDesktopGroup –Name "DeliveryGroupName"–LicenseModel LicenseModel**.

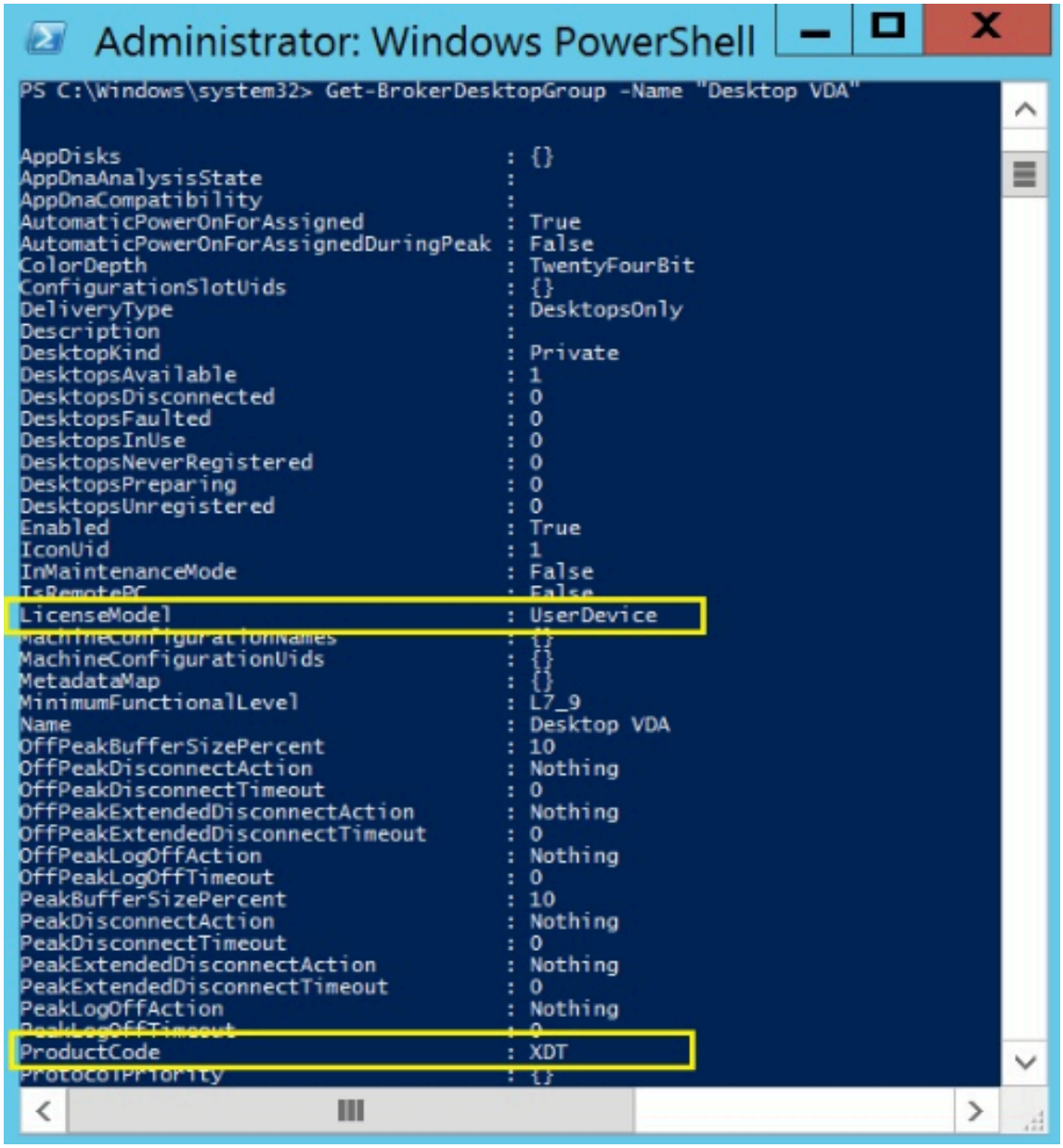


4. Para cambiar el producto de licencia, ejecute el comando **Set-BrokerDesktopGroup** –**Name “DeliveryGroupName”**–**ProductCode ProductCode**.



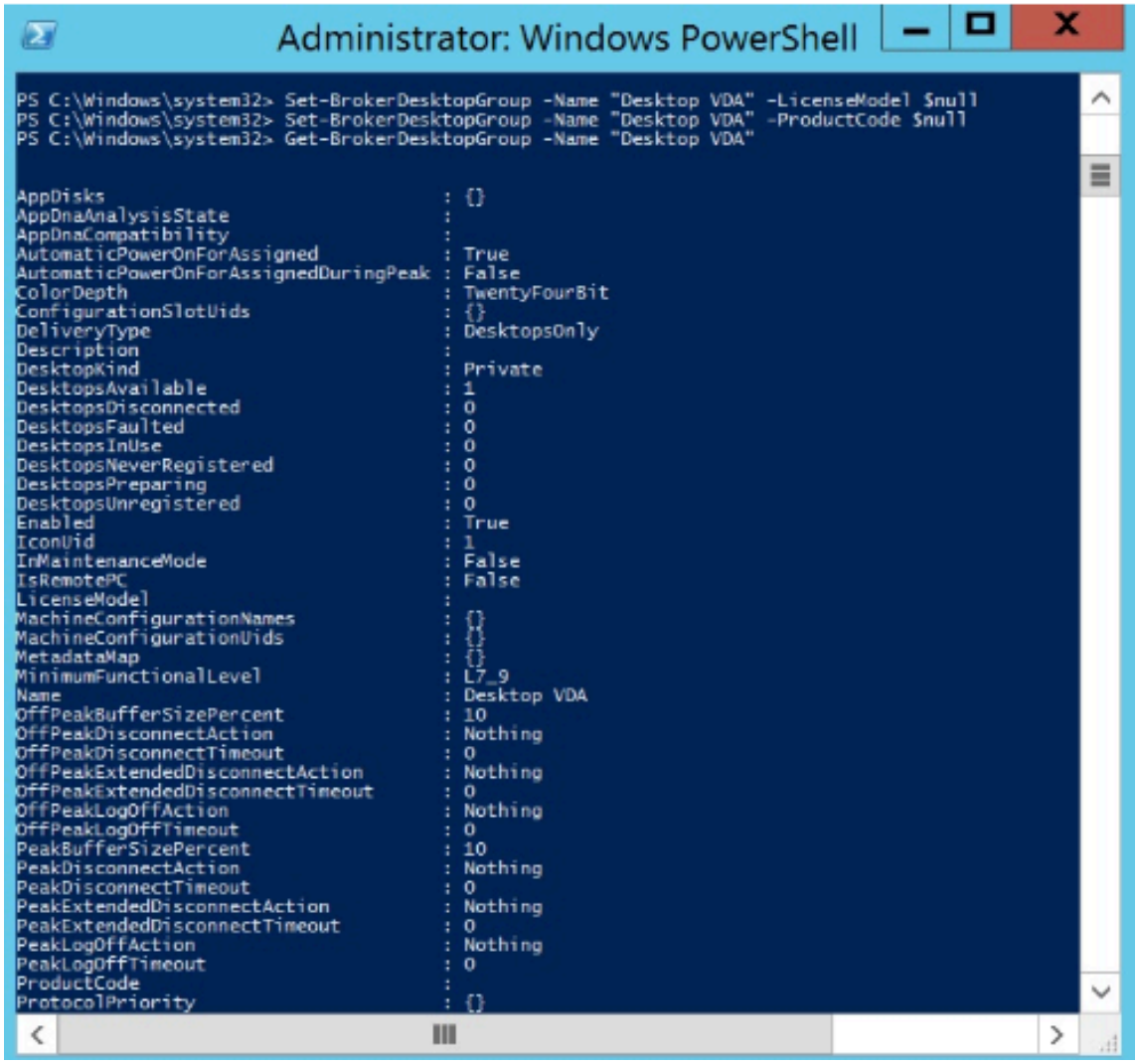
5. Introduzca el comando **Get-BrokerDesktopGroup** –**Name “DeliveryGroupName”** para validar los cambios.

> **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.



6. Para quitar la configuración de licencias, ejecute los mismos comandos que los descritos en los pasos anteriores, **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.



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

Preguntas frecuentes sobre licencias

August 17, 2024

> **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.

Citrix Licensing

¿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:

- La opción **Administrar licencias** de la página Mi cuenta en `citrix.com`. Para obtener más información, consulte Administrar licencias en citrix.com.
- Se utiliza Web 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 Instalar licencias.

¿Cómo asignar una licencia en Mi cuenta?

Consulte Asignar licencias.

¿Cómo agregar licencias asignadas al servidor de licencias?

Consulte Modificar licencias.

¿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.

¿Dónde está Citrix License Administration Console?

License Administration Console ya no es compatible y se quitó de License Server 11.16.6. Le recomendamos que utilice Citrix Licensing Manager.

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 Citrix Licensing Manager.

¿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 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 y Studio ofrecen datos sobre el uso de licencias en tiempo real.

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.

Sistema de licencias en Citrix Virtual Apps and Desktops

¿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 Licencia de usuario o dispositivo, y para las licencias simultáneas, Licencia simultánea.

¿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. Para obtener más información, consulte Licencias Evaluation.

Citrix DaaS (antes, Citrix Virtual Apps and Desktops Service) 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. Para obtener más información, consulte Licencia simultánea.

¿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.

¿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 simultanea 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 simultanea 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.

¿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 XenServer.

¿Cómo funcionan las horas agrupadas de Remote Browser Isolation (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.

¿Puedo usar acceso con Remote PC con licencias CCU?

Sí.

Para obtener información, consulte Acceso con Remote PC.

¿Qué ocurre cuando caduca el mantenimiento del software para mi entorno Citrix?

Los usuarios recibirán un mensaje de advertencia indicando que Citrix Virtual Apps and Desktops no es compatible una vez iniciada la sesión. En este punto, el cliente ya no tiene derecho a ningún tipo de asistencia. Contacte con su partner o representante de ventas de Citrix para renovar las licencias.

Advertencia de Citrix Virtual Apps and Desktops:

```
Your corporate Citrix environment is currently unsupported. Please
contact your IT department to resolve any support related issues.
```


Licencias de usuario o dispositivo

¿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. Para obtener más información, consulte Licencia de usuario/dispositivo.

¿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:

```
(Number of total users) – (number of users that only access
   exclusively
 with shared devices) + (number shared devices) = total number
 of licenses to buy.

For example, there are 1000 total users at the hospital. If 700 of them
    access only
Citrix Virtual Desktops from 300 shared devices in the hospital, the
   number of
licenses to purchase is 1000 – 700 + 300 = 600 licenses.
```

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 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.

¿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.

¿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. Para obtener más información, consulte Mostrar o liberar licencias para usuarios o dispositivos.

¿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.

¿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.

Licencias simultáneas

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 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.

¿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.

¿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.

Licencias de descubierto

¿Cómo obtener licencias de descubierto?

Los productos (excepto Citrix Cloud) que admiten modelos de licencia de usuario/dispositivo, usuario o dispositivo incluyen una función de descubierto de licencias que permite utilizar una cantidad limitada de licencias adicionales para evitar la denegación de acceso. La función de descubierto se ofrece como una comodidad, no como un derecho de licencias. Las licencias simultáneas y de servidor no conllevan la función de descubierto. Toda licencia de descubierto utilizada debe adquirirse dentro de los 30 días siguientes al primer uso, pero el uso no está limitado a 30 días. Citrix se reserva el derecho de eliminar cualquier función de descubierto en las nuevas versiones de productos. Para obtener más información, consulte Descubierto de 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 descubierto ofrece el mismo acceso y la misma funcionalidad que las demás licencias.

¿Puedo recibir una alerta cuando se utilicen mis licencias de descubierto?

Por el momento, no existen alertas concretas cuando se utilizan las licencias de descubierto.

¿Durante cuánto tiempo puede utilizarse una licencia de descubierto?

Debe adquirir las licencias de descubierto dentro de los 30 días siguientes al primer uso.

Información adicional sobre licencias específicas de productos

- Citrix ADC
- Citrix Cloud
- Citrix Endpoint Management
- Citrix Gateway
- XenServer

- Citrix Licensing

Equilibrar la carga de las máquinas

August 17, 2024

> **Nota:**
>
> Puede administrar la implementación de Citrix Virtual Apps and Desktops mediante dos consolas de administración: Web Studio (basada en la web) y Citrix Studio (basada en Windows). Esta función solo está disponible en Web Studio.
>
> Esta función se aplica a todos los catálogos, ya sean de SO de sesión única o de SO multisesión. El equilibrio de carga vertical solo se aplica a las máquinas con SO multisesión.

El equilibrio de carga se puede configurar a nivel de sitio y de grupo de entrega. Tiene dos opciones: vertical y horizontal. El equilibrio de carga horizontal está habilitado de forma predeterminada.

Parámetros de equilibrio de carga a nivel de sitio

- **Equilibrio de carga vertical**. Asigna la carga entrante a la máquina más cargada que aún no haya alcanzado la carga máxima. De esta forma, se saturan las máquinas existentes antes de pasar a otras máquinas. Cuando los usuarios se desconectan de las máquinas existentes, se libera capacidad en esas máquinas. A continuación, las cargas entrantes se asignan a esas máquinas. El equilibrio de carga vertical degrada la experiencia del usuario, pero reduce los costes (las sesiones maximizan la capacidad de las máquinas encendidas).

  Ejemplo: Tiene dos máquinas configuradas para 10 sesiones cada una. La primera máquina gestiona las 10 primeras sesiones simultáneas. La segunda máquina gestiona la undécima sesión.

  > **Sugerencia:**
  >
  > Para especificar la cantidad máxima de sesiones que puede alojar una máquina, utilice la configuración de directiva Número máximo de sesiones.

  También puede utilizar PowerShell para habilitar o inhabilitar el equilibrio de carga vertical en todo el sitio. Utilice el parámetro `UseVerticalScalingForRdsLaunches` del cmdlet `Set-BrokerSite`. Use `Get-BrokerSite` para mostrar el valor del parámetro `UseVerticalScalingForRdsLaunches`. Para obtener más información, consulte la ayuda del cmdlet.

- **Equilibrio de carga horizontal**. Asigna una sesión de usuario entrante a la máquina encendida con menos carga que esté disponible. El equilibrio de carga horizontal mejora la experiencia de usuario, pero aumenta los costes (porque se mantienen encendidas más máquinas). El equilibrio de carga horizontal está habilitado de forma predeterminada.

  Ejemplo: Tiene dos máquinas configuradas para 10 sesiones cada una. La primera máquina gestiona cinco sesiones simultáneas. La segunda máquina también gestiona cinco.

Para configurar esta función, desde **Administrar > Configuración completa**, seleccione **Parámetros** en el panel de la izquierda. Seleccione una opción en **Equilibrar la carga de catálogos multisesión**.

Parámetros de equilibrio de carga a nivel de grupo de entrega

Configurar el equilibrio de carga a nivel de grupo de entrega le permite anular los parámetros de equilibrio de carga heredados del nivel de sitio. Puede lograr la máxima utilización de cada máquina si selecciona el equilibrio de carga vertical en el nivel de grupo de entrega. Esto ayudará a reducir los costes en nubes públicas. Esta configuración se puede realizar durante la creación de un nuevo grupo de entrega o durante la modificación de un grupo de entrega existente.

Equilibrio de carga horizontal. Las sesiones se distribuyen entre las máquinas encendidas. Por ejemplo, si tiene dos máquinas configuradas para 10 sesiones cada una, la primera máquina gestiona cinco sesiones simultáneas y la segunda también gestiona cinco.

Equilibrio de carga vertical. Las sesiones maximizan la capacidad de las máquinas encendidas y ahorran costes de máquina. Por ejemplo, si tiene dos máquinas configuradas para 10 sesiones cada una, la primera máquina gestionará las 10 primeras sesiones simultáneas. La segunda máquina gestiona la undécima sesión.

Caché de host local

August 17, 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 funciones disponibles de alta disponibilidad de SQL Server que se admiten, consulte Bases de datos). Sin embargo, las interrupciones del servicio y los problemas de red pueden provocar que los usuarios no puedan conectarse a sus aplicaciones o escritorios.

La función Caché de host local 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:

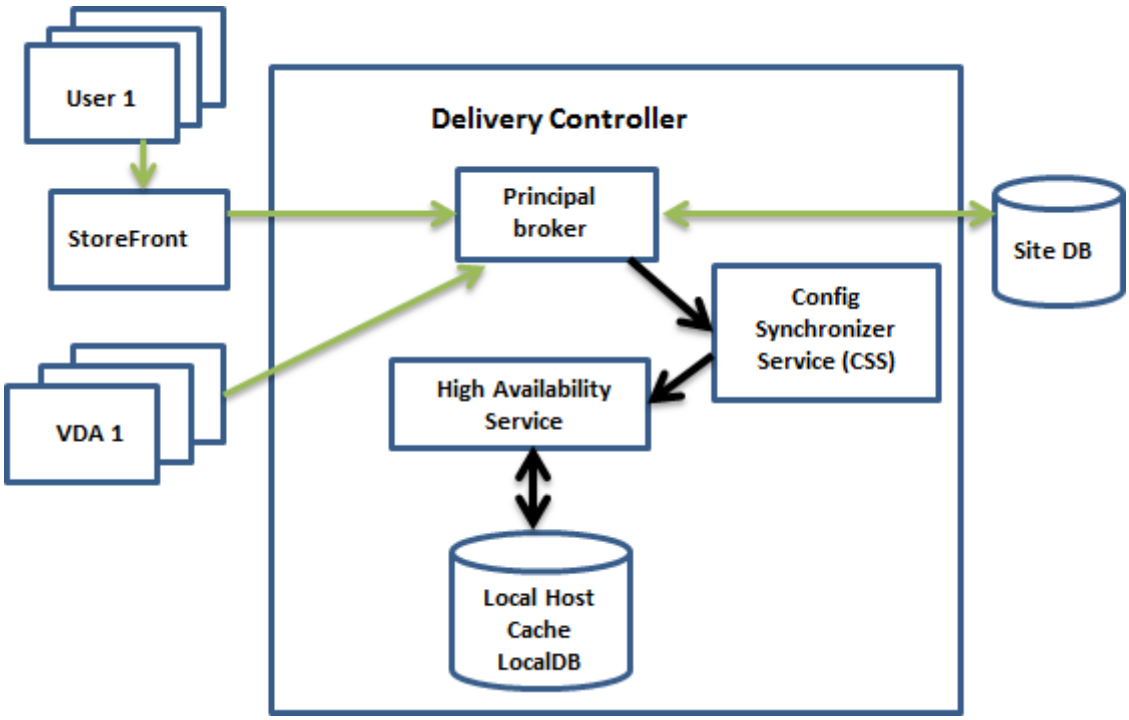
- Identidades de los usuarios y los grupos que tienen derechos asignados a recursos publicados en el sitio.
- Identidades de los usuarios que actualmente usan, o que han utilizado recientemente, recursos publicados en el sitio.
- Identidades de las máquinas VDA (incluidas las máquinas de acceso con Remote 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 normal

- El *broker principal* (conocido también como 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.
- El servicio Citrix Config Synchronizer Service (CSS) se comunica con el broker aproximadamente cada 5 minutos para comprobar si se han hecho cambios. Esos cambios pueden haberse iniciado por la acción de un administrador (si modifica una propiedad del grupo de entrega, por ejemplo) o por acciones del sistema (como las asignaciones de máquinas).
- Si se ha producido un cambio de configuración desde la comprobación anterior, CSS sincroniza la información (la copia) con un broker secundario presente en el Controller. (El broker secundario también se conoce como servicio de alta disponibilidad.)

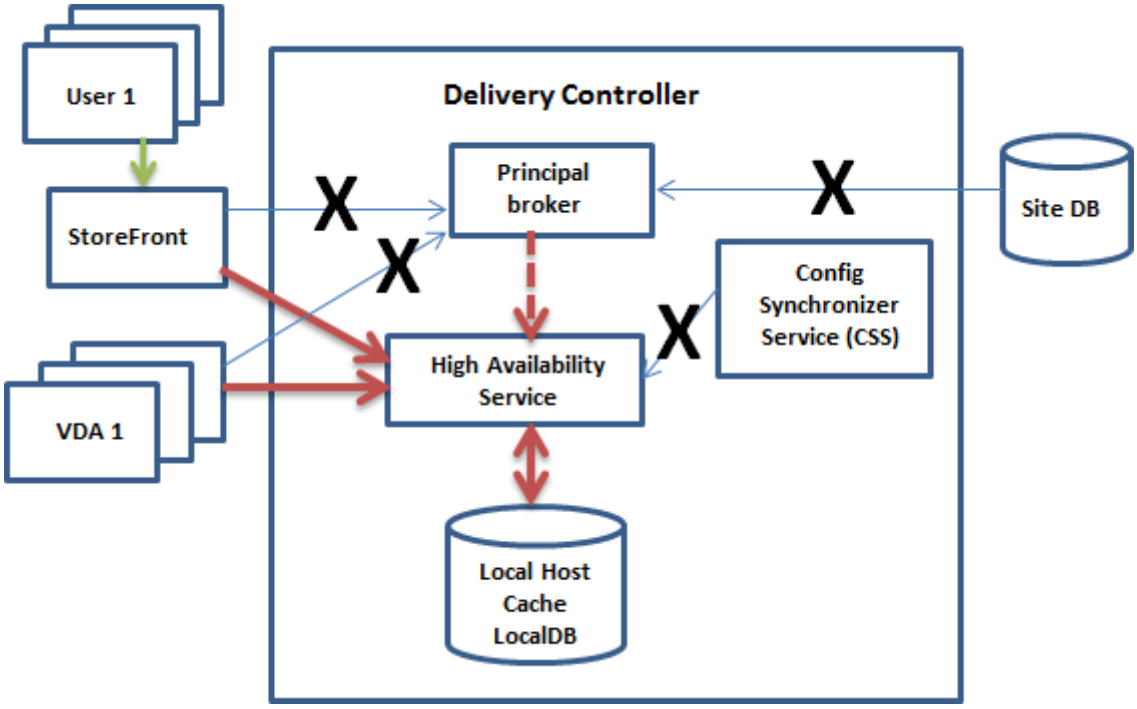
  Se copian todos los datos de la configuración, no solo los elementos que han cambiado desde la comprobación anterior. El servicio CSS importa los datos de configuración en una base de datos LocalDB de Microsoft SQL Server Express ubicada en el Controller. Esta base de datos se conoce como la base de datos de la Caché de host local. El servicio CSS comprueba que la información de la base de datos de caché de host local coincida con la información presente en la base de datos del sitio. La base de datos de la Caché de host local se crea con cada sincronización.

  Microsoft SQL Server Express LocalDB (que la base de datos de caché de host local utiliza) se instala automáticamente al instalar un Controller. Puede prohibir esta instalación al instalar

un Controller desde la línea de comandos. La base de datos de caché de host local no se puede compartir entre Controllers. No es necesario realizar una copia de seguridad de la base de datos de la Caché de host local. Se vuelve a crear cada vez que se detecta un cambio de configuración.

- 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:



Durante una interrupción del servicio

Al principio de una interrupción del servicio:

- El broker secundario comienza a escuchar y a procesar las solicitudes de conexión.
- Cuando empieza la interrupción, el broker secundario no dispone de datos actuales de registro de agentes VDA, pero, en cuanto un VDA se comunica con él, comienza un proceso de registro. Durante este proceso, el broker secundario también obtiene información de sesión actualizada acerca de ese VDA.
- Mientras el broker secundario gestiona las conexiones, el broker principal sigue supervisando la conexión. Cuando se restaura la conexión, el broker principal indica al secundario 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 registro. El broker secundario elimina los registros de VDA restantes desde la interrupción anterior. El servicio CSS reanuda la sincronización de información cuando detecta que se han producido cambios de configuración en la implementación.

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.

No hay límites de tiempo impuestos para el funcionamiento en modo de interrupción.

La transición entre el modo normal y el de interrupción no afecta a las sesiones existentes. Afecta solo al inicio de nuevas sesiones.

También puede desencadenar intencionadamente una interrupción. Consulte 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 broker secundario 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 broker secundario obtiene datos de todos los demás brokers secundarios que se ejecuten en los demás Controllers de la zona.

Los brokers secundarios se comunican entre sí por un canal independiente. Estos brokers utilizan una lista alfabética de nombres de dominio completo (FQDN) de las máquinas en las que están ejecutando para determinar (elegir) qué broker secundario intermediará las operaciones de la zona si se produce una interrupción. Durante la interrupción, todos los VDA vuelven a registrarse en el broker secundario que se haya elegido. Los brokers secundarios de la zona que no hayan sido elegidos rechazan las solicitudes entrantes de conexión y de registro que les envíen los agentes VDA.

Si un broker secundario elegido falla durante una interrupción del servicio, se elegirá otro broker secundario para que le releve, y los VDA se registrarán en el broker secundario que acaba de elegirse.

Durante una interrupción, si se reinicia un Controller:

- Si ese Controller no es el broker elegido, el reinicio no tiene repercusión.
- Si ese Controller es el broker 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 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.

Los registros de eventos proporcionan información sobre las opciones elegidas.

Lo que no está disponible durante una interrupción y otras diferencias

No hay límites de tiempo impuestos para el funcionamiento en modo de interrupción. Sin embargo, Citrix recomienda restaurar la conectividad lo antes posible.

Durante una interrupción:

- No puede utilizar Studio.
- Tiene acceso limitado al SDK de PowerShell.
  - Primero debe:
    * Agregar una clave del Registro `EnableCssTestMode` con un valor de 1: `New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTestMode -PropertyType DWORD -Value 1`
    * Utilizar el puerto 89: `Get-BrokerMachine -AdminAddress localhost:89 | Select MachineName, ControllerDNSName, DesktopGroupName, RegistrationState`
  - Después de ejecutar esos comandos, puede acceder a:
    * Todos los cmdlets `Get-Broker*`.
- 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 servidores 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 broker secundario actualmente activo o elegido. Durante una interrupción, no se admiten inicios entre zonas (desde un broker secundario de una zona a 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.

- La preferencia de zonas no puede configurarse. Si se configura, no se tienen en cuenta las preferencias para el inicio de sesión.
- 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.

Compatibilidad con aplicaciones y escritorios

LHC admite los siguientes tipos de VDA y modelos de entrega:

Tipo de VDA	Modelo de entrega	Disponibilidad de los VDA durante los eventos LHC
SO multisesión	Aplicaciones y escritorios	Siempre disponible.
Sistema operativo de sesión única estático (asignado)	Escritorios	Siempre disponible.
Sistema operativo de sesión única con administración de energía aleatorio (agrupado)	Escritorios	No está disponible de forma predeterminada. De forma predeterminada, fallarán todos los intentos de iniciar sesión en los VDA con administración de

> **Nota:**
>
> Permitir el acceso a los VDA de escritorio con administración de energía en grupos de entrega agrupados no afecta al funcionamiento de la propiedad `ShutdownDesktopsAfterUse` configurada durante las operaciones normales. Cuando se habilita el acceso a estos escritorios en el modo LHC, los VDA no se reinician automáticamente una vez finalizado el evento de 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. El reinicio del VDA puede producirse cuando un usuario cierra sesión en el VDA durante operaciones ajenas al LHC o cuando los administradores reinician el VDA.

Importante: Habilitar el acceso a máquinas agrupadas de sesión única con administración de energía puede provocar que los datos y los cambios de las sesiones de usuario anteriores estén presentes en las sesiones posteriores.

Habilite el LHC para los VDA agrupados de SO de sesión única con administración de energía mediante la Configuración completa

Con la Configuración completa, puede hacer que esas máquinas estén disponibles para nuevas conexiones durante los eventos de LHC para los grupos de entrega que seleccione:

- Para habilitar esta función durante la creación de grupos de entrega, consulte Crear grupos de entrega.

- Para habilitar esta función para un grupo de entrega existente, consulte Administrar grupos de entrega.

> **Nota:**
>
> Este parámetro solo está disponible en Configuración completa para los grupos de entrega de escritorios agrupados que entregan VDA con administración de energía.

Habilitar LHC para los VDA agrupados de SO de sesión única con administración de energía mediante PowerShell

Para habilitar LHC para los VDA en un grupo de entrega específico, siga estos pasos:

1. Ejecute este comando para habilitar esta función para todo el sitio:

   ```
   Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
   ```

2. Ejecute este comando con un nombre del grupo de entrega especificado para habilitar LHC para ese grupo de entrega:

   ```
   Set-BrokerDesktopGroup -Name "name"-ReuseMachinesWithoutShutdownInOutage
    $true
   ```

Para cambiar la disponibilidad de LHC predeterminada para los grupos de entrega agrupados recién creados con agentes VDA con administración de energía, ejecute el siguiente comando:

```
Set-BrokerSite -DefaultReuseMachinesWithoutShutdownInOutage $true
```

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 broker secundario 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.

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 período de interrupción cuando la base de datos no está disponible y el broker secundario 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 incurre en más E/S 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 broker secundario 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 broker secundario elegido deba gestionar muchas más solicitudes durante una interrupción que en una situación normal. Por lo tanto, la necesidad de CPU será mucho mayor. Todos los brokers secundarios del sitio (zona) deben ser capaces de gestionar la carga adicional impuesta por la base de datos de caché de host local y todos los agentes VDA afectados, ya que el broker secundario elegido durante una interrupción puede 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 se registran en un broker secundario, 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 cree una nueva sesión aunque la reconexión a una sesión existente fuera posible. Este intervalo (mientras el "nuevo"broker secundario obtiene la información de sesión de todos los VDA durante el proceso de rerregistro) no se puede evitar. 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 broker secundario.
- Fallo de broker secundario durante una interrupción: Al migrar desde un broker secundario en que se produjo el fallo a otro broker secundario que acaba de elegirse.
- 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 brokers secundarios aumenta con la cantidad de objetos (como agentes VDA, aplicaciones, grupos). Por ejemplo: sincronizar 5000 agentes VDA podría llevar 10 minutos o más.

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

El software de 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. Solo el broker secundario se comunica con esta base de datos. 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 `XenDesktopServerSetup.exe` e incluya la opción `/exclude "Local Host Cache Storage (LocalDB)"`. No obstante, tenga en cuenta que la funcionalidad Caché de host local no funcionará sin la base de datos, y no se puede usar otra base de datos con el broker secundario.

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 el valor de 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. Esto garantiza que el broker secundario pueda hacerse cargo, si fuera necesario.
  - En el servidor del Delivery Controller, vaya a `C:\Windows\ServiceProfiles\NetworkService`.
  - Compruebe 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. Esto puede tardar aproximadamente 15 minutos.

Registros de eventos

Los registros de eventos indican cuándo tienen lugar las sincronizaciones y las interrupciones. En los registros del visor de eventos, el modo de interrupción se conoce como *modo de alta disponibilidad (HA).**

Config Synchronizer Service:

Durante las operaciones normales, pueden producirse los siguientes eventos cuando el servicio CSS importa los datos de configuración en la base de datos de la Caché de host local a través del broker correspondiente.

- 503: Citrix Config Sync Service recibió una configuración actualizada. Este evento indica el inicio del proceso de sincronización.

- 504: Citrix Config Sync Service importó una configuración actualizada. La importación de la configuración se completó correctamente.
- 505: Falló una importación de Citrix Config Sync Service. La importación de la configuración no se completó correctamente. Si hay una configuración previa disponible, se utiliza si ocurre una interrupción. Sin embargo, estará desactualizada frente a la configuración actual. Si no hay ninguna configuración previa disponible, el servicio no puede participar en la intermediación de sesiones durante una interrupción. En este caso, consulte la sección Solucionar problemas y póngase en contacto con la asistencia de Citrix.
- 507: Citrix Config Sync Service abandonó una importación porque el sistema está en modo de interrupción del servicio y el broker de la Caché de host local se está utilizando para la intermediación. El servicio recibió una nueva configuración, pero la importación fue abandonada debido a una interrupción. Este es el comportamiento esperado.
- 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):

Este servicio también se conoce como broker de la Caché de host local.

- 3502: Se ha producido una interrupción y el broker de caché de host local está llevando a cabo operaciones de intermediación.
- 3503: Se ha resuelto una interrupción y se ha reanudado el funcionamiento normal.
- 3504: Indica el broker de la Caché de host local elegido, además de otros brokers de caché de host local que hayan participado en la elección.
- 3507: Proporciona una actualización de estado de la memoria caché de host local cada 2 minutos, lo que indica que el modo de caché de host local está activo en el intermediario elegido. Contiene un resumen de la interrupción del servicio, que incluye la duración de la interrupción, el registro de VDA e información de la sesión.
- 3508: Anuncia que la memoria caché de host local ya no está activa en el intermediario elegido y que se han restablecido las operaciones normales. Contiene un resumen de la interrupción del servicio, que incluye la duración de la interrupción, la cantidad de máquinas que se registraron durante el evento de caché de host local y la cantidad de inicios correctos durante dicho evento.
- 3509: Notifica que la memoria caché de host local está activa en los intermediarios no elegidos. Contiene una duración de interrupción del servicio cada 2 minutos e indica el intermediario elegido.
- 3510: Anuncia que la memoria caché de host local ya no está activa en los intermediarios no elegidos. Contiene la duración de la interrupción del servicio e indica el intermediario elegido.

Forzar una interrupción del servicio

Puede que quiera forzar deliberadamente una interrupción.

- Si la red tiene altibajos repetidos. Forzar una interrupción hasta que se resuelvan los problemas de red impide una transición continua entre los modos normal y de interrupción (con las avalanchas de registros de VDA que ello conlleva).
- Para probar un plan de recuperación ante desastres.
- Para comprobar que la Caché de host local funciona correctamente.
- 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`, cree y establezca `OutageModeForced` como `REG_DWORD` con el valor `1`. Este parámetro indica al broker de la caché de host local que entre en el modo de interrupción, independientemente del estado de la base de datos. Establecer este valor en `0` saca al broker de la Caché de host local del modo de interrupción del servicio.

Para comprobar los eventos, supervise el archivo de registros `Current_HighAvailabilityService` que hay en `C:\ProgramData\Citrix\WorkspaceCloud\Logs\Plugins\HighAvailabilityServ`.

Solucionar problemas

Existen varias herramientas de solución de problemas disponibles cuando falla una importación de sincronización a la base de datos de la Caché de host local 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: Si falla una importación de sincronización, puede generar un informe. Este informe se detiene en el objeto que causa el 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 seguimiento de CSS, escriba el siguiente comando:

```
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\CitrixBrokerConfigSyncReport.html`.

Una vez generado el informe, introduzca el siguiente comando para inhabilitar 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`.

Comandos de PowerShell para la memoria caché de host local

Puede administrar la caché de host local (LHC) en sus Delivery Controllers mediante comandos de PowerShell.

El módulo de PowerShell se encuentra en esta ubicación de los Delivery Controllers:

```
C:\Program Files\Citrix\Broker\Service\ControlScripts
```

> **Importante:**
>
> Ejecute este módulo solo en los Delivery Controllers.

Importar módulo de PowerShell Para importar el módulo, ejecute lo siguiente en su Delivery Controller.

```
cd C:\Program Files\Citrix\Broker\Service\ControlScripts Import-
Module .\HighAvailabilityServiceControl.psm1
```

Comandos de PowerShell para administrar la LHC Estos comandos le ayudan a activar y administrar el modo LHC en los Delivery Controllers.

Cmdlets	Función
`Enable-LhcForcedOutageMode`	Ponga al intermediario en modo LHC. Los archivos de bases de datos de LHC debe haberlos creado correctamente ConfigSync Service para que `Enable-LhcForcedOutageMode` funcione correctamente. Este cmdlet solo fuerza a la LHC del Delivery Controller en que se ejecutó. Para que la LHC se active, este comando debe ejecutarse en todos los Delivery Controllers de la zona.
`Disable-LhcForcedOutageMode`	Saque al intermediario del modo LHC. Este cmdlet solo inhabilita el modo LHC en el Delivery Controller en el que se ejecutó. `Disable-LhcForcedOutageMode` debe ejecutarse en todos los Delivery Controllers de la zona.
`Set-LhcConfigSyncIntervalOverride`	Establece el intervalo en que Citrix Config Synchronizer Service (CSS) comprueba cambios de configuración en el sitio. El intervalo de tiempo puede oscilar entre 60 segundos (un minuto) y 3600 segundos (una hora). Este parámetro solo se aplica al Delivery Controller en el que se ejecutó. Para mantener la coherencia entre los Delivery Controllers, considere la posibilidad de ejecutar este cmdlet en cada Delivery Controller. Por ejemplo: `Set-LhcConfigSyncIntervalOverride -Seconds 1200`
`Clear-LhcConfigSyncIntervalOverride`	Establece el intervalo en que Citrix Config Synchronizer Service (CSS) comprueba cambios de configuración en el sitio en función del valor predeterminado de 300 segundos (cinco minutos). Este parámetro solo se aplica al Delivery Controller en el que se ejecutó. Para mantener la coherencia entre los Delivery Controllers, considere la posibilidad de ejecutar este cmdlet en cada Delivery Controller.

Cmdlets	Función
`Enable-LhcHighAvailabilitySDK`	Habilita el acceso a todos los cmdlets `Get-Broker*` del Delivery Controller en que se ejecutó.
`Disable-LhcHighAvailabilitySDK`	Inhabilita el acceso a los cmdlets del intermediario del Delivery Controller en que se ejecutó.

> **Nota:**
>
> - Use el puerto 89 cuando ejecute los cmdlets `Get-Broker*` en el Delivery Controller. Por ejemplo:
>
>   ```
>   - Get-BrokerMachine -AdminAddress localhost:89
>   ```
>
> - Cuando no está en modo LHC, el intermediario de la LHC del Delivery Controller solo contiene información de configuración.
> - Durante el modo LHC, el agente de la LHC del Delivery Controller elegido contiene esta información:
>   - Estados de los recursos
>   - Detalles de la sesión
>   - Registros de VDA
>   - Información de configuración

Supervisar y administrar máquinas y sesiones con Buscar

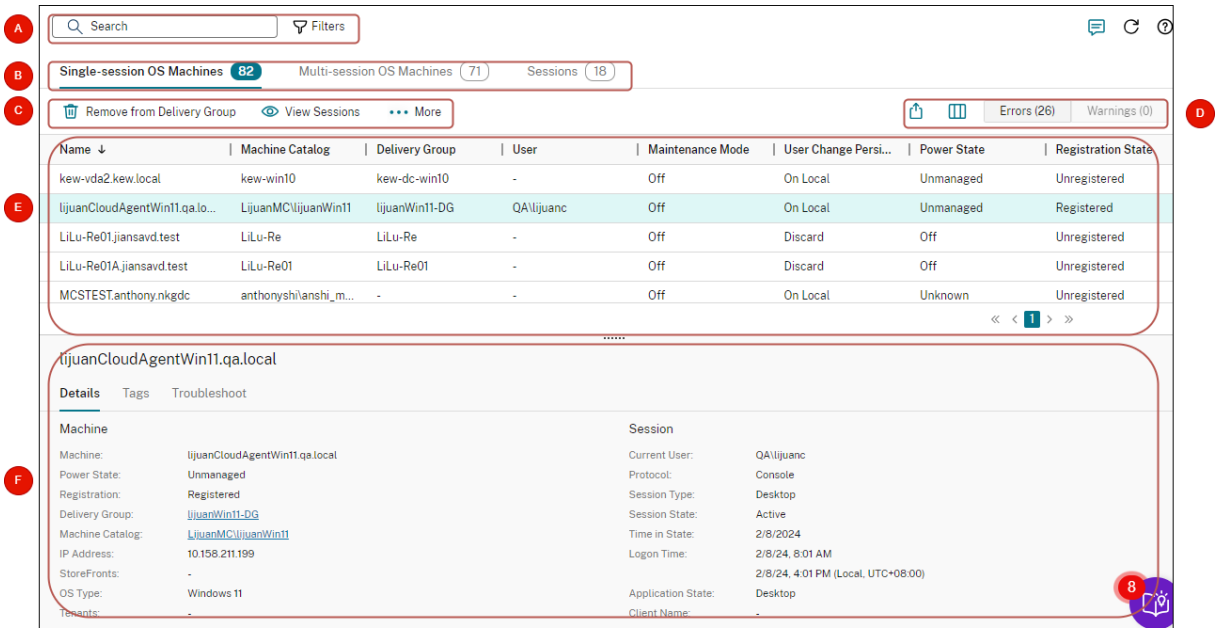
August 17, 2024

> **Nota:**
>
> Puede administrar la implementación de Citrix Virtual Apps and Desktops mediante dos consolas de administración: Web Studio (basada en la web) y Citrix Studio (basada en Windows). Este artículo se refiere únicamente a Web Studio. Para obtener información sobre Citrix Studio, consulte el artículo equivalente en Citrix Virtual Apps and Desktops 7 2212 o versiones anteriores.

En este artículo se explica cómo supervisar y administrar las máquinas y las sesiones mediante el nodo **Configuración completa > Buscar**.

Más información sobre el nodo

El nodo **Buscar** proporciona un lugar centralizado para supervisar y administrar las máquinas y las sesiones de usuario.



Leyenda	Área	Descripción
A	Barra de búsqueda	Proporciona una búsqueda rápida y una búsqueda basada en filtros que permiten definir criterios de búsqueda complejos. Para obtener más información, consulte Búsqueda de instancias.
B	Fichas de tipos	Muestra fichas para enumerar las máquinas por tipo o todas las sesiones. Los recuentos de instancias aparecen en los nombres de las fichas.
C	Acciones en el nivel de instancia	Muestra las acciones que puede realizar en las *instancias seleccionadas* (máquinas o sesiones). Para obtener más información, consulte Acciones de máquina y Acciones de sesión.

Leyenda	Área	Descripción
D	Acciones en el nivel de lista	Muestra las acciones que puede realizar en la *lista* actual -Icono **Exportar**: Exporta la lista de instancias que se muestra en la vista principal a un archivo CSV. -Icono **Columna que mostrar**: Personaliza la vista principal de la lista.
E	Vista principal	Muestra las instancias y sus propiedades. Puede personalizar la vista principal seleccionando el icono **Columna que mostrar**. Para obtener más información sobre las columnas disponibles, consulte Columnas de máquina y Columnas de sesión. -Etiqueta **Errores**: Habilite esta etiqueta para mostrar solo las máquinas no registradas con errores en la vista principal. Para ver detalles del problema, vaya a la ficha **Solución de problemas** del panel **Detalles**.
F	Recuadro Detalles	Muestra los siguientes detalles -Etiqueta de **advertencia**: Habilite esta etiqueta para mostrar solo las máquinas no registradas con advertencias en la vista principal. Para ver detalles del problema, vaya a la ficha **Solución de problemas** del panel **Detalles**. Detalles de la instancia seleccionada (máquina o sesión) Etiquetas aplicadas a la máquina seleccionada Detalles de los errores o advertencias de la máquina seleccionada, incluidos los problemas, las posibles causas y las soluciones sugeridas

Búsqueda de instancias

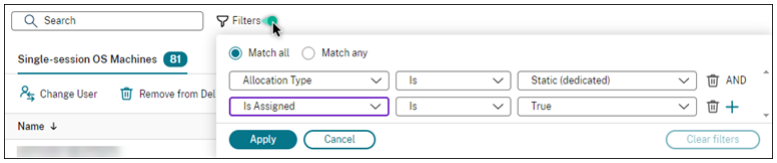
Use la función de búsqueda para localizar máquinas y sesiones específicas.

- Búsqueda mediante filtros
- Guardar el conjunto de filtros actual para una búsqueda rápida
- Anclar un campo de filtro en la barra de búsqueda
- Buscar usando el cuadro de búsqueda rápida
- Sugerencias para mejorar las búsquedas

Búsqueda mediante filtros

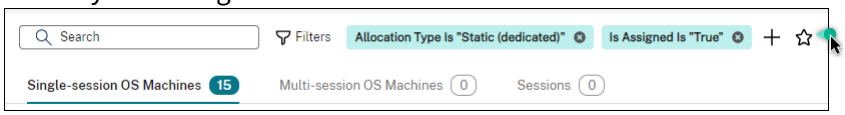
Por ejemplo, para localizar todas las máquinas con sistema operativo de sesión única que son *estáticas* y están *asignadas a usuarios*, siga estos pasos:

1. En la ficha **Máquinas con SO de sesión única**, haga clic en el icono **Filtros**. Aparecerá el panel Filtros.
2. Agregue los criterios de filtro necesarios.



3. Seleccione **Hacer coincidir todo** (operador AND) si quiere que la búsqueda devuelva resultados que coincidan con todos los criterios del filtro. Seleccione **Hacer coincidir cualquiera** (operador OR) si quiere que la búsqueda devuelva resultados que coincidan con cualquiera de los criterios del filtro.
4. Haga clic en **Aplicar**.

   La lista filtrada muestra todas las máquinas con sistema operativo de sesión única que son estáticas y están asignadas a usuarios.

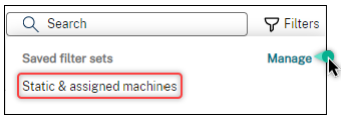


Guardar el conjunto de filtros actual para una búsqueda rápida

Por ejemplo, para guardar el conjunto de filtros para localizar las máquinas con sistema operativo de sesión única que son estáticas y están asignadas a usuarios para su uso futuro, siga estos pasos:

1. Tras realizar una búsqueda basada en filtros, haga clic en el icono de **estrella** de la barra de búsqueda, como se muestra en la figura anterior.
2. En la página que aparece, introduzca un nombre para este conjunto de filtros (por ejemplo, *Máquinas estáticas y asignadas*).
3. Haga clic en **Guardar**.

   El conjunto de filtros guardado aparece en la lista del historial de búsqueda al hacer clic en el cuadro de búsqueda.

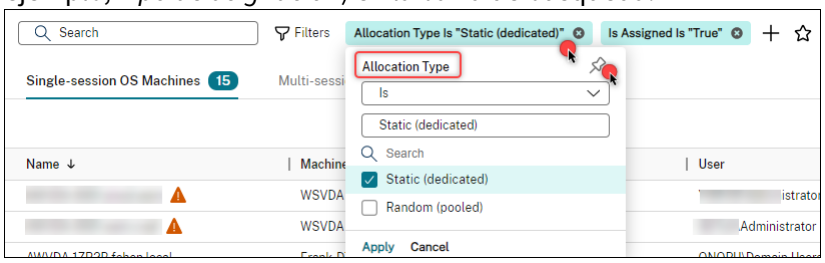


> **Nota:**
>
> Los conjuntos de filtros se guardan por cuenta de usuario. Para administrar los conjuntos de filtros guardados, seleccione **Administrar**.

Anclar un campo de filtro en la barra de búsqueda

Para facilitar el acceso, puede anclar *campos* de filtro de uso frecuente en la barra de búsqueda. Por ejemplo, después de realizar una búsqueda basada en filtros, puede que quiera anclar **Tipo de asignación** en la barra de búsqueda. Siga estos pasos:

1. Haga clic en el *parámetro del filtro* en la barra de búsqueda.
2. En el panel que aparece, haz clic en el icono de **chincheta** para anclar el campo de filtro (en este ejemplo, *Tipo de asignación*) en la barra de búsqueda.



Buscar usando el cuadro de búsqueda rápida

El cuadro de búsqueda rápida proporciona una forma cómoda de buscar instancias en función de las propiedades relacionadas con el nombre o los conjuntos de filtros guardados. Estos son los pasos detallados:

1. Haga clic en el cuadro de búsqueda. Las búsquedas recientes y los conjuntos de filtros guardados aparecen en la lista desplegable. Puede hacer clic en una búsqueda anterior o en un conjunto de filtros para realizar una búsqueda rápida.
2. Para iniciar una nueva búsqueda, introduzca un nombre completo o parcial de una de las siguientes opciones:
    - Nombre de máquina o nombre DNS
    - Nombre de catálogo de máquinas
    - Nombre de grupo de entrega
    - Nombre de usuario de la sesión
    - Nombre del cliente de la sesión
    - Nombre descriptivo de la máquina virtual que aloja la sesión, tal como lo usa su hipervisor
    - Nombre del servidor de alojamiento

Sugerencias para mejorar las búsquedas

Tenga en cuenta estos consejos al utilizar la función Buscar:

- En el nodo **Buscar**, seleccione cualquier columna para ordenar los elementos.

- Para mostrar más características que se deben incluir en la pantalla donde puede buscar y ordenar, seleccione **Columnas que mostrar** o haga clic en una columna y seleccione **Columnas que mostrar**. En la ventana **Columnas que mostrar**, marque la casilla de verificación situada junto a los elementos que quiere mostrar y seleccione **Guardar** para salir.

  > **Nota:**
  >
  > Las columnas que degradan el rendimiento se marcan con la etiqueta **Degrada el rendimiento**.

- 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 mostrar todas las máquinas de un grupo de entrega, seleccione **Grupos de entrega** en el panel de la izquierda. Seleccione el grupo y, a continuación, seleccione **Ver máquinas** en la barra de acciones o en el menú contextual.

Tenga en cuenta las siguientes consideraciones al realizar operaciones de ordenación:

- Siempre que el número de elementos no supere los 5000, puede hacer clic en cualquier columna para ordenar los artículos que contiene. Cuando el número supera los 5000, solo se puede ordenar por nombre o por usuario actual (según la ficha en la que se encuentre). Para habilitar la ordenación, utilice filtros para reducir el número de artículos a 5000 o menos.
- Cuando el número de elementos es superior a 500 pero no superior a 5000:
  - Almacenamos en caché todos los datos localmente para mejorar el rendimiento de ordenación. En las fichas **Máquinas con SO de sesión única** y **Máquinas con SO multisesión**, almacenamos los datos en caché la primera vez que se hace clic en una columna (cualquier columna, excepto la columna **Nombre**) para ordenarlos. En la ficha **Sesiones**, almacenamos en caché los datos la primera vez que se hace clic en una columna (cualquier columna, excepto la columna **Usuario actual**) para ordenarlos. Por ese motivo, la ordenación tarda más en completarse. Para lograr una mayor rapidez, ordene por nombre o usuario actual, o utilice filtros para reducir el número de elementos.
  - El siguiente mensaje bajo la tabla indica que los datos están almacenados en caché: Última actualización: <`the time when you refreshed the table`>. En ese caso, las operaciones de ordenación se basan en elementos que se han cargado anteriormente. Es posible que esos elementos no estén actualizados. Para actualizarlos, haga clic en el icono de actualización.

Personalizar columnas que mostrar

Cree una vista principal personalizada para mostrar las propiedades y los estados cruciales para sus operaciones diarias. Estos son los pasos detallados:

1. En el nodo **Buscar**, seleccione la ficha **Máquinas con SO multisesión**, **Máquinas con SO de sesión única** o **Sesiones**, según sea necesario.
2. Haga clic en el icono **Columnas que mostrar** de la barra de acciones y seleccione las columnas.

   Para obtener más información sobre las columnas disponibles y sus descripciones, consulte Columnas de máquina y Columnas de sesión.

Al elegir columnas, podrá ver columnas marcadas con la etiqueta **Degrada el rendimiento**. Es posible que, al seleccionar esas columnas, se degrade el rendimiento de la consola. Tenga en cuenta estas consideraciones:

- Una vez completada la personalización, la tabla se actualiza para mostrar las columnas seleccionadas. Es posible que su presencia cause demoras al actualizar la tabla.
- Tras actualizar el explorador o cerrar sesión en la consola y, a continuación, iniciar sesión, aparece un mensaje en el que se pregunta si se deben conservar esas columnas. Si decide conservarlas, no podrá actualizar la tabla más de una vez por minuto para que la consola funcione de forma óptima. Para actualizaciones más frecuentes, elimine cualquier columna que degrade el rendimiento.

Administrar máquinas y sesiones

Use las acciones del nodo Buscar para solucionar problemas de máquinas y sesiones o para procesar solicitudes de los usuarios.

Información útil

Puede administrar las máquinas en diferentes niveles:

- En el nivel de máquina individual. Use el nodo **Buscar** para localizar las máquinas de destino y realizar acciones.
- En el nivel de catálogo de máquinas, como cambiar las imágenes maestras de un catálogo, eliminar máquinas de un catálogo y agregar máquinas a un catálogo. Para obtener más información, consulte Administrar catálogos de máquinas.
- En el nivel de grupo de entrega, como activar o desactivar el modo de mantenimiento para las máquinas de un grupo. Para obtener más información, consulte Administrar grupos de entrega.

Además del nivel de sesión individual, también puede administrar las sesiones a nivel de grupo de entrega, por ejemplo, configurar el preinicio y la duración de la sesión para un grupo de entrega. Para obtener más información, consulte Administrar de grupos de entrega.

Realizar acciones en máquinas o sesiones

Para administrar máquinas o sesiones en el nivel de instancia individual, siga estos pasos:

1. En el nodo **Buscar**, seleccione la ficha **Máquinas con SO multisesión**, **Máquinas con SO de sesión única** o **Sesiones**.
2. Seleccione una o más instancias según sea necesario.
3. En la barra de acciones o en el menú del botón secundario, seleccione una acción en función de los problemas que encuentre con esas instancias o solicitudes de usuario.

   Para obtener más información sobre las acciones disponibles y sus descripciones, consulte Acciones de máquina y Acciones de sesión.

> **Nota:**
>
> Si selecciona dos o más instancias, solo estarán disponibles las acciones aplicables a todas ellas.

Exportar datos de máquinas o sesiones a archivos CSV

Puede exportar la lista de instancias (máquinas o sesiones) que se muestra en una ficha (hasta 30 000 elementos) a un archivo CSV. Estos son los pasos detallados:

1. En el nodo **Buscar**, seleccione la ficha **Máquinas con SO multisesión**, **Máquinas con SO de sesión única** o **Sesiones**, según sea necesario.
2. Para ello, haga clic en el icono **Exportar** de la esquina superior derecha.
3. En el cuadro de diálogo que aparece, haga clic en **Continuar**.

   Es posible que la exportación tarde varios minutos en completarse. Puede encontrar el archivo en la carpeta de descargas predeterminada de su explorador.

> **Nota:**
>
> En las fichas del nodo **Buscar**, no puede realizar otra exportación mientras haya una exportación en curso.

Acciones y columnas de máquina

August 17, 2024

En este artículo se enumeran las acciones y las columnas de máquina con descripciones para referencia.

Acciones

Consulte las acciones que puede realizar en las máquinas y sus descripciones.

Acción	Descripción	Aplicable a
Quitar del grupo de entrega	Quite una máquina de un grupo de entrega.	Sesión única y multisesión
Agregar a grupo de entrega	Agregue una máquina a un grupo de entrega.	Sesión única y multisesión
Ver sesiones	Consulte las sesiones que se están ejecutando en una máquina	Sesión única y multisesión
Administrar etiquetas	Agregue y administre las etiquetas de una máquina. Para obtener más información sobre los casos de uso típicos de las etiquetas, consulte Etiquetas.	Sesión única y multisesión
Activar modo de mantenimiento	Puede poner una máquina en modo de mantenimiento antes de aplicar parches o para solucionar problemas. Este modo impide que se establezcan nuevas conexiones con esa máquina. Los usuarios pueden conectarse a las sesiones existentes de esa máquina, pero no pueden iniciar nuevas sesiones en la misma.	Sesión única y multisesión

Acción	Descripción	Aplicable a
Desactivar modo de mantenimiento	Desactive el modo de mantenimiento de una máquina.	Sesión única y multisesión
Actualizar versión de VDA	Actualice la versión del agente VDA de una máquina.	Máquinas con sistema operativo de sesión única o multisesión que cumplen ciertos requisitos: Más información.
Cerrar sesión	Fuerce el cierre de sesión de una máquina	Sesión única y multisesión
Eliminar	Elimine una máquina virtual de un catálogo de máquinas mientras la deja intacta en el hipervisor o el servicio de nube.	Sesión única y multisesión
Cambiar usuario	Asigne una máquina a un usuario específico.	Máquinas *estáticas* de sesión única.
Iniciar	Inicie una máquina.	Sesión única y multisesión
Apagar	Apague una máquina.	Sesión única y multisesión
Reiniciar	Reinicie una máquina	Sesión única y multisesión
Suspender	Ponga una máquina en estado de hibernación o suspensión. Cuando suspende una máquina, los Delivery Controllers almacenan el contenido en memoria de esa máquina en un archivo y, a continuación, la apagan.	Máquinas con SO de sesión única
Reanudar	Reanude una máquina suspendida. Al reanudar una máquina suspendida, los Delivery Controllers la inician y la restauran al estado anterior.	Máquinas con SO de sesión única
Forzar reinicio	Fuerce el reinicio de una máquina.	Máquinas con SO de sesión única
Forzar apagado	Fuerce el apagado de una máquina.	Máquinas con SO de sesión única

Columnas

Vea todas las columnas de una máquina y sus descripciones por tipo:

- Máquina
- Detalles de la máquina
- Aplicaciones
- Alojamiento
- Conexión
- Registro
- Detalles de la sesión
- Sesión

Máquina

Columnas de la categoría **Máquina**.

Columna	Descripción	Aplicable a
Nombre	El nombre de host DNS de la máquina.	Sesión única y multisesión
Catálogo de máquinas	El nombre del catálogo al que pertenece la máquina.	Sesión única y multisesión
Grupo de entrega	El nombre del grupo de entrega al que pertenece la máquina.	Sesión única y multisesión
Nombre simplificado de usuario	Los nombres completos de los usuarios asociados a la máquina (normalmente con el formato `Firstname Lastname`). Los usuarios asociados son los usuarios actuales de las máquinas compartidas y los usuarios asignados de las máquinas dedicadas.	Sesión única y multisesión

Columna	Descripción	Aplicable a
Usuario	Los nombres de usuario de los usuarios asociados a la máquina (con el formato "dominio\ usuario"). Los usuarios asociados son los usuarios actuales de las máquinas compartidas y los usuarios asignados de las máquinas dedicadas.	Sesión única y multisesión
Nombre principal del usuario	Los nombres principales de usuario de los usuarios asociados a la máquina (con el formato "usuario @dominio"). Los usuarios asociados son los usuarios actuales de las máquinas compartidas y los usuarios asignados de las máquinas dedicadas.	Sesión única y multisesión
Nombre simplificado de escritorio	El nombre publicado de la máquina usada originalmente para iniciar la sesión. Es el nombre que aparece en la aplicación Citrix Workspace o StoreFront. **Nota:** Para cambiar la pantalla de un escritorio, necesita el permiso **Realizar actualización de máquina**, ya que el cambio del nombre de la pantalla implica actualizar la propiedad de la máquina.	Solo sesión única
Condiciones de escritorio	La lista de condiciones particulares de escritorio para la máquina. Valores posibles: Desconocido, CPU, ICALatency y UPMLogonTime.	Sesión única y multisesión

Columna	Descripción	Aplicable a
Tipo de asignación	El tipo de asignación de la máquina: **Permanente**, cuando se asigna a un usuario de forma permanente. **Aleatoria**, cuando se asigna de forma aleatoria.	Sesión única y multisesión
Modo de mantenimiento	Indica si la máquina está en modo de mantenimiento.	Sesión única y multisesión
Parámetro de conexión de Windows	Modo de inicio de sesión notificado por Windows. Valores posibles: LogonEnabled, Draining, DrainingUntilRestart y LogonDisabled.	Solo multisesión
Está asignado	Indica si un escritorio dedicado se ha asignado a un usuario o a un cliente (nombre/dirección). Los usuarios se pueden asignar de forma explícita o mediante la asignación en el primer uso de la máquina.	Sesión única y multisesión
Es físico	Indica si la máquina es física o no. `True` indica que la máquina es física, lo que significa que los Delivery Controllers no administran la energía. `False` indica lo contrario.	Sesión única y multisesión
Tipo de aprovisionamiento	Cómo se aprovisionó la máquina. Valores posibles Manual: No se aprovisiona mediante PVS o MCS. PVS: Se aprovisiona mediante PVS (máquinas físicas, blade y virtuales) MCS: Se aprovisiona mediante MCS (solo máquinas virtuales)	Sesión única y multisesión
Reinicio programado	El estado de cualquier operación de reinicio programada para la máquina. Valores posibles Ninguno: No hay ningún reinicio programado. Pendiente: En espera de reiniciarse, pero disponible para uso. Purgando: En espera de reiniciarse y no disponible para	Sesión única y multisesión

Columna	Descripción	Aplicable a
Zona	El nombre de la zona en la que se encuentra la máquina.	Sesión única y multisesión
Estado	El estado general del escritorio asociado a la máquina, derivado de diversos estados específicos, como el estado de la sesión, el estado del registro y el estado de energía. Posibles estados: Desactivado, Sin registrar, Disponible, Desconectado, En uso y En preparación.	Sesión única y multisesión
Etiquetas	La lista de etiquetas asociadas a la máquina.	Sesión única y multisesión
Actualización de versión de VDA	El estado de la máquina para las acciones de actualización de las versiones de los paquetes del agente VDA. Valores posibles: MissingUpgradeType, UpgradeScheduled, UpgradeAvailable, UpToDate y Desconocido.	Sesión única y multisesión
Con capacidad de suspensión	Indica si la máquina admite acciones de alimentación (Suspender y Reanudar).	Sesión única y multisesión
Índice de carga	El índice de carga actual. Para obtener más información, consulte Más información.	Solo multisesión

Columna	Descripción	Aplicable a
Estado de purga	Indica si la máquina se está purgando y se apagará cuando terminen todas las sesiones en la máquina. True solo aparece en máquinas multisesión con administración de energía. **Nota:** La máquina no se apaga si está en modo de mantenimiento. Se apaga solo cuando no está en el modo de mantenimiento.	Solo multisesión

Detalles de la máquina

Columnas de la categoría **Detalles de la máquina**.

Columna	**Descripción**	**Aplicable a**
Versión del agente	La versión del Citrix Virtual Delivery Agent (VDA) instalada en la máquina.	Sesión única y multisesión
Dirección IP	La dirección IP de la máquina.	Sesión única y multisesión
Está asignado	Indica si un escritorio dedicado se ha asignado a un usuario o a un cliente (nombre/dirección). Los usuarios se pueden asignar de forma explícita o mediante la asignación en el primer uso de la máquina.	Sesión única y multisesión
Tipo de SO	El sistema operativo que se ejecuta en la máquina.	Solo sesión única

Aplicaciones

Columnas de la categoría **Aplicaciones**.

Columna	Descripción	Aplicable a
Aplicación en uso	La lista de aplicaciones en uso en la máquina (se muestran como nombres de explorador).	Sesión única y multisesión
Aplicaciones publicadas	La lista de aplicaciones publicadas por la máquina (se muestran como nombres de explorador).	Sesión única y multisesión

Conexiones

Columnas de la categoría **Conexiones**.

Columna	Descripción	Aplicable a
Cliente (IP)	La dirección IP del cliente conectado a la máquina.	Solo sesión única
Cliente	El nombre de host del cliente conectado a la máquina.	Solo sesión única
Versión del plug-in	La versión de la aplicación Citrix Workspace en el cliente conectado.	Solo sesión única
Conectado	El nombre de host de la conexión entrante, normalmente una puerta de enlace, un enrutador o un cliente.	Solo sesión única
Conectado (IP)	La dirección IP de la conexión entrante, normalmente una puerta de enlace, un enrutador o un cliente.	Solo sesión única
Tipo de conexión	El protocolo usado para la sesión. Valores posibles: HDX, RDP y Consola. Nota: El campo se deja en blanco para las sesiones de consola en los VDA de XenDesktop 5.	Solo sesión única

Columna	Descripción	Aplicable a
Última conexión (UTC)	La hora del último intento de conexión detectado que falló o tuvo éxito.	Sesión única y multisesión
Usuario de la última conexión	El nombre SAM (con el formato "DOMINIO\usuario") del usuario que intentó conectarse a la máquina por última vez. Si el nombre SAM no está disponible, se usa el SID.	Sesión única y multisesión
Secure ICA activo	Indica si SecureICA está activo en la sesión actual. Siempre es nulo para máquinas multisesión.	Sesión única y multisesión

Alojamiento

Columnas de la categoría **Alojamiento**.

Columna	Descripción	Aplicable a
VM	El nombre descriptivo de una máquina alojada que ejecuta la sesión, tal como lo usa su hipervisor. No tiene por qué coincidir necesariamente con el nombre DNS o AD de la máquina.	Sesión única y multisesión
Nombre del servidor de alojamiento	El nombre DNS del hipervisor que está alojando la máquina si está administrada.	Sesión única y multisesión
Conexión	El nombre de la conexión de host asignada a la máquina que aloja la sesión.	Sesión única y multisesión

Columna	Descripción	Aplicable a
Actualización pendiente	Indica si la imagen de máquina virtual de una máquina hospedada no está actualizada y se actualizará con una nueva imagen en el próximo reinicio de la máquina.	Sesión única y multisesión
Persistencia de cambios de usuario	Indica cómo se gestionan los cambios de usuario y si estos cambios son persistentes Local: Persistentes. Los cambios de usuario se guardan localmente. Descartar: No persistentes. Los cambios de usuario se descartan.	Sesión única y multisesión
Acción de energía pendiente	Indica si hay alguna acción de energía pendiente para la máquina.	Sesión única y multisesión
Estado de energía	El estado de energía de la máquina. Valores posibles: No administrado, Desconocido, No disponible, Desactivado, Activado, Suspendido, Iniciándose, Apagándose, Suspendiéndose y Reanudándose.	Sesión única y multisesión
Se apagará después de usarse	Solo se aplica a máquinas de sesión única con administración de energía. Indica si la máquina está contaminada y se apagará cuando finalicen todas las sesiones. **Nota:** La máquina no se apagará si está en modo de mantenimiento. Se apagará solo después de salir del modo de mantenimiento.	Solo sesión única

Registro

Columnas de la categoría **Registro** .

Columna	Descripción	Aplicable a
Último fallo de registro	El motivo de la última cancelación del registro de la máquina con el broker. Los valores posibles son: AgentShutdown, AgentSuspended, AgentRequested, IncompatibleVersion, AgentAddressResolutionFailed, AgentNotContactable, AgentWrongActiveDirectoryOU, EmptyRegistrationRequest, MissingRegistrationCapabilities, MissingAgentVersion, InconsistentRegistrationCapabilities, NotLicensedForFeature, UnsupportedCredentialSecurityVersion, InvalidRegistrationRequest, SingleMultiSessionMismatch, FunctionalLevelTooLowForCatalog, FunctionalLevelTooLowForDesktopGroup, PowerOff, DesktopRestart, DesktopRemoved, AgentRejectedSettingsUpdate, SendSettingsFailure, SessionAuditFailure, SessionPrepareFailure, ContactLost, SettingsCreationFailure, UnknownError y BrokerRegistrationLimitReached.	Sesión única y multisesión
Hora de último fallo de registro (UTC)	La hora de la última cancelación del registro de la máquina.	Sesión única y multisesión

Columna	Descripción	Aplicable a
Estado de registro	El estado de registro de la máquina. Valores posibles: Sin registrar, Inicializando, Registrado y Error del agente.	Sesión única y multisesión
Estado de fallo	El estado resumido de cualquier estado de fallo actual de la máquina. Valores posibles Ninguno: Sin fallos. La máquina está en buen estado. No se inició: Falló la última operación de encendido de la máquina. Atascado en arranque: La máquina no se pudo iniciar después de encenderse. Sin registrar. La máquina no se ha registrado en el período previsto o se ha rechazado su registro. Capacidad máxima. La máquina informa que está a su máxima capacidad.	Sesión única y multisesión

Detalles de la sesión

Columnas de la categoría **Detalles de la sesión**.

Columna	**Descripción**	**Aplicable a**
Iniciado	El nombre de host del servidor de StoreFront usado para iniciar la sesión de intermediación con broker actual. Siempre es nulo para máquinas multisesión.	Sesión única y multisesión
Iniciado (IP)	La dirección IP del servidor de StoreFront usada para iniciar la sesión de intermediación con broker actual. Siempre es nulo para máquinas multisesión.	Sesión única y multisesión
Hora de cambio de sesión (UTC)	La hora del último cambio de estado de la sesión actual.	Solo sesión única
Filtros SmartAccess	Etiquetas Smart Access para la sesión actual. Siempre es nulo para máquinas multisesión.	Sesión única y multisesión

Sesión

Columnas de la categoría **Sesión**.

Columna	Descripción	Aplicable a
Estado de la sesión	El estado de la sesión actual. Valores posibles: Otro, Preparando sesión, Conectado, Activo, Desconectado, Reconectando, Sesión sin broker y Desconocido.	Solo sesión única
Usuario actual	El nombre del usuario de la sesión actual (con el formato "DOMINIO\usuario").	Solo sesión única
Inicio (UTC)	Hora de inicio de la sesión actual.	Solo sesión única
Recuento de sesiones	El número de sesiones en la máquina.	Solo multisesión

Acciones y columnas de sesión

August 17, 2024

En este artículo se enumeran las acciones y las columnas de máquina con descripciones para referencia.

Acciones

Vea las acciones que puede realizar en las sesiones y sus descripciones.

Acción	Descripción	Se aplica a sesiones de
Cerrar sesión	Cierra la sesión de un usuario.	Máquinas con SO de sesión única o máquinas con SO multisesión.

Acción	Descripción	Se aplica a sesiones de
Enviar mensaje	Envía un mensaje al usuario de una sesión.	Máquinas con SO de sesión única o máquinas con SO multisesión.
Ver máquinas	Muestra la máquina host de una sesión.	Máquinas con SO de sesión única o máquinas con SO multisesión.
Desconectar	Desconecta una sesión. Si una sesión se desconecta, la sesión permanece activa y sus aplicaciones siguen ejecutándose, pero el dispositivo de usuario ya no se comunica con los Delivery Controllers.	Máquinas con SO de sesión única o máquinas con SO multisesión.
Apagar máquina	Apaga la máquina asociada a una sesión.	Máquinas con SO de sesión única
Reiniciar máquina	Reinicia la máquina asociada a una sesión.	Máquinas con SO de sesión única

Columnas

Consulte las columnas de la sesión y sus descripciones.

Columna	Descripción
Usuario actual	El nombre del usuario; el nombre principal de usuario (UPN) del usuario.
Nombre	El nombre de host DNS de la máquina que aloja la sesión.
Grupo de entrega	El nombre del grupo de entrega que contiene la máquina que aloja la sesión.
Catálogo de máquinas	El nombre del catálogo de máquinas que contiene la máquina que aloja la sesión.
Versión del agente	La versión del Citrix Virtual Delivery Agent (VDA) instalada en la máquina que aloja la sesión.
Aplicación en uso	La lista de aplicaciones en uso en la sesión, identificadas por sus nombres administrativos.

Columna	Descripción
Con broker autónomo	Si se trata de una sesión HDX establecida mediante una conexión directa sin intermediación con broker.
Hora de broker (UTC)	La hora en la que se intermedió la sesión.
Nombre de usuario de broker	El nombre del usuario broker.
Cliente (IP)	La dirección IP del cliente conectado a la sesión.
Cliente	El nombre de host del cliente conectado a la sesión.
Versión del plug-in	La versión de la aplicación Citrix Workspace que se ejecuta en el cliente conectado a la sesión.
Conectado	El nombre de host de las conexiones entrantes, normalmente una puerta de enlace, un enrutador o un cliente.
Conectado (IP)	La dirección IP de la conexión entrante, normalmente una puerta de enlace, un enrutador o un cliente.
Tipo de asignación	Si la sesión es compartida o dedicada.
Oculto	Si la sesión está oculta para el usuario y no se va a volver a conectar a ella.
VM	El nombre descriptivo de la máquina virtual que aloja la sesión, tal como lo usa su hipervisor. No tiene por qué coincidir necesariamente con el nombre DNS o AD de la máquina.
Nombre del servidor de alojamiento	El nombre DNS del hipervisor que aloja la máquina en la que se ejecuta la sesión.
Conexión	El nombre de la conexión de host asignada a la máquina que aloja la sesión.
Actualización pendiente	Si la imagen de máquina virtual de una máquina hospedada no está actualizada y se actualizará con una nueva imagen en el próximo reinicio de la máquina.
Modo de mantenimiento	Si la máquina que aloja la sesión está en modo de mantenimiento.
Dirección IP	La dirección IP de la máquina que aloja la sesión.

Columna	Descripción
Es físico	Si la máquina que aloja la sesión es física o no. `True` indica que la máquina es física, lo que significa que los Dellivery Controllers no administran la energía. `False` indica lo contrario.
Iniciado	El nombre de host del servidor de StoreFront usado para iniciar la sesión. Está en blanco si la sesión se inició a través de Workspace.
Iniciado (IP)	La dirección IP del servidor de StoreFront usado para iniciar la sesión. Está en blanco si la sesión se inició a través de Workspace.
Tipo de SO	La cadena de identificación del sistema operativo que aloja la sesión.
Persistencia de cambios de usuario	Indica cómo se gestionan los cambios de usuario y si estos cambios son persistentes Local: Persistentes. Los cambios de usuario se guardan localmente. Descartar: No persistentes. Los cambios de usuario se descartan.
Tipo de conexión	El protocolo usado para la sesión, como HDX, RDP o Consola. **Nota:** El campo está en blanco para las sesiones de consola en los VDA de XenDesktop 5.
Tipo de aprovisionamiento	Cómo se aprovisionó la máquina que aloja la sesión Manual: No se aprovisiona mediante PVS o MCS. PVS: Se aprovisiona con PVS (máquinas físicas, blade y virtuales). MCS: Se aprovisiona con MCS (solo máquinas virtuales).
Secure ICA activo	Si SecureICA está activo en la sesión.
Estado de la sesión	El estado de la sesión. Valores posibles: Conectado, Activo o Desconectado. Puede haber otros estados para las sesiones en máquinas con niveles funcionales anteriores a L7, como Preparando sesión, Reconectando, Sesión sin broker, Otro y Desconocido.
Hora de cambio de sesión	La hora del último cambio de estado de la sesión.
Estado de la aplicación	El estado de las aplicaciones de la sesión. Valores posibles: Preinicio de sesión, Preiniciada, Activa, Escritorio, Persistente y NoApps.

Columna	Descripción
Respaldo para la sesión	Si la máquina que aloja la sesión admite sesiones únicas o multisesión.
Zona	Nombre de la zona en la que se encuentra la máquina que aloja la sesión.
Filtros SmartAccess	Etiquetas Smart Access para la sesión.
Inicio (UTC)	Cuándo se inició la sesión.
Estado	El estado resumido de la máquina. Valores posibles: Sin registrar, Desconectada o En uso.
Tiempo en este estado (UTC)	Cuánto tiempo ha estado la sesión en su estado actual.
Delivery Controller	El nombre de host DNS del controlador en el que está registrada la máquina que aloja la sesión.
Nombre simplificado de usuario	El nombre completo del usuario.
Nombre simplificado de escritorio	El nombre publicado de la máquina usada originalmente para iniciar la sesión. Es el nombre que aparece en la aplicación Citrix Workspace o StoreFront. En el caso de las sesiones de aplicación, es el nombre de la primera aplicación que se inició en la sesión, incluso si esa aplicación ha finalizado. El nombre se mantiene sin cambios aunque el recurso cambie de nombre o se elimine más adelante.

Administrar las claves de seguridad

August 17, 2024

> **Importante:**
>
> - Debe utilizar esta función en combinación con StoreFront 1912 LTSR CU2 o una versión posterior.
> - La función Secure XML solo se admite en Citrix ADC y Citrix Gateway 12.1 y versiones posteriores.
>
> **Nota:**

> Puede administrar la implementación de Citrix Virtual Apps and Desktops mediante dos consolas de administración: Web Studio (basada en la web) y Citrix Studio (basada en Windows). Este artículo se refiere únicamente a Web Studio. Para obtener información sobre Citrix Studio, consulte el artículo equivalente en Citrix Virtual Apps and Desktops 7 2212 o versiones anteriores.

Esta función permite especificar que solo las máquinas StoreFront y Citrix Gateway aprobadas se comuniquen con los Delivery Controllers. 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 Web Studio para mostrar los parámetros de las funciones.
2. Configure los parámetros de su sitio.
3. Configure los parámetros de StoreFront.
4. Configure los parámetros de Citrix ADC.

Habilitar Web Studio para mostrar los parámetros de las funciones

De forma predeterminada, los parámetros de las claves de seguridad están ocultos en Web Studio. Para permitir que Web Studio los muestre, utilice el SDK de PowerShell de esta manera:

1. Ejecute el SDK de PowerShell 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_SecurityKeyManageme "-Value "True"`

Para obtener más información sobre el SDK de PowerShell, consulte SDK y API.

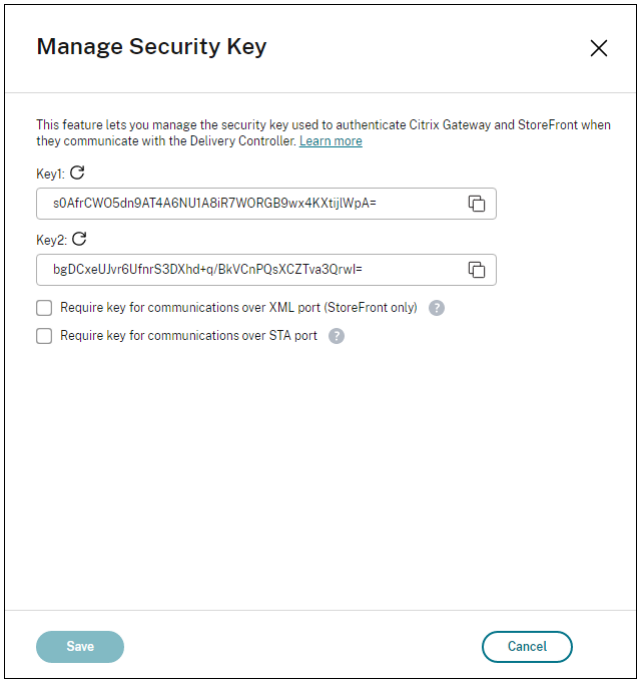
Configurar los parámetros del sitio

Puede usar Web Studio o PowerShell para configurar los parámetros de las claves de seguridad de su sitio.

Usar Web Studio

1. Inicie sesión en Web Studio y seleccione **Parámetros** en el panel de la izquierda.

2. Busque el mosaico **Administrar clave de seguridad** y haga clic en **Modificar**. Aparecerá la página **Administrar clave de seguridad**.



3. Haga clic en el icono de actualización para generar las claves.

> **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.

4. Seleccione dónde se necesita una clave para las comunicaciones:

   - **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.

5. Haga clic en **Guardar** para aplicar los cambios y cerrar la ventana.

Usar PowerShell

Estos son los pasos en PowerShell equivalentes a las operaciones en Web 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 parámetros de StoreFront

Una vez completada la configuración de su sitio, debe configurar los parámetros relevantes de 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 [Set-STFStoreFarm	https://developer-docs.citrix.com/en-us/storefront-powershell-sdk/current-release/Set-STFStoreFarm.html]. Por ejemplo

```
$store = Get-STFStoreService -VirtualPath [Path to store]
$farm = Get-STFStoreFarm -StoreService $store -FarmName [Resource feed
    name]
Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true -
    XMLValidationSecret [secret]
```


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:

```
$gateway = Get-STFRoamingGateway -Name [Gateway name]
$sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL] -
    StaValidationEnabled $true -StaValidationSecret [secret]
$sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL] -
    StaValidationEnabled $true -StaValidationSecret [secret]
Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
    $sta1,$sta2
```

Introduzca los valores adecuados para los siguientes parámetros:

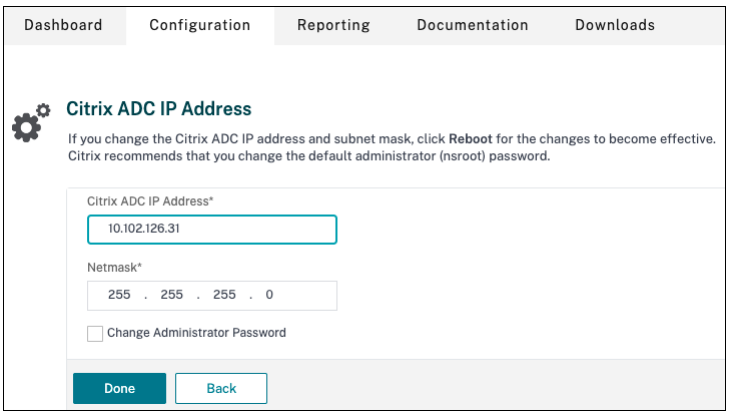
- `Gateway name`
- `STA URL`
- `Secret`

Consulte la ayuda de los comandos de PowerShell para ver instrucciones y sintaxis.

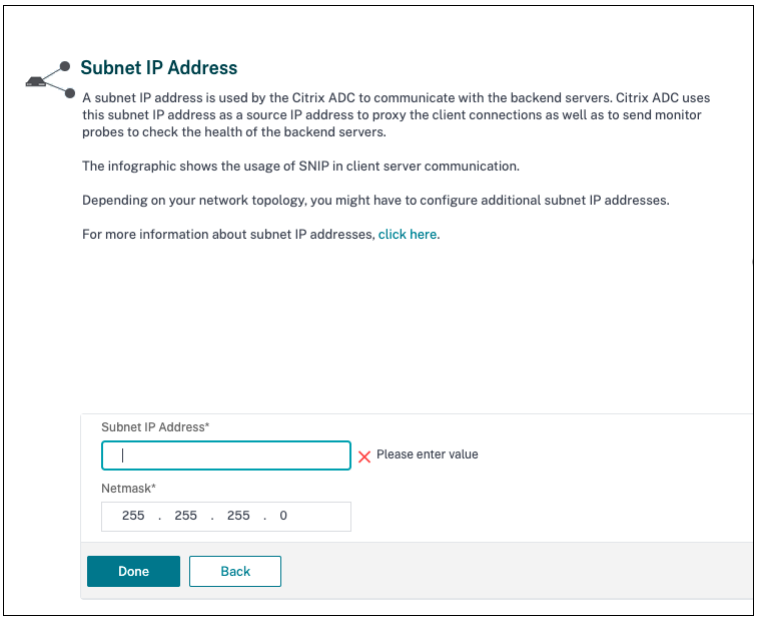
Configurar parámetros de Citrix ADC

> **Nota:**
>
> No es necesario configurar esta función para Citrix ADC, a no ser que utilice Citrix ADC como puerta de enlace. Si usa Citrix ADC, siga estos pasos:

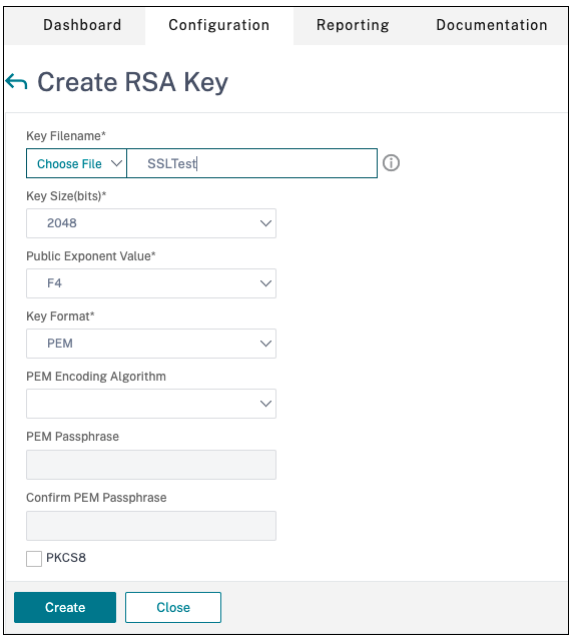
1. Asegúrese de que ya está implementada la siguiente configuración de requisitos previos:
    - Se configuran las siguientes direcciones IP relacionadas con Citrix ADC.
        - Dirección IP de administración (NSIP) de Citrix ADC para acceder a la consola de Citrix ADC. Para obtener más información, consulte Configurar la dirección IP de NetScaler.



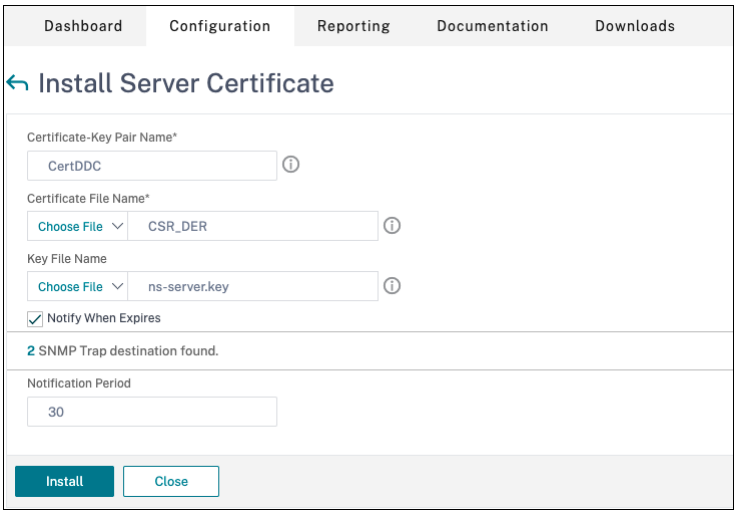
  - Dirección IP de subred (SNIP) para permitir la comunicación entre el dispositivo Citrix ADC y los servidores back-end. Para obtener más información, consulte Configurar direcciones IP de subred.
  - Dirección IP virtual de Citrix Gateway y dirección IP virtual del equilibrador de carga para iniciar sesión en el dispositivo ADC para el lanzamiento de sesiones. Para obtener más información, consulte Crear un servidor virtual.

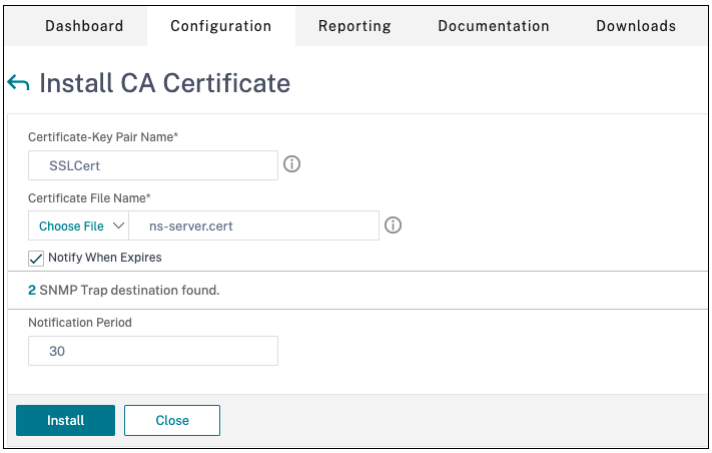


- Los modos y las funciones requeridos en el dispositivo Citrix ADC están habilitados.
  - Para habilitar los modos, en la GUI de Citrix ADC vaya a **System > Settings > Configure Mode**.
  - Para habilitar las funciones, en la GUI de Citrix ADC vaya a **System > Settings > Configure Basic Features**.
- 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.

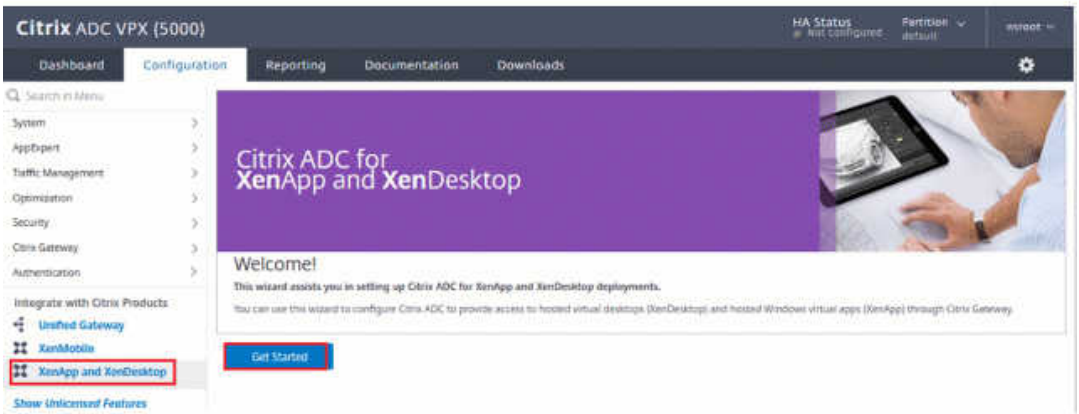


- Los certificados de CA y del servidor y los certificados raíz están instalados. Para obtener más información, consulte Instalación, enlace y actualizaciones.





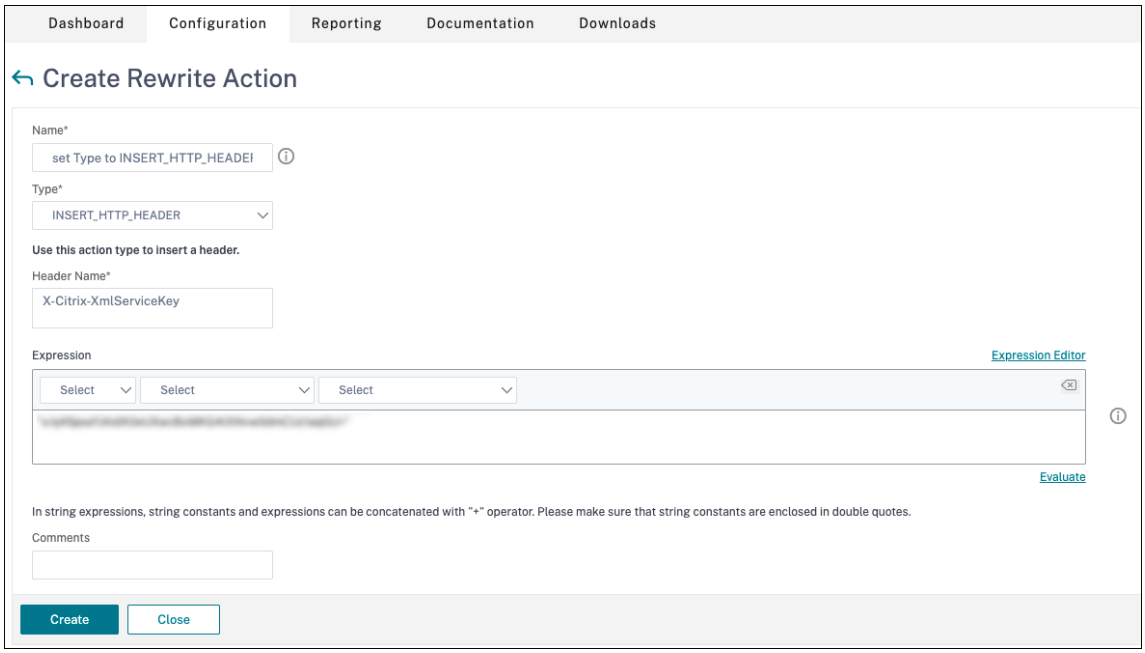
- Se ha creado una conexión de Citrix Gateway para Citrix Virtual Desktops. Pruebe la conectividad. Para ello, haga clic en el botón **Test STA Connectivity** para confirmar que los servidores virtuales están conectados. Para obtener más información, consulte Configurar Citrix ADC para Citrix Virtual Apps and Desktops.



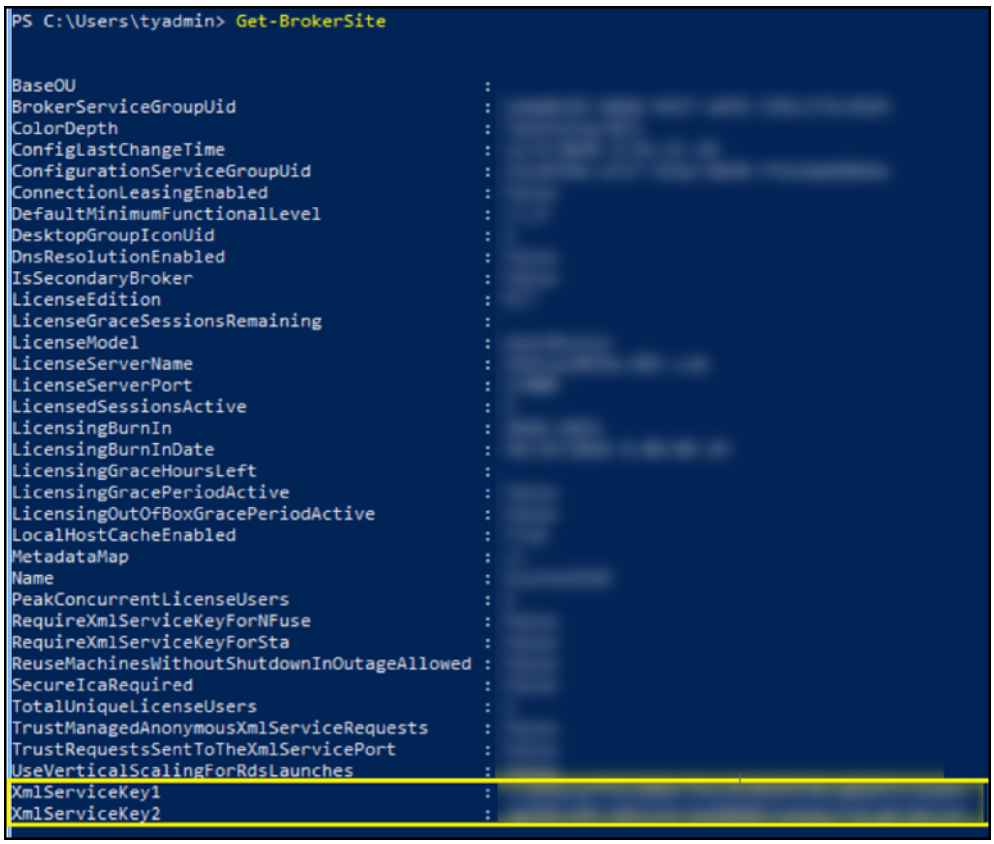
2. Agregue una acción de reescritura. Para obtener más información, consulte Configurar una acción de reescritura.

   a) Vaya a **AppExpert > Reescribir > Acciones**.

   b) Haga clic en **Add** para agregar una nueva acción. Puede asignar a la acción el nombre "set Type to INSERT_HTTP_HEADER".

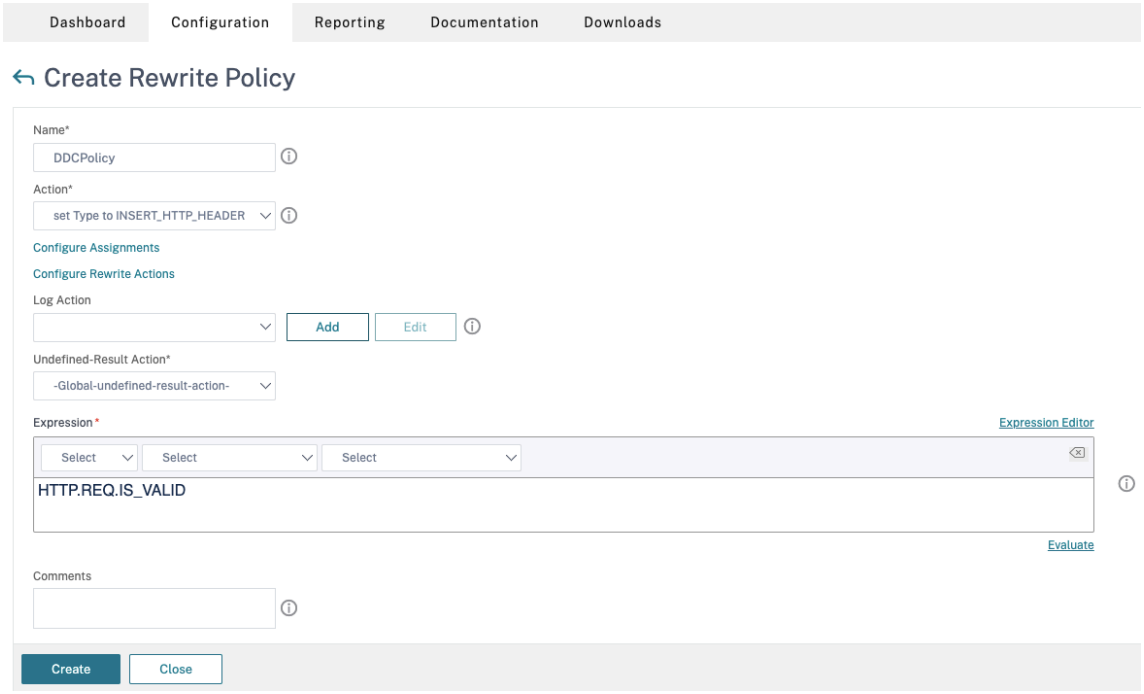


a) En **Type**, seleccione **INSERT_HTTP_HEADER**.
b) En **Header Name**, escriba X-Citrix-XmlServiceKey.
c) En **Expression**, agregue <XmlServiceKey1 value> con las comillas. Puede copiar el valor XmlServiceKey1 desde la configuración de Desktop Delivery Controller.



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 **Add** para agregar una nueva directiva.



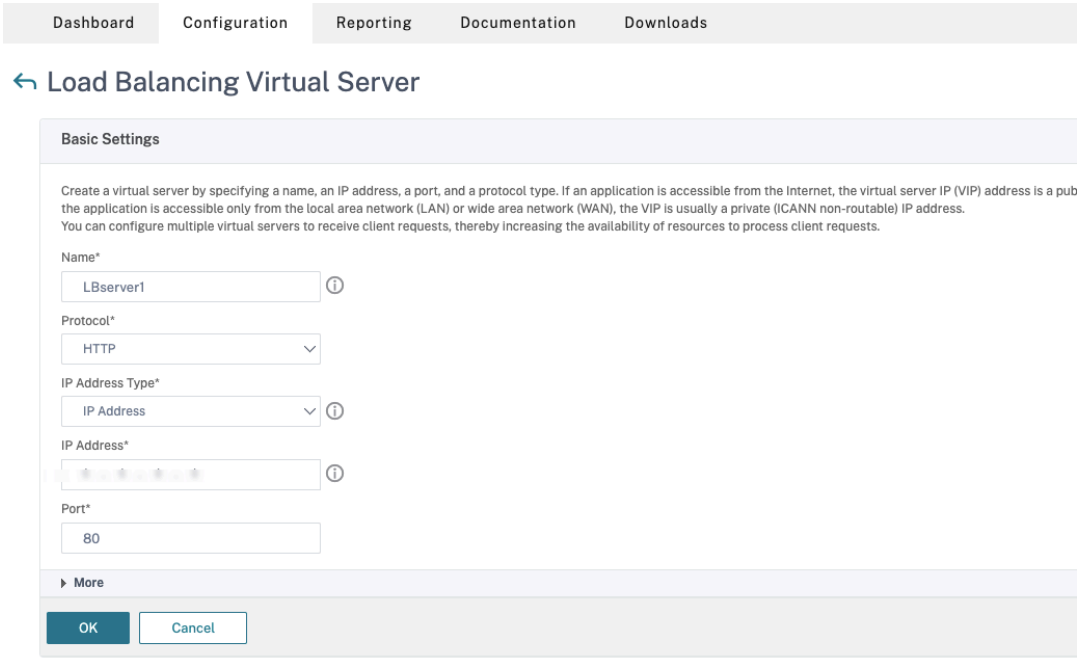
a) En **Action**, seleccione la acción creada en el paso anterior.
b) En **Expression**, agregue HTTP.REQ.IS_VALID.
c) Haga clic en **Aceptar**.

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.

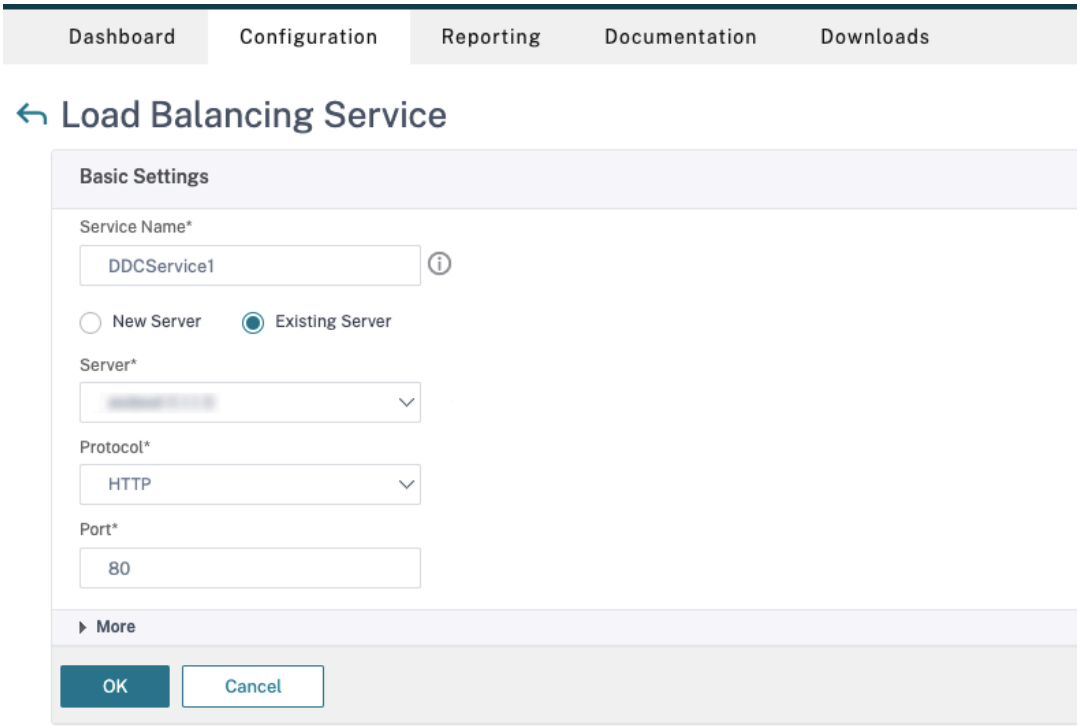
      - Vaya a **Traffic Management > Load Balancing > Servers**.
      - En la página **Virtual Servers**, haga clic en **Add**.



- 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.

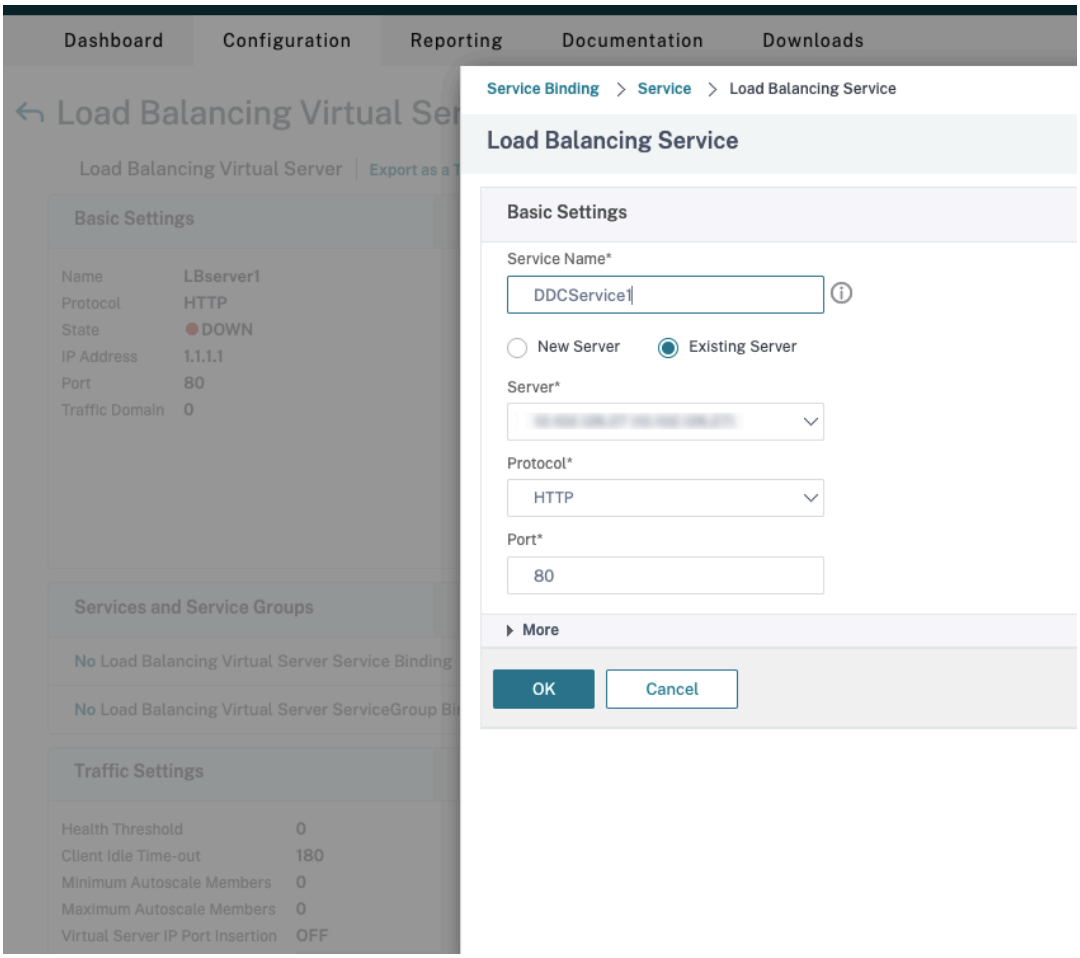
- Vaya a **Traffic Management > Load Balancing > Services**.



- 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.

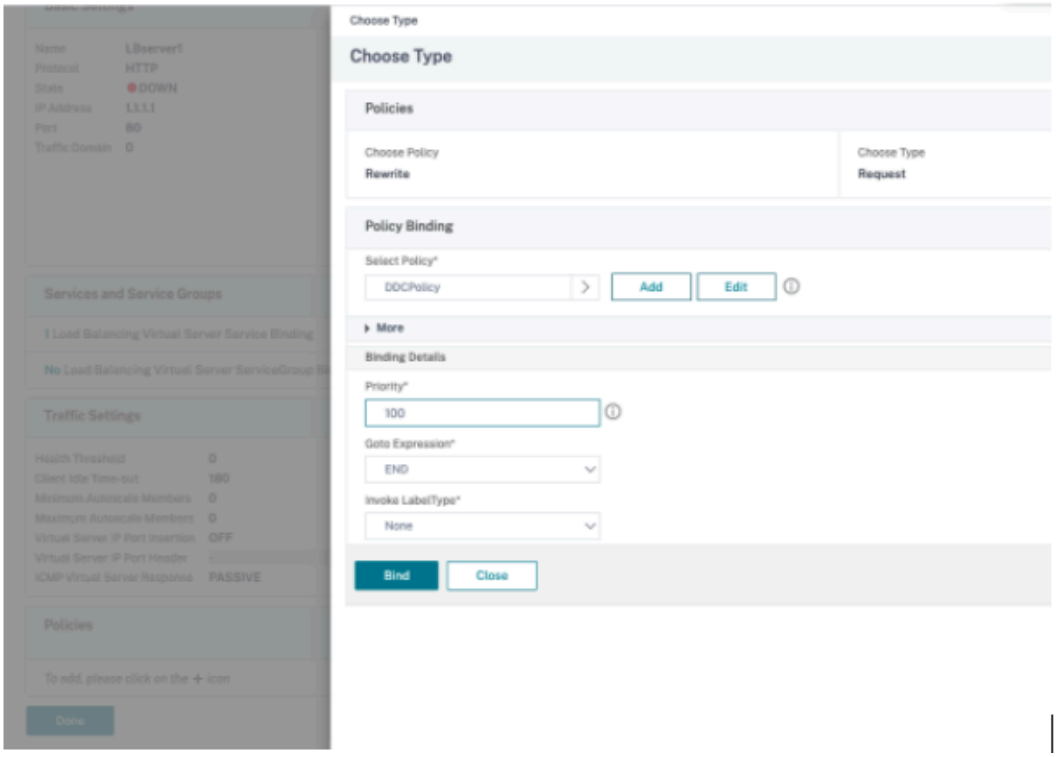
- Seleccione el servidor virtual creado anteriormente y haga clic en **Edit**.
- En **Services and Service Groups**, haga clic en **No Load Balancing Virtual Server Service Binding**.



- En **Service Binding**, seleccione el servicio creado anteriormente.
- Haga clic en **Bind**.

d) Vincule la directiva de reescritura creada anteriormente al servidor virtual.

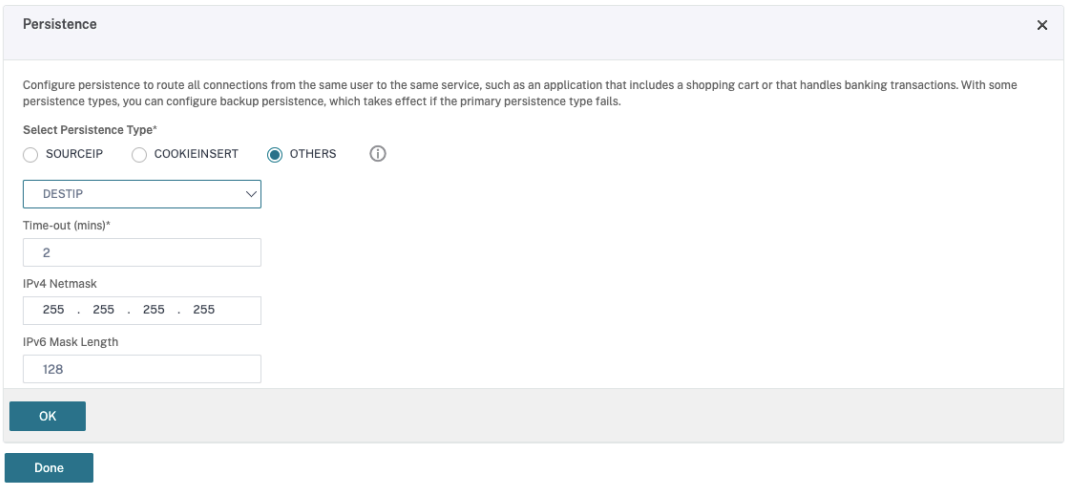
- Seleccione el servidor virtual creado anteriormente y haga clic en **Edit**.
- En **Advanced Settings**, haga clic en **Policies,** y, a continuación, en la sección **Policies** haga clic en **+**.



- 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**.

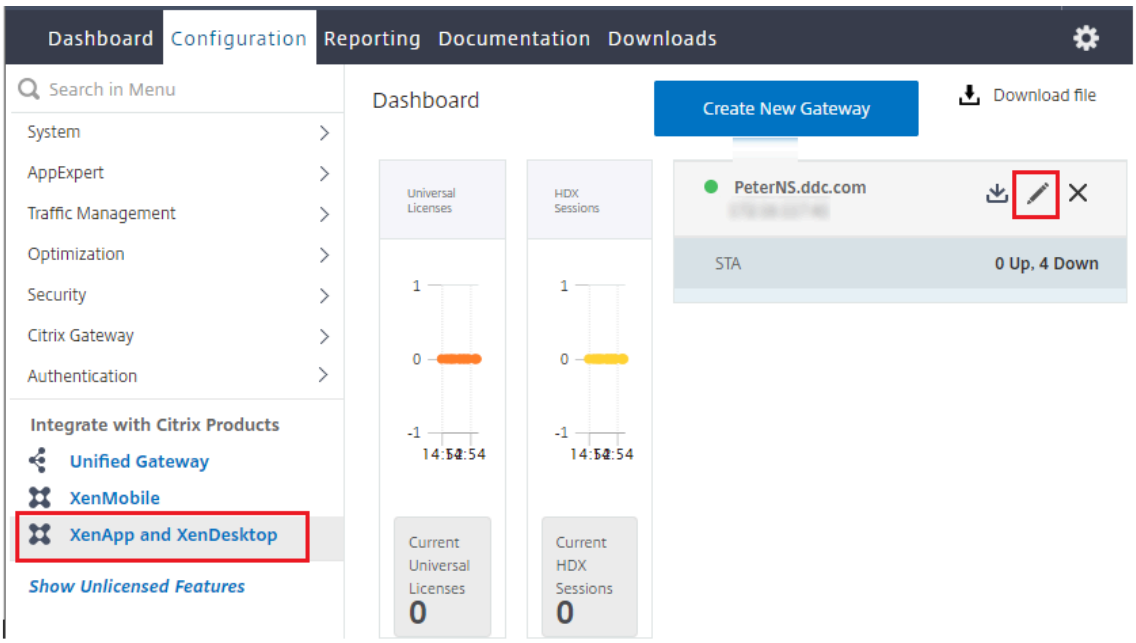
f) Repita estos pasos para el otro servidor virtual.

La configuración cambia si el dispositivo Citrix ADC ya está configurado con Citrix Virtual Desktops

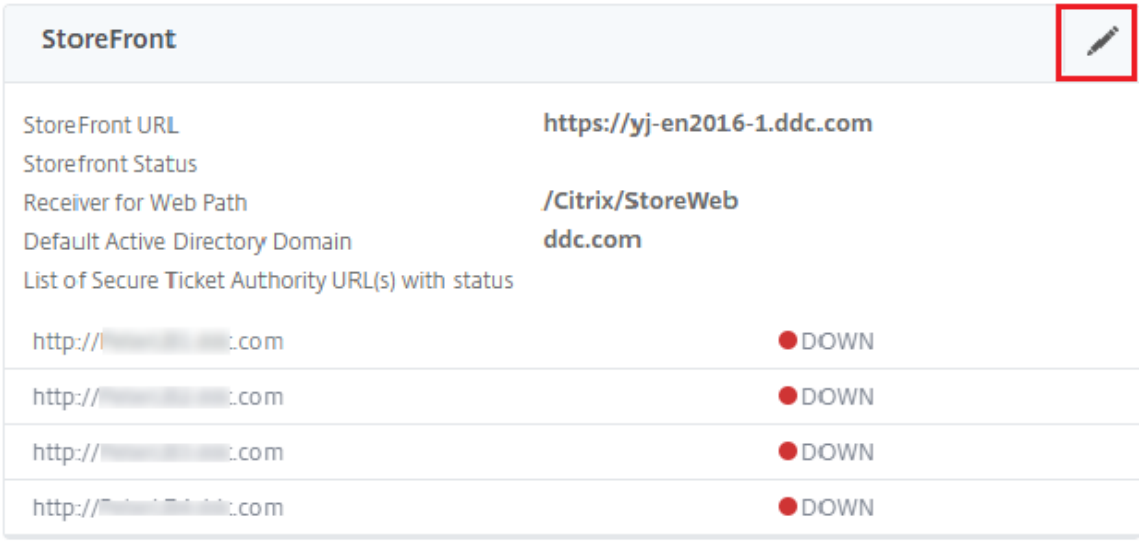
Si ya ha configurado el dispositivo Citrix ADC con Citrix Virtual Desktops, para utilizar la funcionalidad Secure XML, debe realizar los siguientes cambios de configuración.

- 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.

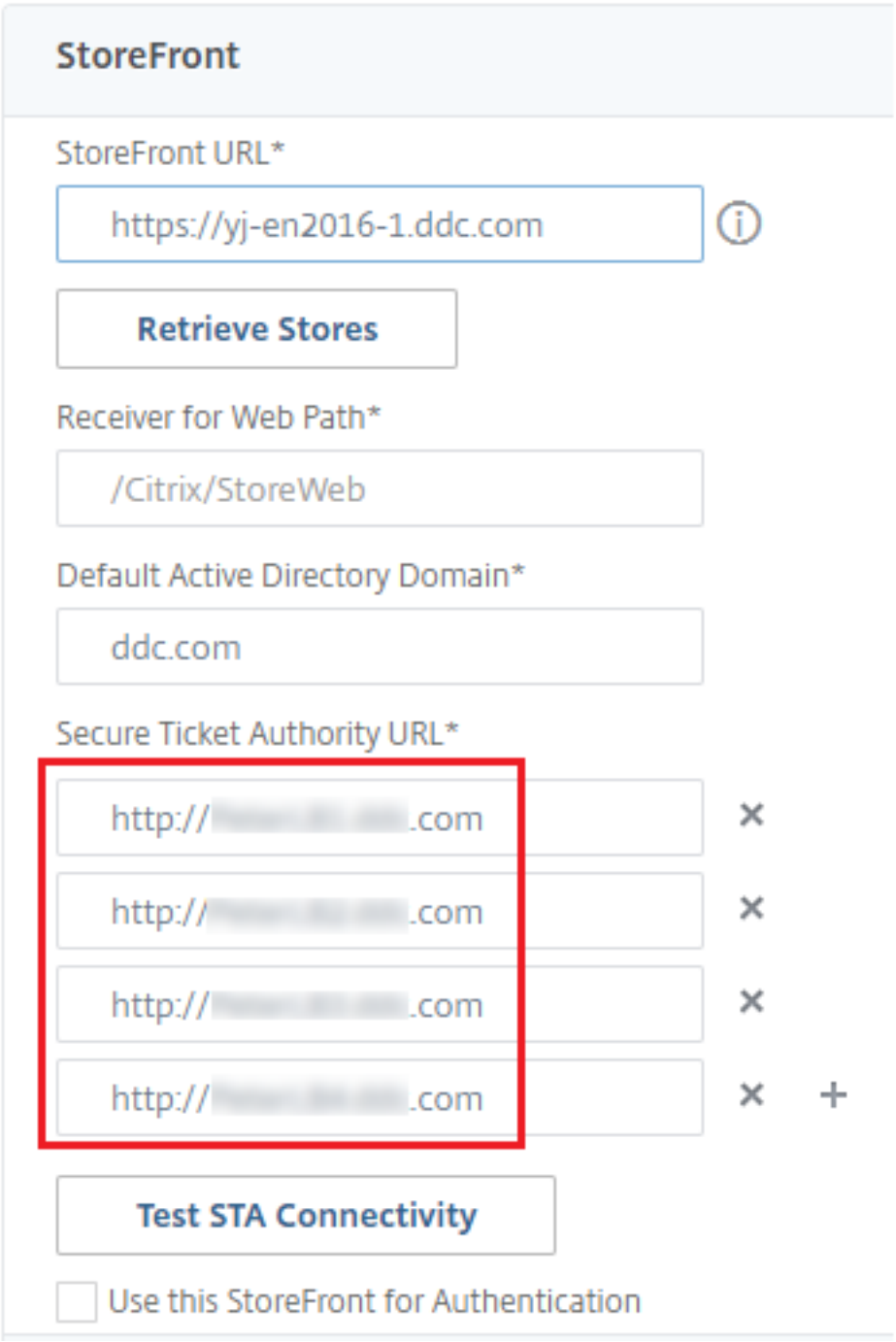


3. En el panel StoreFront, haga clic en el icono de modificación.



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 `TrustRequestsSentToTheXmlServiceP` del Desktop Delivery Controller debe establecerse en True.



Parámetros de resistencia de las sesiones

August 17, 2024

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 un dispositivo a otro 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 trabajadores del sector de la salud.

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.

Fiabilidad de la sesión

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.

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 conectarse de nuevo. Con la función Fiabilidad de la sesión, la sesión permanece activa en la máquina. Para indicar la pérdida de 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 predeterminado de 180 segundos, o tres minutos. Aunque puede ampliar el tiempo en que la fiabilidad de la sesión mantiene abierta una sesión, esta función está diseñada para mayor comodidad del usuario. Por lo tanto, no pide al usuario que vuelva a autenticarse. A medida que prolonga el tiempo que una sesión se mantiene abierta, aumentan las probabilidades de que un usuario se distraiga y se aleje de su dispositivo. Estas acciones pueden dejar la sesión accesible para usuarios no autorizados.

- 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.
- Para evitar que los usuarios reconecten con sesiones interrumpidas sin tener que repetir la autenticación, utilice 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 trascurrido 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, modifique el siguiente parámetro del Registro en el dispositivo de usuario (donde `seconds` es la cantidad de segundos después de los que no hay más intentos para volver a conectarse a la sesión).

```
HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds
; DWORD;<seconds>
```

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 prede-

terminada. 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 que han tenido lugar en todos los servidores.

> **Nota:**
>
> La reconexión automática de clientes sin reautenticación solo se admite para la autenticación por contraseña. Si usa el Servicio de autenticación federada o la autenticación con tarjetas inteligentes, no se admite la reconexión automática de clientes sin reautenticación. En estos casos, se redirige a los usuarios a la pantalla de inicio de sesión.

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. Además, el servidor 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 describió 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. Cuando una sesión se restablece, los intentos de reconexión inician una nueva sesión. No obstante, en lugar de restaurar al usuario a la posición en que se encontraba en la aplicación en uso, 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 está habilitada, si el servidor no detecta ninguna actividad, esta funcionalidad impide que Servicios de Escritorio remoto desconecten esa sesión. Ejemplos de ninguna actividad incluyen ningún cambio en el reloj, ningún movimiento del puntero ni actualizaciones de pantalla. 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 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, además de 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 deben 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, 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: un trabajador sanitario cierra sesión en un dispositivo ubicado en la sala de emergencias y, a continuación, inicia sesión en una estación de trabajo del laboratorio de rayos X. Las directivas, las asignaciones de impresoras y las asignaciones de unidades de cliente correspondientes de la sesión en el laboratorio de rayos X entran en vigor al iniciarse la 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

> **Nota:**
>
> Esta información le guía para configurar la itinerancia de sesiones mediante PowerShell. En su lugar, puede utilizar Web Studio. Para obtener más información, consulte Administrar grupos de entrega.

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. A menudo, 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.

- Cuando 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.
- Cuando 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 uno de los siguientes valores:

- **Always:** Las sesiones siempre se mueven, independientemente del dispositivo cliente y si la sesión está conectada o desconectada. Este es el valor predeterminado.
- **DisconnectedOnly:** Reconectarse 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. Microsoft controla el tiempo de espera de inicio de sesión en las máquinas con servidores VDA.

Parámetros

August 17, 2024

> **Nota:**
>
> Puede administrar la implementación de Citrix Virtual Apps and Desktops mediante dos consolas de administración: Web Studio (basada en la web) y Citrix Studio (basada en Windows). Este artículo se refiere únicamente a Web Studio. Para obtener información sobre Citrix Studio, consulte el artículo equivalente en Citrix Virtual Apps and Desktops 7 2212 o versiones anteriores.

Puede usar Web Studio para administrar estos parámetros:

- Administrar la autenticación
- Customer Experience Improvement Program (CEIP) de Citrix
- Quitar Delivery Controllers
- Cambiar la base de datos de registros
- Establecer fecha y hora
- Centralizar la administración de sitios
- Habilitar la asignación automática de varios usuarios para el acceso con Remote PC
- Habilitar resolución de DNS
- Habilitar la confianza en XML
- Administrar clave de seguridad
- Configurar el tiempo de espera por inactividad para la consola de Studio

Administrar la autenticación

De forma predeterminada, los usuarios inician sesión en Web Studio con su nombre de usuario y contraseña de dominio. También puede elegir un método de autenticación diferente para los usuarios, como la autenticación con tarjeta inteligente o la autenticación de Windows integrada.

Para elegir un método de autenticación para los usuarios, siga estos pasos:

1. Inicie sesión en Web Studio y seleccione Parámetros en el panel de la izquierda.
2. Busque el mosaico Autenticación y haga clic en Modificar para seleccionar una opción:
    - Credenciales de dominio
    - Credenciales de dominio o autenticación de Windows integrada

      Con la autenticación de Windows integrada habilitada, los usuarios pueden acceder a Web Studio con sus credenciales de Windows (Kerberos/NTLM) o un certificado de cliente.

Cuando Web Studio y el Delivery Controller estén instalados en máquinas diferentes, para que funcione la autenticación de Windows integrada, habilite Permitir el acceso entre orígenes y agregue la URL del servidor de Web Studio a la lista de permitidos.

> **Importante**
>
> La autenticación de Windows integrada no funciona cuando Web Studio está configurado como proxy para los Delivery Controllers.

- Autenticación con tarjeta inteligente.
- Credenciales de dominio o autenticación con tarjeta inteligente

  Habilitar la autenticación con tarjeta inteligente requiere una configuración adicional. Para obtener más información, consulte Configurar la autenticación con tarjeta inteligente para Web Studio.

Tras habilitar la opción **Autenticación de Windows integrada**, la próxima vez que los usuarios inicien sesión, iniciarán sesión automáticamente. Como usuario, si no puede iniciar sesión automáticamente, siga estos pasos para configurar su explorador web para permitir la autenticación de Windows integrada.

Para Google Chrome:

1. En el Panel de control, seleccione Opciones de Internet.
2. Seleccione la ficha **Avanzado**.
3. Seleccione **Habilitar la autenticación de Windows integrada**.
4. Seleccione la ficha **Seguridad**.
5. Seleccione **Intranet local > Sitios > Avanzado**.
6. En el cuadro **Agregar este sitio web a la zona**:
   - Si Web Studio y el Delivery Controller residen en el mismo servidor, escriba la URL del host que ejecuta Web Studio.
   - Si no, escriba un dominio comodín. Ejemplo: Si el Delivery Controller está en `ddc.domain.com`, escriba `*.domain.com`.
7. Haga clic en **Agregar > Cerrar**.

Para Mozilla Firefox:

1. Desde el explorador web, escriba `about:config` en el cuadro de URL.
2. En el cuadro **Buscar**, escriba `network negotiate`.
3. Haga clic con el botón secundario en **network.negotiate-auth.trusted-uris** y seleccione **Modificar**.

4. En el cuadro **Introduzca el valor de la cadena**:

    - Si Web Studio y el Delivery Controller residen en el mismo servidor, agregue una lista de direcciones URL o alias separados por comas que hagan referencia al nombre del servidor que aloja Web Studio.
    - Si no, agregue las direcciones URL de esta manera. Ejemplo: Si el Delivery Controller está en `ddc.domain.com`, escriba `*.domain.com`.

Después de configurar el explorador web, puede hacer clic en **Inicio de sesión integrado de Windows** en la página de inicio de sesión para intentarlo de nuevo.

Si Web Studio y el Delivery Controller están instalados en máquinas diferentes, para que funcione la autenticación de Windows integrada, debe habilitar **Permitir el acceso entre orígenes**.

Sigue estos pasos para habilitar **Permitir el acceso entre orígenes**:

1. Marque la casilla **Permitir el acceso entre orígenes**.
2. Agregue la URL del servidor de Web Studio a la lista de permitidos.
3. En el campo **Introduzca la URL**, introduzca la URL. Haga clic en **Agregar** para agregar más si es necesario.

    > **Nota**
    >
    > - La URL debe tener el formato correcto:`<scheme>://<hostname>`. Asegúrese de no incluir rutas ni barras diagonales al final.
    > - Se admiten direcciones IP y FQDN. Al agregar una URL, esta debe corresponder a la forma en que accede a Web Studio. Por ejemplo, si accede a Web Studio con una dirección IP, agregue la URL basada en direcciones IP a la lista.
    > - Si utiliza un puerto que no es el predeterminado, asegúrese de incluir el número de puerto.

4. Haga clic en **Agregar** para agregar más si es necesario.
5. Cuando haya terminado, haga clic en **Listo** para guardar y salir.

Configurar la zona horaria

Para personalizar el formato de fecha y hora según sus preferencias, siga estos pasos:

1. Inicie sesión en Web Studio y seleccione **Parámetros** en el panel de la izquierda.
2. Busque el mosaico **Fecha y hora** y haga clic en **Modificar** para configurar estas opciones:

    - **Formato de hora:**

  - Seleccione esta opción para mostrar la hora con un reloj de 12 horas (por ejemplo, las 09:00 p. m.) o un reloj de 24 horas (por ejemplo, las 21:00).

- **Formato de fecha:**
  - Configure el formato de fecha para que coincida con sus preferencias, como aaaa/M-M/dd.
- **Zona horaria:**
  - **UTC:** Muestra la fecha y la hora en UTC en toda la interfaz de usuario. Al pasar el mouse por encima de la fecha y la hora, se muestra esa información en la zona horaria local.
  - **Zona horaria local:** Muestra la fecha y la hora en su zona horaria local en toda la interfaz de usuario. Al pasar el mouse por encima de la fecha y la hora, se muestra esa información en UTC.

> **Nota:**
>
> Estos parámetros son específicos de cada cuenta de usuario.

Habilitar resolución de DNS

Para presentar nombres de DNS en lugar de direcciones IP en el archivo ICA, siga estos pasos:

1. Inicie sesión en Web Studio y seleccione **Parámetros** en el panel de la izquierda.
2. Active el parámetro **Habilitar resolución de DNS**.

Configurar el tiempo de espera por inactividad para la consola de Studio

Puede establecer la duración de la inactividad tras la cual se cierra automáticamente la sesión de los administradores en la consola de Studio.

1. Inicie sesión en Web Studio y seleccione **Parámetros** en el panel de la izquierda.
2. Escriba una duración que oscile entre 10 minutos y 24 horas.
3. Para aplicar este parámetro, actualice la página o cierre sesión y, a continuación, inicie sesión de nuevo.

Centralizar la administración de sitios

Esta función permite usar una consola de Web Studio para administrar varios sitios de Citrix Virtual Apps and Desktops. Para obtener más información, consulte Habilitar la administración de varios sitios.

Etiquetas

August 17, 2024

> **Nota:**
>
> Puede administrar la implementación de Citrix Virtual Apps and Desktops mediante dos consolas de administración: Web Studio (basada en la web) y Citrix Studio (basada en Windows). Este artículo se refiere únicamente a Web Studio. Para obtener información sobre Citrix Studio, consulte el artículo equivalente en Citrix Virtual Apps and Desktops 7 2212 o versiones anteriores.

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 Web 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 Web 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 por etiquetas 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 por etiquetas 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 por etiquetas 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 un subconjunto de las 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** del asistente para la creación de directivas, seleccione la etiqueta y marque 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 Web Studio:

- Un escritorio en un grupo de entrega compartido
- Un grupo de aplicaciones

Restricciones por etiquetas para un grupo de escritorios o aplicaciones

Una restricción por etiquetas implica varios pasos:

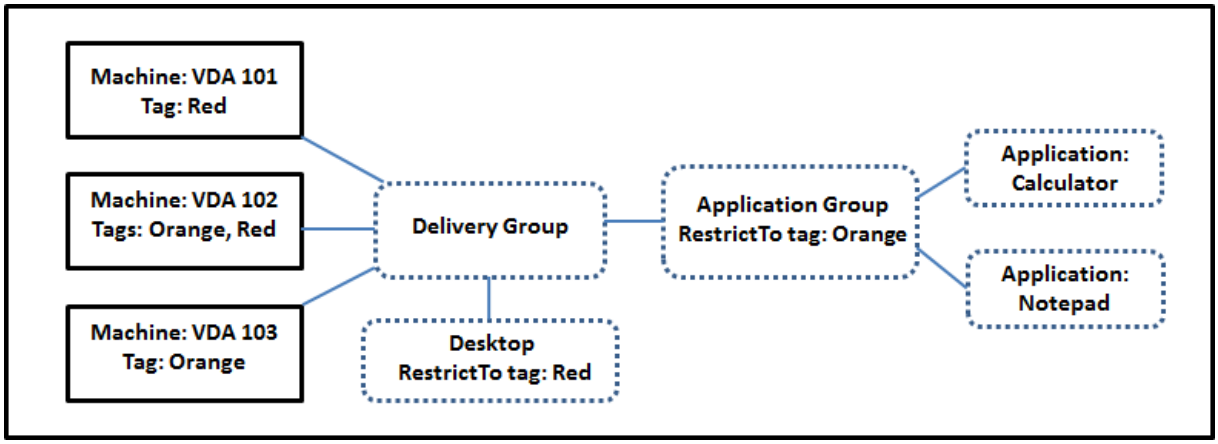
- Crear la etiqueta y, a continuación, agregarla (aplicarla) a las máquinas.
- Crear o modificar un grupo con la restricción de etiqueta (en otras palabras, "restringir inicios a máquinas con la etiqueta x").

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.



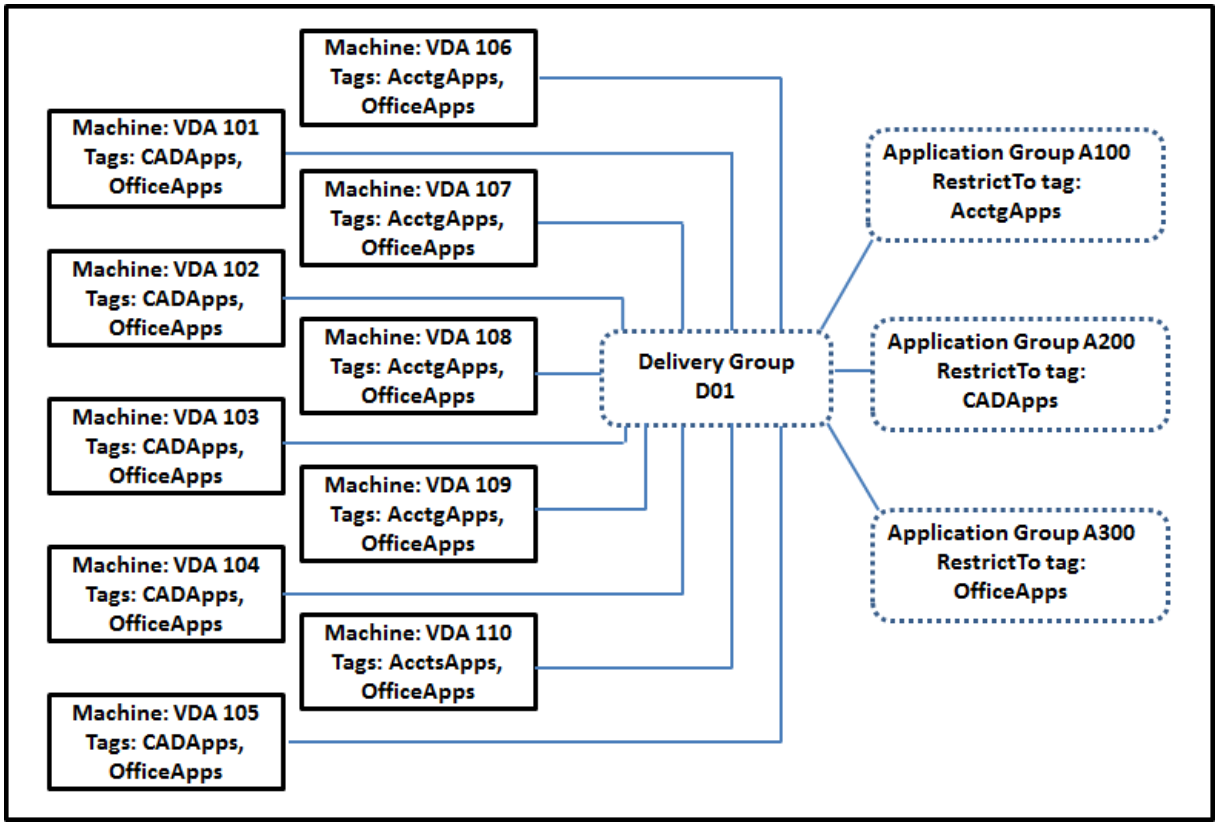
- Se han agregado etiquetas a cada una de las tres máquinas (VDA 101, 102 y 103).
- El escritorio del grupo de entrega compartido se creó con una restricción de etiqueta llamada "Rojo". Un escritorio solo puede iniciarse en máquinas de ese grupo de entrega que tengan la etiqueta "Rojo": VDA 101 y 102.
- El grupo de aplicaciones se creó con la restricción por etiquetas "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.

La máquina VDA 102 tiene ambas etiquetas (Rojo y Naranja); 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 por 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 (agentes VDA de 101 a 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 por 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 Web 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 Web Studio. Sin embargo, las etiquetas

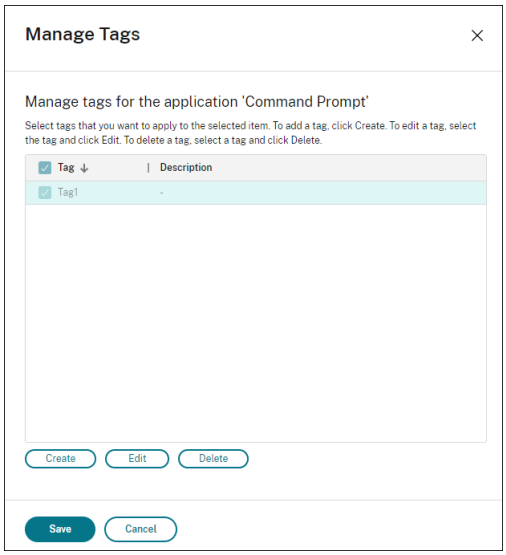
se aplican (se asignan) en el momento de crear la directiva. Consulte Crear directivas para obtener información detallada).

Las restricciones por 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 Web Studio

En Web Studio, seleccione los elementos a los que quiere aplicar una etiqueta (una o varias máquinas o aplicaciones, un escritorio, un grupo de entrega o un grupo de aplicaciones) y, a continuación, seleccione **Administrar etiquetas** en la barra de acciones. Este cuadro de diálogo 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 máquina seleccionada tiene aplicada la etiqueta llamada "Tag1".)
- 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**. Asegúrese de revisar 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 una o varias máquinas y resulta que esa etiqueta se usa como una restricción en un grupo de aplicaciones, se le advertirá de que la acción puede provocar que esas máquinas estén disponibles para el inicio. Si es lo que pretende, continúe.

- **Para quitar una o varias etiquetas:**

  Desmarque la casilla de verificación situada junto al nombre de la etiqueta. Si marcó varios elementos y la casilla de verificación ubicada junto a una etiqueta contiene un guión (para indicar que algunos pero no todos los elementos seleccionados ya tienen aplicada la etiqueta), desmarcar la casilla quitará la etiqueta de todas las máquinas seleccionadas.

  Si intenta quitar una etiqueta desde una máquina que la utiliza como una restricción, se le advertirá de que su acción podría afectar a las máquinas que se tienen en cuenta para el inicio. Si es lo que pretende, 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 Web Studio para eliminar una etiqueta que se usa como una restricción. Primero, debe modificar el grupo de aplicaciones y quitar la restricción por etiquetas 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 la izquierda. Seleccione un grupo de entrega en el panel central y, a continuación, seleccione **Ver máquinas** en la barra de 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 por etiquetas es un proceso de varios pasos: Primero, debe crear la etiqueta y agregar 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 por etiquetas 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 por etiquetas de un grupo de aplicaciones:**

  Modifique el grupo. En la página **Grupos de entrega**, seleccione otra etiqueta en la lista o quite la restricción por etiquetas 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 por etiquetas 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 las listas 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 Web Studio. Puede utilizar la misma etiqueta como restricción al configurar un grupo de aplicaciones o un escritorio. La etiqueta 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 después de que la etiqueta se haya configurado como una restricción de etiqueta para un escritorio o un grupo de aplicaciones, aparecerá 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, puede cancelar la operación.

Por ejemplo: supongamos que crea un grupo de aplicaciones con la restricción de etiqueta "Rojo". Posteriormente, agrega otras máquinas a los mismos grupos de entrega que utiliza ese grupo de aplicaciones. Si, a continuación, intenta agregar la etiqueta "Rojo"a esas máquinas, Web Studio muestra un mensaje similar a: "La etiqueta 'Rojo'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 un grupo de aplicaciones utiliza una etiqueta para restringir inicios, Web Studio le advierte que no puede eliminar la etiqueta hasta modifique el grupo para quitarla como restricción. (Si pudiera eliminar una etiqueta que se usa como una restricción en un grupo de aplicaciones, eso 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 por etiquetas, 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 por etiquetas diferente y conjuntos de máquinas diferentes o iguales de los grupos de entrega. En la tabla siguiente, se ofrece una lista de cómo se tienen en cuenta las máquinas.

Cuando una aplicación se ha agregado a	Estas máquinas de los grupos de entrega seleccionados se tienen en cuenta para el inicio
Un grupo de aplicaciones sin restricción por etiquetas	Cualquier máquina
Un grupo de aplicaciones con una restricción por etiquetas A	Máquinas que tienen aplicada la etiqueta A
Dos grupos de aplicaciones: uno con una restricción por etiquetas A y otro con una restricción por etiquetas 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 por etiquetas A y otro sin restricción por etiquetas	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 este 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 Web Studio, seleccione el grupo de entrega D01 y, a continuación, seleccione **Ver máquinas** en la barra de acciones.
2. Seleccione las máquinas VDA de la 101 a la 105 y, a continuación, seleccione **Administrar etiquetas** en la barra de acciones.
3. En el cuadro de diálogo Administrar etiquetas, haga clic en **Crear** y, a continuación, cree una etiqueta llamada `CADApps`. Haga clic en **Aceptar**.
4. Haga clic de nuevo en **Crear** y cree una etiqueta llamada "OfficeApps". Haga clic en **Aceptar**.
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`). Cuando haya terminado, cierre el cuadro de diálogo.
6. Seleccione el grupo de entrega D01 y, a continuación, seleccione **Ver máquinas** en la barra de acciones.
7. Seleccione las máquinas VDA de la 106 a la 110 y, a continuación, seleccione **Administrar etiquetas** en la barra de acciones.
8. En el cuadro de diálogo **Administrar etiquetas**, haga clic en **Crear**. Cree una etiqueta llamada `AcctgApps`. Haga clic en **Aceptar**.
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 y, a continuación, cierre el cuadro de diálogo.

Cree los grupos de aplicaciones con restricciones por etiqueta.

1. En Web Studio, seleccione **Aplicaciones** en el panel de la izquierda, seleccione la ficha **Grupos de aplicaciones** y, a continuación, seleccione **Crear grupo de aplicaciones** en la barra de acciones. Se iniciará el asistente Crear grupo de aplicaciones.
2. En la página **Grupos de entrega** del asistente, seleccione el grupo de entrega D01. Seleccione la opción **Restringir inicios a máquinas con la etiqueta** y, 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 Web Studio para aplicar ni quitar etiquetas de catálogos. Las pantallas de los catálogos en Web Studio no indican si se han aplicado etiquetas.

Resumen: Puede utilizar Web 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 Web Studio o PowerShell).

Consulte la ayuda de los cmdlets de PowerShell para obtener más instrucciones y ver la sintaxis.

Etiquetas automáticas (Technical Preview)

El etiquetado automático permite a los administradores establecer etiquetas en varios objetos de Citrix Virtual Apps and Desktops automáticamente, o quitarlas, conforme a reglas personalizadas. Esta

mejora elimina la necesidad de mantener diferentes scripts que se ejecutan periódicamente para optimizar el entorno.

Casos de uso

Con el etiquetado automático, puede implementar reglas conforme a sus prioridades empresariales clave, como reducir los costes, optimizar la infraestructura e impulsar el consumo. A continuación, se indican algunos casos de uso:

- **Recuperar VDI no utilizados**: Para liberar las cargas de trabajo dedicadas que no se han utilizado durante más de un número de días preconfigurado.
- **Eliminar el desorden de aplicaciones**: Para reducir el desorden mediante la identificación de las aplicaciones que no se han utilizado durante más de un número de días preconfigurado.
- **Grupos de entrega con un nivel funcional inferior a X**: Para encontrar grupos de entrega con un nivel funcional inferior a uno específico.
- **Usuarios inactivos**: Para obtener los recursos de los usuarios que no han iniciado sesión durante más de un número de días preconfigurado.

Comandos de PowerShell

Puede crear etiquetas automáticas con los comandos de PowerShell. Una vez creada una regla de etiquetado automático, se evalúa con una frecuencia de 600 segundos. Para obtener más información, consulte New-BrokerAutoTagRule.

Ejemplos `New-BrokerAutoTagRule` utiliza el mismo tipo de objeto y los mismos parámetros de filtro que el cmdlet `Get-BrokerMachine`. Para obtener más información, consulte GetBrokerMachine.

1. Etiquete los VDI dedicados que no se hayan utilizado durante más de 30 días con un ID 123:

    a) Defina una etiqueta para etiquetar los VDI no usados, por ejemplo, **VDI-sin-usar**.

    - Nombre de etiqueta: VDI-sin-usar
    - ID de etiqueta : 123

    b) Cree la regla de etiquetado automático para etiquetar las máquinas no usadas. Defina los parámetros de regla:

    - Nombre : Nombre genérico de la regla.
    - Tipo de objeto: Máquina.
    - Texto de la regla : Máquinas estáticas asignadas cuya hora última de conexión es > 30 días o no tiene un valor.

- UID de etiqueta : El identificador de etiqueta al que quiere asociar 123.

```
New-BrokerAutoTagRule -Name 'UnusedVdi' -ObjectType 'Machine' -
RuleText "-AllocationType Static -IsAssigned $true -Filter {
SummaryState -ne `"InUse`" -and ( LastConnectionTime -lt '-30'
 -or LastConnectionTime -eq `$null )} " -TagUid 123
```

c) Compruebe las máquinas marcadas con la etiqueta **VDI-sin-usar** y libérelas.

2. Para etiquetar grupos de entrega con un nivel funcional inferior a X (mediante**L7_20** como nivel funcional de umbral):

```
New-BrokerAutoTagRule -Name 'LowFL'-ObjectType 'DesktopGroup'-RuleText
 "-Filter { MinimumFunctionalLevel -lt 'L7_20' } "-TagUid 123
```

1. Para etiquetar aplicaciones visibles por el usuario publicadas sin una carpeta:

```
New-BrokerAutoTagRule -Name 'NoFolder'-ObjectType 'Application'-
RuleText "-Enabled $true -Filter { ClientFolder -eq $null )} "-TagUid
 123
```

Más información

Entrada de blog: How to assign desktops to specific servers.

Perfiles de usuario

August 17, 2024

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.

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). A veces, los sistemas aprovisionados tienen almacenamiento local persistente. Están clasificados 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 almacenamiento local persistente, creadas con Machine Creation Services.

- **Persistentes y compartidas**. Por ejemplo: máquinas con SO multisesión creadas con Machine Creation Services y servidores de Citrix Virtual Apps.
- **Aprovisionadas y dedicadas**. Por ejemplo: máquinas con SO de sesión única y una asignación estática pero sin almacenamiento persistente, creadas con Citrix Provisioning Service (en Citrix Virtual Desktops).
- **Aprovisionadas y compartidas**. Por ejemplo: máquinas con SO de sesión única y una asignación aleatoria, creadas con Citrix Provisioning Service (en Citrix Virtual Desktops) y servidores de Citrix Virtual Apps.

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

Directiva	Aprovisionadas y dedicadas	Aprovisionadas y compartidas
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**. Esta configuración 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. La redirección de carpetas 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 coherente en todos los sistemas operativos, necesita una configuración diferente para cada sistema operativo, es decir, la redirección avanzada de carpetas. 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 redirigir solo una carpeta, en lugar de ambas. Este enfoque 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. Puede producirse un comportamiento impredecible, a menos que se utilice correctamente la redirección de carpetas.

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

La implementación contiene aplicaciones (incluidas las versiones de Microsoft Outlook y de Internet Explorer) que funcionan en escritorios Windows 10, así como aplicaciones (incluidas otras versiones de Outlook y de Internet Explorer) entregadas por Windows Server 2019. Para conseguirlo, ya 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 las 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	¿Carpeta redirigida en Windows 10?	¿Carpeta redirigida en Windows Server 2019?
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, es seguro guardarlas 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 10. Para las tareas diarias, los usuario cuentan más con Windows 10. Los usuarios solo acceden ocasionalmente a las aplicaciones entregadas por Windows Server. Además, en este caso, los datos no compartidos son más relevantes para el entorno de escritorio que para un entorno 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 10, 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 Introducción al redireccionamiento de carpetas, archivos sin conexión y perfiles de usuario móvil.

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 y exclusión de carpetas funcionan juntas. Asegurarse de que no se excluyan carpetas redirigidas permite a Profile Management volver a moverlas a la estructura de carpetas de perfil y conserva la integridad de los datos si posteriormente decide no redirigirlas. Para obtener más información acerca de las exclusiones, consulte Incluir y excluir elementos.

Registro de VDA

August 17, 2024

Introducción

> **Nota:**
>
> En un entorno local, los agentes VDA se registran con un Delivery Controller. En un entorno de servicio Citrix Cloud, los agentes VDA se registran con un Cloud Connector. En un entorno híbrido, algunos agentes VDA se registran con un Delivery Controller, mientras que otros se registran con un Cloud Connector.

Para poder utilizar un VDA, este debe registrarse en (o establecer comunicación con) uno o varios Controllers o Cloud Connectors del sitio. El VDA busca un Controller o 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 una información precisa acerca de los Controllers o Cloud Connectors (una información que se actualiza a medida que agrega o quita Controllers o Cloud Connectors), ese VDA podría rechazar inicios de sesión si interviene como intermediario un Controller o Cloud Connector 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 loca, 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 con 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 (registro inicial). Durante el 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.

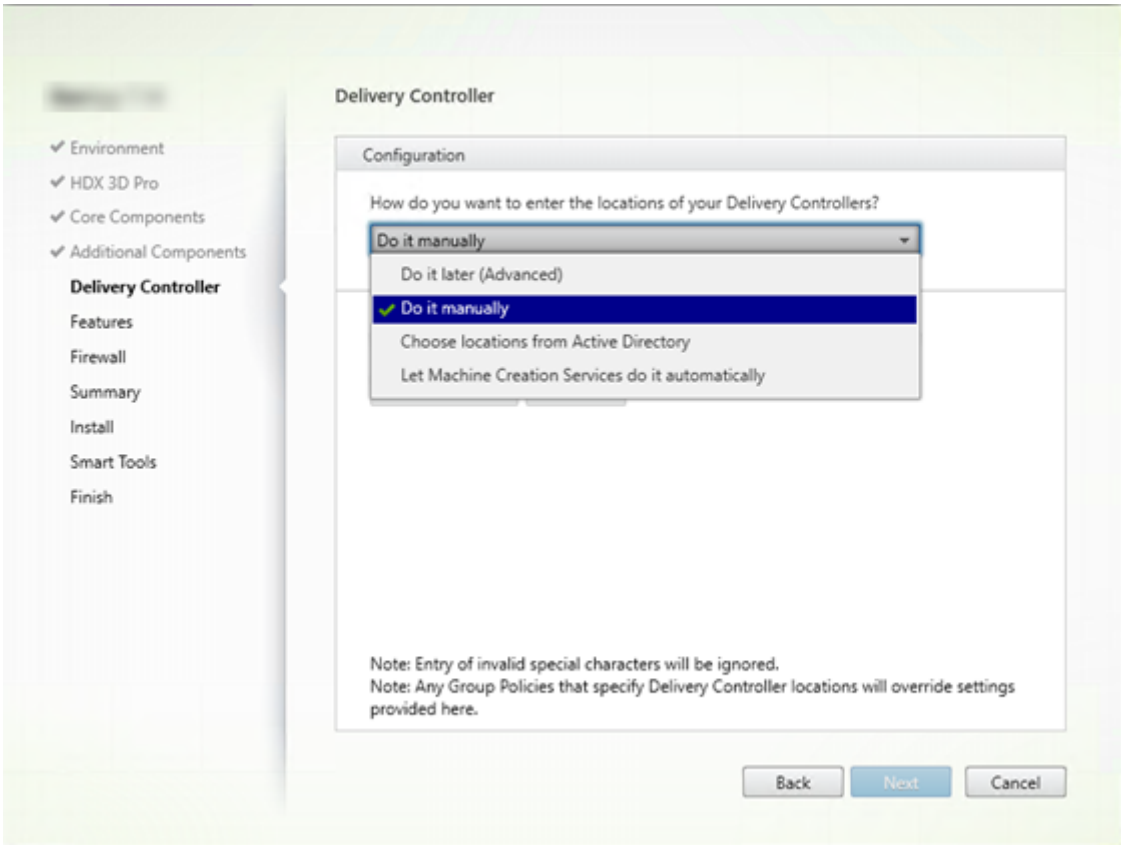
La forma más fácil de recuperar esa lista en los registros subsiguientes es mediante la función de actualización automática. De forma predeterminada, la actualización automática está habilitada. Para obtener más información, consulte Actualización automática.

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, preferencias de directiva de grupo (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 utiliza en 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. (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` bajo 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 enumera 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.

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**.

Revisión y 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. Por ejemplo:

```
DDC7x.xd.local DDC7xHA.xd.local

32-bit: HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\
    ListOfDDCs

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 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. Este proceso tiene lugar 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 de Citrix Provisioning. La caché del servidor 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 o Cloud Connector desde la última comprobación, o bien si se ha producido un cambio de directiva que afecte al registro de VDA, el Controller o Cloud Connector envía una lista actualizada a sus VDA registrados y la memoria caché se actualiza. El VDA acepta conexiones provenientes de todos los Controllers o Cloud Connectors de la lista más reciente que contenga en su memoria caché.
- Si un VDA recibe una lista que no incluye el Controller o Cloud Connector en el que está registrado (en otras palabras, el Controller o Cloud Connector se quitó del sitio), el VDA vuelve a registrarse en algún Controller o Cloud Connector que sí conste en la lista `ListofDDCs`.

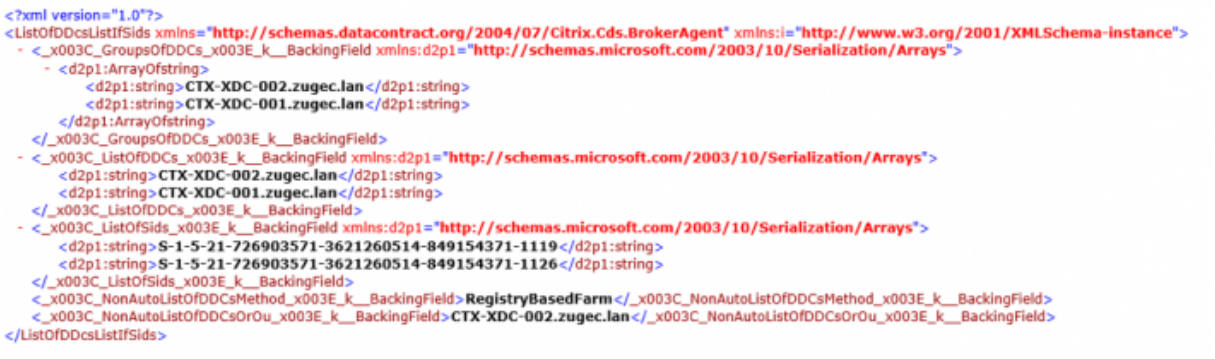
Ejemplo:

- 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.



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. Este proceso puede ser útil cuando se mueve un VDA a otro sitio (por ejemplo, durante la recuperación ante desastres).

Consideraciones sobre la configuración

Consulte una configuración de registro de VDA común.

Esto es un vídeo incrustado. Haga clic en el enlace para ver el vídeo.

Consulte los pasos de registro de VDA.

Esto es un vídeo incrustado. Haga clic en el enlace para ver el vídeo.

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/Cloud Connector y Controller/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 utilizarse 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 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`. Asimismo, un VDA también debe saber en qué Controllers puede confiar; los VDA no confían automáticamente en los Controllers de 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`.

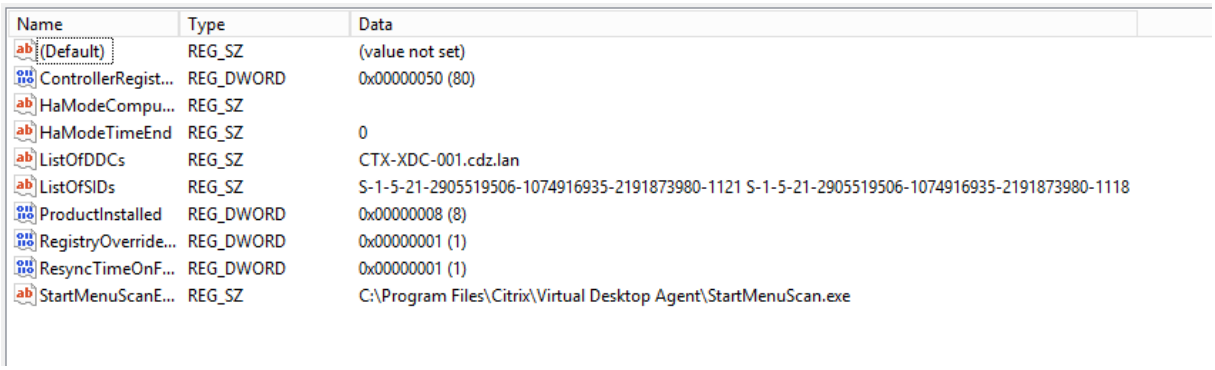
Por lo general, no es necesario modificar manualmente la lista `ListofSIDs`. Sin embargo, existen varias excepciones a ello. Las dos primeras excepciones ya no son válidas, porque están disponibles tecnologías más recientes.

- **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`. Esta no es una configuración típica o recomendada. No la use en entornos más nuevos. 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 (ListOfSIDs).



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.

Secuenciación de enlaces LDAP durante el registro de VDA mediante un controlador de dominio de solo lectura

Cuando un VDA se registra en un controlador de dominio de solo lectura (RODC), el agente intermediario debe seleccionar qué enlace o enlaces del Protocolo ligero de acceso a directorios (LDAP) debe ignorar. Para realizar esta selección, el agente intermediario requiere una clave del Registro adecuada.

Si no se proporciona una clave del Registro o el campo de la clave del Registro está vacío, el registro del VDA en el RODC tarda más porque es necesario seguir la secuencia del enlace LDAP original.

Para modificar la secuencia del enlace LDAP, se agregó la clave del Registro `ListofIgnoredBindings` a `HKEY_LOCAL_MACHINE\Software\Policies\Citrix\VirtualDesktopAgent`. El uso de `ListofIgnoredBindings` le permite modificar la secuencia del enlace LDAP según sea necesario y, por lo tanto, acelerar el registro de VDA en un RODC.

- Nombre: `ListofIgnoredBindings`
- Tipo: `REG_SZ`
- Valores: `DefaultPath`, `DomainPath`, `PDCPath`

El valor es una lista de opciones de ruta de enlace, separadas por comas. La clave del Registro ignorará los valores que no reconozca como válidos.

Solucionar problemas en el registro de VDA

Como se ha indicado anteriormente, un VDA debe registrarse en un Delivery Controller o Cloud Connector para que se le tenga en cuenta al iniciar sesiones con broker. Los VDA no registrados pueden derivar en una infrautilización 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 obtenido información acerca de una máquina (posiblemente porque nunca se registró), 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, podría necesitar 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 la ficha **Solución de problemas** del panel de detalles 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 utilizar las comprobaciones de estado de Citrix Scout para solucionar problemas de registros de VDA y de inicios de sesión. Para obtener más información, consulte Acerca de las comprobaciones de estado.

IP virtual y bucle invertido virtual

August 17, 2024

> **Importante:**
>
> - La multisesión de Windows 10 Enterprise no incluye la función de virtualización de IP de Escritorio remoto (IP virtual) y nosotros no incluimos la función de Virtualización de IP de Escritorio remoto ni bucle invertido virtual en multisesión con Windows 10 Enterprise.
> - La virtualización de IP de escritorio remoto (IP virtual) no es compatible con las máquinas alojadas en la nube.
>
> Para obtener más información, consulte la documentación de Microsoft.

La virtualización de IP de escritorio remoto y las funciones de bucle invertido virtual son compatibles con las máquinas Windows Server 2016, Windows Server 2019 y Windows Server 2022. Sin embargo, no se aplican a las máquinas con SO de escritorio Windows.

La función de dirección de Virtualización de IP de Microsoft proporciona una dirección IP exclusiva a una aplicación publicada, asignada dinámicamente para cada sesión. Con la función de bucle invertido virtual de Citrix, puede 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, lo que requiere una dirección IP exclusiva o una dirección de bucle invertido. Otras aplicaciones pueden enlazar con un puerto estático, por lo que, al intentar iniciar instancias adicionales de una aplicación en un entorno multiusuario, se produce 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.

La virtualización de IP de escritorio remoto y el bucle invertido virtual son funciones independientes entre sí. Puede usar solo una de ellas o ambas.

Sinopsis de acciones de administrador:

- Para usar la virtualización IP de escritorio remoto de Microsoft, habilítela y configúrela 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.

Virtualización de IP de escritorio remoto (IP virtual)

Cuando la función de Virtualización de IP 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 la virtualización IP de escritorio remoto 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 usar direcciones de virtualización IP de escritorio remoto:

1. Obtenga la herramienta **TCPView** de Microsoft. Esta herramienta muestra todas las aplicaciones que enlazan puertos y direcciones IP específicas. Para obtener más información sobre TCPView, consulte la documentación de Microsoft.
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 o 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. Para obtener más información sobre la configuración de la virtualización de IP de escritorio remoto, consulte la documentación de Microsoft.

- 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). Todas las conexiones de origen abiertas por la aplicación se originan 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 virtualización de IP de escritorio remoto examina la dirección IP devuelta y la cambia a la dirección de virtualización de IP de escritorio remoto 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 de Virtualización de IP de escritorio remoto 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 direcciones de virtualización IP de escritorio remoto también busca

0.0.0.0 en estos tipos de llamadas. Cambia la llamada para escuchar en la dirección de virtualización de IP de escritorio remoto 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 de virtualización IP de escritorio remoto 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 los **parámetros de la directiva de bucle invertido de virtualización de IP de escritorio remoto 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.
- Exclusión de puerto de bucle invertido de IP virtual. Cuando una aplicación llama a la dirección de bucle invertido en los puertos especificados en este parámetro, el bucle invertido virtual no cambia la llamada a la dirección de bucle invertido específica de la sesión.

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. Esta funcionalidad 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. De lo contrario, podría obtener resultados imprevistos.
- 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.

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>

Zonas

August 17, 2024

> **Nota:**
>
> Puede administrar la implementación de Citrix Virtual Apps and Desktops mediante dos consolas de administración: Web Studio (basada en la web) y Citrix Studio (basada en Windows). Este artículo se refiere únicamente a Web Studio. Para obtener información sobre Citrix Studio, consulte el artículo equivalente en Citrix Virtual Apps and Desktops 7 2212 o versiones anteriores.

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 Web Studio, Citrix Director y la base de datos del sitio. Esto disminuye los costes de implementación, personal, licencias y operación de más 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". Esta zona contiene la base de datos SQL Server del sitio (y servidores SQL de alta disponibilidad, si los hay), Web Studio, Director, Citrix StoreFront, el servidor de licencias Citrix y Citrix Gateway. Mantenga siempre la base de datos del sitio en la zona principal.

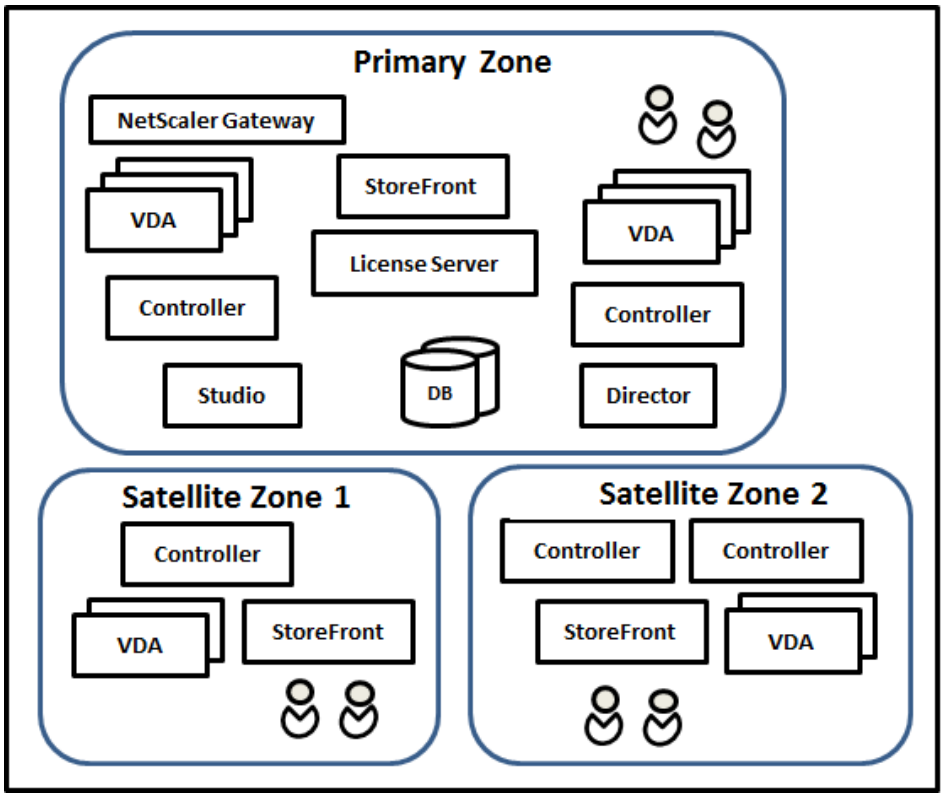
La zona principal debe tener al menos dos Controllers para la redundancia. Asimismo, la zona principal puede tener agentes VDA con aplicaciones estrechamente ligadas a la base de datos y la infraestructura.

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 almacenar máquinas de esa zona. Al configurar una zona satélite, puede asociarle una conexión de hipervisor u otro servicio. (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, Web 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. Tal implementación puede ser efectiva en una oficina donde los trabajadores utilizan un sitio local de StoreFront y el Controller local para acceder a sus recursos locales.

- **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 intenta 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 una zona satélite vuelva a estar disponible. Un VDA de una zona satélite no intenta 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:

- Web Studio no puede conectarse al sitio.
- No se puede establecer conexiones con los VDA de la zona principal.
- El rendimiento del sitio se degrada cada vez más hasta que los Controllers de la zona principal vuelven a estar disponibles.

En caso de sitios que contienen versiones de VDA anteriores a 7.7:

- Un VDA en una zona satélite acepta 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 registra 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.

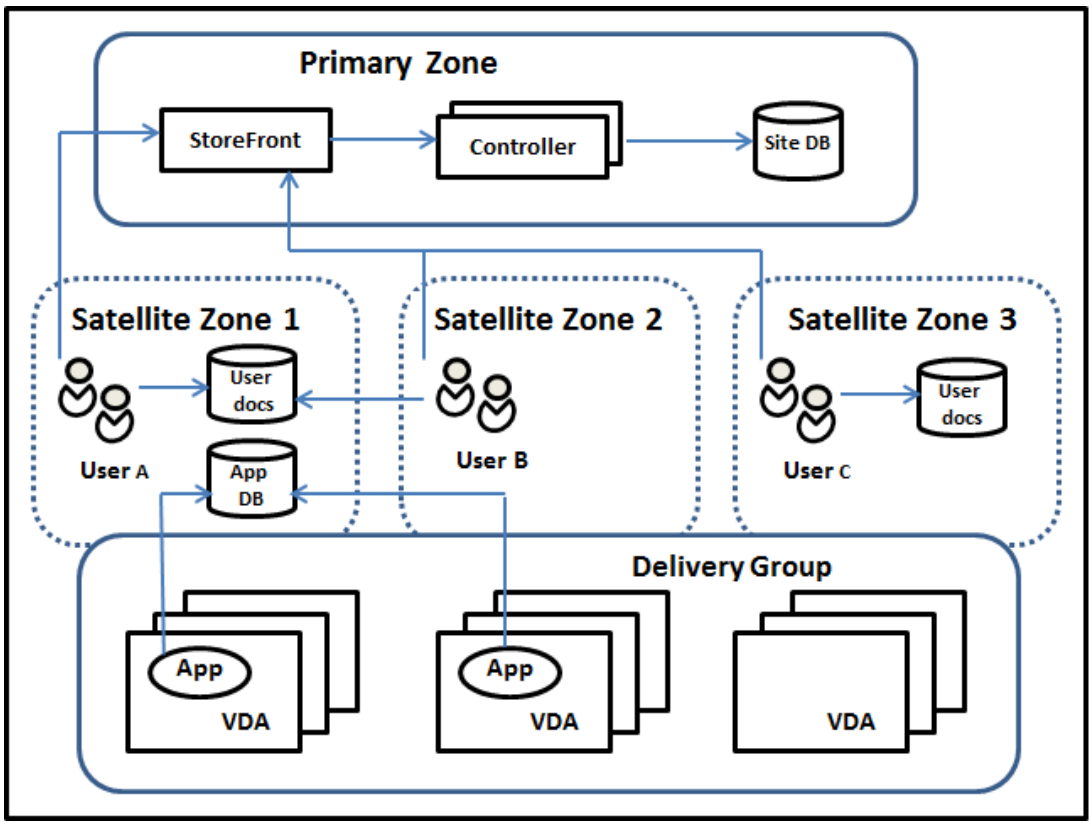
En un sitio de varias zonas, la función Preferencia de zonas ofrece más flexibilidad al administrador para controlar qué VDA se utiliza para iniciar una aplicación o un escritorio.

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 se indica que hay varias ubicaciones en las que los usuarios pueden ejecutar sus dispositivos de punto final con la aplicación Citrix Workspace:

- El usuario A está utilizando un dispositivo con la aplicación Citrix Workspace en la zona satélite 1.
- El usuario B está utilizando un dispositivo en la zona satélite 2.
- Los documentos de un usuario se pueden almacenar en varias ubicaciones.
  - Los usuarios A y B utilizan un recurso de red compartido ubicado en la zona satélite 1.
  - El usuario C utiliza un recurso compartido de la zona satélite C.
  - 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 de una aplicación, puede limitar aún más cómo se utilizará la preferencia de zonas.

- **Uso obligatorio de la zona particular del usuario:** En un grupo de entrega, puede especificar que una sesión se inicie en la zona particular del usuario (si está configurada), sin conmutación por error a otra zona si dicha zona no tiene recursos disponibles. 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 se inicie 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:

tal vez prefiera que los usuarios ejecuten una aplicación en un VDA cercano a su dispositivo, mediante la preferencia de zona de la ubicación del usuario, aunque es posible que 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, es posible que el sistema cree una 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 usa una conexión de host, compruebe que el catálogo y la conexión se hallan 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 Controllers en una zona satélite, se presupone que esas máquinas tienen una buena conexión (local) con hipervisores y agentes VDA en la misma zona. 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 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 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 Web 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.
- Mantenga siempre la base de datos del sitio en la zona principal.
- Después de crear una zona, puede mover elementos de una zona a otra. Esta flexibilidad le permite separar potencialmente elementos que funcionan mejor si están cerca. Por ejemplo: mover un catálogo de máquinas a otra zona distinta de la zona de la conexión (host) que crea las máquinas del catálogo podría afectar al rendimiento. 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 Web Studio y Director solo en la zona principal. Puede acceder a Web Studio y a Director desde una zona satélite (por ejemplo, una zona satélite que contenga Controllers para la conmutación por error si la zona principal deja de estar accesible) porque son aplicaciones web.
- Preferiblemente, Citrix Gateway de una zona satélite se usa para conexiones de usuario procedentes 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 una zona a otra, debe tener el permiso de modificar ese catálogo. Para obtener más información, consulte Administración delegada.

Si utiliza Citrix Provisioning: La consola de Citrix Provisioning no reconoce zonas, por lo que se recomienda usar Web Studio para crear catálogos para las zonas satélite. Cree el catálogo en Web Studio y especifique la zona satélite correcta. A continuación, utilice la consola de Citrix Provisioning para aprovisionar las máquinas de ese catálogo (si crea el catálogo con el asistente Citrix Provisioning Wizard, el catálogo se coloca en la zona principal; deberá usar Web Studio para moverlo a la zona satélite).

Crear una zona

1. Inicie sesión en Web Studio.
2. Seleccione **Zonas** en el panel de la izquierda.
3. Seleccione **Crear zona** en la barra de acciones.
4. Escriba un nombre para la zona y una descripción (opcional). El nombre debe ser único dentro del sitio.
5. 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.
6. Haga clic en **Guardar**.

Como alternativa a este método, puede seleccionar uno o varios elementos en Web Studio y, a continuación, seleccionar **Crear zona** en la barra de acciones.

Cambiar el nombre o la descripción de una zona

1. Inicie sesión en Web Studio.
2. Seleccione **Zonas** en el panel de la izquierda.
3. Seleccione una zona en el panel central y, a continuación, seleccione **Modificar zona** en la barra de acciones.
4. Cambie el nombre de la zona, la descripción o ambos. Si cambia el nombre de la zona principal, tenga en cuenta que la zona debe ser fácilmente identificable como zona principal.
5. Haga clic en **Guardar** o **Aplicar**.

Mover elementos de una zona a otra

1. Inicie sesión en Web Studio.
2. Seleccione **Zonas** en el panel de la izquierda.
3. Seleccione una zona en el panel central y, a continuación, seleccione uno o varios elementos.
4. Arrastre los elementos a la zona de destino o seleccione **Mover elementos** en la barra de 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: Cuando un catálogo emplea una conexión de host con un hipervisor u otro servicio, coloque el catálogo y la conexión 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. Inicie sesión en Web Studio.
2. Seleccione **Zonas** en el panel de la izquierda.
3. Seleccione una zona en el panel central.
4. Seleccione **Eliminar zona** en la barra de acciones. Si la zona no está vacía (contiene elementos), se le pedirá que seleccione la zona a la que se moverán los elementos.
5. 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. Inicie sesión en Web Studio.

2. Seleccione **Zonas** en el panel de la izquierda y, a continuación, seleccione una zona en el panel central.
3. Seleccione **Agregar usuarios a la zona** en la barra de acciones.
4. 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.
5. Haga clic en **Aceptar**.

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. Inicie sesión en Web Studio.
2. Seleccione **Zonas** en el panel de la izquierda y, a continuación, seleccione una zona en el panel central.
3. Seleccione **Quitar usuarios de la zona** en la barra de acciones.
4. 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. 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.
5. 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 en el momento de agregarla a un grupo, o más adelante.

- 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 la izquierda. Seleccione una aplicación y, a continuación, seleccione **Modificar propiedades de aplicación** en el panel de acciones.

En la página **Zonas** de las propiedades o ajustes de la aplicación:

- Si quiere que la aplicación tenga una zona particular:
  - Marque la opción **Usar la zona seleccionada para determinar** donde se inicia esta aplicación y, a continuación, seleccione la zona.
  - 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 ni de usuario para determinar dónde iniciar esta aplicación.

Otras acciones que implican especificar zonas

Después de crear al menos una zona satélite, puede especificar una zona al agregar una conexión de host o al crear un catálogo.

Normalmente, la zona principal es la predeterminada. Si utiliza Machine Creation Services para crear un catálogo, 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.

Supervisar

August 17, 2024

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 sirven 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

August 17, 2024

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. Esta función está habilitada de forma predeterminada. Puede usar el contenido registrado para:

- Diagnosticar y solucionar problemas tras haberse realizado cambios de configuración. El registro proporciona un rastro de los pasos seguidos.
- Ayudar en la administración de cambios y en el seguimiento de las configuraciones.
- Realizar informes sobre las 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. Inicie sesión en Web Studio y seleccione **Registros** en el panel de la izquierda.
2. Seleccione **Preferencias** en la barra de 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. Inicie sesión en Web Studio y seleccione **Registros** en el panel de la izquierda.
3. Seleccione **Preferencias** en la barra de 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 después de utilizar la búsqueda, borre el texto del cuadro **Buscar**.
- Elija qué columnas aparecerán en la pantalla. Para ello, seleccione el icono **Columnas que mostrar** en la esquina superior derecha de la tabla. Por ejemplo, para ver la dirección IP que usa el administrador para acceder a Web Studio, haga clic en el icono y agregue la columna **IP de cliente**.

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 la barra de 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 más seguridad, 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. Inicie sesión en Web Studio y seleccione **Registros** en el panel de la izquierda.
2. Seleccione **Eliminar registros** en la barra de 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.

Ver los registros de API y PowerShell

Para supervisar las solicitudes de API realizadas durante la sesión actual, haga clic en la ficha **API**. Los registros de API se borran después de cerrar sesión en Web Studio.

Para ver los comandos de PowerShell correspondientes a las acciones de interfaz de usuario que realizó durante el día, haga clic en la ficha **PowerShell**.

Asociar metadatos a registros de configuración

Puede adjuntar metadatos a los registros de configuración asociando un par `name-value` llamado `MetadataMap` a los registros de registro.

> **Nota:**
>
> - Solo puede adjuntar metadatos a objetos de operaciones de alto nivel.
> - Los metadatos se asocian a los registros existentes en el momento de la ejecución.

Establecer los metadatos

Ejecute el comando `Set-LogHighLevelOperationMetadata` de PowerShell para asociar un registro a `MetadataMap`.
`Set-LogHighLevelOperationMetadata` toma los siguientes parámetros:

- **Id**: ID de la operación de alto nivel.
- **InputObject**: Las operaciones de alto nivel a las que se agregan los metadatos. Esta es una alternativa al parámetro `Id`, en el que se pasa un objeto de operación de alto nivel o una lista de objetos al comando de PowerShell.

Name: Nombre de la propiedad de los metadatos por agregar. La propiedad debe ser única para la operación de alto nivel especificada. La propiedad no puede contener ninguno de los siguientes caracteres ()/;:#.*?=<> []'".	

-

- **Value**: Valor de la propiedad.
- **Mapa**: Diccionario de pares (nombre, valor) para las propiedades. Esta es una alternativa a configurar los metadatos mediante los parámetros `-Name` y `-Value`.

Por ejemplo, para adjuntar los metadatos a todos los registros de registro de alto nivel con el ID 40, ejecute el siguiente comando de PowerShell:

```
Get-LogHighLevelOperation – Id 40 | Set-LogHighLevelOperationMetadata
 -Name A -Value B
```

Para adjuntar los metadatos al registro de alto nivel con el usuario `abc@example.com`, ejecute el siguiente comando de PowerShell:

```
Get-LogHighLevelOperation – User `abc@example.com` | Set-LogHighLevelOperation
 -Name C -Value D
```

Obtención con los metadatos

Ejecute los siguientes comandos de PowerShell para usar los metadatos asociados para obtener los registros:

- Búsqueda por clave y valor:

  ```
  Get-LogHighLevelOperation -Metadata "Key:Value"
  ```

- Búsqueda por valor y cualquier clave:

  ```
  Get-LogHighLevelOperation -Metadata "*:Value"
  ```

- Búsqueda por clave y cualquier valor:

  ```
  Get-LogHighLevelOperation -Metadata "Key:*"
  ```

Quitar los metadatos

Ejecute el comando `Remove-LogHighLevelOperationMetadata` de PowerShell para quitar los metadatos asociados.
`Remove-LogHighLevelOperationMetadata` toma los siguientes parámetros:

- **Id**: ID de la operación de alto nivel.
- **InputObject**: Las operaciones de alto nivel a las que se agregan los metadatos. Esta es una alternativa al parámetro `Id`‘, en el que se pasa un objeto de operación de alto nivel o una lista de objetos al comando de PowerShell.
- **Name**: Nombre de la propiedad de los metadatos por quitar. Establézcalo en $null para quitar todos los metadatos del objeto especificado.

- **Mapa**: Diccionario de pares (nombre, valor) para las propiedades. Puede ser una tabla hash (creada con @{“nombre1”= “val1”; “nombre2”= “val2”}) o un diccionario de cadenas (creado con el nuevo objeto “System.Collections.Generic.Dictionary[Cadena, Cadena]”). Se quitan las propiedades cuyos nombres coinciden con las claves del mapa.

Registros de eventos

August 17, 2024

Los siguientes artículos contienen listas y descripciones de los eventos que registran los servicios de Citrix Virtual Apps and Desktops.

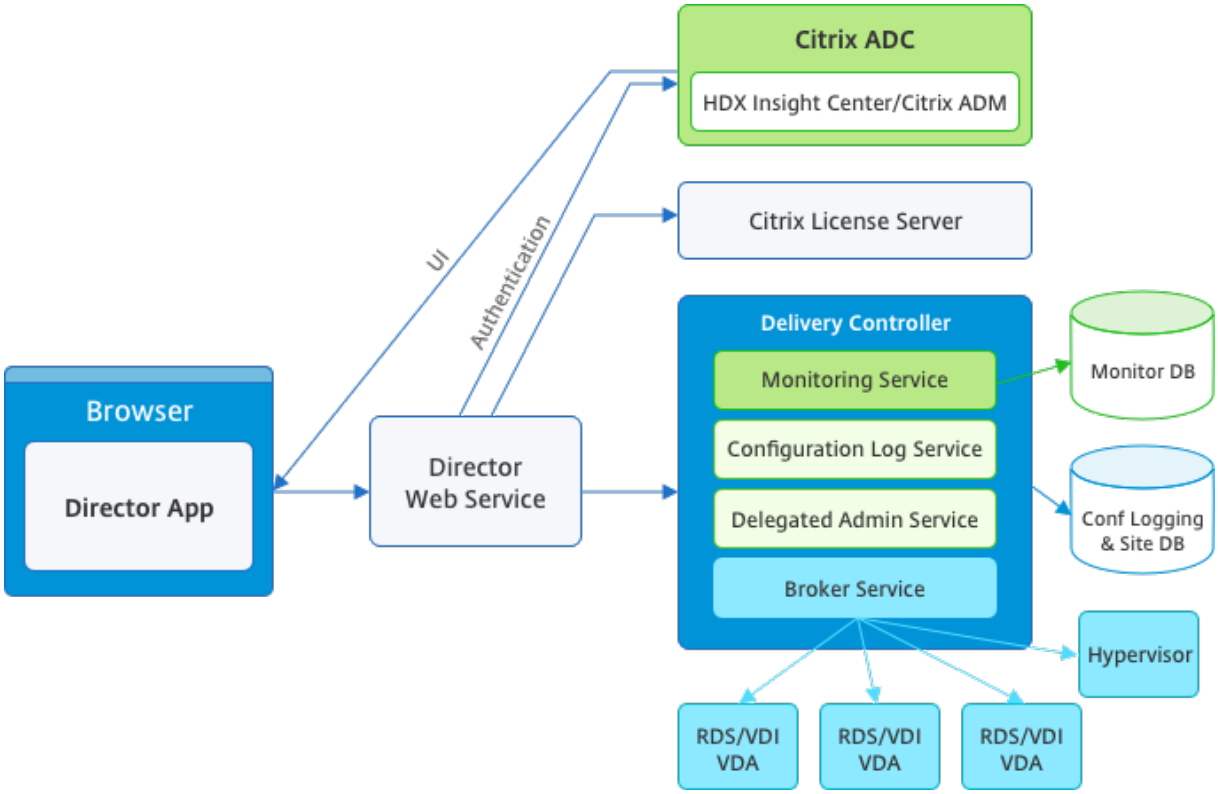
Esta información es general. Debe consultar los artículos de las funciones concretas para obtener más información sobre los eventos.

- Eventos de Citrix Broker Service
- Eventos del Citrix FMA Service SDK
- Eventos de Citrix Configuration Service
- Eventos de Citrix Delegated Administration Service

Director

August 17, 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, con tecnología de Citrix ADM, sirven para identificar posibles cuellos de botella debido a problemas de red en el entorno de Citrix Virtual Apps and Desktops:
  - Administración del rendimiento para garantizar el estado y la capacidad de la implementación
  - Análisis de red y tendencias históricas
- 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. 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 se encuentra en https o `http://<Server FQDN>/Director`.

Si uno de los sitios en la implementación de varios sitios está inactivo, el inicio de sesión tarda un poco más porque intenta conectarse con el sitio que está inactivo.

Usar Director con la autenticación con tarjetas inteligentes PIV

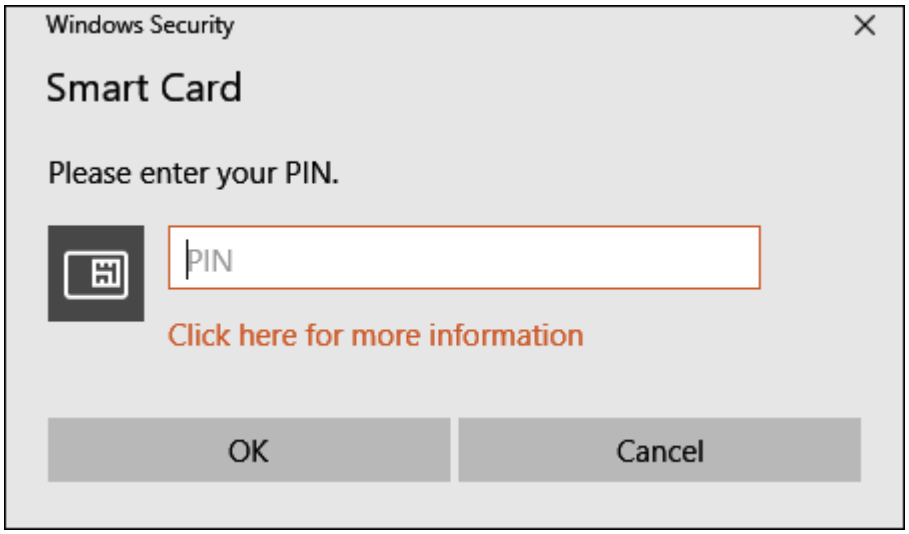
Ahora Director admite la autenticación con tarjetas inteligentes basadas en PIV (Personal Identity Verification) para iniciar sesión. Esta función es útil para organizaciones y agencias gubernamentales que usan la autenticación basada en tarjetas inteligentes para controlar el acceso.
La autenticación 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.

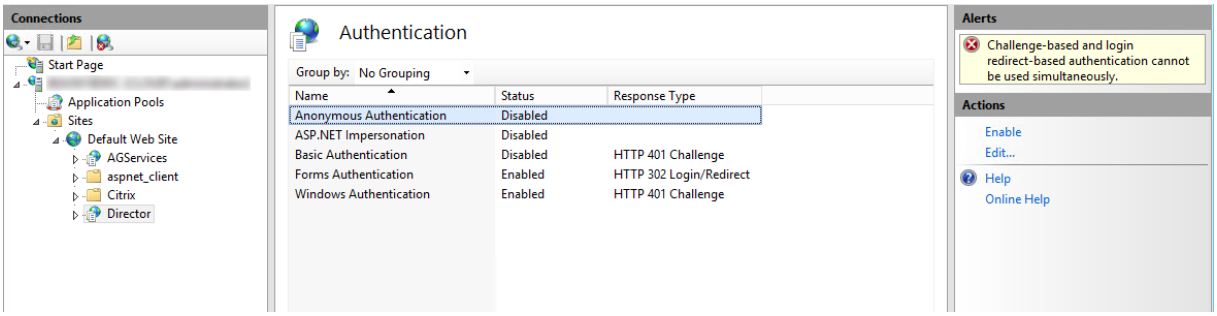


5. Después de autenticarse, puede acceder a Director sin tener que suministrar credenciales extra en la página de inicio de sesión de Director.

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 compatibilizar 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 podría 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 a ese usuario. Por ejemplo: el estado de las aplicaciones y procesos del 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 Pendo

Después de instalar Director, el servicio de Director usa Pendo para recopilar datos de uso. 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 Pendo, modifique la clave de Registro en la máquina donde está instalado Director. Si la clave de Registro 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. Use el Editor del Registro 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

> **Nota:**
>
> Anteriormente, Director Service utilizaba Google Analytics para recopilar los datos. La misma clave de registro se usa ahora para Pendo.

Valor: 0 = habilitado (de forma predeterminada), 1 = inhabilitado

Puede usar el siguiente cmdlet de PowerShell para inhabilitar la recopilación de datos por parte de Pendo:

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director

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 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 del sistema puede causar problemas graves que pueden obligarle 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. 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:

```
New-Item HKLM:\SOFTWARE\Citrix -Name Director

New-ItemProperty HKLM:\SOFTWARE\Citrix\Director -Name DisableGuidedHelp
    -PropertyType DWORD -Value 1
```

Artículos de referencia

- Reducir el MTTR de Citrix Director
- Citrix Director: Administrar y configurar alertas y notificaciones con PowerShell
- Documentación para desarrolladores de Citrix Virtual Apps and Desktops

Novedades en los productos relacionados

- Citrix DaaS
- StoreFront
- Secure Private Access
- Citrix Enterprise Browser

- Citrix Workspace
- Provisioning

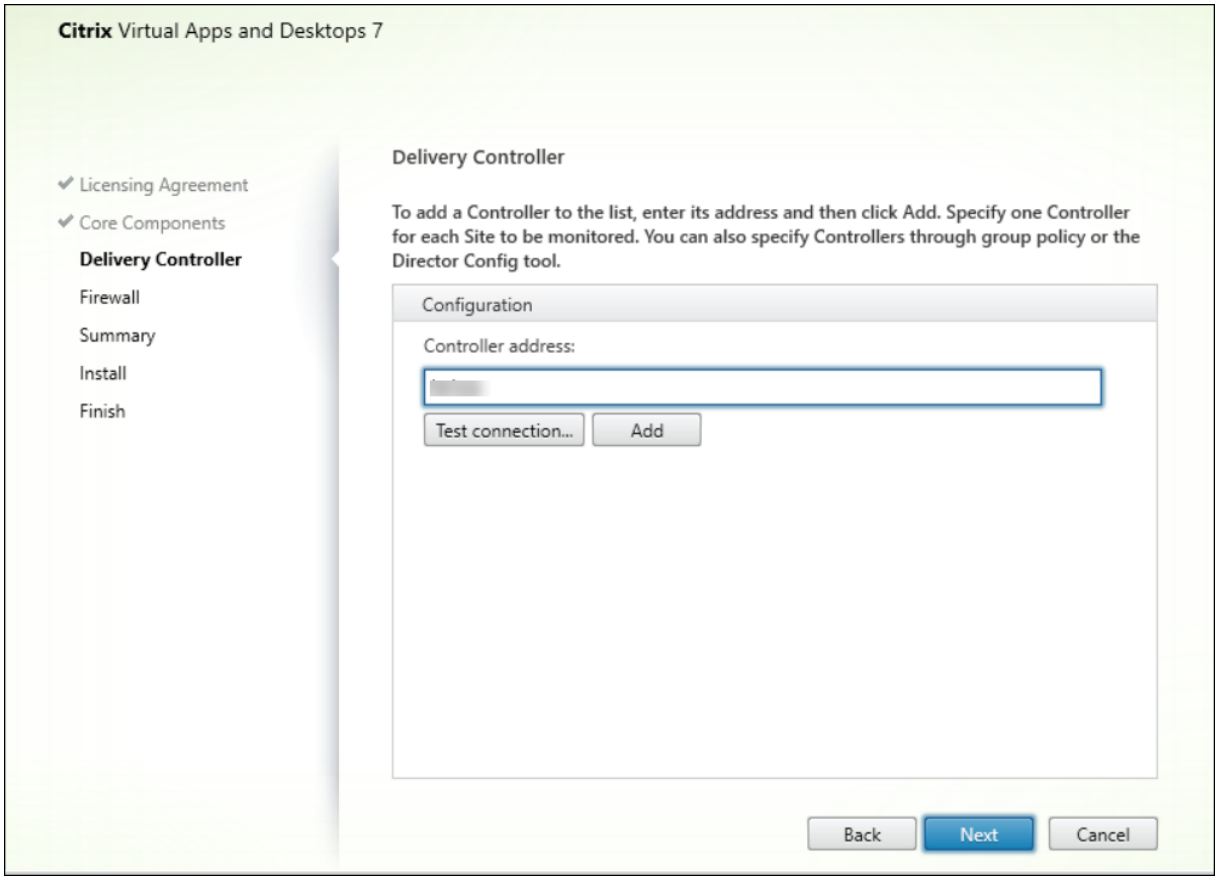
Instalación y configuración

August 17, 2024

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 falten, 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, autorice 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.

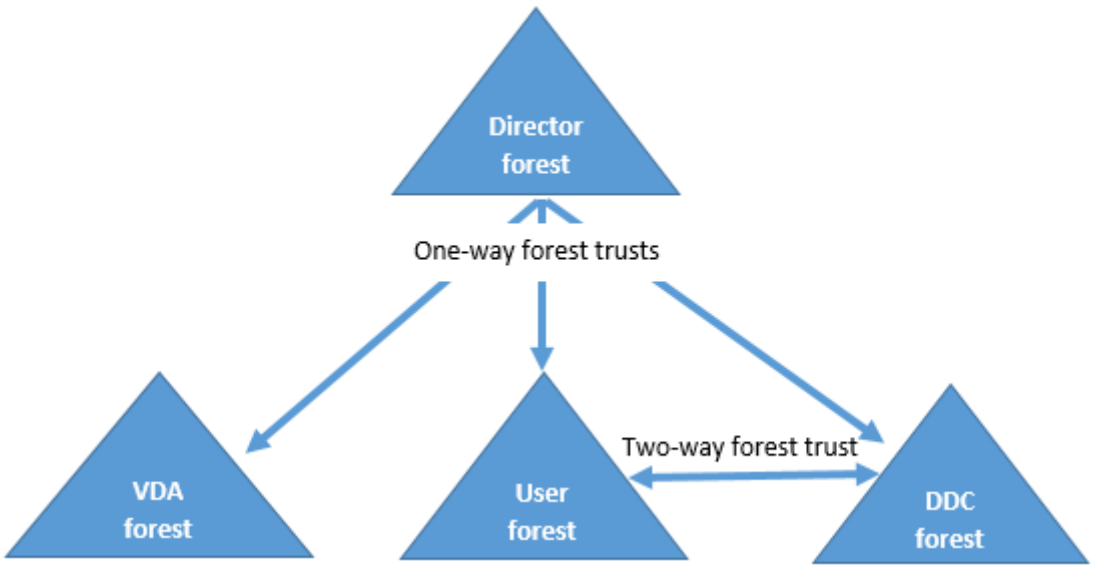
Configuración avanzada

August 17, 2024

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 más información 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:

```
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:

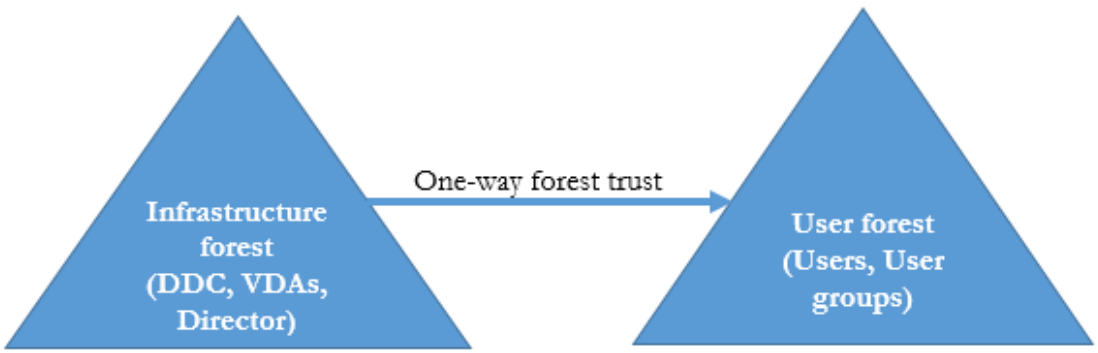
```
Connector.ActiveDirectory.Domains = (user),(server),\<domain1\>,\<
    domain2\>
```

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/CSP) tienen configuraciones de entorno similares, que constan de agentes VDA, Delivery Controllers y Director en el bosque de infraestructura. Los registros de usuarios o grupos de usuarios 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:

   ```
   Connector.ActiveDirectory.DomainLocalGroupSearch= true

   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 Web 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 configurar esto, 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:

```
Service.AutoDiscoveryAddresses = SiteAController,SiteBController
```

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 la ven 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 garantiza 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.

1. En el VDA, modifique la clave de Registro en HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerD
   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, realice ambos cambios para que los datos no se muestren en el Administrador de actividades.

Configurar la autenticación con tarjetas inteligentes PIV

August 17, 2024

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.

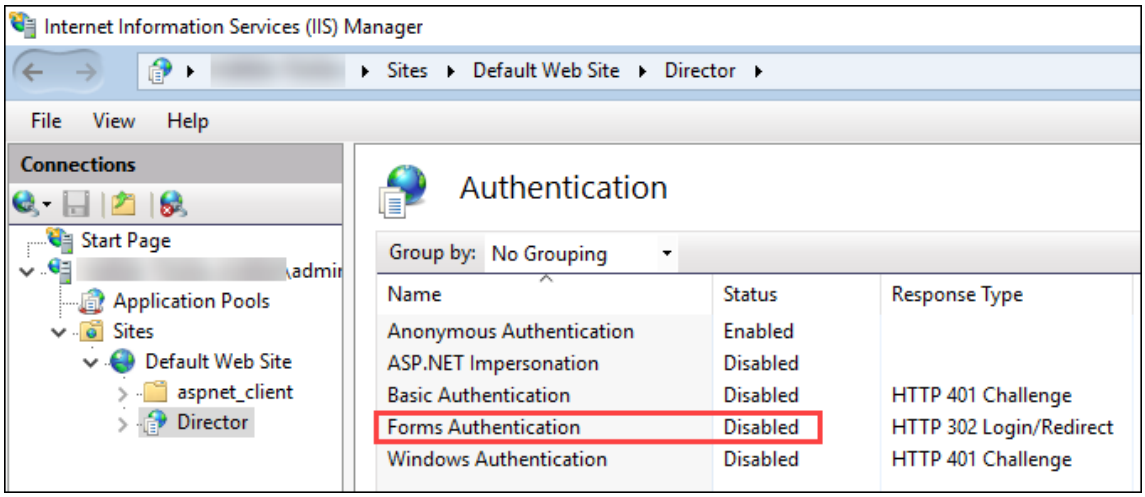
2. Inhabilite la autenticación mediante formularios en el sitio de Director.

   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 **Inhabilitar**.



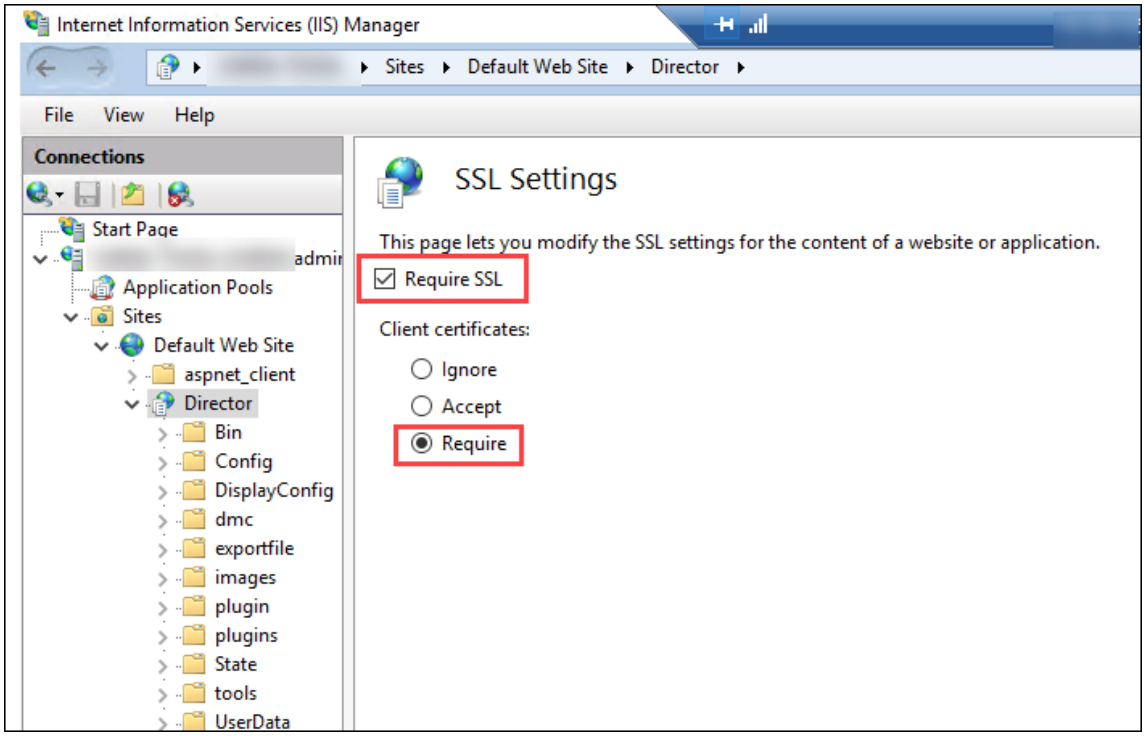
3. Configure la URL de Director para el protocolo HTTPS (más seguro que HTTP) para la autenticación de certificados de cliente.

   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:

```
<defaultDocument>
   <files>
       <add value="LogOn.aspx"/>
   </files>
</defaultDocument>
```

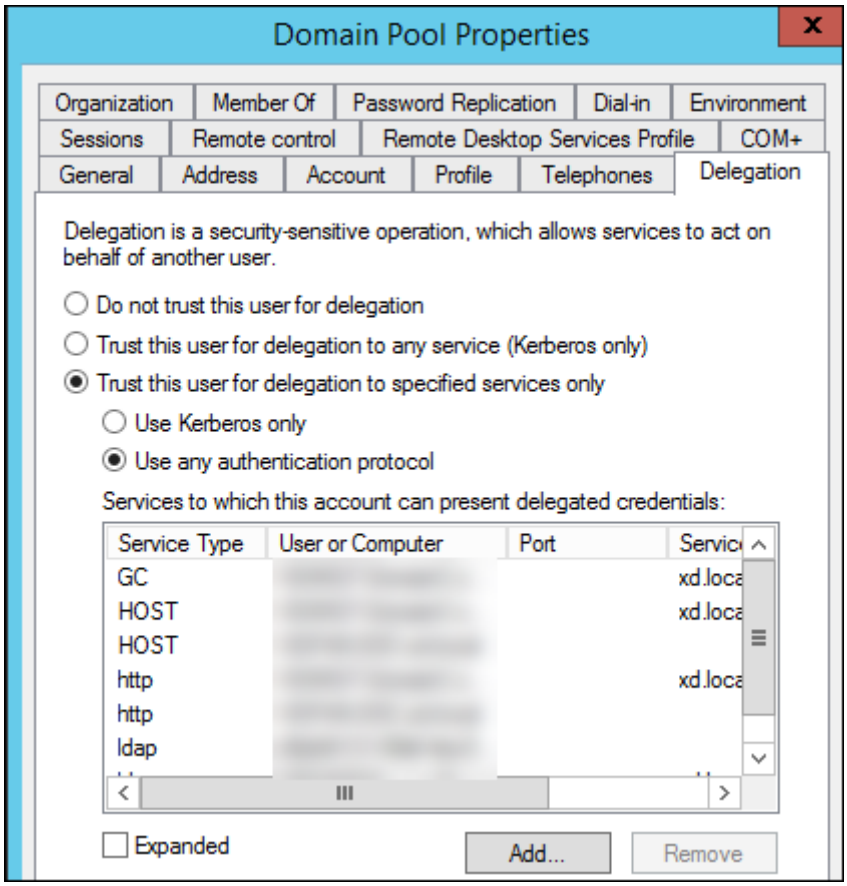
Configurar Active Directory

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 identidad 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 MSDN.

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.

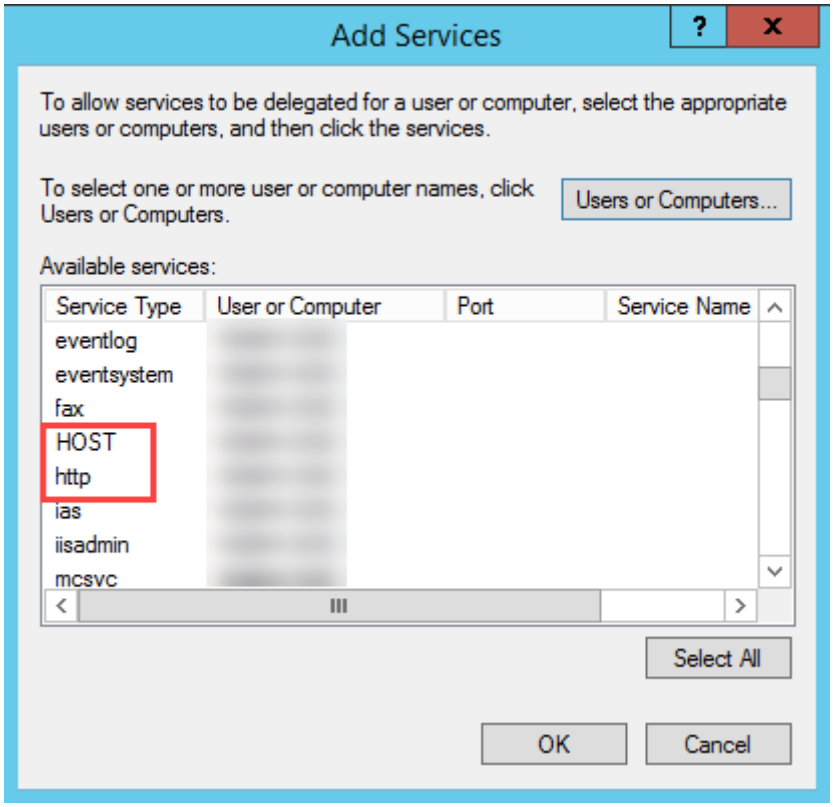


Configure los siguientes servicios para esta cuenta:

- Delivery Controller: HOST, HTTP
- Director: HOST, HTTP
- Active Directory: GC, LDAP

Para configurar,

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**.

Crear registros de los nombres de entidades de seguridad de servicio

Debe crear una cuenta de servicio para cada servidor de Director y las IP virtuales (VIP) con equilibrio de carga que se utilizan para acceder a un grupo de servidores de Director. Debe crear registros de los nombres de entidades de seguridad de servicio (SPN) para configurar una delegación a la cuenta de servicio recién creada.

- Use este comando para crear un registro SPN para un servidor de Director:

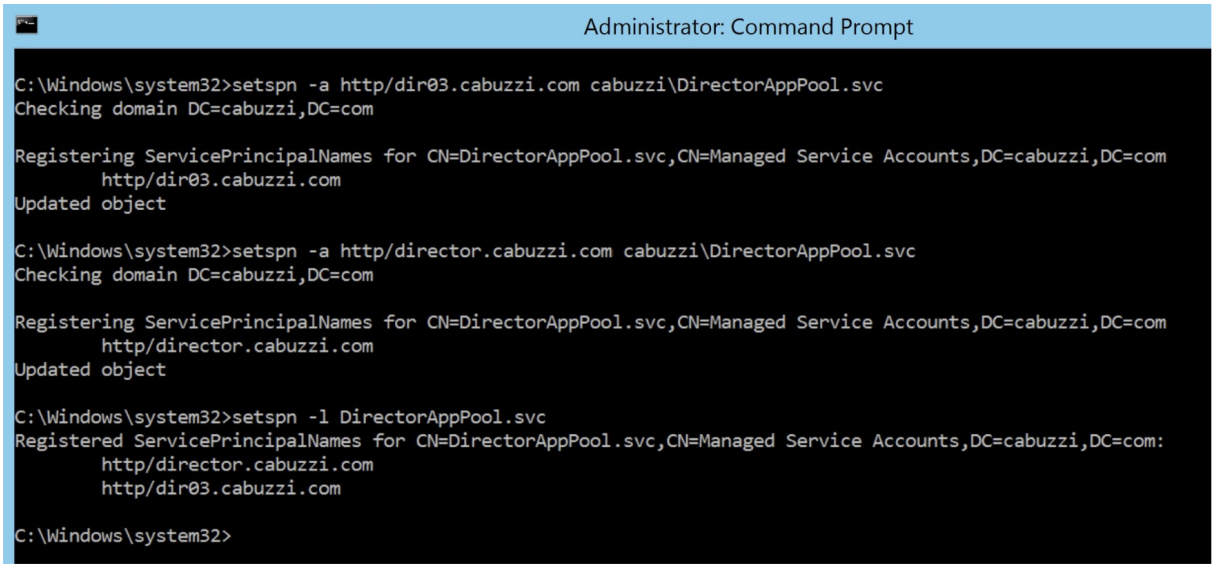
```
setspn -a http/<directorServer>.<domain_fqdn> <domain><
   DirectorAppPoolServiceAcct>
```

- Use the following command to create an SPN record for a load-balanced VIP:

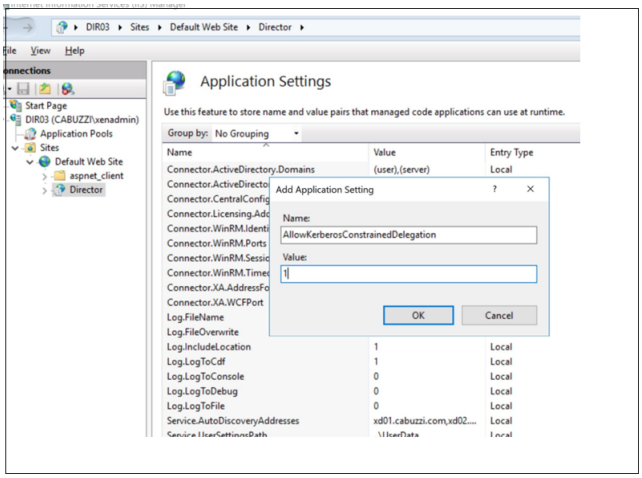
```
setspn -S http/<DirectorFQDN> <domain>\<
   DirectorAppPoolServiceAcct>
```

- Use este comando para ver o probar los SPN creados:

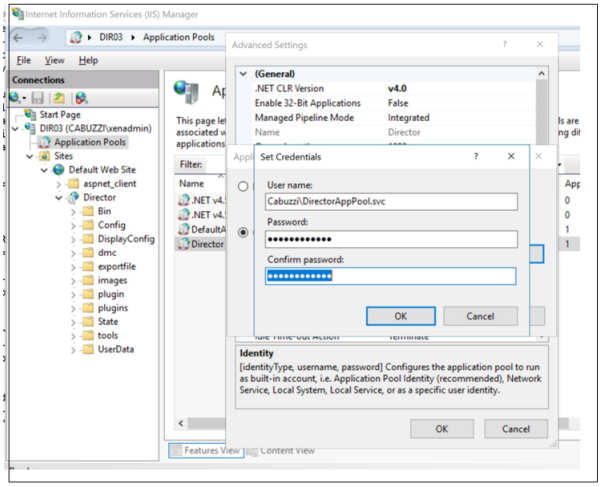
```
setspn – l <DirectorAppPoolServiceAcct>
```

- Select the Director virtual directory in the left pane and double click **Application Settings**. Inside the Application Settings window, click **Add** and ensure **AllowKerberosConstrainedDelegation** is set to 1.



- Select **Application Pools** in the left-hand pane, then right-click the Director application pool and select **Advanced Settings**.
- Select **Identity**, click the ellipses ("…") to enter the service account domain\logon and password credentials. Close the IIS console.

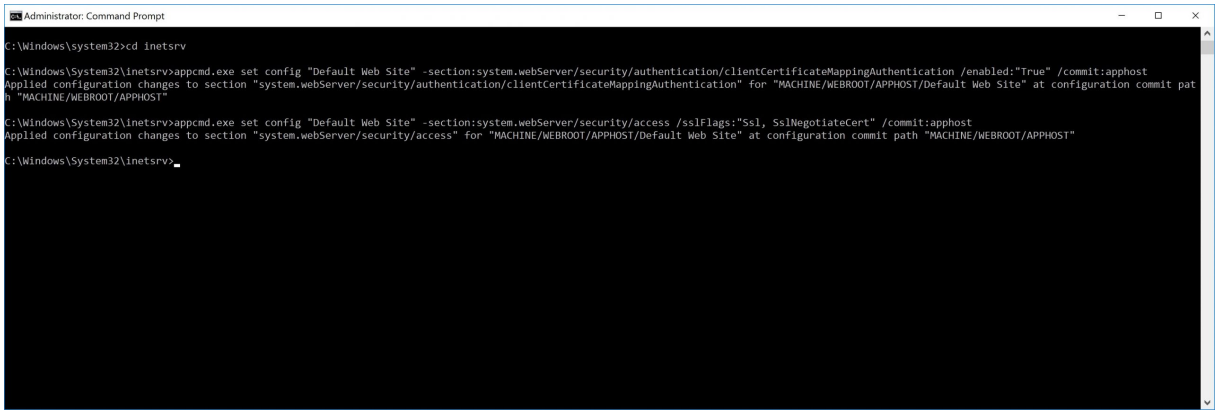


- From an elevated command prompt, change the directory to C:\Windows\System32\inetsrv and enter the following commands:

```
appcmd.exe set config " Sitio web predeterminado " -section:system.
    webServer/security/authentication/
    clientCertificateMappingAuthentication /enabled: " True " /commit:
    apphost
```

“‘

```
appcmd.exe set config " Default Web Site " -section:system.webServer/
    security/access /sslFlags: " Ssl, SslNegotiateCert " /commit:apphost
    \`\`\`
```



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

August 17, 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 versiones del 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 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.

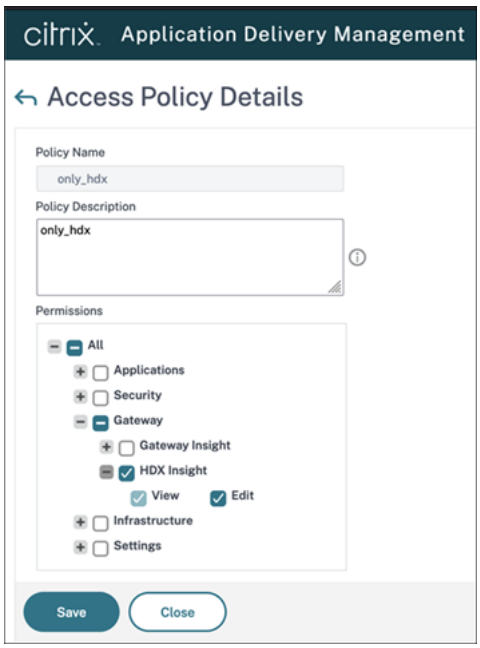
Nota:

Citrix NetScaler Insight Center alcanzó el 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 indique, 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

August 17, 2024

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 sobre la 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, administrar la energía y las sesiones, 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, además de 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.

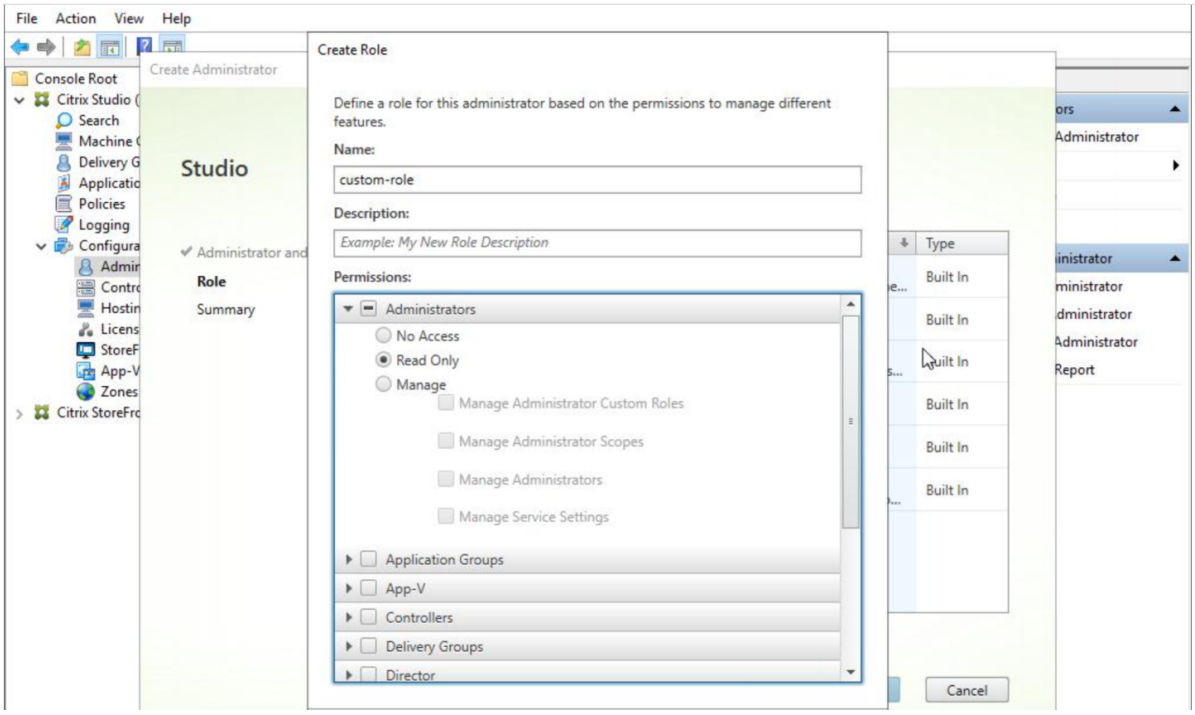
Rol de administrador	Los permisos en Director
Administrador de asistencia técnica	Puede acceder únicamente a las vistas del Servicio de asistencia y de los Detalles del usuario y solo puede ver los objetos que le han sido delegados para que los administre. Puede remedar la sesión de un usuario y ejecutar 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

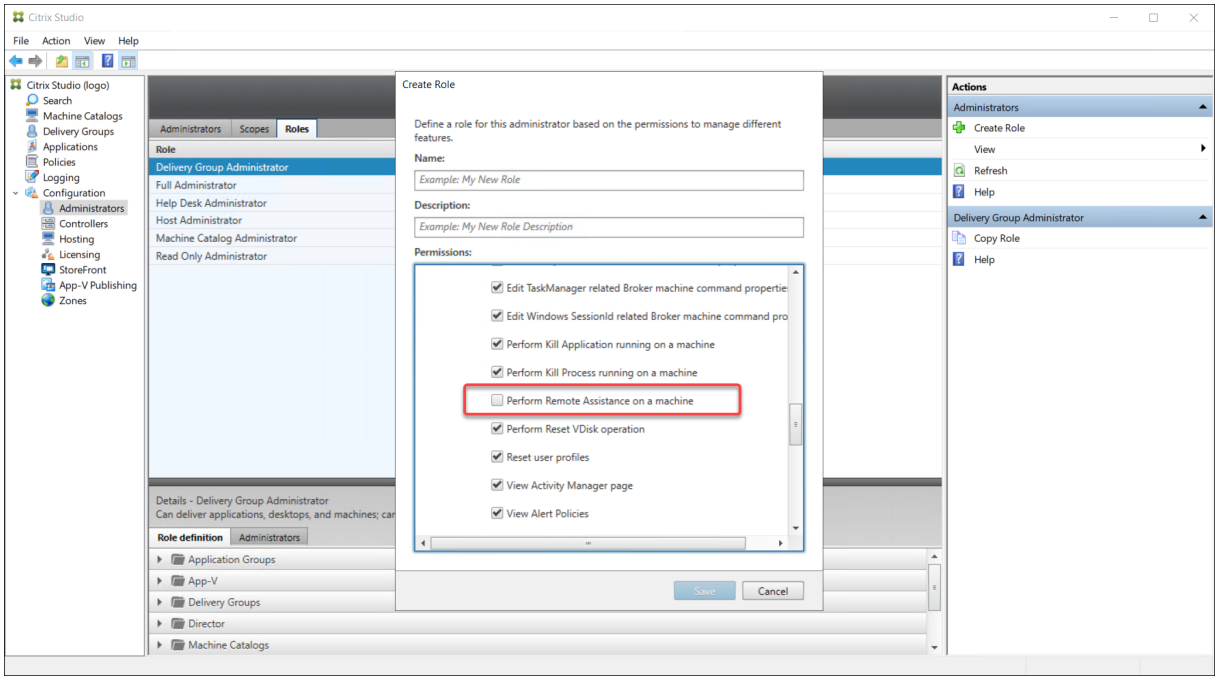


También puede crear un rol personalizado mediante la copia de un rol existente e incluir permisos extra para vistas diferentes. Por ejemplo: puede copiar el rol del servicio de asistencia e incluir permisos para ver las páginas Panel de mandos o Filtros.

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 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

August 17, 2024

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.

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
- .png
- .json
- .woff
- .woff2
- .ttf

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 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 Director está instalado, a sus grupos de aplicaciones se les concede lo siguiente:

- Derecho de **Iniciar sesión como un servicio**
- Privilegios **Ajustar las cuotas de memoria para un proceso**, **Generar auditorías de seguridad** y **Reemplazar un símbolo (token) de nivel de proceso**

Los derechos y privilegios mencionados representan 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, utilice el protocolo de seguridad de Internet (IPsec) o 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. Puesto que IPsec es un conjunto de protocolos de capa de red, los protocolos con niveles más elevados pueden utilizarlo sin necesidad de realizar ninguna modificación. HTTPS utiliza el protocolo Transport Layer Security (TLS) para brindar un cifrado de datos avanzado.

> **Nota:**
>
> - Citrix recomienda encarecidamente que restrinja el acceso a la consola de Director dentro de la red de intranet.
> - 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.
> - Proteja 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

Puede implementar cualquier aplicación web en el mismo dominio web (nombre de dominio y puerto) que Director. Sin embargo, los riesgos de seguridad en esas aplicaciones web podrían reducir 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.

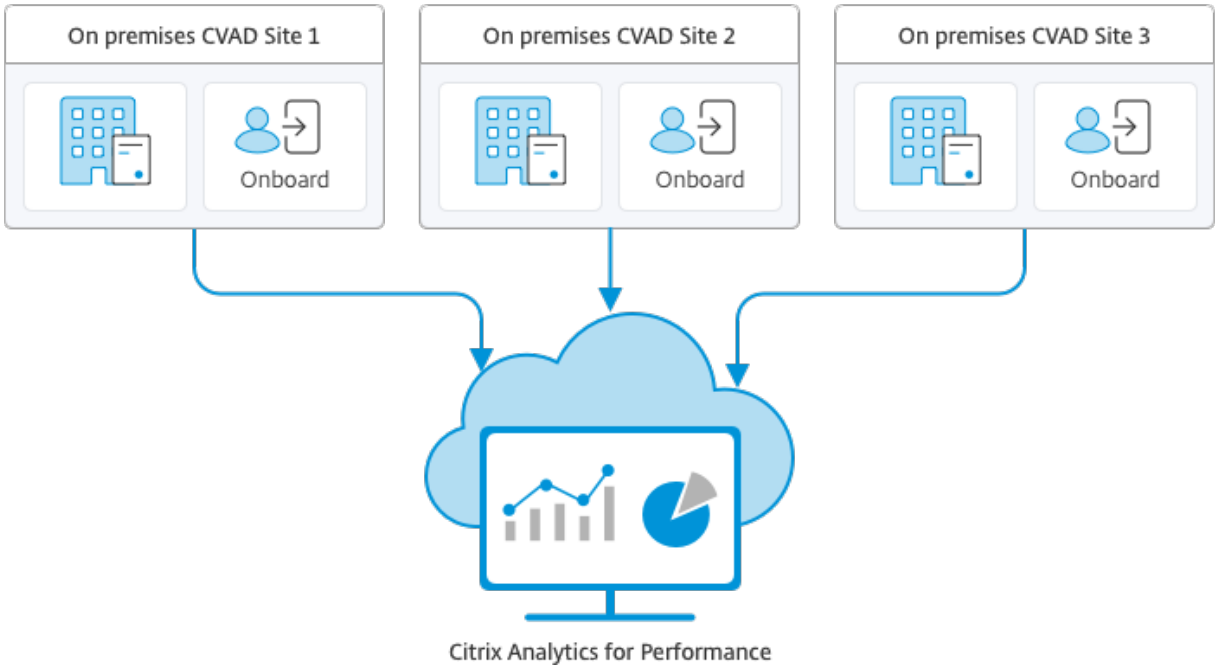
Configurar sitios locales con Citrix Analytics for Performance

August 17, 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**.



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/`
  - Citrix Cloud: `https://*.citrixworkspacesapi.net/`
  - Citrix Analytics: `https://*.cloud.com/`
  - Microsoft Azure: `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**:

```
<system.net>
    <defaultProxy>
        <proxy  usesystemdefault = "false"  proxyaddress = "http
            ://<your_proxyserver_address>:80" bypassonlocal = "
            true"  />
    </defaultProxy>
</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.

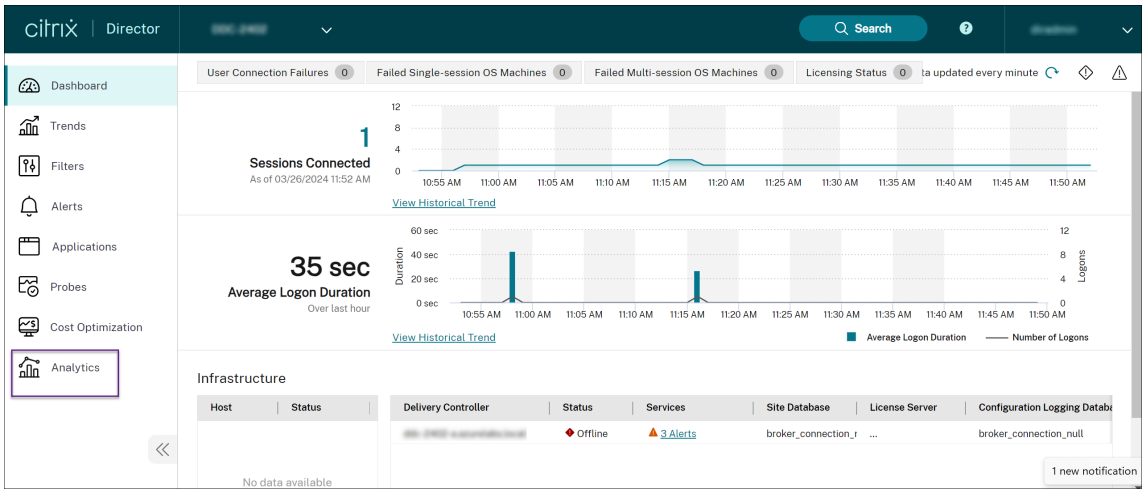
  Microsoft proporciona este parámetro en IIS. Para obtener más información, consulte `https://docs.microsoft.com/en-us/dotnet/framework/network-programming/proxy-configuration`.
  El campo **defaultproxy** del archivo de configuración controla el acceso saliente de Director y Monitor Service. La configuración 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.

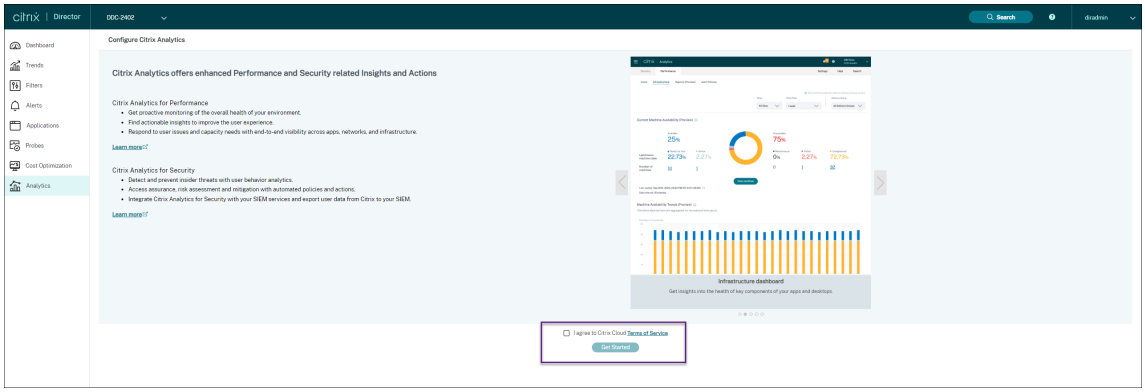
Pasos de configuración

Después de verificar los requisitos previos, haga lo siguiente:

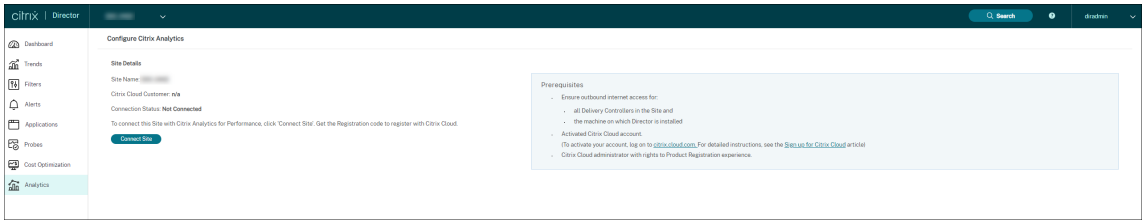
1. Inicie sesión en Director como administrador total y seleccione el sitio que quiere configurar con el análisis de rendimiento. Aparece la página Panel de mandos de Director.



2. Haga clic en la ficha **Analytics**. Aparece la página **Configurar Citrix Analytics**.

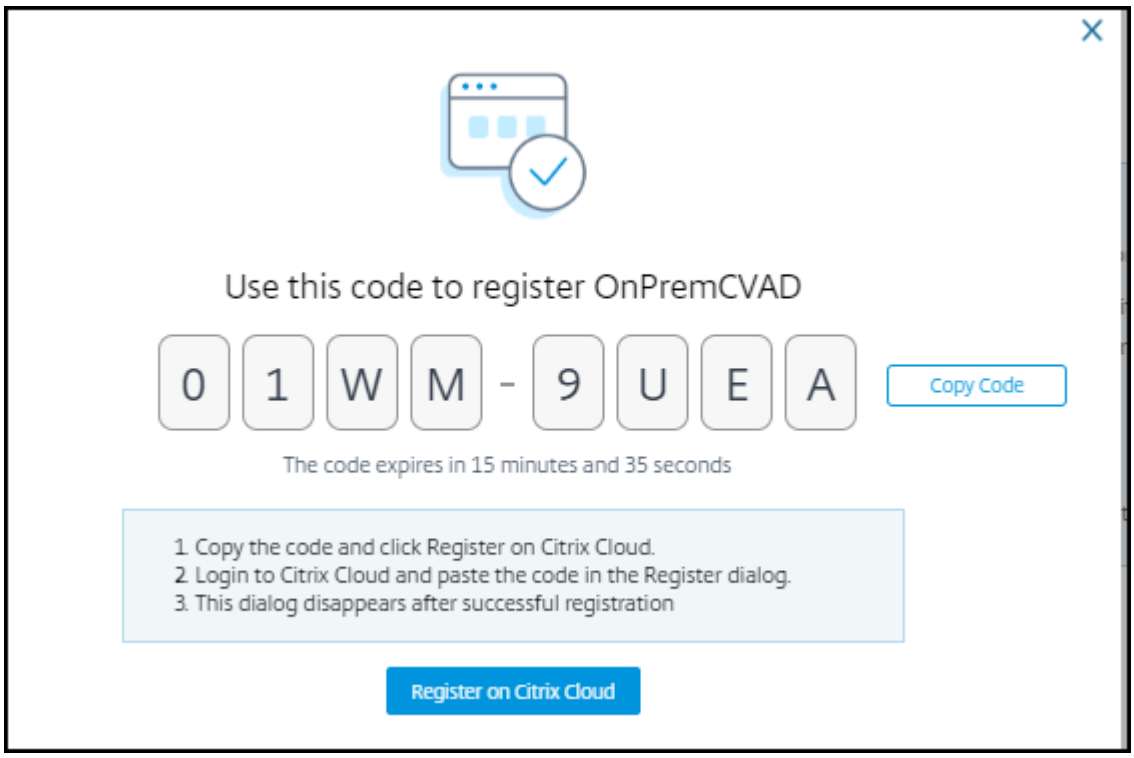


3. Revise los pasos, seleccione las condiciones de servicio y, a continuación, haga clic en **Comenzar**. Aparecerá la página **Detalles del sitio**.

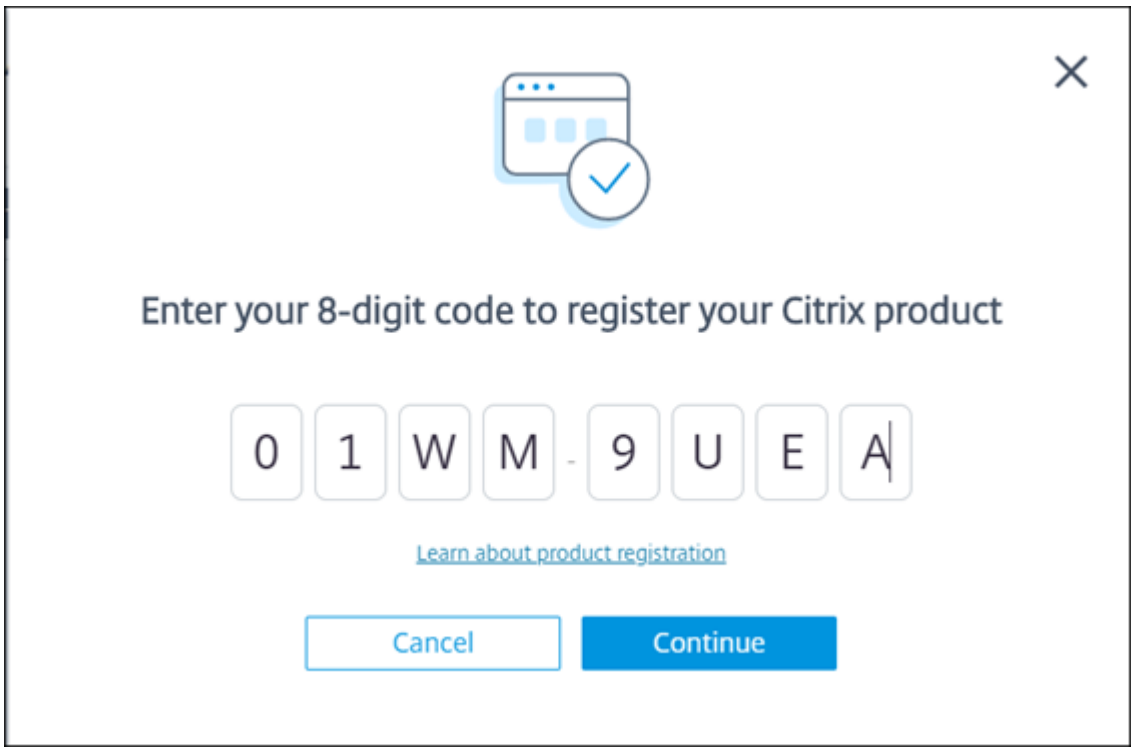


4. Revise los requisitos previos y asegúrese de que se cumplen. Revise los detalles del sitio.
5. Haga clic en **Conectar sitio** para iniciar el proceso de configuración.

   Se genera un código único de registro de 8 dígitos que se utilizará para registrar este sitio en Citrix Cloud.

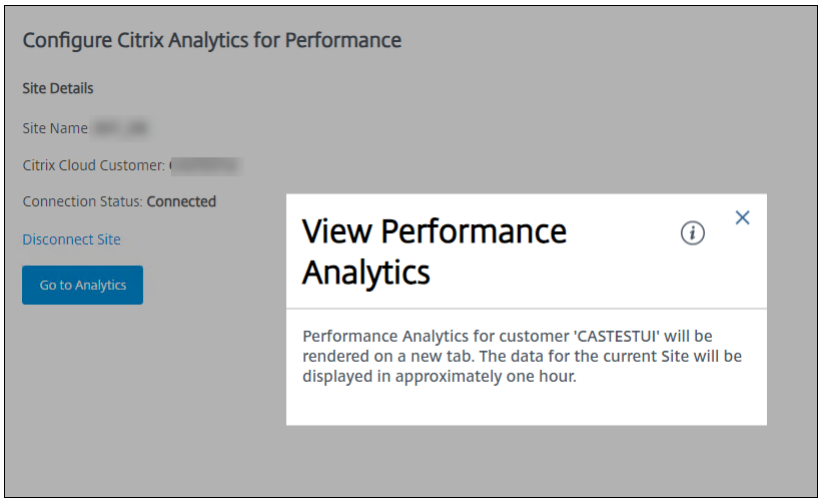


6. Haga clic en **Copiar código** para copiar el código y, a continuación, haga clic en **Registrar en Citrix Cloud**. Se le redirigirá a la URL de registro de Citrix Cloud.
7. Inicie sesión con sus credenciales de Citrix Cloud y seleccione el cliente.
8. Pegue el código de registro copiado en la página Registros de productos de Citrix Cloud. Haga clic en **Continuar** para registrarse. Revise los detalles de registro y haga clic en **Registrar**.

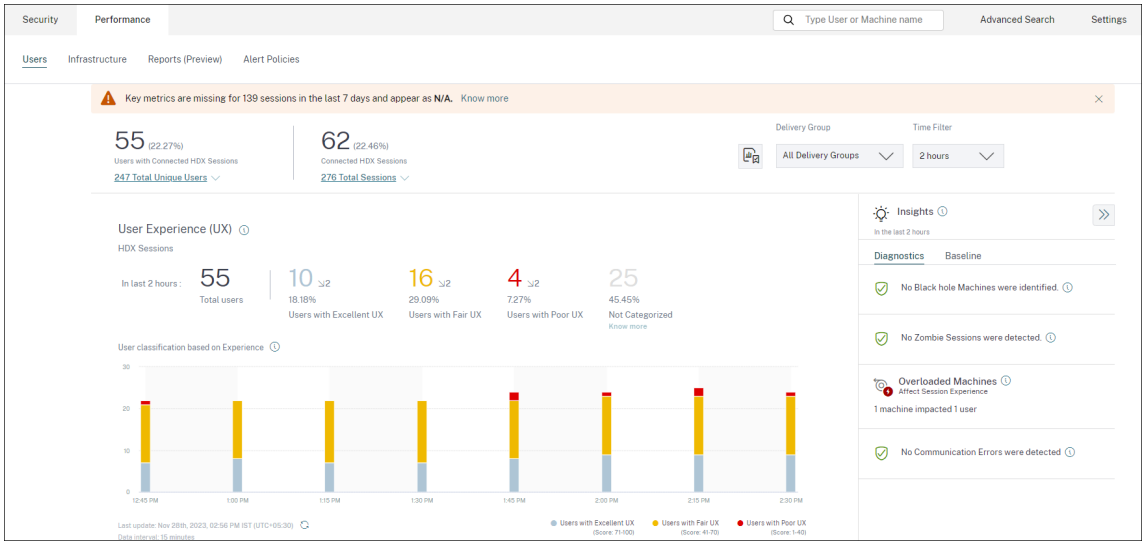


El sitio local se registra en Citrix Cloud.

9. Desde **Director**, haga clic en **Ir a Analytics**, en la ficha **Analytics**.



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.

10. 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.

    En caso de que tenga más de una instancia de Director ejecutándose por sitio, configure desde cualquier instancia de Director. Todas las demás instancias de Director conectadas al sitio se actualizan en la siguiente actualización, tras el proceso de configuración.

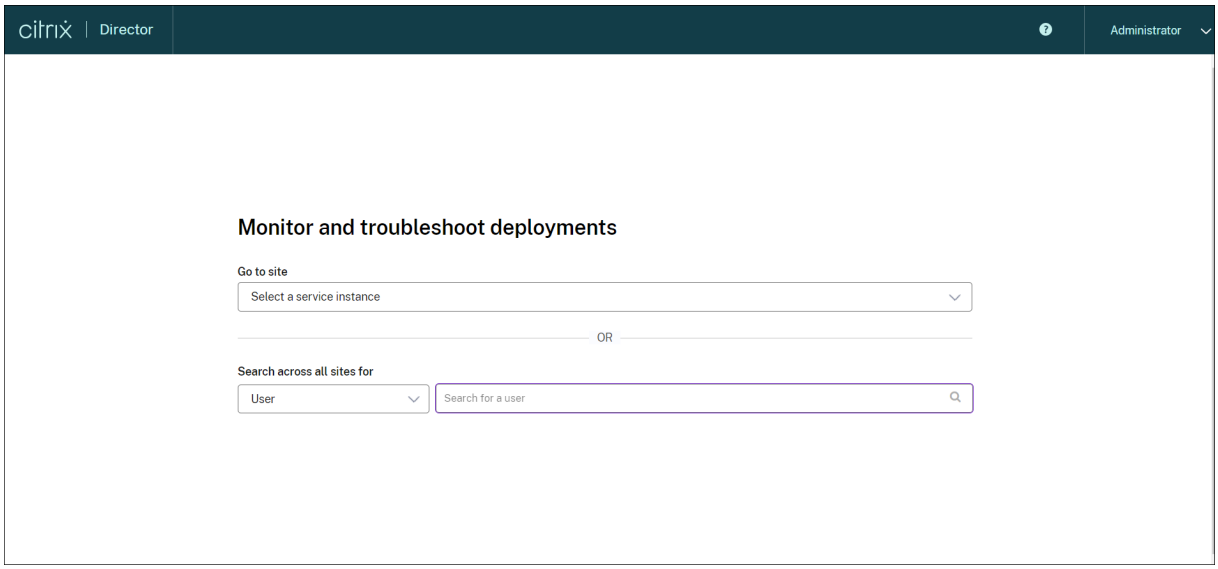
11. Para desconectar el sitio de Citrix Cloud, haga clic en **Desconectar sitio**. Esta opción elimina la configuración existente.

    > **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 utilizar Citrix Analytics Service, se tarda hasta un día en dejar de enviar las métricas del sitio al análisis de rendimiento.

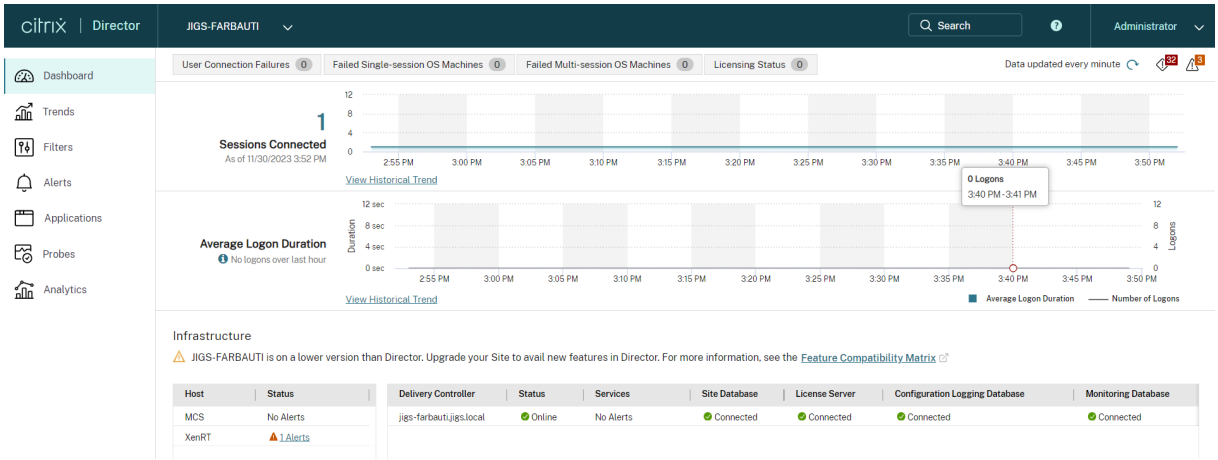
Análisis de sitios

August 17, 2024

Con Director, puede supervisar el estado de sus implementaciones. Puede solucionar los problemas de rendimiento buscando un usuario, un dispositivo de punto final o una máquina en todos los sitios incorporados.



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:**
>
> Puede que algunas opciones o funciones no estén disponibles, ya que dependen de la licencia

> que tenga su organización y de sus privilegios de administrador.

Paneles del panel de mandos de Director

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 Aplicaciones.

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.

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 **Delivery Controllers** > **Detalles** > **Ediciones de producto** > **PLT** indica **Premium** y no **Platinum**.

Estado de gracia

Director muestra uno de los siguientes estados de gracia. Esta información se obtiene del Delivery Controller.

1. **No activo:** No en ningún tipo de período de gracia. Se aplican límites normales de licencia.
2. **Gracia de emergencia:** Entra en vigor cuando el servidor de licencias es inaccesible o cuando la información de licencia no se puede obtener mientras se establece una conexión con broker. Los usuarios no se ven afectados. Los errores que se muestran en Director no se pueden descartar hasta que se pueda acceder al servidor de licencias.

3. **Gracia caducada:** El período de gracia de emergencia ha caducado.

Para obtener más información, consulte Descubierto de licencias y Período de gracia complementario.

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 Diagnosticar problemas de inicio de sesión de los usuarios.

Infraestructura

Ofrece una lista de la infraestructura de su sitio: hosts y Controllers. Para conocer la infraestructura de XenServer 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 documentación del producto XenServer.

> **Nota:**
>
> Si no aparece el icono de 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 (que se documentan en las siguientes secciones):

- 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 Restaurar sesiones.
Ver la cantidad total de sesiones conectadas en todos los grupos de entrega	En el Panel de mandos, en el panel **Sesiones conectadas**, 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 Solucionar problemas de aplicaciones.

Acción	Descripción
Ver datos para un período de tiempo más largo	En la vista "Tendencias", seleccione la ficha **Sesiones** 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 **Ver tendencias históricas**.

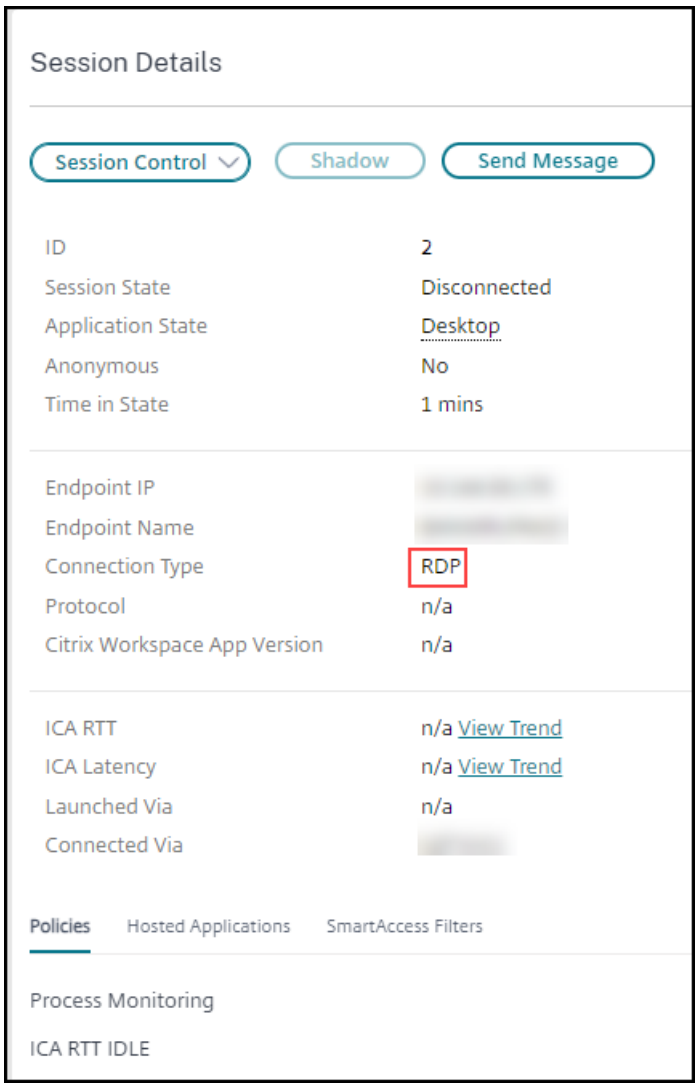
> **Nota:**
>
> Si el dispositivo del usuario ejecuta un agente Virtual Delivery Agent (VDA) antiguo (por ejemplo, un VDA anterior a la versión 7 o Linux VDA), Director no puede mostrar información completa sobre la sesión. En vez de ello, aparece un mensaje donde se indica que la información no está disponible.

Limitación de reglas de asignación de escritorios:
Web 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:

```
Get-BrokerDesktopGroup | Where-Object {
  \$\_.Uid -eq \(Get-BrokerAssignmentPolicyRule | Where-Object {
  \$\_.PublishedName -eq \"\<Name on StoreFront\>\"  }
 ).DesktopGroupUid  }
  | 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	5000
Excel	100 000	UI.ExportExcelDrilldownLimit	1 000 000

Formato del informe	Cantidad predeterminada de registros admitidos	Campos de "Configuración de aplicaciones"en Director	Cantidad máxima admitida de registros
CSV	100 000 (10 000 000 en la ficha **Sesiones**)	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 predeterminados.

> **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 deberse a problemas de red o a 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 deberse a problemas de red o a 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:

```
asnp Citrix.*
Get-MonitorConfiguration
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
Reiniciar	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.
Forzar reinicio	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.
Apagar	Realiza un cierre ordenado (estable) de la VM, y todos los procesos que se estén ejecutando se detienen uno por uno.
Forzar apagado	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.
Suspender	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.
Reanudar	Reanuda una VM que fue suspendida, devolviéndola al estado de ejecución en el que se encontraba.
Iniciar	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 este se encuentra en el modo de mantenimiento, aparecerá un mensaje indicándole que el escritorio no se encuentra disponible. No se pueden establecer nuevas conexiones hasta que se inhabilite el modo de mantenimiento.

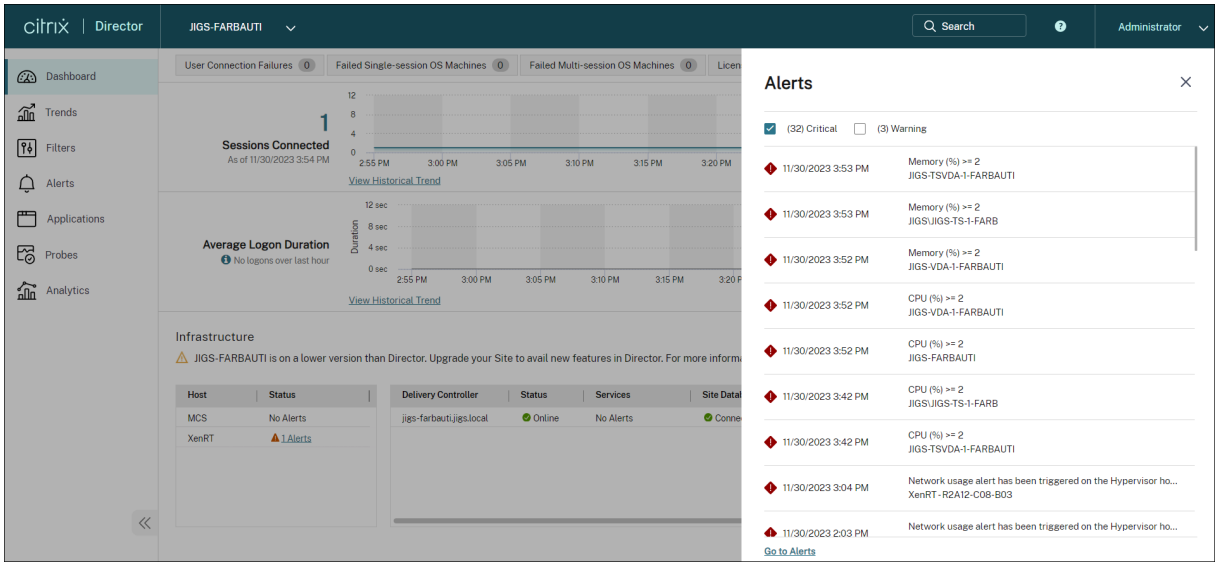
Análisis de aplicaciones

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

August 17, 2024

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.

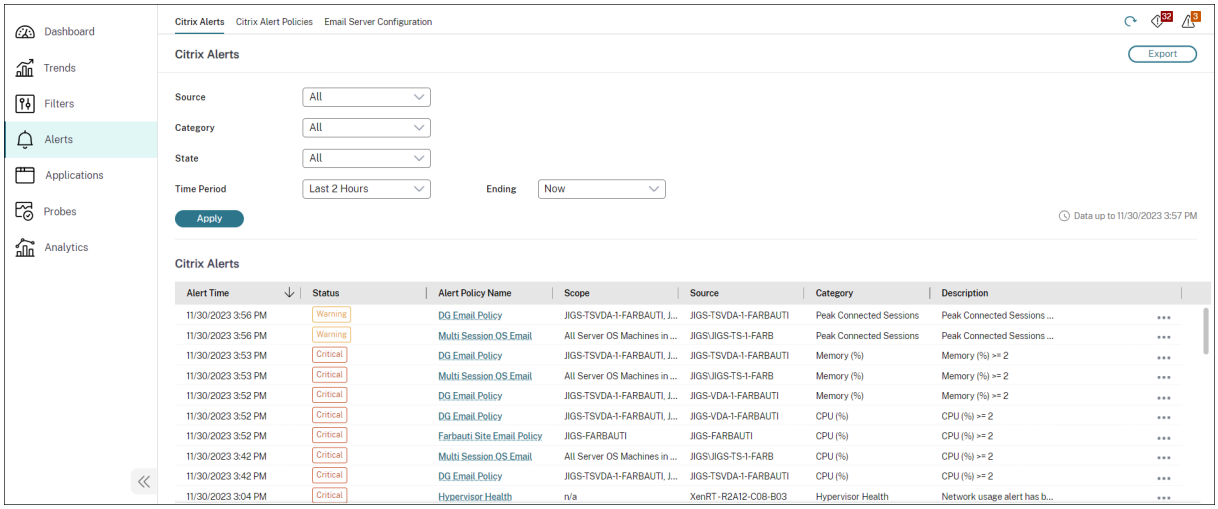


Una alerta de advertencia (un triángulo ámbar) indica que se ha alcanzado o superado el umbral de advertencia de una condición.

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.

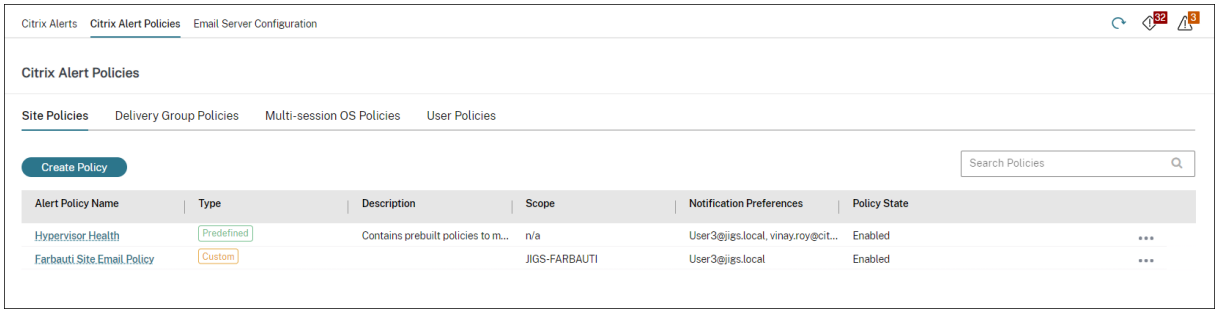
> **Nota:**
>
> Compruebe que el firewall, el proxy o Microsoft Exchange Server no bloqueen las alertas por correo electrónico.

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 Supervisar.

Para conocer los valores de umbral que tienen las directivas de alertas integradas, consulte la sección Condiciones para directivas de alertas.



Directivas de alerta avanzadas

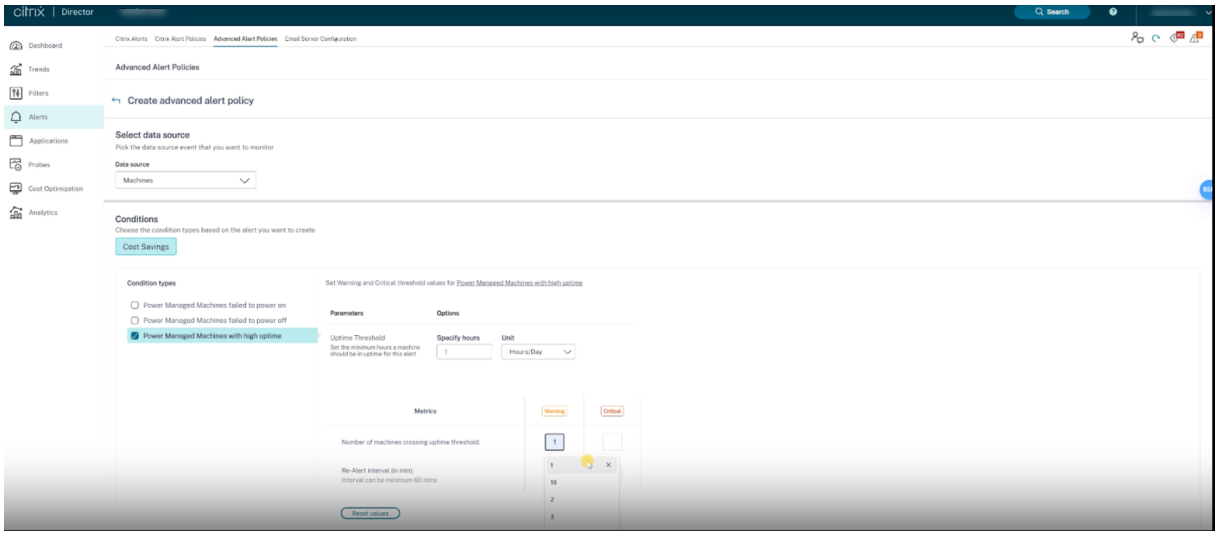
La función de notificación y alertas proactivas de Director se ha mejorado para incluir un nuevo marco de alertas denominado **Directivas de alerta avanzadas**. Con esta función, puede crear alertas al

incluir detalles granulares para cada elemento o condición, lo que mejora el control sobre el ámbito de las alertas. Actualmente, estas directivas incluyen alertas de ahorro de costes e infraestructura.

Con la introducción de las directivas de alerta avanzadas, que son alertas basadas en orígenes de datos, puede usar el filtrado de ámbito multicondición.

Esta función le ayuda a reducir el exceso de alertas, que podría reducir la capacidad de respuesta o la eficacia a la hora de abordar problemas importantes. Esta directiva ayuda a medir la eficacia de las directivas de alerta y la interacción por parte de los administradores.

Puede crear una directiva de alerta avanzada en la sección **Alertas** > **Directiva de alerta avanzada** > **Crear directiva**.



Puede seleccionar la categoría: **Las máquinas con administración de energía no se encendieron**, **Las máquinas con administración de energía no se apagaron**, **Máquinas con administración de energía con tiempo de actividad elevado** y, a continuación, seleccionar las condiciones requeridas para la directiva. Para obtener más información sobre cómo crear una directiva, consulte Crear directivas de alerta. Una vez creada la directiva, puede modificarla, eliminarla o inhabilitarla en la página Alertas de Citrix.

Puede seleccionar los parámetros específicos y las opciones correspondientes para cada una de las condiciones anteriores.

La categoría **Máquinas con administración de energía con tiempo de actividad elevado**comprueba las siguientes métricas:

- Cantidad de máquinas que superan el umbral de tiempo de actividad
- El intervalo de repetición de alerta (en minutos) puede ser 60 minutos como mínimo

Las categorías **Las máquinas con administración de energía no se encendieron** y **Las máquinas con administración de energía no se apagaron** comprueban las siguientes métricas:

- Cantidad de máquinas que superan el umbral de tiempo de actividad

- Intervalo de muestreo (en minutos) en múltiplos de 30 minutos
- Intervalo de repetición de alerta (en minutos) en múltiplos de 60 minutos

Puede establecer la gravedad de las categorías anteriores según sea necesario. También puede programar intervalos de repetición para estas alertas.

Definir el ámbito de la directiva

Puede definir el ámbito de la directiva y agregar excepciones. La alerta se genera solo para el ámbito seleccionado, y los subámbitos excluidos mediante la adición de excepciones no se incluyen en la generación de alertas. Esta función le ayuda a crear alertas de forma granular.

Puedes crear notificaciones a través de correos electrónicos o URL de webhook. También puede seleccionar el idioma en el que prefiere recibir las alertas. También puede seleccionar una opción para recibir los parámetros de alerta en un archivo adjunto CSV para correo electrónico o en una carga útil JSON a través de una URL de webhook. El archivo adjunto incluye detalles de los parámetros requeridos. Para obtener más información, consulte Mejoras en el contenido de las alertas.

Los siguientes datos se reciben como alertas por correo electrónico o en la página **Alertas de Citrix**:

Campo	Descripción
ID de cliente	El ID de cliente del sitio.
Nivel de alerta	Este es el valor predefinido establecido para cada condición de alerta. Los valores posibles son Crítico y Advertencia.
Condición	Este valor es la condición establecida al crear la directiva. Por ejemplo, la cantidad de máquinas no registradas es igual o superior a 20.
Dispositivo de destino	El nombre del sitio o grupo de entrega para el que se desencadena la alerta.
Sitio	El nombre del sitio.
Ámbito	El ámbito de la directiva. Este valor también incluye el subámbito.
Directiva	El nombre de la directiva.
Descripción	La descripción del problema por el que se desencadena la alerta.

¿Cómo crear una directiva de alerta avanzada mediante un script de PowerShell?

Script de PowerShell para crear una directiva de alerta:

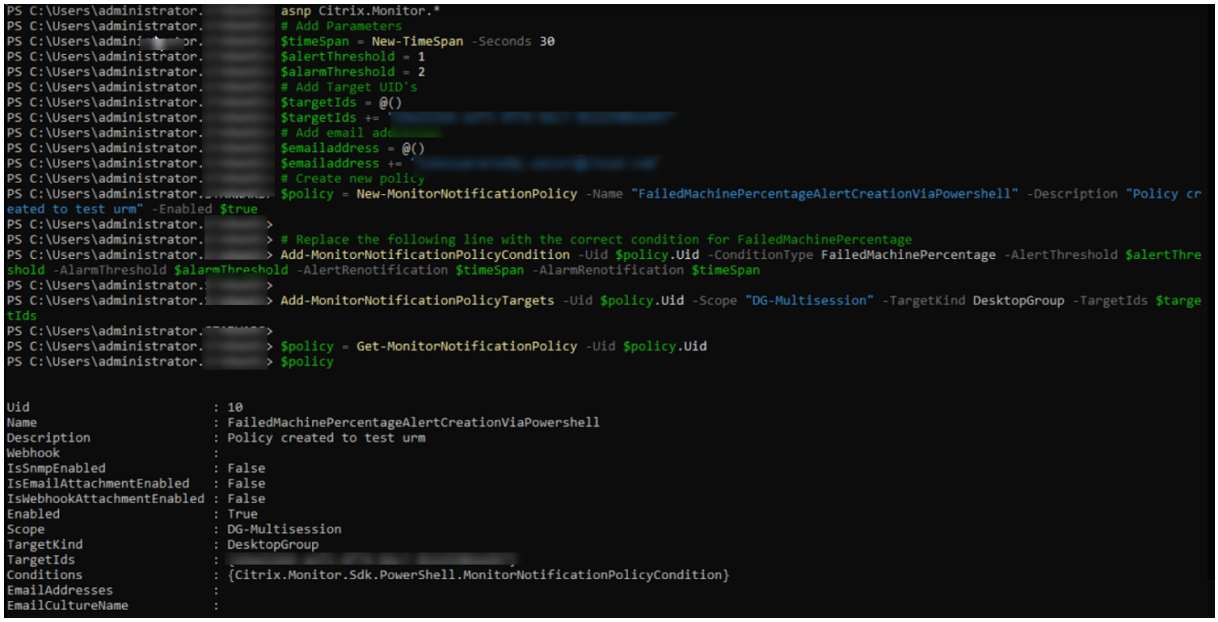
```
asnp Citrix.Monitor.*
# Add Parameters
$timeSpan = New-TimeSpan -Seconds 30
$alertThreshold = 1
$alarmThreshold = 2
# Add Target UID's
$targetIds = @()
$targetIds += "e9a211b4-a1f3-4f74-b6c7-85225902e997"
# Add email addresses
$emailaddress = @()
$emailaddress += "loki@abc.com"
# Create new policy
$policy = New-MonitorNotificationPolicy -Name "
    FailedMachinePercentageAlertCreationViaPowershell" -Description "
    Policy created to test urm" -Enabled $true
```

Sustituya la siguiente línea por la condición correcta para FailedMachinePercentage

```
Add-MonitorNotificationPolicyCondition -Uid $policy.Uid -ConditionType
    FailedMachinePercentage -AlertThreshold $alertThreshold -
    AlarmThreshold $alarmThreshold -AlertRenotification $timeSpan -
    AlarmRenotification $timeSpan

Add-MonitorNotificationPolicyTargets -Uid $policy.Uid -Scope "DG-
    Multisession" -TargetKind DesktopGroup -TargetIds $targetIds

$policy = Get-MonitorNotificationPolicy -Uid $policy.Uid
$policy
```



En la imagen anterior, puede ver que la directiva se ha creado y que el Uid es 10.

Para agregar el correo electrónico a la configuración

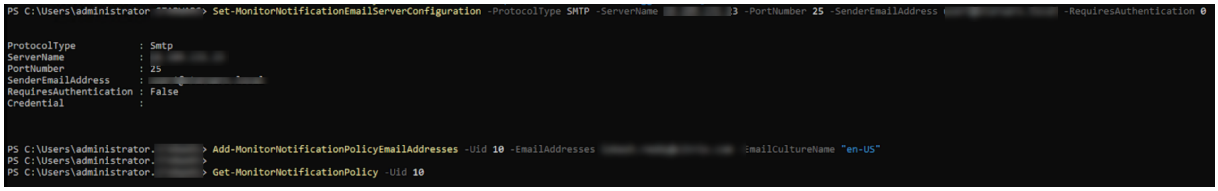
```
Set-MonitorNotificationEmailServerConfiguration -ProtocolType SMTP -
    ServerName NameOfTheSMTPServerOrIPAddress -PortNumber 80 -
    SenderEmailAddress loki@abc.com -RequiresAuthentication 0
```

Para agregar el correo electrónico a la directiva

```
Add-MonitorNotificationPolicyEmailAddresses -Uid $policy.Uid -
    EmailAddresses $emailaddress -EmailCultureName "en-US"
```

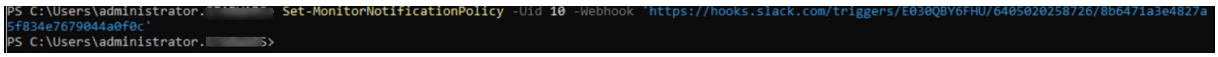
Ejemplo de script para agregar correo electrónico:

```
Add-MonitorNotificationPolicyEmailAddresses -Uid 10 -EmailAddresses
    $emailaddress -EmailCultureName "en-US"
```



Para agregar la URL de Webhook a la directiva

```
Set-MonitorNotificationPolicy  – Uid $polcy.Uid  – Webhook 'URL'
```

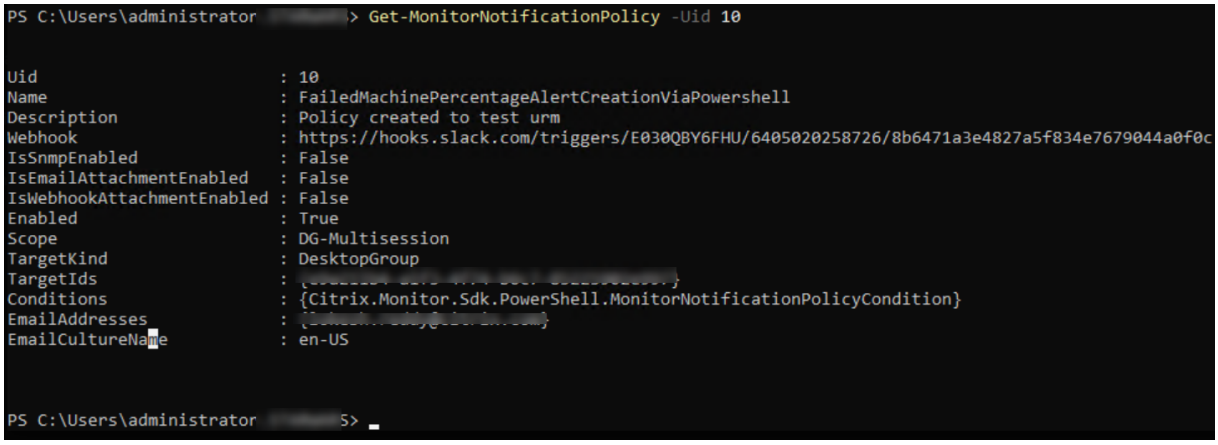


Ejemplo de script para agregar una URL de webhook:

```
Set-MonitorNotificationPolicy  – Uid 10  – Webhook  'https://hooks.slack
    .com/triggers/E030QBY6FHU/6405020258726/8
    b6471a3e4827a5f834e7679022a1f1c'
```

Obtener detalles de la directiva creada

```
Get-MonitorNotificationPolicy -Uid 10
```



Directivas de infraestructura (Technical Preview)

Estas directivas se introducen para crear alertas relacionadas con el estado de los componentes compatibles con Citrix Virtual Apps and Desktops.

Una vez completada la configuración de Supervisión de la infraestructura, puede usar los datos de estado disponibles en Director para configurar las alertas para cualquier componente requerido. Los administradores pueden establecer condiciones, ámbitos y medios de notificación para recibir alertas importantes por correo electrónico o una carga JSON a través de webhooks. Las alertas generadas también están disponibles en la sección **Alertas de Citrix** para su análisis y administración.

Como parte de la directiva de infraestructura recientemente introducida, las condiciones de alerta se clasifican en cuatro secciones de la siguiente manera:

- Accesibilidad
- Servicios dependientes
- Impacto
- Utilización de recursos

Las condiciones de cada categoría se pueden establecer con una gravedad **crítica** y de **advertencia** en función de las prioridades de la organización. También puede programar intervalos de repetición para estas alertas.

Puede crear una directiva de infraestructura en la sección **Alertas** > **Directivas de alertas de Citrix**. Puede seleccionar la categoría requerida y, a continuación, las condiciones requeridas para la directiva. Para obtener más información sobre cómo crear una directiva, consulte Crear directivas de alerta. Una vez creada la directiva, puede modificarla, eliminarla o inhabilitarla en la página Alertas de Citrix.

Para obtener más información sobre las condiciones admitidas en cada categoría y componente, consulte lo siguiente:

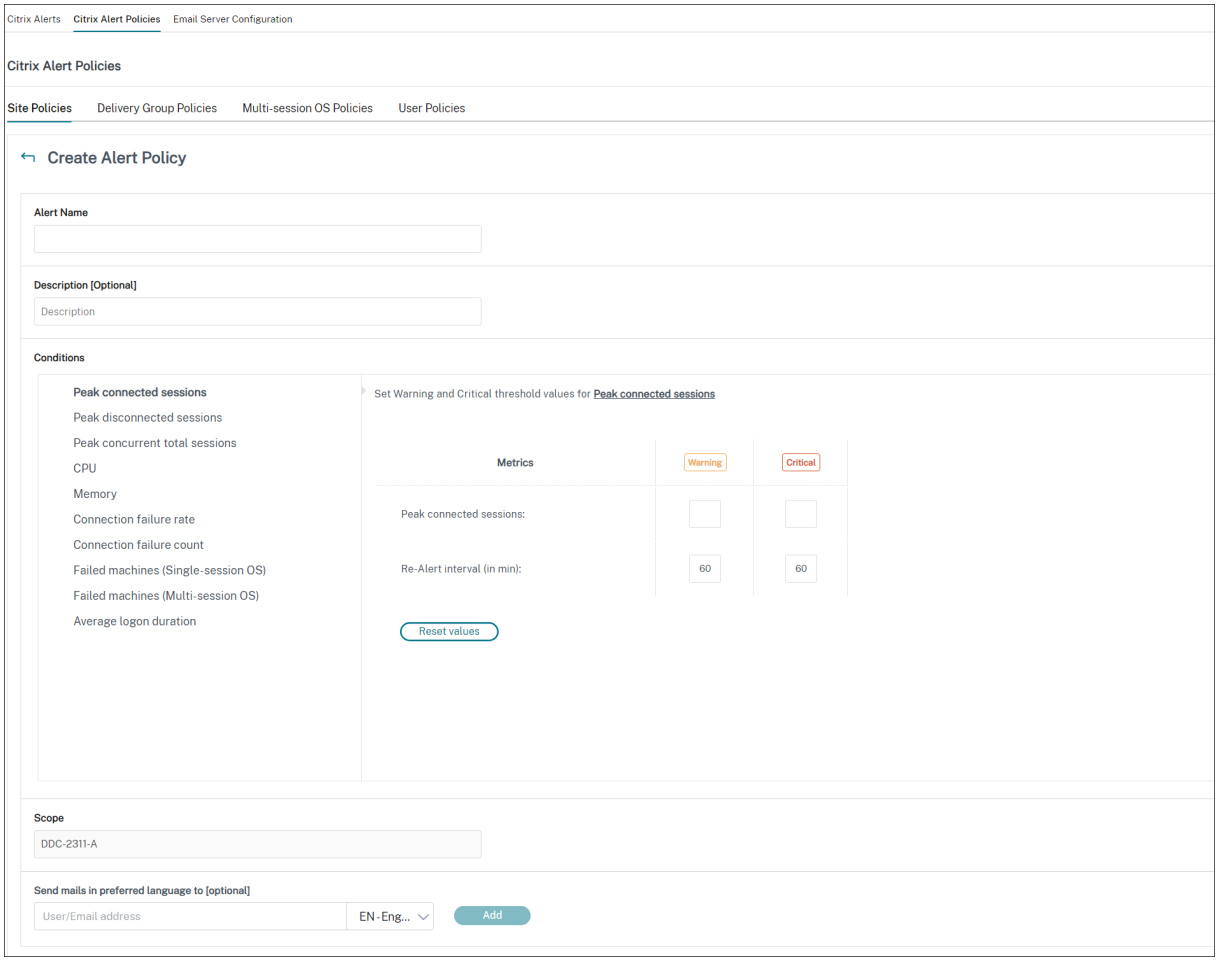
- Métricas de estado de PVS
- Métricas de estado de StoreFront

Los siguientes datos se reciben como alertas por correo electrónico o en la página de alertas de Citrix:

Campo	Descripción
ID de cliente	El ID de cliente del sitio.
Nivel de alerta	Los valores posibles son Crítico y Advertencia.
Dispositivo de destino	El nombre de la máquina para la que se desencadena la alerta.

Campo	Descripción
Hora	Hora en la que se desencadena la alerta.
Ámbito	El ámbito de la directiva.
Directiva	El nombre de la directiva.
Descripción	La descripción del problema por el que se desencadena la alerta.

Crear directivas de alertas



Para crear una directiva de alerta (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 **Configuración del servidor de correo electrónico** para poder establecer preferencias de notificación en las directivas de alertas.

    a) También puedes recibir el contenido de la alerta en un archivo adjunto CSV o a través de la carga útil JSON. Para ello, seleccione las siguientes casillas de verificación:

    - **Incluir una carga útil JSON como adjunto en el webhook**
    - **Incluir un archivo CSV como adjunto en el correo electrónico**

    > **Nota:**
    >
    > Para recibir el contenido de las alertas a través del archivo adjunto CSV y la carga útil JSON, las opciones solo están disponibles actualmente para algunas alertas. Para obtener más información, consulte Mejoras en el contenido de las 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.

> **Nota:**

> Después de eliminar una directiva de alertas, es posible que pasen hasta 30 minutos hasta que se detengan las notificaciones de alerta generadas por la directiva.

Mejoras en el contenido de las alertas

La función de alerta de Director se ha mejorado para incluir un archivo adjunto CSV y una carga útil JSON. Con esta mejora, puede obtener los detalles de las alertas en un archivo adjunto CSV por correo electrónico o como carga útil JSON si hay un webhook. Con este archivo adjunto CSV o la carga útil JSON, puede recibir contenido enriquecido de forma detallada, lo que ayuda a identificar y resolver rápidamente los problemas.

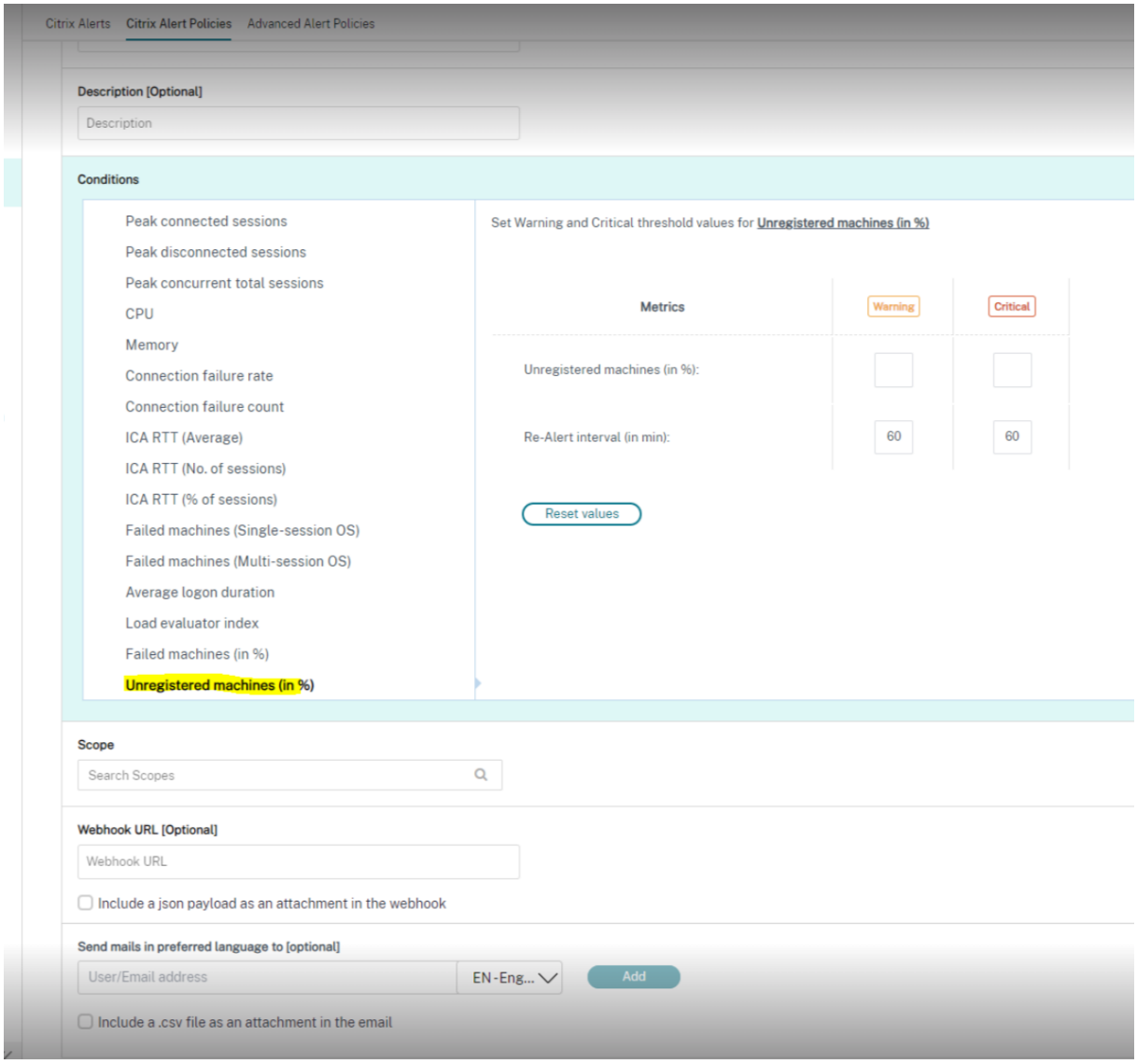
Actualmente, esta mejora solo está disponible en las siguientes alertas:

- Tiempo de actividad de máquina
- Acciones de encendido fallidas
- Acciones de apagado fallidas
- Máquinas no registradas (en %)

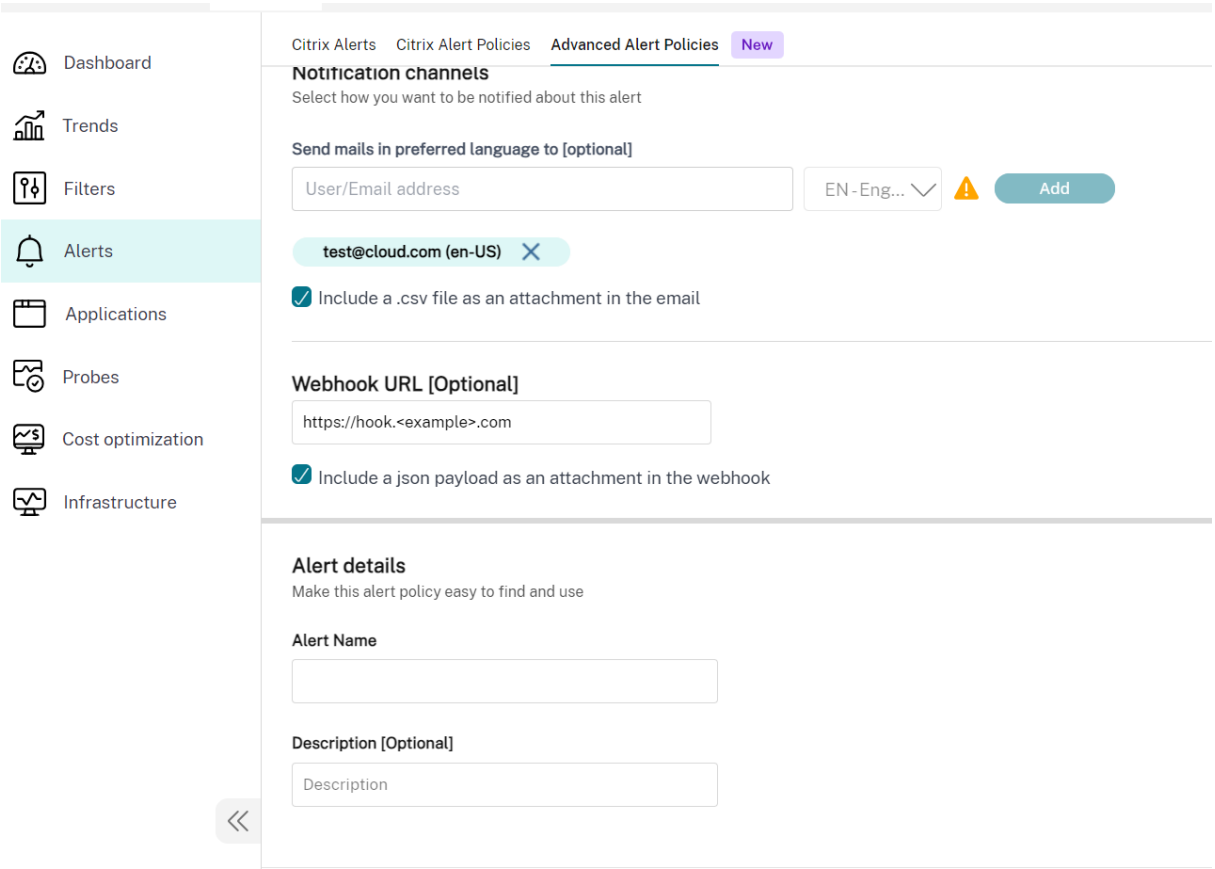
Para usar esta función, vaya a la alerta y seleccione las siguientes casillas de verificación:

- **Incluir una carga útil JSON como adjunto en el webhook**
- **Incluir un archivo CSV como adjunto en el correo electrónico**

A continuación, se muestra una captura de pantalla de la sección **Directivas de alertas de Citrix**:



Esta es una captura de pantalla de la sección **Directivas de alerta avanzadas**:



Adjunto CSV En la siguiente tabla se muestran las columnas del archivo adjunto CSV para todas las alertas admitidas:

Columna	Alerta aplicable
Nombre de la máquina, dirección IP y nombre del grupo de entrega	Tiempo de actividad de la máquina, acción de apagado fallida, acción de encendido fallida y máquinas no registradas (en %)
Estado de registro actual, fecha del fallo, estado de fallo y estado del ciclo de vida	Máquinas no registradas (en %)
Motivo del último fallo de la última acción de energía, última acción de energía desencadenada por, tipo de última acción de energía y fecha de finalización de la última acción de energía	Acción de apagado fallida y acción de encendido fallida
Estado de energía, fecha de encendido y total de tiempo de actividad en minutos	Tiempo de actividad de máquina

Carga útil de webhook

Alerta de porcentaje de máquinas no registradas

```
Webhook Payload
{

    "Address": "<Webhook URL>",
    "NotificationId": "<NotificationGUID>",
    "NotificationState": "NotificationActive",
    "Priority": "<Critical/Warning>",
    "Target": "<DeliveryGroupName>",
    "Condition": "Unregistered machines (in %)",
    "Value": "<Value Set as Threshold>",
    "Timestamp": "<Timestamp string Eg: April 25, 2024 9:33 PM (UTC +5)
       >",
    "PolicyName": "<Alert Policy Name>",
    "Description": "<Alert Policy Description>",
    "Scope": "DeliveryGroup",
    "Site": "<Name of the Site>",
    "AttachmentData": [{

                                        "Machine Name": "<Name of the
                                           Machine>",
                                        "IP Address": “ <IP Address>” ,
                                        "Delivery Group Name": "<Name of
                                           the DeliveryGroup>",
                                        "Current Registration State": "
                                           Unregistered",
                                        "Failure Date": “ <Date of
                                           Failure>” ,
                                        "Fault State": "<Fault State of
                                           the Machine>",
                                        "Lifecycle State": "<Lifecycle
                                           state of the Machine>"
                                    }
 ,
                                   {

                                        "Machine Name": "<Name of the
                                           Machine>",
                                        "IP Address": “ <IP Address>” ,
                                        "Delivery Group Name": "<Name of
                                           the DeliveryGroup>",
                                        "Current Registration State": "
                                           Unregistered",
                                        "Failure Date": “ <Date of
                                           Failure>” ,
                                        "Fault State": "<Fault State of
                                           the Machine>",
                                        "Lifecycle State": "<Lifecycle
                                           state of the Machine>"
                                    }
 ]
```



```
}
```

Alerta de acciones de encendido fallidas

```
Webhook Payload Body
{

    "Address": "<Webhook URL>",
    "NotificationId": "<NotificationGUID>",
    "NotificationState": "NotificationActive",
    "Priority": "<Critical/Warning>",
    "Target": "<DeliveryGroupName>",
    "Condition": "Failure To PowerOn Action",
    "Value": "<Value Set as Threshold>",
    "Timestamp": "<Timestamp string Eg: April 25, 2024 9:33 PM (UTC +5)
       >",
    "PolicyName": "<Alert Policy Name>",
    "Description": "<Alert Policy Description>",
    "Scope": "DeliveryGroup",
    "Site": "<Name of the Site>",
    "AttachmentData": [{

                                        "Machine Name": "<Name of the
                                           Machine>",
                                        "IP Address": " <IP Address> " ,
                                        "Delivery Group Name": "<Name of
                                           the DeliveryGroup>",
                                       "Last Power Action Failure Reason"
                                          : "<HypervisorReportedFailure,
                                          HypervisorRateLimitExceeded,
                                          UnknownError,Power Action Type>
                                          ",
                                        "Last Power Action Triggered By":
                                            "<End-User,Administrator,Auto
                                           -Scale,Schedule>",
                                        "Last Power Action Type": " <
                                           PowerOn/PowerOff> " ,
                                        "Last Power Action Completed Date
                                           ": "<Time string Eg:
                                           2024-05-15T15:04:27.723>",
                                    {

                                        "Machine Name": "<Name of the
                                           Machine>",
                                        "IP Address": " <IP Address> " ,
                                        "Delivery Group Name": "<Name of
                                           the DeliveryGroup>",
                                        "Last Power Action Failure Reason
                                           ": "<HypervisorReportedFailure
                                           ,HypervisorRateLimitExceeded,
                                           UnknownError,Power Action Type
                                           >",
                                        "Last Power Action Triggered By":
                                            "<End-User,Administrator,Auto
```



```
                                        -Scale,Schedule>",
                                    "Last Power Action Type": " <
                                        PowerOn/PowerOff> " ,
                                    "Last Power Action Completed Date
                                        ": "<Time string Eg:
                                        2024-05-15T15:04:27.723>"
                                }
    ]
    }
```

Alerta de acciones de apagado fallidas

```
{

    "Address": "<Webhook URL>",
    "NotificationId": "<NotificationGUID>",
    "NotificationState": "NotificationActive",
    "Priority": "<Critical/Warning>",
    "Target": "<DeliveryGroupName>",
    "Condition": "Failure To PowerOff Action",
    "Value": "<Value Set as Threshold>",
    "Timestamp": "<Timestamp string Eg: April 25, 2024 9:33 PM (UTC +5)
        >",
    "PolicyName": "<Alert Policy Name>",
    "Description": "<Alert Policy Description>",
    "Scope": "DeliveryGroup",
    "Site": "<Name of the Site>",
    "AttachmentData": [{

                                    "Machine Name": "<Name of the
                                        Machine>",
                                    "IP Address": " <IP Address> " ,
                                    "Delivery Group Name": "<Name of
                                        the DeliveryGroup>",
                                    "IP Address": "<IPV4 Address of
                                        the Machine>",
                                    "Last Power Action Failure Reason
                                        ": "<HypervisorReportedFailure
                                        ,HypervisorRateLimitExceeded,
                                        UnknownError,Power Action Type
                                        >",
                                    "Last Power Action Triggered By":
                                         "<End-User,Administrator,Auto
                                        -Scale,Schedule>",
                                    "Last Power Action Type": " <
                                        PowerOn/PowerOff> " ,
                                    "Last Power Action Completed Date
                                        ": "<Time string Eg:
                                        2024-05-15T15:04:27.723>"
                                }
    ,
                                {

                                    "Machine Name": "<Name of the
```



```
                                        Machine>",
                                    "IP Address": " <IP Address> " ,
                                    "Delivery Group Name": "<Name of
                                        the DeliveryGroup>",
                                    "IP Address": "<IPV4 Address of
                                        the Machine>",
                                   "Last Power Action Failure Reason"
                                       : "<HypervisorReportedFailure,
                                       HypervisorRateLimitExceeded,
                                       UnknownError,Power Action Type>
                                       ",
                                    "Last Power Action Triggered By":
                                        "<End-User,Administrator,Auto
                                        -Scale,Schedule>",
                                    "Last Power Action Type": " <
                                        PowerOn/PowerOff> " ,
                                    "Last Power Action Completed Date
                                        ": "<Time string Eg:
                                        2024-05-15T15:04:27.723>"
                                }
 ]
 }
```

Alerta de tiempo de actividad de máquina

```
{

    "Address": "<Webhook URL>",
    "NotificationId": "<NotificationGUID>",
    "NotificationState": "NotificationActive",
    "Priority": "<Critical/Warning>",
    "Target": "<DeliveryGroupName>",
    "Condition": "Machine Uptime Alert",
    "Value": "<Value Set as Threshold>",
    "Timestamp": "<Timestamp string Eg: April 25, 2024 9:33 PM (UTC +5)
        >",
    "PolicyName": "<Alert Policy Name>",
    "Description": "<Alert Policy Description>",
    "Scope": "DeliveryGroup",
    "Site": "<Name of the Site>",
    "AttachmentData": [{

                                    "Machine Name": "<Name of the
                                        Machine>",
                                    "IP Address": " <IP Address> " ,
                                    "Delivery Group Name": "<Name of
                                        the DeliveryGroup>",
                                    "IP Address": "<IPV4 Address of
                                        the Machine>",
                                    "Power State": "<On/Off>",
                                    "Powered On Date": "Time sting Eg
                                        : 2024-05-15T15:04:27.723",
                                    "Total Uptime In Minutes": 180
                                }
```



```
25  ,
26                                  {
27
28                                      "Machine Name": "<Name of the
                                           Machine>",
29                                      "IP Address": “ <IP Address>” ,
30                                      "Delivery Group Name": "<Name of
                                           the DeliveryGroup>",
31                                      "IP Address": "<IPV4 Address of
                                           the Machine>",
32                                      "Power State": "<ON/OFF>",
33                                      "Powered On Date": "<Time string
                                           Eg: 2024-05-15T15:04:27.723>",
34                                      "Total Uptime In Minutes": <
                                           Uptime Duration>
35                                   }
36  ]
37  }
```

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.

  Condiciones para directivas inteligentes:

  - **Ámbito:** Grupo de entrega, SO multisesión
  - **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)

Máquinas fallidas (en %)

El porcentaje de máquinas con sistema operativo de sesión única y multisesión que han fallado en un grupo de entrega en función del número de máquinas que han fallado. Esta condición de alerta le permite configurar los umbrales de alerta como un porcentaje de máquinas fallidas de un grupo de entrega y se calcula cada 30 segundos.
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.

Acción de encendido fallida y acción de apagado fallida

La cantidad de acciones de encendido fallidas y la cantidad de acciones de apagado fallidas en un grupo de entrega se calculan en función de la cantidad de **Máquinas con administración de energía** que no se encendieron o apagaron. Esta condición de alerta le permite configurar umbrales como la cantidad de **Máquinas con administración de energía** que no se encendieron o apagaron en un grupo de entrega y se calcula cada 30 minutos.

El administrador puede configurar los siguientes parámetros para estas alertas en la directiva de alerta avanzada:

- Desencadenado por: Qué desencadenó la acción de energía
- Motivo del fallo: Por qué falló la acción

- Umbral: Cantidad límite de máquinas en las que falló la acción de energía para desencadenar la directiva
- Intervalo de muestreo: El intervalo en el que se debe comprobar la acción de energía fallida
- Intervalo entre repeticiones de alertas: La cantidad de tiempo tras la cual se debe enviar de nuevo la alerta

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.

Máquinas no registradas (en %)

Se considera que una máquina no está registrada cuando se vuelve inestable debido a un reinicio o cuando hay un problema de comunicación entre el Delivery Controller y las máquinas virtuales. El valor de **Máquinas no registradas (en %)** es el porcentaje de máquinas con sistema operativo de sesión única y multisesión no registradas en un grupo de entrega, calculado en función de la cantidad de máquinas no registradas. Esta condición de alerta le permite configurar los valores de umbral crítico y de advertencia como un porcentaje de máquinas no registradas en un grupo de entrega. Puede establecer un intervalo para repetición de alerta. También puede agregar una dirección de correo electrónico para recibir una notificación cuando se cumplan las condiciones para **Máquinas no registradas (en %)**. Cuando se supera el valor del umbral crítico o de advertencia, se generan alertas y correos electrónicos. Puede ver las alertas en **Alertas de Citrix**. Puede filtrar por categoría de **Máquinas no registradas (en %)** y por el estado y tiempo requeridos.

También puede recibir los detalles de la alerta en un archivo CSV adjunto en caso del correo electrónico o mediante una carga JSON en caso de un webhook.

> **Nota:**
>
> El valor crítico debe ser mayor que el valor de advertencia.

Condiciones de directiva:

- **Ámbito**: Grupo de entrega con SO de sesión única y SO multisesión
- **Valores de umbral**: Advertencia y Crítico

Alerta de tiempo de actividad de máquina

El tiempo de actividad de máquina en un grupo de entrega se calcula en función del número de horas por día, horas por semana u horas por mes de una máquina que está encendida en un grupo de entrega. Esta condición de alerta le permite configurar los umbrales de alerta según las horas en que una máquina está encendida en un grupo de entrega. Las alertas de tiempo de actividad de máquina funcionan de la siguiente manera en caso de:

- Horas por día: Puede especificar la cantidad de horas que una máquina permanece encendida durante un día y se calcula cada 30 minutos. La cantidad máxima de horas por día que puede establecer es de 24 horas.
- Horas por semana: Puede especificar la cantidad de horas que una máquina permanece encendida durante una semana y se calcula cada seis horas. La cantidad máxima de horas por semana que puede establecer es de 168 horas.
- Horas por mes: Puede especificar la cantidad de horas que una máquina permanece encendida durante un mes y se calcula una vez al día. La cantidad máxima de horas por mes es de 720 horas.

  El valor mínimo del intervalo de repetición de alerta que puede establecer es de 60 minutos. Puede introducir la cantidad de máquinas que superan el valor límite de tiempo de actividad de máquina en la sección de alertas críticas y de advertencia. También puede agregar excepciones para cualquier máquina.

Por ejemplo, si se han agregado cinco grupos de entrega para una alerta y si en el primer grupo de entrega y en el cuarto grupo de entrega el número de máquinas supera los valores del umbral crítico o de advertencia, la alerta se activa por separado para el primer grupo de entrega y para el cuarto grupo de entrega.

Esta alerta ayuda a los administradores a analizar el tiempo de actividad de las máquinas y, basándose en este análisis, a optimizar el coste. También puede recibir los detalles de la alerta en un archivo CSV adjunto en caso del correo electrónico o mediante una carga JSON en caso de un webhook.

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%)

Configurar directivas de alertas con webhooks

Además de las notificaciones por correo electrónico, puede configurar directivas de alertas con webhooks.

Nota: Esta función requiere Delivery Controllers de la versión 7.11 o posterior.

Puede configurar una directiva de alertas con una respuesta HTTP o un POST HTTP mediante cmdlets de PowerShell. Se han ampliado para permitir el uso de webhooks.

Para obtener información sobre cómo crear un nuevo flujo de trabajo de Octoblu y obtener la URL de webhook correspondiente, consulte Octoblu Developer Hub.

Si quiere configurar una URL de webhook para una directiva de alertas nueva o ya existente, use los siguientes cmdlets de PowerShell.

Crear una directiva de alertas con una URL de webhook:

```
$policy = New-MonitorNotificationPolicy -Name <Policy name> -
    Description <Policy description> -Enabled $true -Webhook <Webhook
    URL>
```

Agregar una URL de webhook a una directiva de alertas:

```
Set-MonitorNotificationPolicy - Uid <Policy id> -Webhook <Webhook URL>
```

Para ver la ayuda de los comandos de PowerShell, escriba, por ejemplo:

```
Get-Help  <Set-MonitorNotificationPolicy>
```

Las notificaciones que se generan a partir de la directiva de alertas activan el webhook con una llamada POST a la URL de webhook. El mensaje POST contiene la información de notificación en el formato JSON:

```
{
```



```
 "NotificationId" : \<Notification Id\>,

"Target" : <Notification Target Id>,

"Condition" : <Condition that was violated>,

"Value" : <Threshold value for the Condition>,

"Timestamp": <Time in UTC when notification was generated>,

"PolicyName": <Name of the Alert policy>,

"Description": <Description of the Alert policy>,

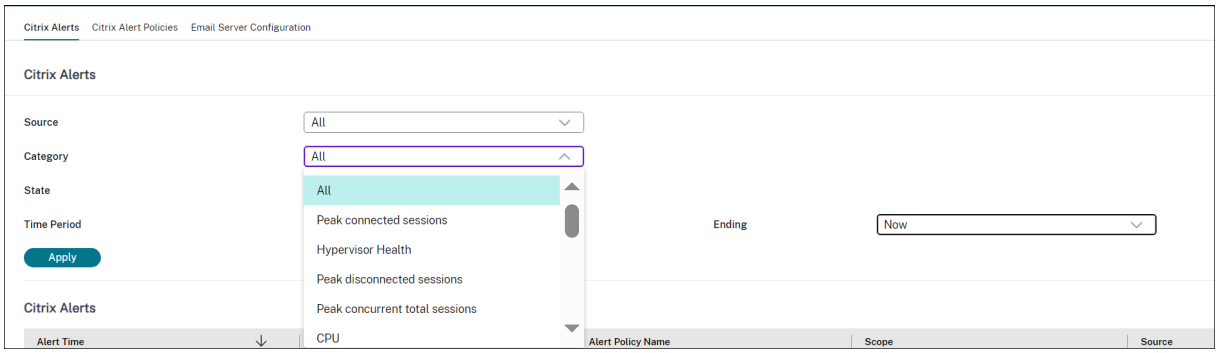
"Scope" : <Scope of the Alert policy>,

"NotificationState": <Notification state critical, warning, healthy or
   dismissed>,

"Site" : \<Site name\> }
```

Supervisar alertas de hipervisor

Director muestra alertas para supervisar el estado del hipervisor. Las alertas de XenServer 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.

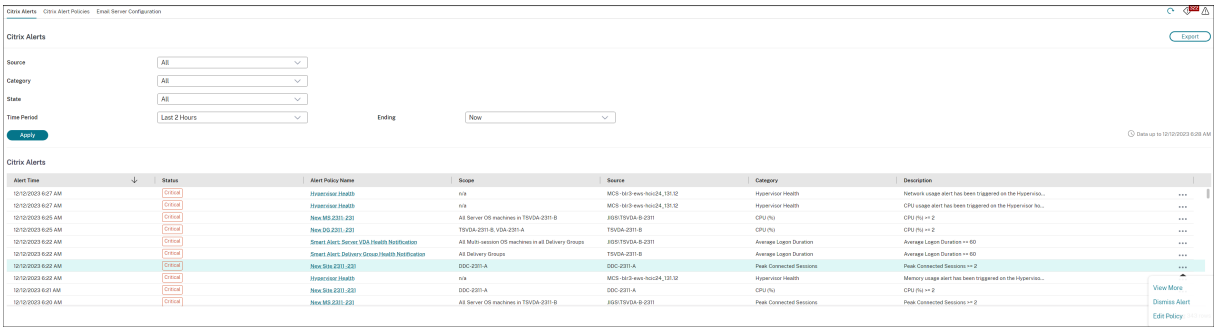


Para recibir las alertas de hipervisor, compruebe que se haya creado una conexión de alojamiento en Web Studio. Para obtener más información, consulte Conexiones y recursos. Solo se supervisan estas conexiones para las alertas de hipervisor.

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.

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	XenServer, VMware vSphere	Hypervisor	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	XenServer, VMware vSphere	Hypervisor	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	XenServer, VMware vSphere	Hypervisor	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	Hypervisor	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	Hypervisor	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	XenServer, 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 XenCenter 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. Puede inhabilitar la alerta si su rol no implica supervisar la infraestructura.

> **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 Hypervisor.

Filtrar datos para solucionar fallos

August 17, 2024

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. Asimismo, 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**. Filtre las sesiones por diferentes períodos de tiempo, incluidos los últimos 60 minutos, las últimas 24 horas, los últimos 7 días o un período de tiempo personalizado. 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. Haga clic en el **Usuario asociado** para abrir el Administrador de actividades del usuario. Al hacer clic en el nombre del **dispositivo de punto final**, se abre el Administrador de actividades del dispositivo de punto final. Al hacer clic en **Ver detalles**, se abre la página **Detalles del usuario** o **Detalles del dispositivo de punto final**, respectivamente. Para obtener más información, consulte Detalles del usuario.
    - **Conexiones**. Filtre las conexiones por diferentes períodos de tiempo, incluidos los últimos 60 minutos, las últimas 24 horas, los últimos 7 días o un período de tiempo personalizado.
    - **Instancias de aplicación**. Filtre las instancias de la aplicación por diferentes períodos de tiempo, incluidos los últimos 60 minutos, las últimas 24 horas, los últimos 7 días o un período de tiempo personalizado. 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, si es necesario, para solucionar problemas más complejos.
5. Guarde el filtro y cámbiele el nombre.
6. Para acceder a los filtros desde varios 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 configurar, ejecute **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 Motivos de fallo y solución de problemas en Citrix Director.
11. En la vista **Máquinas**, haga clic en un enlace del nombre de la máquina para ir a la página **Detalles de la máquina** correspondiente. 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 la instancia de aplicación inactiva 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:**
> Web 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:

```
Get-BrokerDesktopGroup | Where-Object {
  $_.Uid -eq (Get-BrokerAssignmentPolicyRule | Where-Object {
  $_.PublishedName -eq "<Name on StoreFront>"  }
 ).DesktopGroupUid  }
  | Select-Object -Property Name, Uid
```

Supervisar tendencias históricas en un sitio

August 17, 2024

En la vista "Tendencias", se accede a información histórica sobre tendencias de cada sitio con relación a los siguientes parámetros:

- sesiones
- fallos de conexión
- fallos de máquinas
- rendimiento de los inicios de sesión
- patrones de carga
- administración de la capacidad

- uso de máquinas
- utilización de recursos
- 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, acercar el 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 quién o qué resulta afectado.

Para cambiar el ámbito predeterminado de cada gráfico, aplique un filtro distinto a los datos.

Elija un período de tiempo para el que necesite información histórica de 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. Para el período de tiempo "Último mes"(con una fecha de finalización personalizada) o "Último año", la información de tendencias se representa en gráficos, 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.
> - Estos parámetros del Administrador de IIS controlan el intervalo de las fechas de finalización personalizadas que se pueden seleccionar. 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 de clientes 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 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. También analiza las redes que tienen una experiencia fluida. 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 de Citrix Gateway.

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. También puede exportar estos informes a un archivo.CSV.
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**. Seleccione el grupo de entrega y el período de tiempo para ver un gráfico con el uso simultáneo máximo y una tabla que muestra el uso por 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 con 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 con 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 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 di-

> rectiva está establecida en **Prohibida**. De forma predeterminada, se recopilan los datos referentes al uso de recursos. Se pueden inhabilitar mediante la directiva **Habilitar supervisión de recursos**. La tabla situada bajo los gráficos muestra los datos de utilización de recursos por máquina. Para obtener más información, consulte Configuraciones de directiva de Supervisión.
> - 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.)
> - El desglose de las máquinas muestra procesos con el uso medio de CPU o de memoria que sea superior al 1 %, lo que podría significar que, a veces, aparecen menos de 10 procesos en la lista.

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 de la **versión 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: En la ficha **Resultados del sondeo**, se muestran los resultados del sondeo de las aplicaciones y los escritorios 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.

Para obtener más información, consulte Sondeo de aplicaciones y escritorios.

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 de la **versión 7.12** o de una versión 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 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.

Supervisar máquinas administradas con Autoscale

August 17, 2024

Autoscale es una función de administración de energía que permite administrar de forma proactiva la energía de todas las máquinas de SO de sesión única y de SO multisesión registradas en un grupo de entrega. Puede configurar Autoscale para un grupo de entrega seleccionado en Web Studio. Para

obtener más información, consulte Autoscale.
Puede supervisar las métricas clave de las máquinas habilitadas para Autoscale mediante Director.

Uso de máquinas

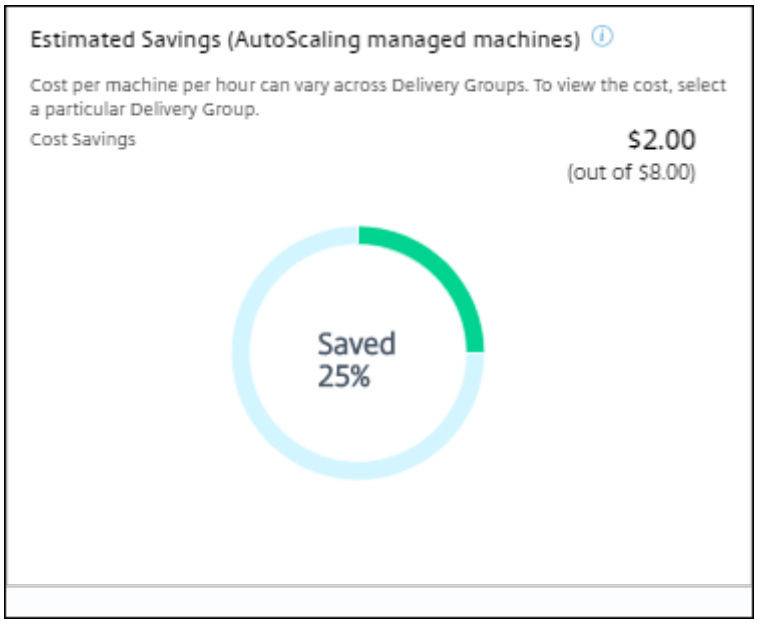
La página **Uso de máquinas** muestra la cantidad total de máquinas encendidas con SO de sesión única y SO multisesión con Autoscale habilitado para un grupo de entrega y un período de tiempo determinados. Esta métrica indica el uso real de las máquinas que hay en el grupo de entrega.
En la ficha **Máquinas con SO de sesión única** o en la ficha **Máquinas con SO multisesión**, seleccione el grupo de entrega y el período de tiempo.

El gráfico indica las siguientes métricas:

- **Máquinas encendidas**: La cantidad de máquinas con Autoscale habilitado que están encendidas.
- **Máquinas registradas**: La cantidad de máquinas de SO de sesión única o de SO multisesión registradas.
- **Máquinas en mantenimiento**: La cantidad de máquinas de SO de sesión única o de SO multisesión con el modo de mantenimiento activado.

Ahorro estimado

La página **Uso de máquinas** también muestra una estimación del ahorro de costes logrado al habilitar Autoscale en el grupo de entrega seleccionado.



El ahorro estimado se calcula como el porcentaje de ahorro por máquina y hora (en USD) configurado en **Modificar grupo de entrega** > **Autoscale**. Para obtener más información sobre cómo configurar los ahorros por máquina, consulte Autoscale.

Al seleccionar todos los grupos de entrega, se muestra el valor medio del ahorro estimado para todos los grupos de entrega.

El ahorro estimado ayuda a los administradores a consolidar la infraestructura existente y a planificar la capacidad para maximizar el ahorro y el uso.

Notificaciones de alerta para máquinas y sesiones

El panel de mandos Director muestra notificaciones de alerta que se pueden detallar más. La información detallada de las alertas aparece en la página **Alertas**.

- Para crear una directiva de alerta en un grupo de entrega, vaya a **Alertas** > **Directiva de alertas de Citrix** > **Directiva de grupo de entrega**.
- Aquí puede establecer los siguientes umbrales de advertencia y aviso crítico:
  - Máquinas fallidas (SO de sesión única) y Máquinas fallidas (SO multisesión),
  - Máximo de sesiones conectadas, máximo de sesiones desconectadas y máximo total de sesiones simultáneas en el grupo de entrega.
- Las alertas se generan cuando la métrica correspondiente del grupo de entrega alcanza el umbral.

Para obtener información detallada sobre las condiciones de la directiva de alertas y la creación de directivas de alerta, consulte Alertas y notificaciones.

Estado de la máquina

- **Filtros** > **Máquinas** muestra el estado de energía de todas las máquinas en formato tabular. Puede filtrar por un grupo de entrega específico.
- **Filtros** > **Sesiones** muestra un filtro por el nombre de la máquina para ver las sesiones asociadas y su estado en tiempo real.
- En **Tendencias** > **Sesiones**, seleccione el grupo de entrega y el período de tiempo para ver la tendencia de las sesiones y sus métricas asociadas.

Para obtener más información, consulte Filtrar datos para solucionar fallos.

Tendencias de los patrones de carga

La página **Tendencias** > **Índice de patrón de carga** muestra un gráfico con información detallada sobre la carga que se distribuye entre las máquinas de 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. El índice del patrón de carga se muestra como porcentajes de la CPU total, la memoria, el disco o las sesiones, y se compara con la cantidad de usuarios conectados en el último intervalo.

Solucionar problemas de implementaciones

August 17, 2024

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. Se pueden resolver rápidamente los problemas supervisando las métricas relevantes y realizando las acciones correspondientes.

Entre las acciones disponibles se incluyen:

- 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 modo de mantenimiento
- Restablecer el perfil de usuario

Solucionar problemas de aplicaciones

August 17, 2024

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.

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 y escritorios.

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 Knowledge 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 sobre las directivas y cómo modificarlas, consulte Directivas para supervisar fallos de aplicación en las configuraciones de la directiva **Supervisión**.

Supervisar aplicaciones en tiempo real

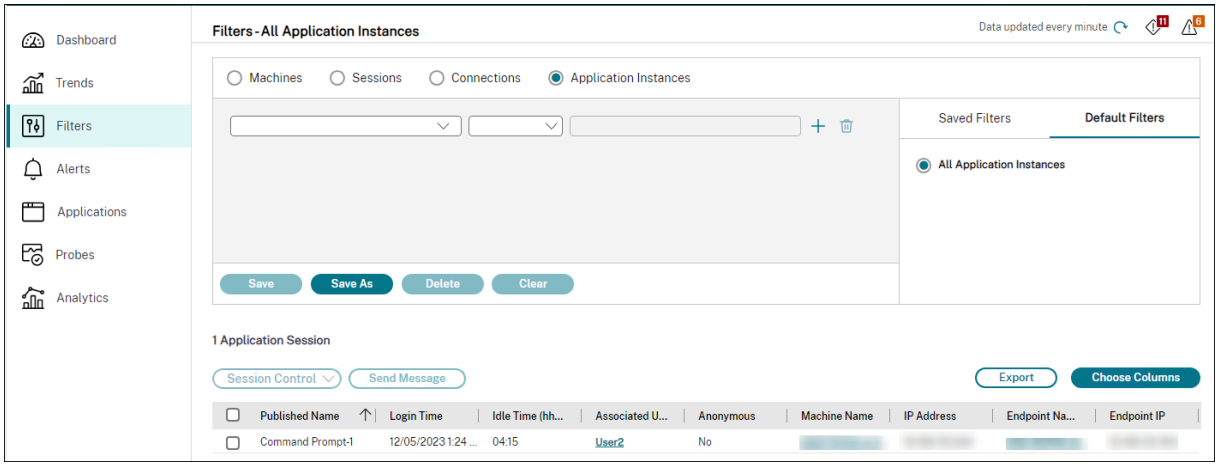
Puede solucionar las aplicaciones y las sesiones con la ayuda de métricas de inactividad para identificar las instancias que llevan inactivas más de un límite de tiempo concreto.

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.

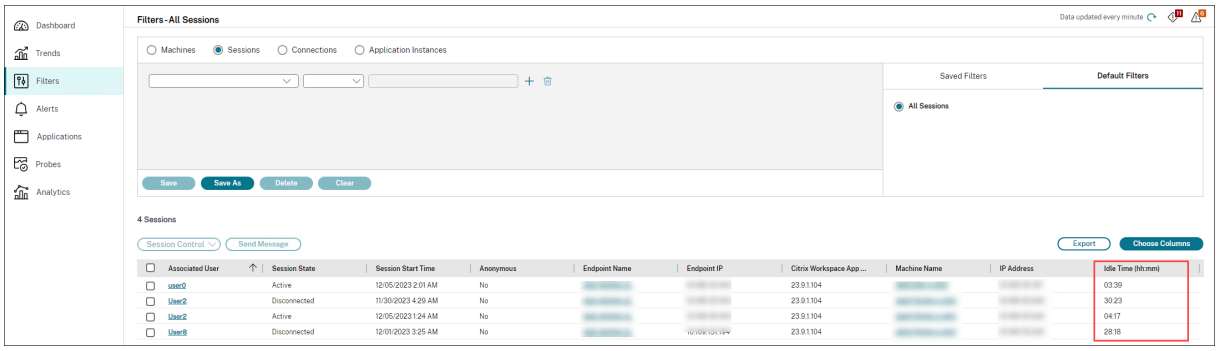


A continuación, se ofrece un filtro de ejemplo. Como criterio **Filtrar por**, elija **Nombre publicado** (de la aplicación) y **Tiempo de inactividad**. A continuación, establezca **Tiempo de inactividad** en **mayor o igual que** un límite de tiempo concreto y guarde el filtro si quiere volver a utilizarlo 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 in-**

actividad 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.

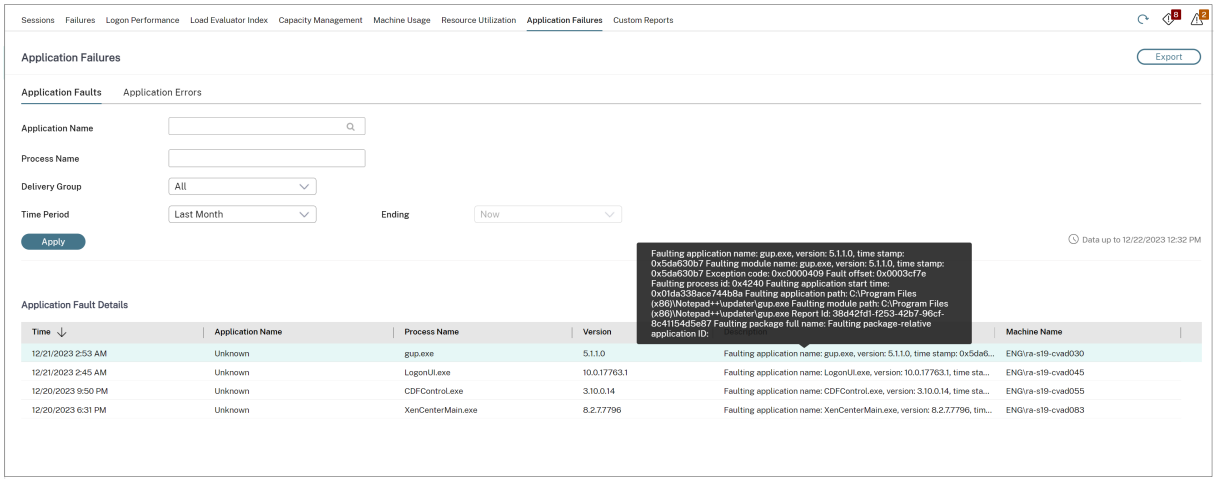
Supervisar fallos históricos de aplicaciones

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
\>
```

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.

Solucionar problemas de máquinas

August 17, 2024

> **Nota:**
>
> **Citrix Health Assistant** es una herramienta para solucionar problemas técnicos de configuración en 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 Motivos de fallo y solución de problemas en Citrix Director.

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.

Utilización de GPU

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 de SO de sesión única o multisesión.

Versiones de GPU compatibles:

- Versión 369.17 de las GPU de NVIDIA Tesla M60 con controlador de pantalla o una posterior. Para obtener más información, consulte NVIDIA vGPU Software.
- Las GPU de AMD Radeon Instinct MI25 y las CPU AMD EPYC 7V12 (Rome). Para obtener más información, consulte AMD Drivers and Support.

Controladores:

Los controladores o extensiones adecuados deben estar instalados en los VDA.

- Para las GPU de NVIDIA, instale los controladores GRID manualmente o mediante extensiones. Para obtener más información, consulte NVIDIA vGPU Software.
  - NVIDIA solo admite controladores GRID. Los controladores CUDA no funcionan con la serie NVadsA10 v5 y no son compatibles.
  - Para ver un ejemplo del proceso de instalación de controladores GRID de GPU de NVIDIA mediante extensiones en máquinas basadas en Azure, consulte Controladores GRID de NVIDIA. Extensión del controlador de GPU de NVIDIA - Máquinas virtuales de Azure Windows - Máquinas virtuales de Azure.
  - Para ver un ejemplo del proceso de instalación manual de controladores GRID de GPU de NVIDIA, consulte Instalación de controladores de GPU de NVIDIA en VM de la serie N con Windows - Máquinas virtuales de Azure.
- Para las GPU de AMD, instale los controladores de gráficos AMD manualmente o mediante extensiones. Para obtener más información, consulte AMD Drivers and Support.
  - Para ver un ejemplo del proceso de instalación de controladores de GPU de AMD mediante extensiones en máquinas basadas en Azure, consulte Extensión del controlador de GPU de AMD - Máquinas virtuales Windows de Azure - Máquinas virtuales de Azure.

  - Para ver un ejemplo del proceso de instalación manual de los controladores de GPU de AMD en máquinas de Azure, consulte Instalación de controladores de GPU de AMD en máquinas virtuales de la serie N con Windows.

Notas de uso:

- Los gráficos de Utilización de GPU solo están disponibles para los VDA con Windows de 64 bits.
- 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.
- Para AMD, el uso del codificador y del decodificador no se permite por separado. Cualquier carga de trabajo de codificación/decodificación que utilice la GPU se registrará como la carga 3D general del uso de la GPU.
- Asegúrese de instalar la WMI de NVIDIA durante la instalación. Esta ventana solo está disponible durante la instalación manual.
- Si los controladores están instalados, pero Director no detecta la GPU
  - Compruebe el Administrador de tareas. Si los controladores están instalados correctamente, la GPU debe aparecer en el Administrador de tareas.
  - Compruebe que la máquina esté registrada. A veces, las máquinas pueden tardar un tiempo en detectarse que están conectadas.
- Si el uso de la GPU no muestra actividad en Director, asegúrese de que la carga de trabajo activa utilice la GPU. Para las cargas de trabajo gráficas, puede habilitar esto desde Configuración > Sistema > Pantalla > Configuración gráfica > Elija la aplicación para configurar las preferencias. Asegúrese de activar Alto rendimiento. A veces, Windows utiliza de forma predeterminada la CPU para cargas de trabajo gráficas cuando está configurada como predeterminada del sistema o para ahorrar energía, según otros parámetros.
- Los datos se actualizan cada minuto y la visualización de los datos comienza un minuto después de seleccionar **Utilización de la GPU**.

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 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". 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**.
2. 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.

3. Haga clic en **Aplicar** y seleccione los gráficos necesarios.
4. 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.

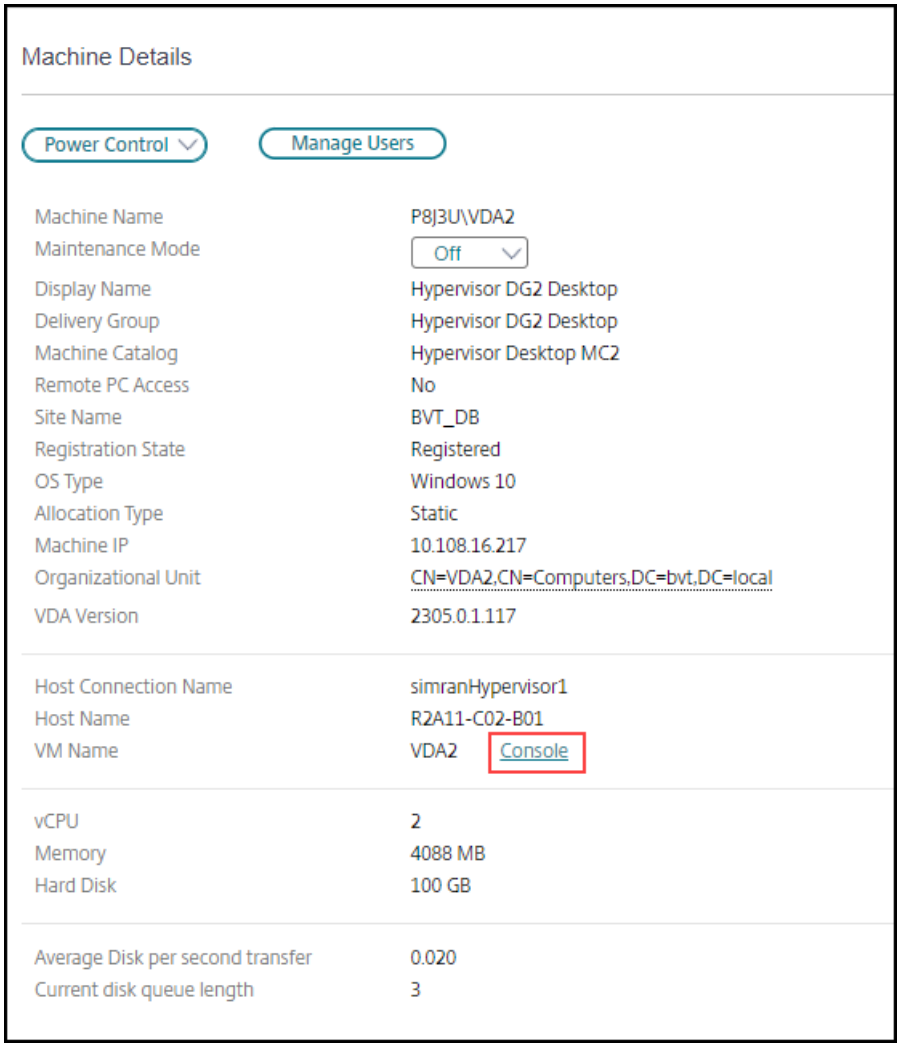
   > **Nota:**
   >
   > El ID de sesión aparece como "0000"para los procesos del sistema.

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.

Inspeccionar las máquinas con acciones de energía recientes

Ahora puede inspeccionar las máquinas con estado correcto o fallido para las acciones de energía. Esta función le ayuda a analizar lo siguiente:

- Fallos de encendido que causan problemas al usuario
- Fallos de apagado que aumentan los costes

> **Nota:**
>
> Los datos solo están disponibles para las máquinas con administración de energía. No hay datos disponibles sobre las acciones de energía ocurridas antes de que se admitiera el uso de esta función.

Para ver el estado de energía de las máquinas, puede usar uno de los métodos siguientes:

En la ficha **Filtros** -> **Máquinas**. En este caso, las columnas **Hora de acción de energía** y **Resultado de la acción de energía** están visibles de forma predeterminada. También puede seleccionar qué columnas quiere hacer visibles.

En la ficha **Optimización de costes**. En este caso, el filtro predeterminado **Acción de energía desencadenada por** está configurado en *Autoscale* y el valor de **Resultado de la acción de energía** está establecido en *Fallido*.

Con esta función, puede ver los detalles de los controles de las acciones de energía. Por ejemplo, puede ver quién desencadenó la acción, qué acción cambió el estado de energía, el motivo del fallo y la hora en que se completó la acción. También puede exportar estos detalles.

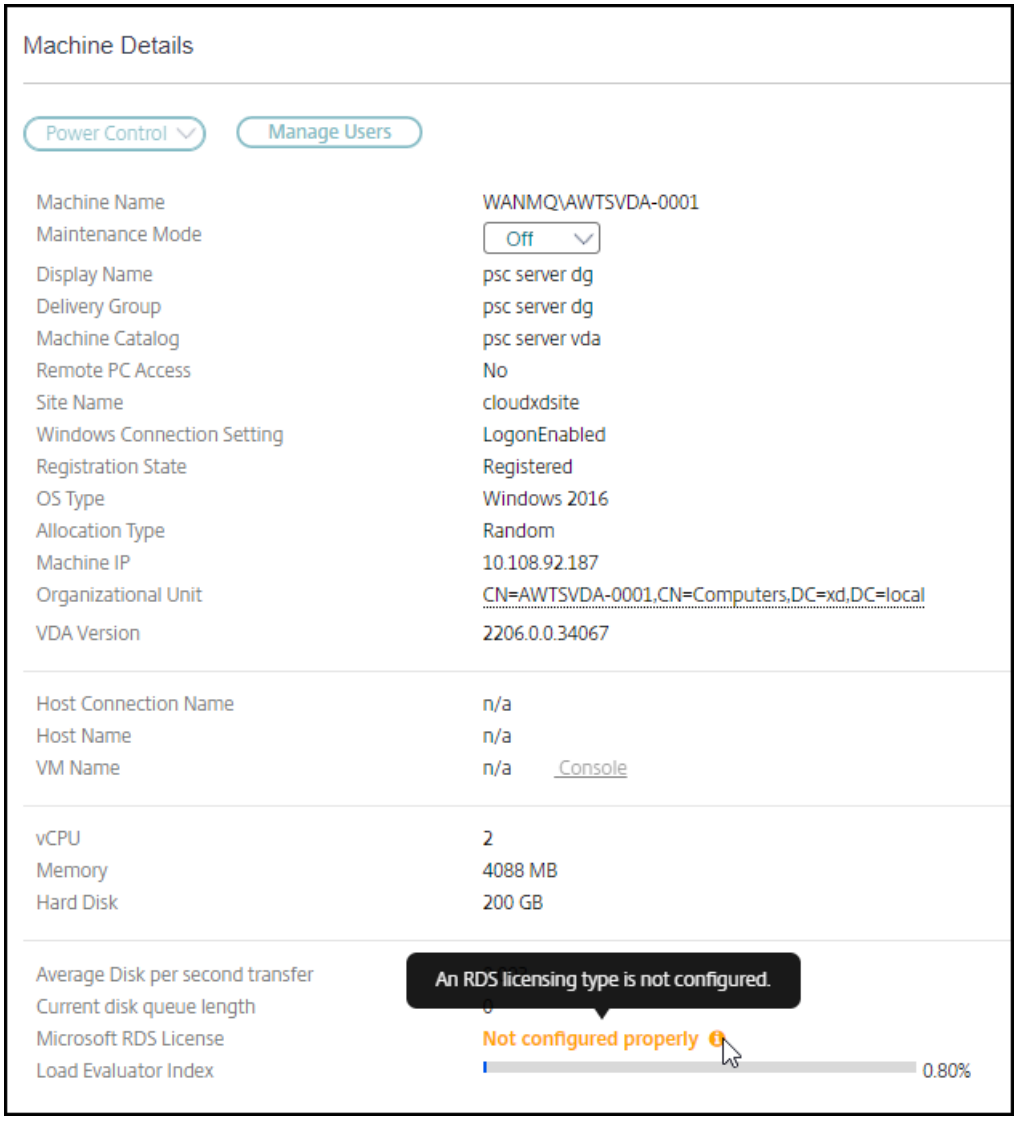
Se agregan estos filtros para ver el estado de la acción de energía:

Filtro	Descripción
Resultado de la acción de energía	Muestra el resultado de la acción de energía. Los valores de filtro posibles son correcto y fallido.
Acción de energía desencadenada por	Muestra quién o qué desencadenó la acción de energía. Los valores de filtro posibles son los siguientes • Autoscale: Este valor aparece cuando lo que desencadena una acción de energía es lo siguiente

Filtro	Descripción
	• Cuando el administrador apaga una VM para limpiar su disco de SO y devolverlo a su estado inicial • Cuando una VM se apaga o suspende en función de las directivas establecidas • Cuando una VM se hace disponible en función de la configuración del tamaño de la agrupación o el tamaño del búfer • Administrador: Este valor aparece cuando un administrador desencadena una acción de energía. Los posibles ejemplos son cuando el administrador solicita apagar, encender, suspender, reanudar o reiniciar una VM. • Usuario: Este valor aparece cuando un usuario desencadena una acción de energía. Los ejemplos son cuando un usuario restablece, inicia o reanuda el trabajo en la máquina virtual. • Otros: Este valor aparece cuando se desencadena una acción de energía por motivos de programación y desconocidos.
Última acción de energía	Muestra la acción exacta de energía que tuvo lugar en la máquina, como encender, apagar, apagar, reiniciar, restablecer o reanudar
Hora de acción de energía	El momento en que se completa la acción de energía. Los valores de filtro posibles son última hora, últimos 5 minutos, últimos 30 minutos, última hora, hoy, últimas 24 horas y ayer.
Motivo del fallo de la acción de energía	Muestra el motivo del fallo. Los valores de filtro posibles son fallo notificado por hipervisor, se ha superado el límite de frecuencia del hipervisor, error desconocido y ninguno. Si la acción se ha realizado correctamente, aparece “Ninguno”.

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 las licencias antes de que caduquen.

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 puede determinar, ya que no se puede acceder al servidor de licencias para el nivel de SO que se requiere.

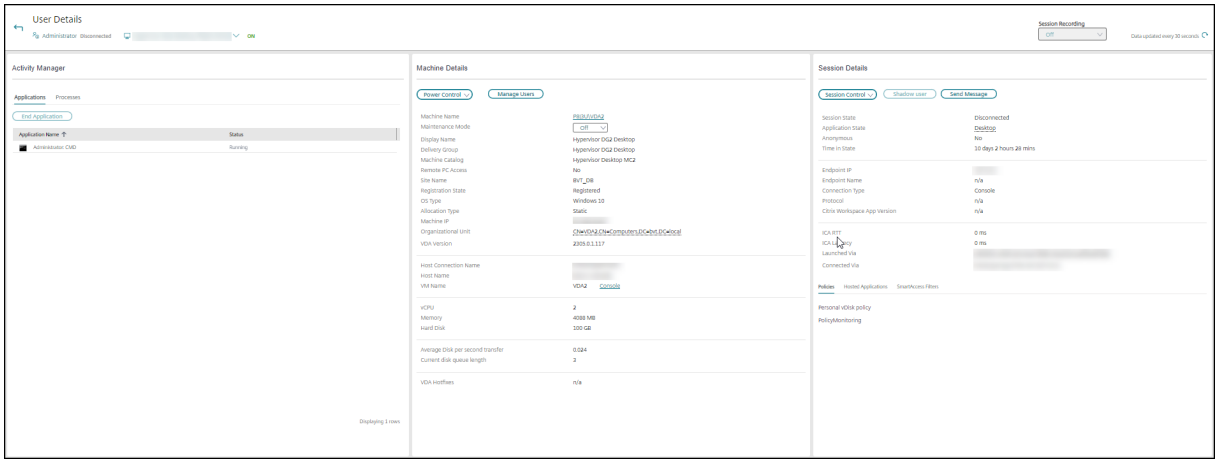
> **Nota:**
>
> Esta función solo se aplica a Microsoft RDS CAL (Licencia de acceso de cliente).

Solucionar problemas de usuarios

August 17, 2024

Use el **Servicio de asistencia** de Director (página **Administrador de actividades**) para ver información sobre el usuario o la sesión:

Al hacer clic en **Ver detalles** en el Administrador de actividades del usuario, se abre la página **Detalles del usuario**.
Al hacer clic en **Ver detalles** en el Administrador de actividades del dispositivo de punto final, se abre la página **Detalles del dispositivo de punto final**.



Selector de sesiones

Si el usuario inició varias sesiones, el selector de sesiones ayuda a seleccionar una sesión.

Elija una sesión para ver los detalles.

- Consulte los detalles de la sesión, la experiencia de inicio de sesión del usuario, el inicio de la sesión, la conexión y las aplicaciones.
- puede reflejar la máquina del usuario.
- Grabe la sesión ICA.

Estado de optimización de Microsoft Teams

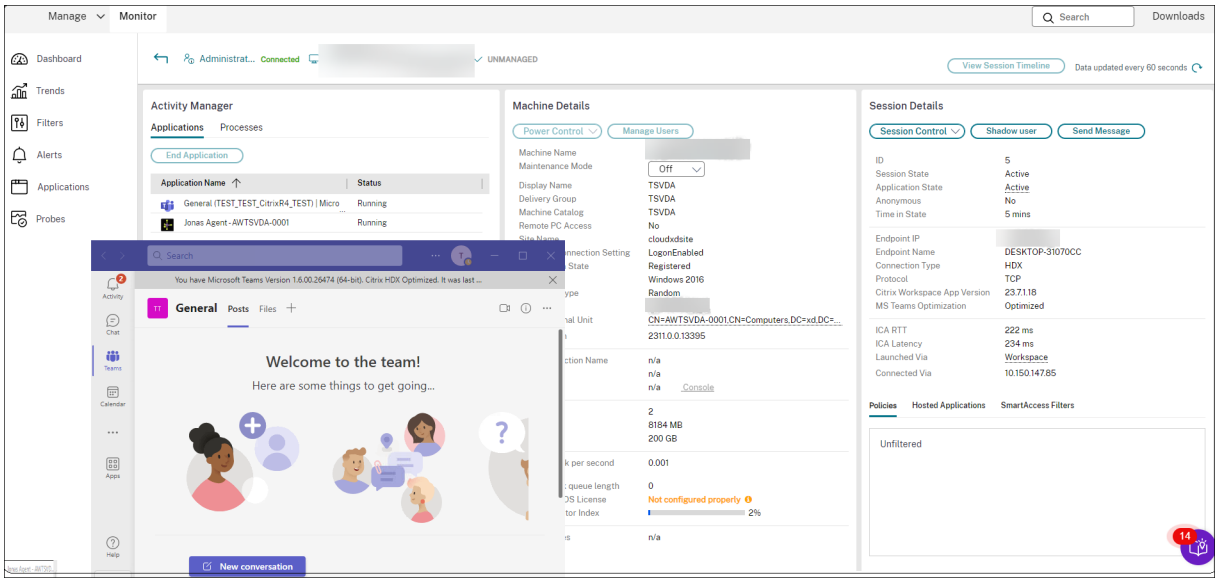
Director muestra el estado de optimización de Microsoft Teams para las sesiones de HDX en la página de **Detalles del usuario** > panel de **Detalles de la sesión** > campo **Optimización de MS Teams**. La optimización de Microsoft Teams es fundamental para una mejor experiencia de usuario, como audio y vídeo nítidos. La visibilidad del estado de optimización de Microsoft Teams es útil para reducir el tiempo necesario para resolver los tíquets y ayuda a los administradores a identificar las métricas importantes durante la solución de problemas.

> **Nota:**
>
> Citrix Director es compatible con la versión 2.1 o anterior de Microsoft Teams.

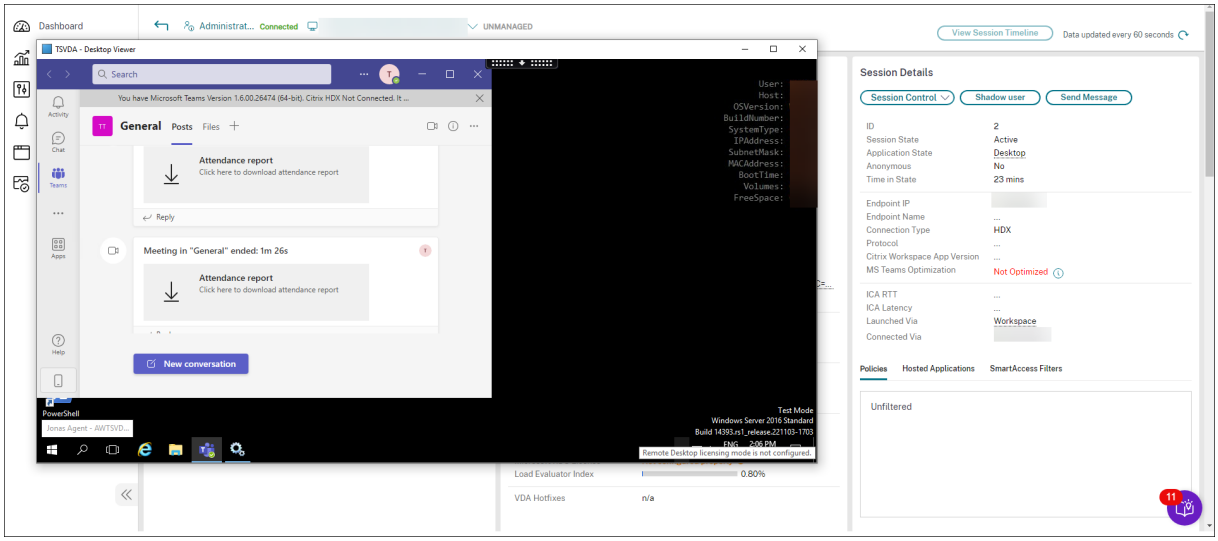
Requisitos previos:

- Los VDA ejecutan la versión 2311 y posteriores.
- Las versiones de la aplicación Citrix Workspace compatibles se enumeran en Optimización para Microsoft Teams.
- Microsoft Teams se ejecuta como una aplicación publicada o dentro de un escritorio publicado.

- Se están ejecutando servicios cruciales, como el servicio de redirección de vídeo HTML5 de Citrix HDX.



Si los MS Teams no están optimizados, el texto de ayuda proporciona un enlace a un artículo externo en directo de resolución de problemas de HDX que contiene consejos para optimizar Microsoft Teams. Solución de problemas de optimización de HDX.



Sugerencias para solucionar problemas

Solucione el problema con las acciones recomendadas en la tabla siguiente y, si es necesario, remita el problema al administrador que corresponda.

Problema de los usuarios	Sugerencias
El inicio de sesión tarda mucho tiempo o falla de forma intermitente o repetidamente	Diagnosticar problemas de inicio de sesión de los usuarios
El inicio de sesión tarda mucho tiempo o falla de forma intermitente o repetidamente	Diagnosticar problemas de inicio de sesión
La respuesta de la sesión es lenta o inexistente	Diagnosticar problemas de rendimiento de sesión
La aplicación es lenta o no responde	Resolver fallos de aplicaciones
La conexión falló	Restaurar conexiones de escritorio
La sesión es lenta o no responde	Restaurar sesiones
Grabar sesiones	Grabar sesiones
El vídeo es lento o de poca calidad	Generar informes del sistema de canales HDX

> **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".

Inicio de sesión

La vista de **Detalles del usuario** > ficha **Inicio de sesión** muestra una vista completa del proceso de inicio de sesión. La ficha contiene el gráfico de fases de duración del inicio de sesión con las distintas fases de inicio de sesión trazadas. Use estos datos para solucionar los problemas de inicio de sesión de los usuarios. Para obtener más información, consulte Diagnosticar problemas de inicio de sesión de los usuarios.

Rendimiento de sesión

La ficha **Rendimiento de sesión** cuenta con flujos de trabajo de solución de problemas mejorados, empezando por la capacidad de correlacionar métricas en tiempo real para identificar problemas dentro de las sesiones de los usuarios. El panel **Topología de sesión** proporciona una representación visual de la ruta de las sesiones de HDX conectadas. El panel de **Métricas de rendimiento** ofrece tendencias para las métricas de sesión como ICARTT, la latencia de ICA, los fotogramas por segundo, el ancho de banda de salida disponible y el ancho de banda de salida consumido, ayudan a indicar el rendimiento de estas métricas a lo largo del tiempo. Para obtener más información, consulte Diagnosticar problemas de rendimiento.

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 que están 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.

Al escribir el nombre de un dispositivo de punto final en el campo Buscar, Director usa las sesiones sin autenticar (anónimas) y las sesiones autenticadas que están conectadas a un dispositivo de punto final específico. Esta búsqueda habilita la solución de problemas para sesiones no autenticadas. Asegúrese de que los nombres de los dispositivos de punto final son exclusivos para poder resolver problemas de sesiones no autenticadas.

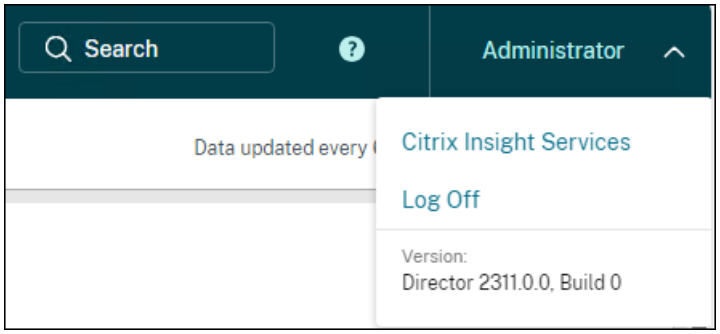
Los resultados de la búsqueda incluyen también usuarios que no están utilizando máquinas en ese momento o no tienen asignada ninguna.

- 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, separadas por un espacio, los resultados incluyen coincidencias para ambas cadenas. Los ejemplos de nombres que constan de dos partes son el nombre de usuario, el apellido y el nombre, o el nombre para mostrar. 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 perspectivas de diagnóstico adicionales. 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 Scout, y para ver las preguntas frecuentes, consulte CTX130147.

Diagnosticar problemas de inicio de sesión

August 17, 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.

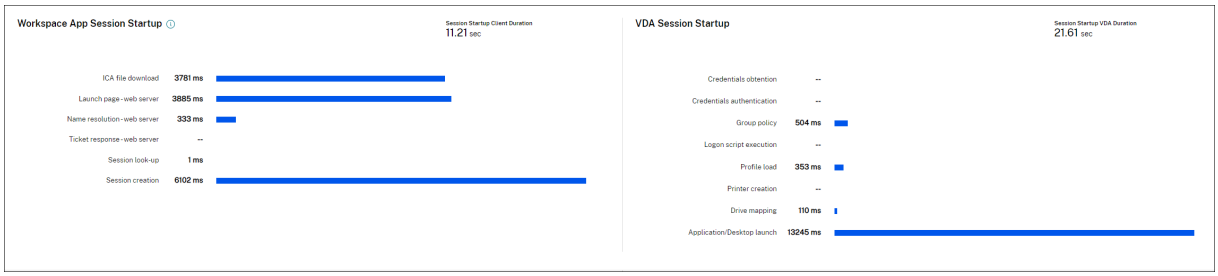
- El servicio Citrix End User Experience Monitoring (EUEM) debe ejecutarse en el VDA.

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. SSCD 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 tíquet 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 puede 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 el 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. Puede ser Kerberos, Active Directory o una interfaz de proveedor de soporte de 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. Esto 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 el valor de 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. Por ejemplo: 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. 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 el momento 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 los retrasos en el tiempo de creación de sesiones en VDA.

Diagnosticar problemas de inicio de sesión de los usuarios

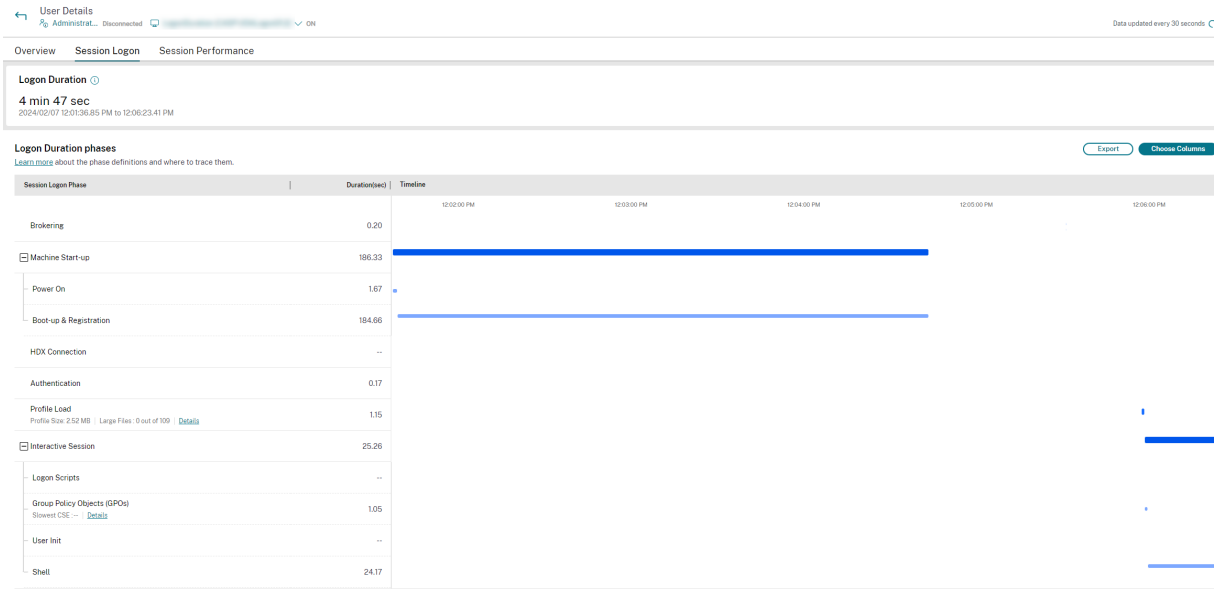
August 17, 2024

La vista de **Detalles del usuario** > ficha **Inicio de sesión** muestra una vista completa del proceso de inicio de sesión. Use estos datos para solucionar los problemas de inicio de sesión de los usuarios.

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.

A medida que los usuarios inician sesión en Citrix Virtual Apps and Desktops, Monitor Service supervisa las fases del proceso de inicio de sesión. Las fases van desde el momento en que el usuario se conecta desde la aplicación Citrix Workspace al momento en que la aplicación o el escritorio están listos para usarse.

La ficha **Inicio de sesión** contiene el gráfico de fases de duración del inicio de sesión con las distintas fases de inicio de sesión trazadas. La duración de inicio de sesión se calcula sumando el tiempo que se tarda en establecer la conexión y en obtener un escritorio o una app desde Delivery Controller y el tiempo que se tarda en autenticarse e iniciar sesión en una app o escritorio virtual. La información de duración se presenta en segundos (o fracciones de segundo).



El gráfico de fases de duración del inicio de sesión proporciona una vista clara de las diferentes fases de inicio de sesión y sus horas de inicio y finalización. El gráfico muestra la superposición de las fases de inicio de sesión individuales. Es posible que el tiempo total de inicio de sesión no sea la suma de las duraciones de las fases de inicio de sesión individuales. Esto se debe a que las fases individuales pueden superponerse y no todas las fases de inicio de sesión forman parte de esta representación. Además, algunas fases pueden extenderse incluso después de que el usuario comience a interactuar con la aplicación o el escritorio virtual, y esta duración no se mide como parte de la duración total del inicio de sesión.

Use esta vista para identificar las fases de inicio de sesión específicas que provocan un retraso en el inicio de la sesión. La definición de cada fase de inicio de sesión y el origen del evento desde el que se puede rastrear la información ayudan a solucionar problemas adicionales. Al desplazar el ratón sobre el gráfico, aparece un texto de ayuda que contiene la duración de la fase de la sesión actual, así como el promedio de 7 días del usuario y el promedio de 7 días del grupo de entrega. Esta información ayuda a comparar la duración actual del inicio de sesión con los valores promedio de 7 días. Puede profundizar en las mediciones de subfase en el caso de los detalles de perfil y GPO. Esta visualización ayuda a comprender y solucionar fácilmente los problemas relacionados con la duración del inicio de sesión.

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 Citrix Profile Management Service se está 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.

> **Notas:**
>
> - La duración del inicio de sesión solo se admite en el shell predeterminado de Windows (explorer.exe), no en los shells personalizados.
> - La duración de inicio de acceso con Remote PC solo está disponible cuando **Citrix User Profile Manager** y **Citrix User Profile Manager WMI Plugin** se instalan como componentes extra durante la instalación de Remote PC. Para obtener más información, consulte el paso 4 de Aspectos que tener en cuenta acerca de la secuencia y configuración de acceso con Remote PC.

Pasos para solucionar problemas en el inicio de sesión de los usuarios

1. En la vista **Detalles del usuario** > ficha **Inicio de sesión**, resuelva problemas del estado de inicio de sesión desde el gráfico "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, 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.

Arranque de la máquina

Si la sesión requería el inicio de una máquina virtual, este es el tiempo que tardó en iniciarse la máquina. La siguiente subsección proporciona un desglose del tiempo necesario para iniciar una máquina virtual durante las diferentes fases:

- **Encender**: Muestra el tiempo necesario para encender una máquina virtual

- **Arranque y registro**: Muestra el tiempo necesario para arrancar y registrar una máquina virtual

Puede usar el botón desplegable para contraer o ampliar las opciones de la sección **Arranque de la máquina**.

Conexión HDX

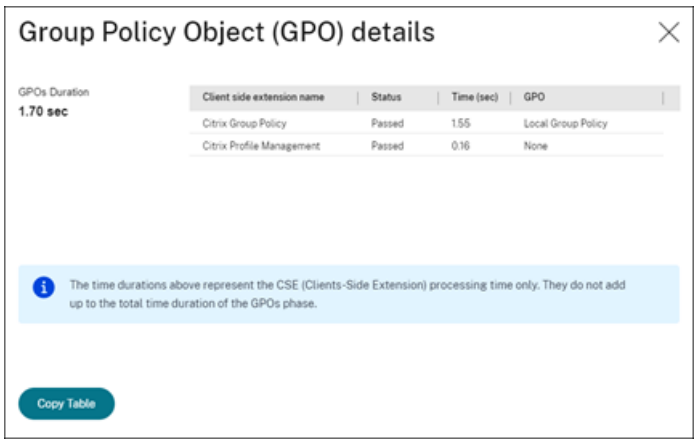
Tiempo que se tardó en completar los pasos requeridos para configurar la conexión HDX desde el cliente a la máquina virtual.

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 **Detalles** 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 de registro de los registros de operaciones, consulte el artículo Configuring the Event Logs de Microsoft TechNet.

Scripts de inicio de sesión

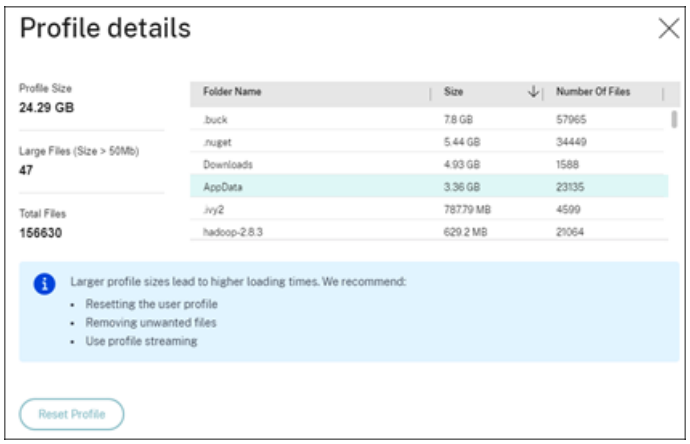
Si había scripts de inicio de sesión configurados para la sesión, este es el tiempo que se tardó en ejecutarlos.

Carga de perfil

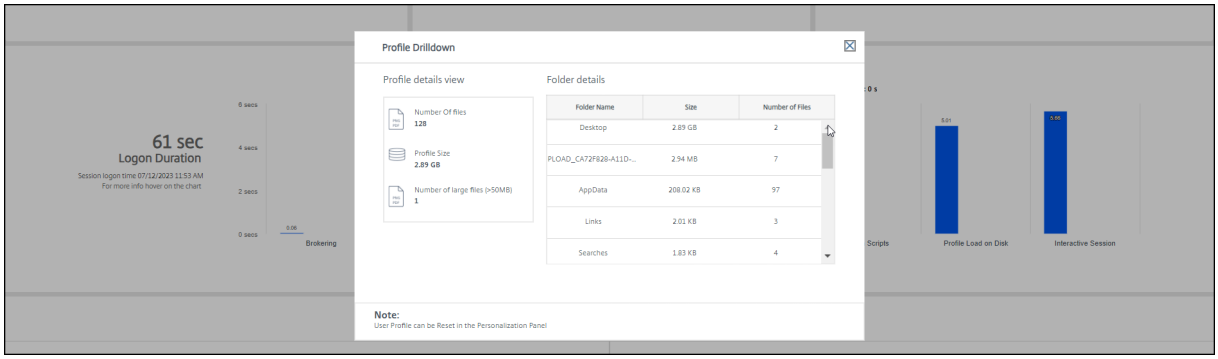
Si había parámetros de perfil configurados para el usuario o para la máquina virtual, este es el tiempo que tardó el perfil en cargarse.

Si Citrix Profile Management y FSLogix están configurados, la barra Carga de perfil indica el tiempo que Citrix Profile Management y FSLogix tardan en procesar perfiles de usuario. Esta información ayuda a los administradores a solucionar problemas con la duración elevada de cargas de perfil. Cuando se configuran Profile Management y FSLogix, 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 las versiones 2407 o posteriores de VDA.

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 **Detalles** 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 garantiza 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.

1. En el VDA, agregue el nuevo valor de Registro **ProfileFoldersNameHidden** a HKEY_LOCAL_MACHINE\Softwa
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.
- Es posible 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.
- El número de archivos y los datos de tamaño de perfil podrían no coincidir con los datos del panel de Personalización, debido a ciertas limitaciones de Windows.

Sesión interactiva

Sesión interactiva 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 muestra lo siguiente:

- subfases
- tiempo empleado para cada subfase
- tiempo total de demora acumulada entre estas subfases

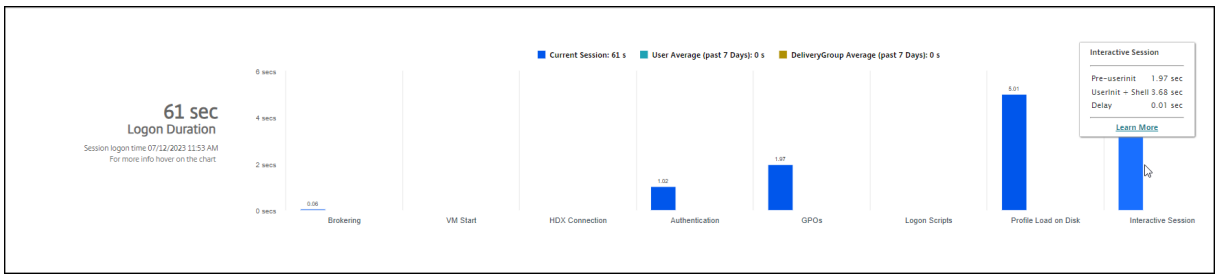
Puede usar el botón desplegable para contraer o expandir las opciones de la **sesión interactiva**.

> **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 con 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 opción "Auditar el seguimiento de procesos"y cómo habilitarlo o inhabilitarlo, consulte Auditar el seguimiento de procesos en la documentación de Microsoft.



Panel "Duración de inicio de sesión"en la vista "Detalles del usuario".

- **Sesión interactiva: Pre-userinit:** 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 otros 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 de 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.

Exportar datos

Además de las opciones predeterminadas de la tabla Fases de duración del inicio de sesión, que son la fase y la duración del inicio de sesión, también puede elegir las siguientes columnas en la página Inicio de sesión:

- Hora de inicio
- Hora de fin
- Grupo de entrega: promedio de 7 días (s)
- Usuario: promedio de 7 días (s)

También puede exportar los datos anteriores a un archivo.CSV.

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 **arranque de la máquina** es lento, el problema puede estar en el hipervisor. En ese caso, contacte con el administrador del hipervisor.

Examine diferencias inusuales, como:

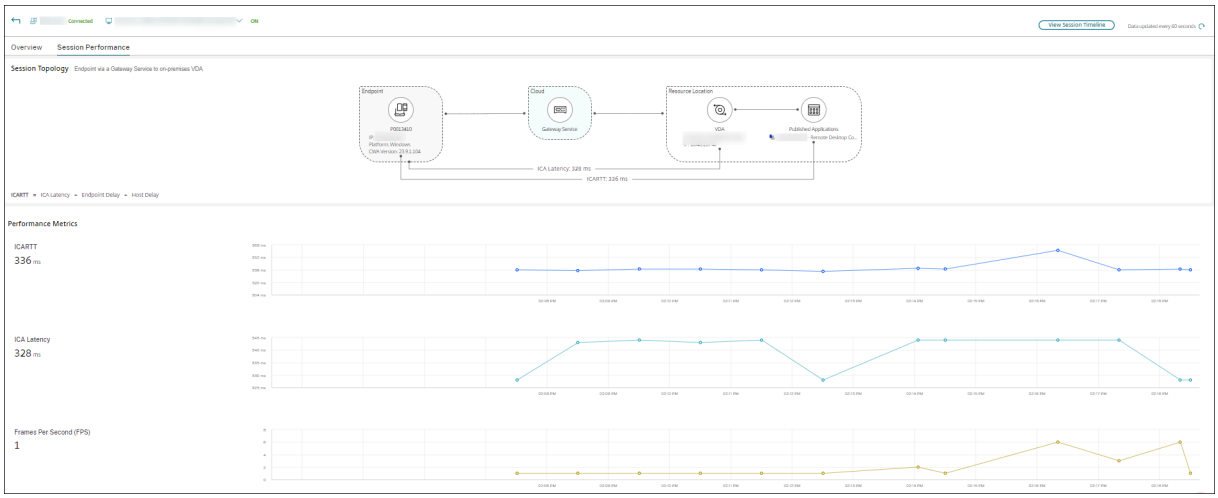
- Cuando falten barras de inicios de sesión (actuales)
- Discrepancias importantes entre los valores de duración actual y de duración promedio para un usuario. Las causas pueden ser:
  - Se ha instalado una nueva aplicación.
  - Se ha actualizado el sistema operativo.
  - Se realizaron cambios en la configuración.
  - El tamaño del perfil del usuario es muy grande. En este caso el valor de Carga del perfil es 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 **arranque de máquina** o **intermediación con broker**.

Diagnosticar problemas de rendimiento de sesión

August 17, 2024

La ficha **Rendimiento de la sesión** en la página Detalles de usuario ha mejorado los flujos de trabajo de solución de problemas para ayudar a identificar problemas en las sesiones de usuario de HDX. Los paneles **Topología de sesión y Métricas de rendimiento** ayudan a correlacionar la vista de componentes y varias métricas de rendimiento de una sesión en una sola vista y reducen el tiempo medio de resolución de los problemas de experiencia de sesión.



Vista de salto de red de extremo a extremo

La vista de salto de red de extremo a extremo es el siguiente paso para mejorar los flujos de trabajo de solución de problemas. La sección **Detalles del usuario** > **Rendimiento de la sesión** > **Topología de la sesión** proporciona una representación visual de la vista de salto de red de extremo a extremo para las sesiones HDX conectadas.

La topología de una sesión conectada muestra los componentes involucrados en la ruta de la sesión con sus metadatos, el enlace entre los componentes y las aplicaciones publicadas en VDA.
Además, se muestran estas métricas de rendimiento de la sesión:

- Latencia de ICA: Esta latencia es básicamente la latencia de la red. Este parámetro indica si la red es lenta.
- ICA RTT: ICA RTT es el intervalo de tiempo entre la acción de un usuario y la respuesta gráfica que se muestra en su pantalla. Esta medición incluye la latencia de ICA, la demora del dispositivo de punto final y la demora del host.

Puede usar esta vista para comprender los componentes a través de los cuales fluyen los datos de la sesión e identificar el salto específico que podría ocasionar problemas de rendimiento.

Las métricas de rendimiento de la vista Topología de sesión solo están disponibles para la sesión de HDX en estado conectado.

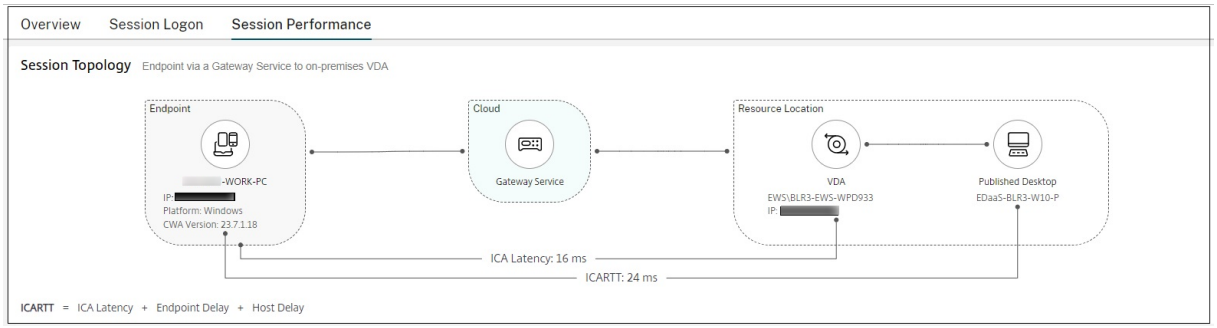
Casos de topología de sesión

Según el casos de implementación del sitio, los componentes involucrados en una sesión son todos o algunos de los siguientes:

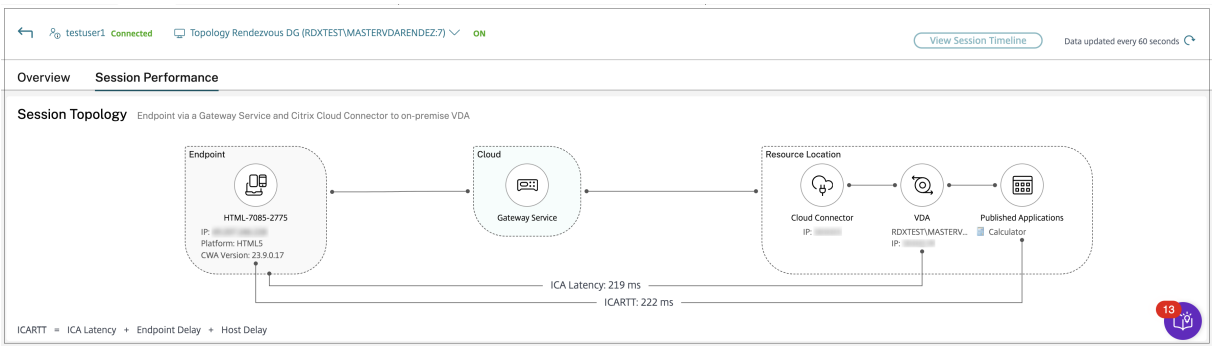
- Aplicación Citrix Workspace en el dispositivo de punto final
- Gateway Service / Gateway local
- Cloud Connector: Gateway se conecta a DaaS a través de un Cloud Connector en el caso de conexiones híbridas.
- VDA

En consecuencia, las posibles topologías de red son las siguientes:

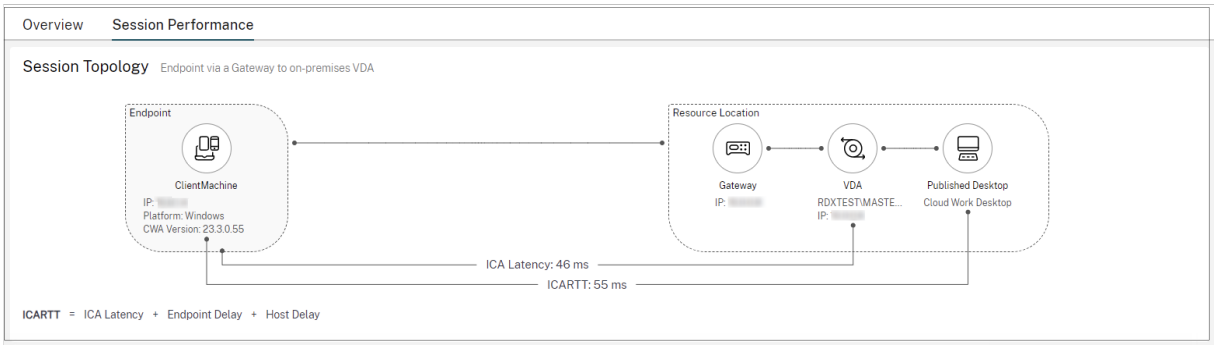
- La aplicación Citrix Workspace del terminal se conecta a través de Citrix Workspace y Gateway Service a un VDA local. No se utiliza ningún Cloud Connector para conectarse a VDA.



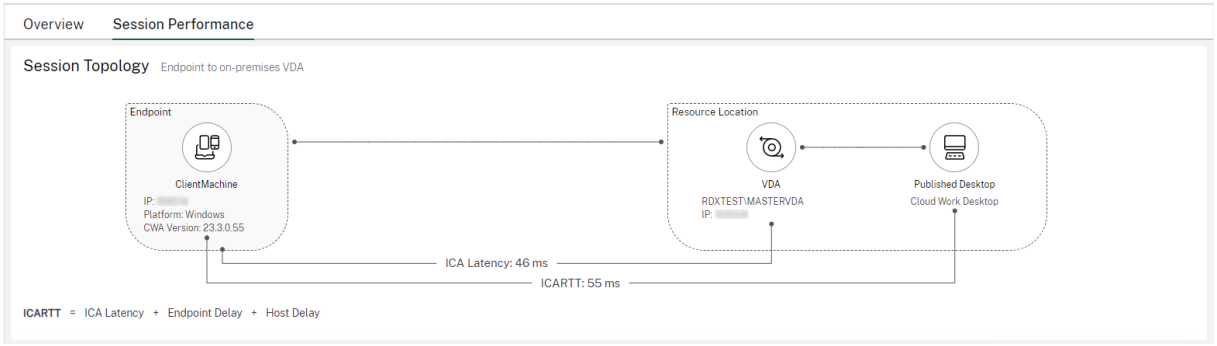
- La aplicación Citrix Workspace del dispositivo de punto final se conecta mediante Citrix Workspace y Gateway Service a un VDA local mediante Cloud Connector.



- La aplicación Citrix Workspace del dispositivo de punto final se conecta mediante StoreFront y Gateway local a un VDA local.



- La aplicación Citrix Workspace del dispositivo de punto final se conecta mediante StoreFront a un VDA local.



Métricas de rendimiento

El panel **Métricas de rendimiento** ofrece la posibilidad de correlacionar métricas en tiempo real para identificar problemas en las sesiones de los usuarios. Las tendencias de las métricas de sesión ayudan a indicar el rendimiento de estas métricas a lo largo del tiempo. Al hacer clic en la ficha **Rendimiento de la sesión**, junto con los datos en tiempo real, puede ver los datos de los últimos 15 minutos y las últimas 24 horas. Los gráficos ayudan a correlacionar las métricas de rendimiento de varios componentes en una sola vista.

Nota:

- Con ayuda de las métricas de los últimos 15 minutos, se traza el gráfico para el tiempo durante el cual la sesión está conectada y desconectada. La métrica de sesión desconectada se muestra con el valor cero.
- Con ayuda de las métricas de las últimas 24 horas, los gráficos de latencia de ICA e ICARTT se actualizan con las métricas de datos históricos.

Además de ICARTT y la latencia de ICA, hay estas métricas disponibles para las métricas en tiempo real y de los últimos 15 minutos:

- Fotogramas por segundo: Los fotogramas por segundo son una métrica importante que indica la capacidad de respuesta de la sesión.
  Ancho de banda de salida disponible: El ancho de banda de salida disponible es una medida del ancho de banda total disponible para transmitir datos desde el VDA al dispositivo de punto final.
- Ancho de banda de salida consumido: El ancho de banda de salida consumido indica la cantidad real de datos transmitidos del VDA al dispositivo de punto final para mostrar sesiones a los usuarios.

El análisis del ancho de banda de salida disponible y del ancho de banda de salida consumido ayuda a comprobar si hay suficiente ancho de banda disponible para cubrir las sesiones y a detectar si una sesión no tiene ancho de banda insuficiente.

Solucionar problemas cuando no se rellenan los datos de RTT de ICA o Duración del inicio de sesión

Antes, cuando los servicios EUEM o Profile Management Service no se ejecutaban, no se mostraba el motivo por el que no se obtenían los datos relacionados con RTT de ICA o Duración del inicio de

sesión. Con esta nueva función, puede obtener el motivo del fallo y la solución correspondiente. Los enlaces **Más información** proporcionan los errores de RTT de ICA y de Duración del inicio de sesión, el motivo del error y la solución, tal como se menciona en la tabla siguiente:

Tipo de error	Error	Mensaje de error	Solución
Error de RTT de ICA	No se muestra el valor de RTT de ICA.	**Citrix End User Experience Monitoring no se está ejecutando.**	1. Abra la consola Servicios. Para abrir esta consola, haga clic en **Iniciar** y, a continuación, escriba **Servicios**. 2. Asegúrese de que el servicio Citrix End User Experience Monitoring se está ejecutando. 3. Vuelva a abrir la sesión de escritorio e inténtelo. Debe mostrarse el valor ICA RTT. 4. Si el problema persiste, contacte con el administrador de Citrix.
Error de RTT de ICA	No se muestra el valor de RTT de ICA.	**Citrix End User Experience Monitoring no está instalado.**	1. Instale de nuevo el VDA. 2. Abra la consola Servicios. Para abrir esta consola, haga clic en **Iniciar** y, a continuación, escriba Servicios 3. Asegúrese de que el servicio Citrix End User Experience Monitoring se está ejecutando.

Tipo de error	Error	Mensaje de error	Solución
			4. Vuelva a abrir la sesión de escritorio e inténtelo. El valor ICA RTT debe mostrarse ahora. 5. Si el problema persiste, contacte con el administrador de Citrix.
Error de RTT de ICA	No se muestra el valor de RTT de ICA.	**Error al obtener los datos.**	1. Abra la consola Servicios. Para abrir esta consola, haga clic en **Iniciar** y, a continuación, escriba Servicios. 2. Asegúrese de que el **servicio Instrumental de administración de Windows** se está ejecutando. 3. Además, asegúrese de que el proceso Wf-Shell.exe/PicaShell.exe se está ejecutando en la ficha **Administrador de actividades** > **Proceso**. Si no se está ejecutando, vuelva a abrir la sesión de escritorio.

Tipo de error	Error	Mensaje de error	Solución
			4. Si los pasos anteriores no funcionan, ejecute este comando para asegurarse de que la instancia Citrix_EUEM_Roundtrip está presente: `Get-CimInstance -Namespace 'ROOT\Citrix\Euem'-Query "select * from Citrix_Euem_RoundTrip"` 5. Si la instancia Citrix_EUEM_Roundtrip está presente, vuelva a abrir la sesión de escritorio. 6. Si el problema persiste, contacte con el administrador de Citrix.
Error de duración del inicio de sesión	El gráfico no se carga.	**Citrix Profile Management no se está ejecutando**	1. Abra la consola Servicios. Para abrir esta consola, haga clic en **Iniciar** y, a continuación, escriba Servicios. 2. Compruebe que el servicio **Citrix Profile Management Service** se está ejecutando.

Tipo de error	Error	Mensaje de error	Solución
			3. Vuelva a abrir la sesión de escritorio e inténtelo. Debe mostrarse el gráfico. 4. Si el problema persiste, contacte con el administrador de Citrix.
Error de duración del inicio de sesión	El gráfico no se carga.	**Citrix Profile Management no está instalado.**	1. Instale Citrix Profile Management Service. 2. Abra la consola Servicios. Para abrir esta consola, haga clic en **Iniciar** y, a continuación, escriba Servicios. 3. Compruebe que el servicio **Citrix Profile Management Service** se está ejecutando. 4. Vuelva a abrir la sesión de escritorio e inténtelo. Debe mostrarse el gráfico. 5. Si el problema persiste, contacte con el administrador de Citrix.
Error de duración del inicio de sesión	El gráfico no se carga.	**Error al obtener los datos.**	1. Abra la consola **Servicios**. Para abrir esta consola, haga clic en **Iniciar** y, a continuación, escriba Servicios.

Tipo de error	Error	Mensaje de error	Solución
			2. Asegúrese de que el **servicio Instrumental de administración de Windows** se está ejecutando. 3. Si el servicio anterior ya se está ejecutando, ejecute el siguiente comando para asegurarse de que `LogonTimings instance is present`: `Get-CimInstance -Namespace 'ROOT\Citrix\Profile\Metrics' -Query "select * from LogonTimings"` 4. Si el problema persiste, contacte con el administrador de Citrix.

Remedar usuarios

August 17, 2024

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 websockify 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 Habilitar o inhabilitar funciones.

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

August 17, 2024

Desde Director, puede enviar un mensaje a un usuario que está conectado a una o varias máquinas. Puede usar esta función para enviar notificaciones inmediatas acerca de acciones administrativas, tales como operaciones de mantenimiento de escritorios que están a punto de tener lugar, cierres de sesión y reinicios de máquinas y restablecimientos de perfiles.

1. En la vista Administrador de actividades, seleccione el usuario y haga clic en Detalles.
2. En la vista Detalles del usuario, busque el panel Detalles de la sesión y haga clic en Enviar mensaje.
3. Escriba la información de mensaje en los campos Asunto y Mensaje, y luego haga clic en Enviar.

Si el mensaje se envió correctamente, aparece un mensaje de confirmación en Director. El mensaje aparece en la máquina del usuario.

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 aplicaciones

August 17, 2024

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 de cada una de ellas.

> **Nota:**
>
> Si la ficha "Aplicaciones"aparece atenuada, contacte 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.
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 fallan.
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 su lugar, cierre la sesión del usuario y permita que el usuario inicie sesión de nuevo.

Acción	Descripción
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

August 17, 2024

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. Por ejemplo: cuando la máquina utilice una cantidad inusualmente alta de recursos de CPU, que puede hacer que la CPU sea inutilizable.

Restaurar sesiones

August 17, 2024

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.
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 del sistema de canales HDX

August 17, 2024

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

August 17, 2024

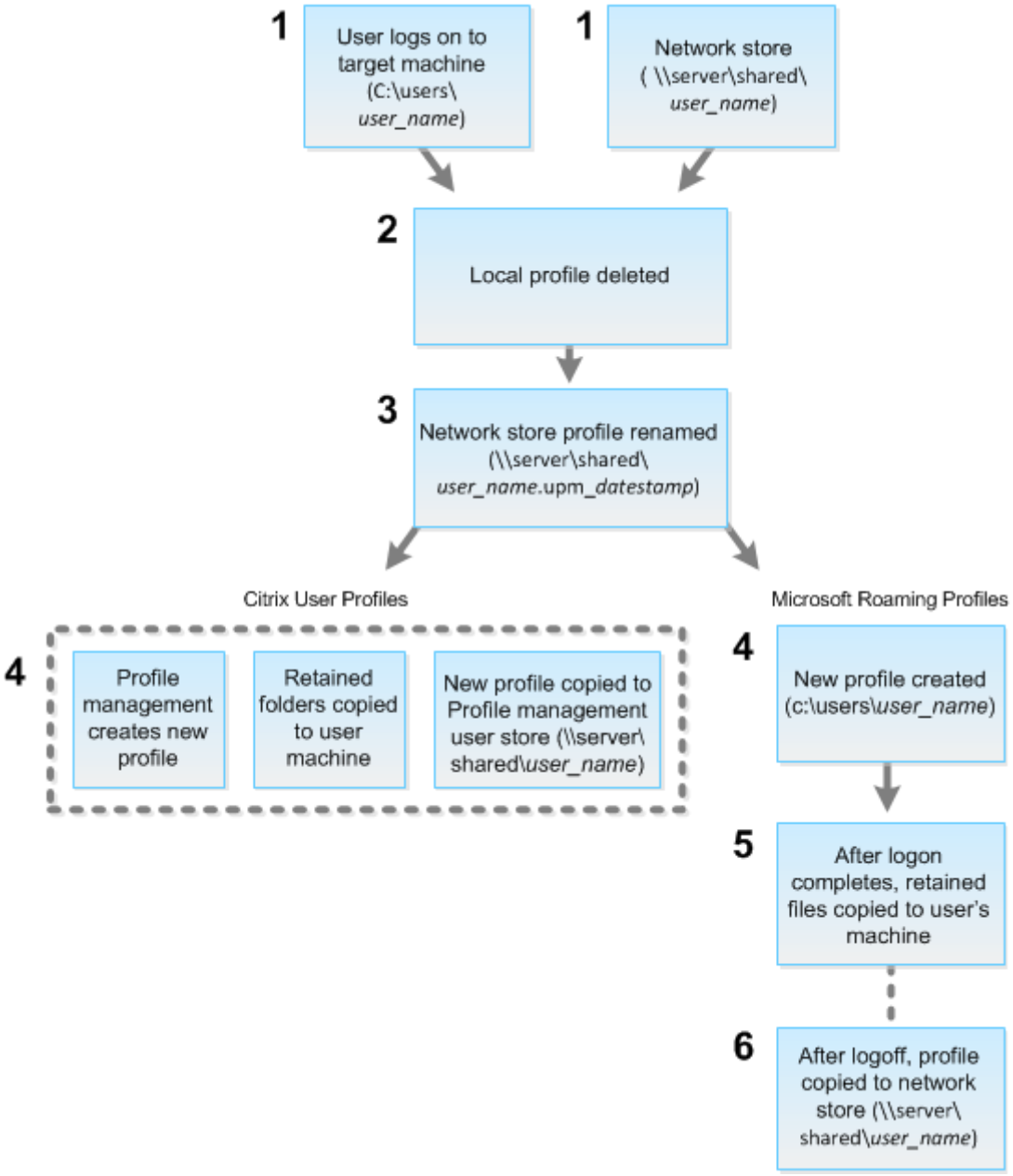
> **PRECAUCIÓN:**
>
> Cuando se restablece un perfil, las carpetas y archivos del usuario se guardan y se copian en el nuevo perfil. Sin embargo, la mayoría de los datos del perfil de usuario faltan (por ejemplo, se restablece el registro y podrían eliminarse los parámetros de la aplicación).

La función de restablecimiento se aplica tanto a las soluciones de perfiles basadas en archivos como a las basadas en contenedores.

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 lo procesa Profile Management, pero recibe un comando de perfil móvil (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 con las reglas de importación de Profile Management. Las carpetas se copian de nuevo en el perfil de red y el usuario puede iniciar sesión 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 de usuario en Director

Si utiliza Citrix Virtual Desktops (VDA de escritorio), haga lo siguiente:

1. En **Director**, busque al usuario cuyo perfil quiere restablecer y, a continuación, 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.

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.

> **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. Esta acción de inicio de sesión 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.

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.

Tenga en cuenta lo siguiente:

- Si el almacén de usuarios está habilitado como solución de perfiles de usuario, el nuevo perfil contiene las siguientes carpetas personales del perfil de usuario original:
  - Escritorio

  - Cookies
  - Favoritos
  - Documentos
  - Imágenes
  - Música
  - Vídeos

- Si el contenedor de perfiles de Citrix Management está habilitado como toda solución de perfiles de usuario, el nuevo perfil no contiene las carpetas personales anteriores.
- En Windows 8 y versiones posteriores, las cookies no se copian en el nuevo perfil al restablecerse los perfiles.

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_fechayhora.
4. Elimine el nombre del perfil actual. Es decir, el que no tiene la extensión upm_datestamp.
5. Cambie el nombre de la carpeta archivada mediante el nombre del perfil original; es decir, elimine la extensión de fecha y hora. Con ello, habrá devuelto el perfil a su estado original, prerrestablecido.

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

August 17, 2024

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**.

Grabación dinámica de sesiones

Puede grabar la sesión activa actual mediante los controles de grabación de sesiones de la pantalla **Detalles del usuario**. Para obtener más información sobre la grabación dinámica de sesiones, consulte el artículo Servicio de grabación de sesiones.

Grabación de sesiones basada en directivas

Para configurar la Grabación de sesiones en Director basada en directivas mediante la herramienta DirectorConfig, consulte la sección **Configurar Director para usar el servidor de Grabación de sesiones** en Configurar directivas de grabación de sesiones.

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 Autorizar a usuarios.

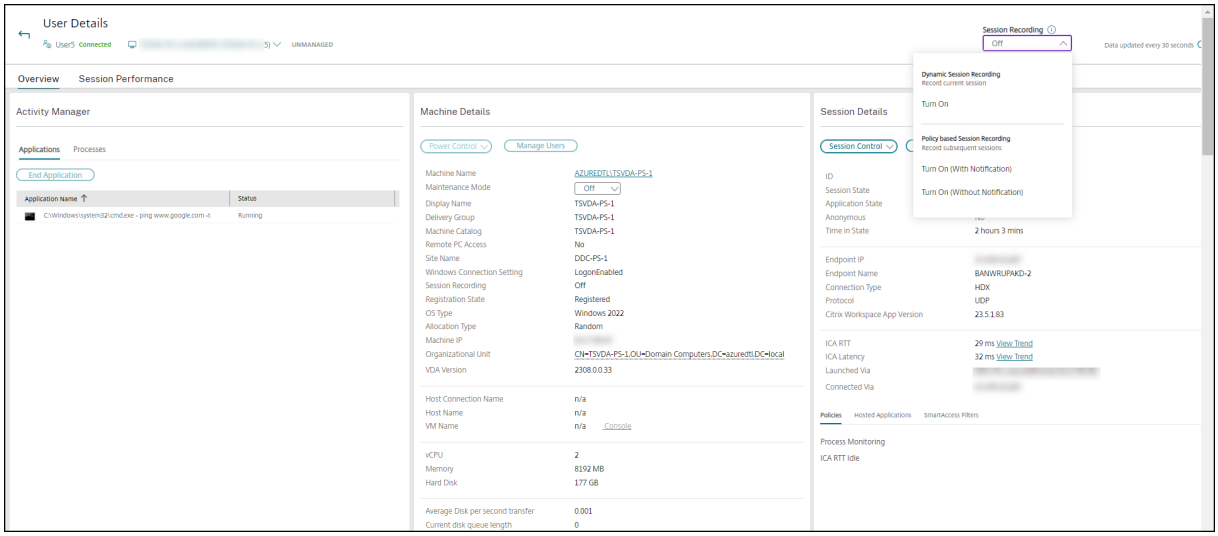
> **Nota:**
> Los cambios realizados en los parámetros de la Grabación de sesiones a través de Director o la Consola de directivas de grabación de sesiones surten efecto a partir de la siguiente sesión ICA.

Controles de Grabación de sesiones en Director

Puede usar las acciones **Detalles del usuario** > **Grabación de sesiones** para grabar las sesiones actuales o posteriores.

- Habilite la grabación dinámica de sesiones: se graba la sesión actual.
- Activar (con notificación): Las siguientes sesiones se graban y se notifica al usuario de que la sesión se está grabando cuando este inicia una sesión ICA.
- Activar (sin notificación): Las siguientes sesiones se graban 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**.



El panel **Detalles de la máquina** muestra el estado de la directiva Grabación de sesiones de la máquina.

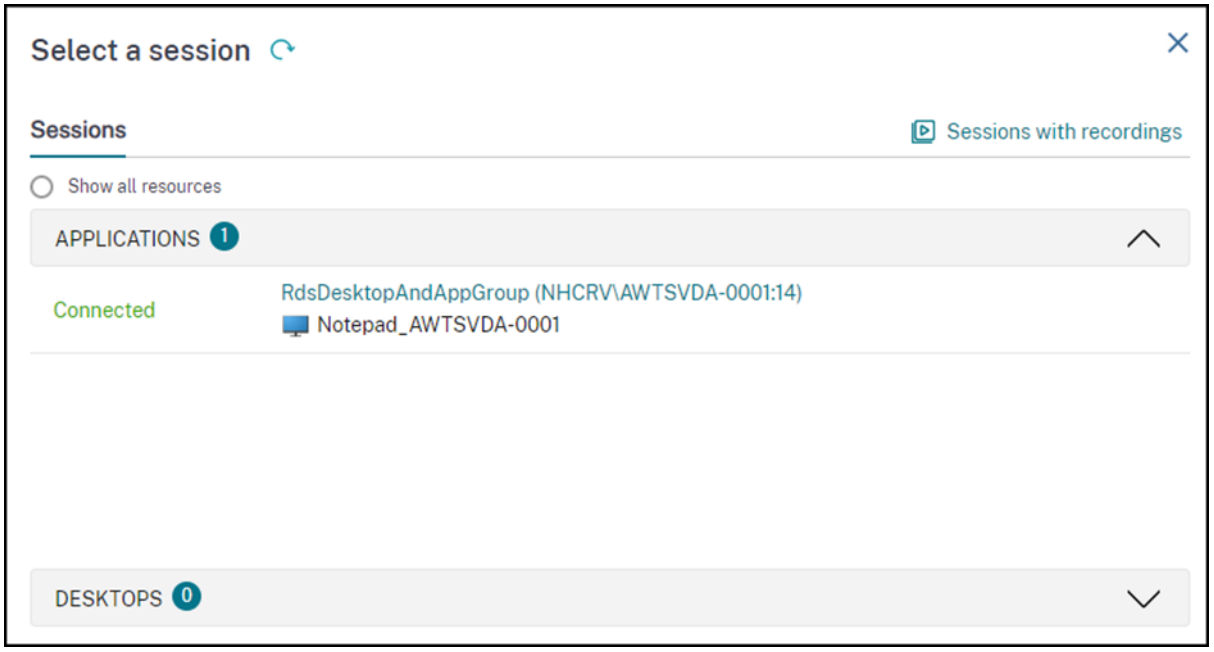
Reproducir sesiones grabadas y en directo

Puede reproducir sesiones de usuario grabadas y en directo para entender los problemas a los que se enfrenta el usuario. El fácil acceso a las grabaciones y a las métricas relacionadas con las sesiones en la consola de Director elimina la necesidad de buscar las grabaciones en varios servidores de grabación de sesiones o de buscar aplicaciones de terceros para ver las grabaciones. Ayuda a correlacionar los problemas descubiertos en las grabaciones con las métricas de rendimiento.

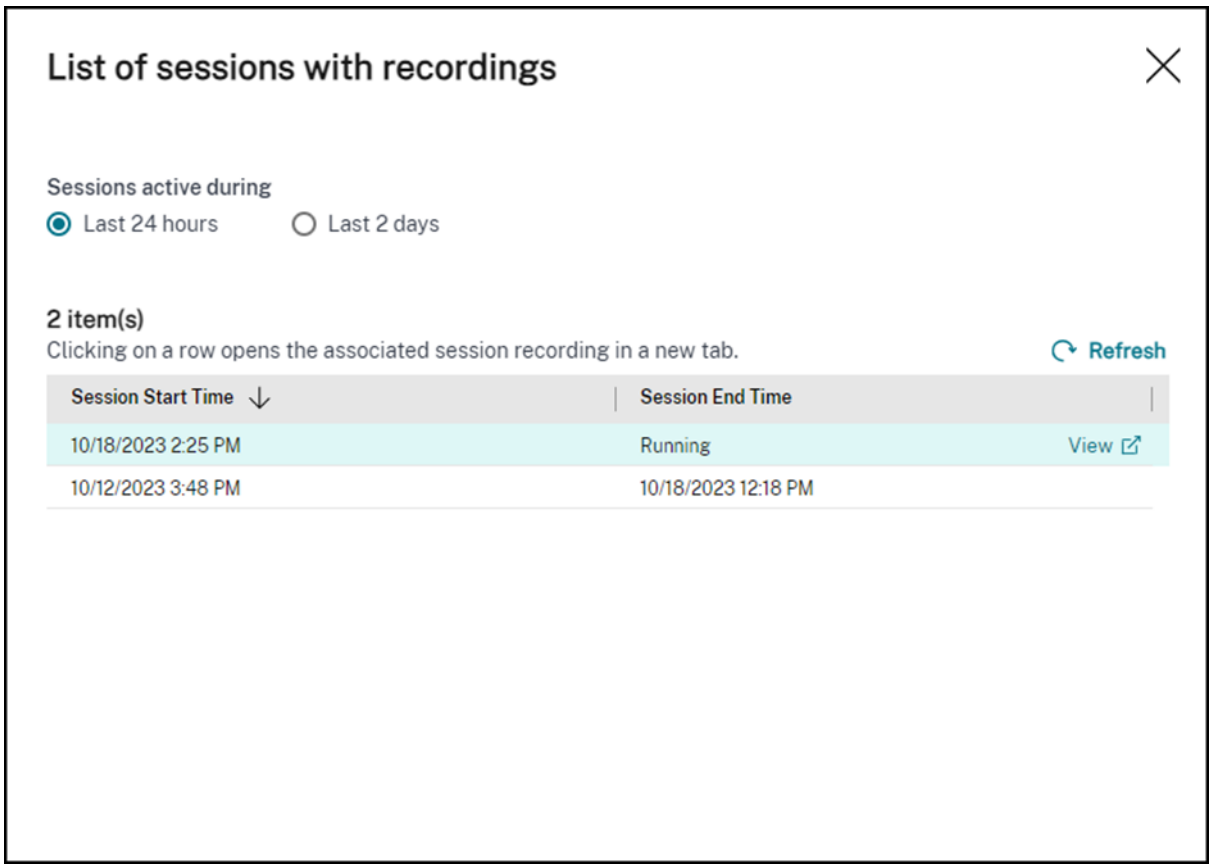
Esta función requiere lo siguiente:

- El VDA y los servidores de grabación de sesiones tienen la versión 2308 o posterior.
- Delivery Controller y Director tienen la versión 2311 o una posterior.

Director almacena las grabaciones de las sesiones en un repositorio centralizado. La lista de grabaciones que pertenecen al usuario se muestra al hacer clic en el enlace modal **Selector de sesiones** > **Sesiones con grabaciones**.



Puede elegir ver las grabaciones de las sesiones que estuvieron activas durante las últimas 24 horas o los últimos 2 días. Las grabaciones en directo de las sesiones actualmente activas se marcan con la **hora de finalización de la sesión** como **En curso**.



Haga clic en el enlace **Ver** para reproducir la grabación en una ficha nueva mediante el servidor de reproducción de grabación de sesiones de Citrix.

Tabla de compatibilidad de funciones

August 17, 2024

Citrix Director 7 2203 es compatible con:

- Citrix Virtual Apps and Desktops 7 2112 y versiones posteriores
- Citrix Virtual Apps and Desktops 7 1912 LTSR

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 la versión de un Delivery Controller, se le solicitará que actualice la versión del sitio cuando abra Studio. Para obtener más información, consulte **Secuencia de actu-**

> **alización** 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, se mostrará una nota en el panel de mandos de Director donde se indica 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.

Versión de Director	Función	Dependencias: Versión mínima requerida	Edición
2311	Reproduce sesiones grabadas y en directo	VDA 2308 y DDC 2311	Todo
2311	Topología de sesión	Ninguno	Todo
2311	Resolución de pantalla óptima	Ninguno	Todo
2311	Optimización de MS Teams	VDA 2311 y DDC más recientes	Todo
2311	Descripción general de los sondeos: mejoras	Ninguno	Todo
2311	Vista de duración de inicio de sesión renovada	Ninguno	Todo
2308	Resumen y desglose de los sondeos	Ninguno	Todo

Versión de Director	Función	Dependencias: Versión mínima requerida	Edición
2308	Compatibilidad con Citrix Probe Agent para la autenticación de varios factores de Citrix Gateway	Citrix Gateway	Todo
2308	Inhabilitar las alertas de Hypervisor	Ninguno	Todo
2308	Tendencias de las métricas de la experiencia en sesión	Ninguno	Todo
2305	Permite la autenticación a través de Citrix Gateway	Ninguno	Todo
2305	Administración de Autoscale en Director	Ninguno	Todo
2303	Alerta de máquinas fallidas	DC 7 2303	Premium
2203	Compatibilidad con TLS 1.3	-	Todo
2212	Utilización de GPU en tiempo real disponible para las GPU de AMD	DC 7.14 y VDA 7.14 con Windows de 64 bits y HDX 3D Pro habilitado	Todo
2212	Programación de sondeo avanzada	DC 7 1906 y Citrix Probe Agent 2209	Premium
1909	Configurar sitios locales con Citrix Analytics for Performance	DC 7 1906 y VDA 1906	Todo
1906	Reconexión automática de sesión	DC 7 1906 y VDA 1906	Todo
1906	Duración de inicio de sesión	DC 7 1906 y VDA 1903	Todo

Versión de Director	Función	Dependencias: Versión mínima requerida	Edición
1906	Sondeo de escritorios	DC 7 1906 y Citrix Probe Agent 1903	Premium
7.9 y versiones posteriores	Duración de Citrix Profile Management en la carga de perfil	VDA 1903	Todo
1811	Desglose de perfil	DC 7 1811 y VDA 1811	Todo
1811	Supervisar alertas de hipervisor	DC 7 1811	Premium
1811	Sondeo de aplicaciones	DC 7 1811 y Citrix Application Probe Agent 1811	Premium
1811	Estado de licencias RDS de Microsoft	DC 7 1811 y VDA 7.16	Todo
1811	Datos clave de RTOP	DC 7 1811 y VDA 1808	Premium
1808	Exportación de datos de filtros	DC 7 1808	Todo
1808	Desglose de la sesión interactiva	DC 7 1808 y VDA 1808	Todo
1808	Desglose de GPO	DC 7 1808 y VDA 1808	Todo
1808	Datos históricos disponibles de la máquina mediante la API de OData	DC 7 1808	Todo
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	Ninguno	Todo

Versión de Director	Función	Dependencias: Versión mínima requerida	Edición
7.18	Desglose de la sesión interactiva	Ninguno	Todo
7.17	Autenticación con tarjetas inteligentes PIV	Ninguno	Todo
7.16	Análisis de aplicaciones	DC 7.16 y VDA 7.15	Todo
7.16	API de OData 4	DC 7.16	Todo
7.16	Remedo de usuarios en Linux VDA	VDA 7.16	Todo
7.16	Admitir el grupo local de dominio	Ninguno	Todo
7.16	Acceso a la consola de la máquina	DC 7.16	Todo
7.15	Supervisión de fallos de aplicación	DC 7.15 y VDA 7.15	Todo
7.14	Solución de problemas de aplicación	DC 7.13 y VDA 7.13	Todo
7.14	Supervisar discos	DC 7.14 y VDA 7.14	Todo
7.14	Supervisar GPU	DC 7.14 y VDA 7.14	Todo
7.13	Protocolo de transporte en el panel “Detalles de la sesión”	DC 7.x y VDA 7.13	Todo
7.12	Descripciones claras de los errores de conexión y de máquina	DC 7.12 y VDA 7.x	Todo
7.12	Mayor disponibilidad de datos históricos en la edición Enterprise	DC 7.12 y VDA 7.x	Empresarial

Versión de Director	Función	Dependencias: Versión mínima requerida	Edición
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	Todo
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	Todo
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	Todo
7.7	Supervisión y alertas mejoradas	DC 7.7 y VDA 7.x	Premium (anteriormente Platinum)
7.7	Integrar en Autenticación de Windows	DC 7.x y VDA 7.x	Todo
7.7	Uso de SO de sesión única y SO multisesión	DC 7.7 y VDA 7.x	Premium (anteriormente Platinum)
7.6.300	Compatibilidad con canal virtual Framehawk	DC 7.6 y VDA 7.6	Todo
7.6.200	Integrar en la Grabación de sesiones	DC 7.6 y VDA 7.x	Premium (anteriormente Platinum)

Versión de Director	Función	Dependencias: Versión mínima requerida	Edición
7	Integrar en HDX Insight	DC 7.6, VDA 7.x y Citrix ADM	Premium (anteriormente Platinum)

Granularidad y retención de datos

August 17, 2024

Agregar valores de datos

Monitor Service recopila diferentes 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. 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, por lo que se exponen como sumas para un período de tiempo.

Evaluar datos simultáneos

Las sesiones deben superponerse para considerarse simultáneas. Sin embargo, cuando el intervalo temporal es de 1 minuto, todas las sesiones de ese minuto (tanto si se superponen como si no) se consideran simultáneas. El tamaño del intervalo es tan pequeño que la sobrecarga de rendimiento que implica el cálculo con precisión no compensa el valor agregado. 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 hay 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 tienen datos. Aunque podrían existir 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 describe en la sección anterior. Se pueden usar para descubrir tendencias históricas, pero los eventos sin procesar podrían 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, se debe considerar que no hay datos de resumen para intervalos parciales que puedan ocurrir ni para el comienzo o el final del período de tiempo en cuestión.
- **Eventos latentes y perdidos.** Las métricas agregadas en tablas de resumen podrían ser ligeramente inexactas si hay eventos perdidos o latentes en el período 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 vacíos 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. Podrían faltar datos porque se hayan limpiado las tablas de resumen y de datos sin procesar. Los

períodos de retención también podrían 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, es posible que los que 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, podría 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 < = 1 hora; se utiliza una granularidad de minutos
- 0 < T <= 30 días; se utiliza una granularidad de horas
- T > 31 días; se utiliza una 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. La limpieza 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 que se produjera una 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:

```
asnp Citrix.*
 Get-MonitorConfiguration
 Set-MonitorConfiguration -<setting name> <value>
```


	Nombre del parámetro	Limpieza afectada	Días de retención para Premium	Días de retención para Advanced
1	GroomSessionsRetentionDays	Retención de registros de conexión y de sesión después de cerrar la sesión	90	31
2	GroomFailuresRetentionDays	Registros de MachineFail-ureLog y Connection-FailureLog	90	31
3	GroomLoadIndexesRetentionDays	Registros de LoadIndex	90	31

	Nombre del parámetro	Limpieza afectada	Días de retención para Premium	Días de retención para Advanced
4	GroomDeletedRetentionDays	Entidades de máquina, catálogo de máquinas, grupo de escritorios e hipervisor cuyo estado de ciclo de vida (LifecycleState) es “Eliminado” (Deleted). Este parámetro también elimina los registros de Session, SessionDetail, Summary, Failure o LoadIndex relacionados.	90	31

	Nombre del parámetro	Limpieza afectada	Días de retención para Premium	Días de retención para Advanced
5	GroomSummariesRetentionDays	Registros de DesktopGroupSummary, FailureLogSummary y LoadIndexSummary. Datos agregados: granularidad diaria	365	31
6	GroomMachineHotfixLogRetentionDays	Parches rápidos aplicados a las máquinas de VDA y Controllers	90	31
7	GroomMinuteRetentionDays	Datos agregados: granularidad de minuto	3	3
8	GroomHourlyRetentionDays	Datos agregados: granularidad horaria	32	31
9	GroomApplicationInstanceRetentionDays	Historial de instancias de aplicación	90	No aplicable
10	GroomNotificationLogRetentionDays	Registro del registro de notificaciones	90	No aplicable

	Nombre del parámetro	Limpieza afectada	Días de retención para Premium	Días de retención para Advanced
11	GroomResourceUsageRawDataRetentionDays	Datos de utilización de recursos: datos sin procesar	3	3
12	GroomResourceUsageMinuteDataRetentionDays	Datos resumidos de utilización de recursos: granularidad de minuto	7	7
13	GroomResourceUsageHourDataRetentionDays	Datos resumidos de utilización de recursos: granularidad de hora	30	30
14	GroomResourceUsageDayDataRetentionDays	Datos resumidos de utilización de recursos: granularidad de día	365	31
15	GroomProcessUsageRawDataRetentionDays	Datos de utilización de procesos: datos sin procesar	1	1
16	GroomProcessUsageMinuteDataRetentionDays	Datos de utilización de procesos: granularidad de minuto	3	3

	Nombre del parámetro	Limpieza afectada	Días de retención para Premium	Días de retención para Advanced
17	GroomProcessUsageHourDataRetentionDays	Datos de utilización de procesos: granularidad horaria	7	7
18	GroomProcessUsageDayDataRetentionDays	Datos de utilización de procesos: granularidad diaria	30	30
19	GroomSessionMetricsDataRetentionDays	Datos de métricas de sesiones	1	1
20	GroomMachineMetricsDataRetentionDays	Datos de métricas de máquinas	3	3
21	GroomMachineMetricsDaySummaryDataRetentionDays	Datos resumidos de métricas de máquinas	365	31
22	GroomApplicationErrorsDataRetentionDays	Datos de errores de aplicaciones	1	1
23	GroomApplicationFaultsDataRetentionDays	Datos de 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.
Asimismo, los parámetros de la retención basada en licencia son los siguientes:

- **Sitios con licencias Premium:** La retención de limpieza para todos los parámetros se limita a 1000 días (Citrix recomienda 365 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 podrían ser altos. Si la cantidad de datos es excesiva, el impacto en el rendimiento podría resultar significativo.

- **Datos de sesiones y eventos.** Los datos recopilados cada vez que se inicia una sesión y se establece una conexión o reconexión. En sitios grandes (100 000 usuarios), estos datos crecen 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

August 17, 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 Solución de problemas al registrar Virtual Delivery Agent en Delivery Controllers en Citrix Virtual Apps and Desktops de Knowledge Center para ver los motivos frecuentes de problemas de comunicación entre el Controller y el VDA.

Categoría	Motivo	Problema	Acción
[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.
[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 el tiempo de espera se agotó 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.

Categoría	Motivo	Problema	Acción
[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] LicenseFeature Refused	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 **Número máximo de sesiones** 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 **Get-BrokerAccessPolicyRule** de PowerShell en un Delivery Controller y compruebe si el valor de **AllowedProtocols** 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, aprovisione más VDA con SO multisesión. Compruebe que haya VDA con SO de sesión única disponibles para las conexiones. Aprovisione 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 **reconexión para sesiones activas** está inhabilitada, el cliente no puede conectarse a la sesión activa.	En el Controller, compruebe que la **reconexión para sesiones activas** está habilitada. Compruebe que el valor de **DisableActiveSessionReconnect** en el Registro, en **HKEY_LOCAL_MACHINE\Software** 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 aprovisionada 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] MaxTotalInstance-sExceeded	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 **Limitar la cantidad de instancias ejecutadas a la vez a**, 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 **Limitar a una sola instancia por usuario** en la configuración de la aplicación.
[1] ClientConnectionFailure	[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 (representada como Carga máxima en Director)	4	La máquina se notifica a sí misma en su capacidad máxima; es decir, al llegar al índice de carga máxima	Compruebe que todos los hipervisores están iniciados. Agregue más máquinas a los grupos de entrega afectados mediante más capacidad para el hipervisor o con 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	1011	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 `nslookup`.
	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 Solución de problemas al registrar Virtual Delivery Agent en Delivery Controllers en Citrix Virtual Apps and Desktops (CTX136668) 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 Solución de problemas al registrar Virtual Delivery Agent en Delivery Controllers en Citrix Virtual Apps and Desktops (CTX136668) de Knowledge Center para ver los motivos frecuentes de problemas de comunicación entre el Controller y el VDA. Contacte con Citrix Support.
AgentWrongActiveDirectoryOU	103	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
EmptyRegistrationReques	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
UnsupportedCredentialSecurityversion	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 Solución de problemas al registrar Virtual Delivery Agent en Delivery Controllers en Citrix Virtual Apps and Desktops (CTX136668) 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	112	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	203	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.	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 **HKEY_LOCAL_MACHINE\Software** Consulte el artículo Entradas de clave de Registro utilizadas por Citrix Virtual Apps and Desktops (CTX117446) de Knowledge Center para obtener más información. Al aumentar esta cantidad, puede que el Controller requiera más recursos de CPU y memoria.

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 Solución de problemas al registrar Virtual Delivery Agent en Delivery Controllers en Citrix Virtual Apps and Desktops (CTX136668) 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.

Avisos legales de terceros

August 17, 2024

Esta versión de Citrix Virtual Apps and Desktops puede incluir software de terceros con licencias definidas en los términos de los siguientes documentos:

- Avisos de terceros sobre Citrix Virtual Apps and Desktops (Descargar PDF)
- Avisos de software para uso no comercial de FlexNet Publisher 2017 (11.15.0.0) (Descargar PDF)
- Software de terceros de FlexNet Publisher Documentation Supplement y software Open Source utilizados en FlexNet Publisher 11.15.0 (Descargar PDF)

SDK y API

August 17, 2024

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.

Este producto es compatible con las versiones 3 a 5 de PowerShell.

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.

Las API REST de Citrix Virtual Apps and Desktops

Con las API de REST de Citrix Virtual Apps and Desktops, puede automatizar la administración de los recursos en una implementación de Citrix Virtual Apps and Desktops.

Las API de REST de Citrix Virtual Apps and Desktops están disponibles en https://developer.cloud.com/citrixworkspace/citrix-daas-rest-apis/docs/citrix-virtual-apps-and-desktops-apis. Las API no aplicables a Citrix Virtual Apps and Desktops están marcadas en consecuencia. Siga las instrucciones que se indican allí para configurar el acceso al servicio de API y utilizarlas para administrar y optimizar sus recursos.

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.