CITRIX

Citrix Virtual Apps and Desktops

Contents

Citrix Virtual Apps and Desktops 7 1811 3

Novedades 4

Problemas resueltos 12

Problemas conocidos 21

Avisos de terceros 25

Obsolescencia 26

Requisitos del sistema 35

Información técnica general 47

Active Directory 58

Bases de datos 61

Métodos de entrega 68

Aplicaciones y escritorios publicados de Citrix Virtual Apps 71

Aplicaciones alojadas en VM 73

Escritorios VDI 75

Puertos de red 76

HDX 80

Transporte adaptable 90

Instalar y configurar 97

Antes de instalar 100

Entornos de virtualización de Microsoft Azure Resource Manager 108

Entornos de virtualización de Microsoft System Center Virtual Machine Manager 119

Entornos de virtualización de XenServer 122

Entornos de Microsoft System Center Configuration Manager 124

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Entornos de virtualización de VMware **126**

Entornos de virtualización de Nutanix **133**

Entornos de virtualización de Microsoft Azure **135**

Instalar componentes principales **139**

Instalar agentes VDA **150**

Instalar mediante la línea de comandos **166**

Instalar agentes VDA usando scripts **178**

Crear un sitio **180**

Crear catálogos de máquinas **185**

Administrar catálogos de máquinas **202**

Crear grupos de entrega **209**

Administrar grupos de entrega **215**

Crear grupos de aplicaciones **237**

Administrar grupos de aplicaciones **246**

Acceso con Remote PC **251**

App-V **259**

AppDisks **274**

Secure Browser de Virtual Apps **305**

Publicar contenido **306**

VDI de servidor **312**

Personal vDisk **314**

Instalar y actualizar **322**

Configurar y administrar **326**

Herramientas **338**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Pantallas, mensajes y solución de problemas **341**

Migrar Personal vDisk a App Layering **352**

Eliminar componentes **365**

Actualizar y migrar **367**

Cambios en 7.x **370**

Actualizar una implementación **377**

Actualizar un servidor de trabajo XenApp 6.5 a un nuevo VDA **392**

Migrar XenApp 6.x **393**

Proteger **427**

Recomendaciones y consideraciones de seguridad **429**

Integrar Citrix Virtual Apps and Desktops con Citrix Gateway **437**

Administración delegada **438**

Tarjetas inteligentes **447**

Implementaciones de tarjeta inteligente **453**

Autenticación PassThrough y Single Sign-On con tarjetas inteligentes **460**

Transport Layer Security (TLS) **462**

Servicio de autenticación federada **474**

Introducción a las arquitecturas del Servicio de autenticación federada **502**

Implementar ADFS y el Servicio de autenticación federada **512**

Integrar Azure AD y el Servicio de autenticación federada **516**

Procedimientos del sistema de autenticación federada: configuración y administración **564**

Configurar el Servicio de autenticación federada para la entidad de certificación **565**

Proteger claves privadas del Servicio de autenticación federada **572**

Seguridad y configuración de red del Servicio de autenticación federada **591**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Soluciones a problemas de inicio de sesión en Windows relacionados con el Servicio de autenticación federada 602

Cmdlets de PowerShell para el Servicio de autenticación federada (FAS) 615

Dispositivos 616

Citrix Ready Workspace Hub 617

Dispositivos USB genéricos 632

Dispositivos móviles y de pantalla táctil 633

Puertos serie 635

Teclados especiales 640

Dispositivos TWAIN 642

Cámaras web 643

Gráficos 644

HDX 3D Pro 646

Aceleración de GPU para sistemas operativos de servidor Windows 647

Aceleración de GPU para sistemas operativos de escritorio Windows 650

Framehawk 656

Thinwire 665

Marca de agua de sesión basada en texto 672

Contenido multimedia 674

Funciones de audio 677

Redirección de contenido de explorador Web 686

Redirección de Flash 694

Redirección multimedia HTML5 704

Conferencias de vídeo de HDX y compresión de vídeo de cámara Web de HDX 707

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Redirección de Windows Media 710

Redirección de contenido general 711

Redirección de carpetas del cliente 712

Redirección del host al cliente 713

Acceso a aplicaciones locales y redirección de URL 721

Consideraciones sobre unidades del cliente y redirección de USB genérico 729

Imprimir 740

Ejemplo de configuración de la impresión 748

Prácticas recomendadas, consideraciones de seguridad y operaciones predeterminadas 752

Directivas y preferencias de impresión 754

Aprovisionar impresoras 756

Mantener el entorno de impresión 765

Directivas 771

Trabajar con directivas 773

Plantillas de directiva 777

Crear directivas 781

Comparar, priorizar, modelar y solucionar problemas de directivas 788

Configuraciones predeterminadas de directivas 792

Referencia para configuraciones de directivas 827

Configuraciones de directiva de ICA 832

Configuraciones de directiva de Reconexión automática de clientes 838

Configuraciones de directiva de Sonido 842

Configuraciones de directiva de Ancho de banda 844

Configuraciones de directiva de Redirección de contenido bidireccional 850

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Redirección de contenido de explorador Web **854**

Configuraciones de directiva de Sensores del cliente **860**

Configuraciones de directiva de Interfaz de usuario de escritorio **861**

Configuraciones de directiva de Supervisión de usuario final **863**

Configuración de directiva de Enhanced Desktop Experience **864**

Configuraciones de directiva de Redirección de archivos **864**

Configuraciones de directiva de Redirección de Flash **869**

Configuraciones de directiva de Gráficos **874**

Configuraciones de directiva de Almacenamiento en caché **880**

Configuraciones de directiva de Framehawk **881**

Configuraciones de directiva de Keep Alive **881**

Configuraciones de directiva de Acceso a aplicaciones locales **882**

Configuraciones de directiva de Experiencia móvil **883**

Configuraciones de directiva de Multimedia **884**

Configuraciones de directiva de Conexiones de multisecuencia **892**

Configuraciones de directiva de Redirección de puertos **894**

Configuraciones de directiva de Impresión **895**

Configuraciones de directiva de Impresoras del cliente **899**

Configuraciones de directiva de Controladores **903**

Configuraciones de directiva de Universal Print Server **904**

Configuraciones de directiva de Impresión universal **907**

Configuraciones de directiva de Seguridad **910**

Configuraciones de directiva de Límites de servidor **911**

Configuraciones de directiva de Límites de sesión **912**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Fiabilidad de la sesión **914**

Configuraciones de directiva de Marca de agua de la sesión **916**

Parámetros de directiva de control de zona horaria **918**

Configuraciones de directiva de Dispositivos TWAIN **919**

Configuraciones de directiva de Dispositivos USB **920**

Configuraciones de directiva de Presentación visual **929**

Configuraciones de directiva de Imágenes en movimiento **931**

Configuraciones de directiva de Imágenes fijas **933**

Configuraciones de directiva de WebSockets **935**

Configuraciones de directiva de Administración de carga **935**

Configuraciones de directiva de Profile Management **937**

Parámetros avanzados de directiva **938**

Parámetros básicos de directiva **939**

Configuraciones de directiva de Multiplataforma **943**

Configuraciones de directiva de Sistema de archivos **944**

Configuraciones de directiva de Exclusiones **945**

Configuraciones de directiva de Sincronización **946**

Configuraciones de directiva de Redirección de carpetas **948**

Configuraciones de directiva de AppData(Roaming) **948**

Configuraciones de directiva de Contactos **949**

Configuraciones de directiva de Escritorio **949**

Configuraciones de directiva de Documentos **950**

Configuraciones de directiva de Descargas **951**

Configuraciones de directiva de Favoritos **951**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Vínculos **952**

Configuraciones de directiva de Música **953**

Configuraciones de directiva de Imágenes **953**

Configuraciones de directiva de Juegos guardados **954**

Configuraciones de directiva de Menú Inicio **955**

Configuraciones de directiva de Búsquedas **955**

Configuraciones de directiva de Vídeos **956**

Configuraciones de directiva de Registro **957**

Configuraciones de directiva de Gestión de perfiles **961**

Configuraciones de directiva de Registro del sistema **965**

Configuraciones de directiva para Perfiles de usuario de streaming **966**

Configuraciones de directiva de Receiver **968**

Configuraciones de directiva de Virtual Delivery Agent **969**

Configuraciones de directiva de HDX 3D Pro **971**

Configuraciones de directiva de Supervisión **972**

Configuraciones de directiva de IP virtual **976**

Configurar la redirección de puertos COM y puertos LPT mediante el Registro **976**

Configuración de directivas de Connector para Configuration Manager 2012 **978**

Administrar **981**

Licencias **983**

Licencias de varios tipos **986**

Aplicaciones **988**

Aplicaciones de la Plataforma universal de Windows **1001**

Zonas **1003**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Conexiones y recursos **1016**

Caché de host local **1030**

IP virtual y bucle invertido virtual **1041**

Delivery Controllers **1044**

Registro de VDA **1049**

Sesiones **1060**

Usar búsquedas en Studio **1068**

Etiquetas **1068**

Compatibilidad con IPv4/IPv6 **1079**

Perfiles de usuario **1082**

Recopilar seguimientos de Citrix Diagnostic Facility (CDF) durante el inicio del sistema **1089**

Citrix Insight Services **1092**

Citrix Scout **1105**

Supervisar **1118**

Registros de configuración **1119**

Registros de eventos **1125**

Director **1125**

Instalar y configurar **1130**

Configuración avanzada **1133**

Configurar la autenticación con tarjetas inteligentes PIV **1137**

Configurar el análisis de red **1141**

Administración delegada y Director **1143**

Proteger la implementación de Director **1146**

Análisis de sitios **1148**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Alertas y notificaciones **1158**

Filtrar datos para solucionar fallos **1176**

Supervisar tendencias históricas en un sitio **1178**

Solucionar problemas de implementaciones **1183**

Solucionar problemas de aplicaciones **1183**

Sondeo de aplicaciones **1188**

Solucionar problemas de máquinas **1192**

Solucionar problemas de usuarios **1200**

Diagnosticar problemas de inicio de sesión de los usuarios **1202**

Remedar usuarios **1208**

Envío de mensajes a los usuarios **1210**

Resolver fallos de aplicación **1211**

Restaurar conexiones de escritorio **1212**

Restaurar sesiones **1213**

Ejecutar informes de sistema de canales HDX **1214**

Restablecer un disco Personal vDisk **1214**

Restablecer un perfil de usuario **1215**

Grabar sesiones **1218**

Matriz de compatibilidad de funciones **1220**

Granularidad y retención de datos **1224**

SDK y API **1231**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Citrix Virtual Apps and Desktops 7 1811

March 13, 2019

Citrix Virtual Apps and Desktops 7 1811 es la versión actual (Current Release) más reciente de Citrix Virtual Apps and Desktops. Esta documentación refleja las características y las configuraciones de esta versión.

Versiones anteriores

Para ver la documentación sobre las versiones anteriores, consulte:

- Citrix Virtual Apps and Desktops 7 1808
- XenApp y XenDesktop 7.18
- XenApp y XenDesktop 7.17
- XenApp y XenDesktop 7.16
- Versiones anteriores de XenApp y XenDesktop Current Release
- XenApp y XenDesktop 7.15 Long Term Service Release
- XenApp y XenDesktop 7.6 Long Term Service Release

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 en Citrix Cloud

La oferta de Virtual Apps and Desktops de Citrix Cloud es el servicio Citrix Virtual Apps and Desktops Service. Para obtener más información, consulte Citrix Virtual Apps and Desktops Service.

Componentes relacionados

Para ver documentación sobre componentes relacionados, consulte:

- AppDNA
- Citrix App Layering
- HDX RealTime Optimization Pack
- Licencias
- Linux Virtual Delivery Agent
- Profile Management
- Citrix Provisioning

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Módulos de administración SCOM de Citrix
- Autoservicio de restablecimiento de contraseñas
- Grabación de sesiones
- StoreFront
- Workspace Environment Management

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

Para conocer los últimos cambios en los nombres y números de versión, consulte:

- Nuevos nombres de producto
- Nuevos números de versión de productos y componentes

Novedades

March 14, 2019

Acerca de esta 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:

- **Instalar o actualizar un sitio**

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

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

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

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

Para obtener instrucciones:

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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Citrix Virtual Apps and Desktops 7 1811

Esta versión del producto presenta las siguientes funciones nuevas, modificadas y mejoradas.

> **Nota:**
>
> Se han introducido nuevos nombres de producto y números de versión en Citrix Virtual Apps and Desktops 7 1808. Esa información se conserva en este artículo como referencia. Para obtener más información, consulte Nuevos nombres de producto al final de este artículo.

Grupos de entrega: Nueva interfaz de Studio para crear programaciones de reinicios de las máquinas

En las versiones anteriores, se utilizaba Studio para crear una programación de reinicios de las máquinas en un grupo de entrega. Además, para crear varias programaciones, se utilizaban los cmdlets de PowerShell. Ahora, la interfaz actualizada de Studio permite crear y administrar una o varias programaciones de reinicios. Para obtener información más detallada, consulte Crear y administrar programaciones de reinicios para las máquinas de un grupo de entrega.

Citrix Scout: Seguimientos de AOT en recursos compartidos de red

En versiones anteriores, los seguimientos AOT que se guardaban en los recursos compartidos de red no se incluían en los diagnósticos recopilados. Ahora, esos seguimientos sí se incluyen. Para obtener más información, consulte Citrix Scout.

Catálogos de máquinas: Nuevo nivel funcional

Se ha agregado un nuevo nivel funcional de catálogo de máquinas. El valor predeterminado sigue siendo 7.9 (o posterior). Puede dejar ese valor predeterminado, a menos que todos los VDA en el catálogo sean de la versión 1811 o una versión posterior compatible. Para obtener más información, consulte Niveles funcionales y versiones de VDA.

Aprovisionar Machine Creation Services a hosts AWS dedicados

En esta versión se agrega compatibilidad para el aprovisionamiento de Machine Creation Services (MCS) a los hosts AWS dedicados. Un administrador puede crear un catálogo de máquinas con el arrendamiento del host definido a través de PowerShell. Consulte Compatibilidad con el arrendamiento de host AWS.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Compatibilidad con roles IAM de AWS

Citrix Studio ofrece la posibilidad de configurar una conexión de host de AWS para utilizar roles de IAM introduciendo **role_based_auth** como valor para los campos “clave de acceso” y “clave secreta”. Asimismo, se requiere un rol de IAM que defina la directiva y los permisos requeridos por Citrix al agregarse a las instancias de Delivery Controllers o Cloud Connectors alojadas de AWS.

Citrix Director

Rendimiento de inicio de sesión: Desglose de perfiles

Ahora el panel “Duración de inicio de sesión” en las páginas de **Detalles del usuario** incluye un desglose sobre la fase de carga del perfil en el proceso de inicio de sesión. Este desglose de perfiles ofrece información útil sobre los perfiles de usuario para la sesión actual, una información que puede ayudar a los administradores a solucionar problemas de carga de perfiles importantes. Se muestra un texto de ayuda con la siguiente información de perfiles de usuario:

- Cantidad de archivos
- Tamaño de perfil
- Cantidad de archivos grandes

Un desglose detallado ofrece información sobre las carpetas individuales, su tamaño y la cantidad de archivos. Esta función está disponible en Delivery Controller 7 1811 o posterior y VDA 1811 o posterior. Para obtener más información, consulte Diagnosticar problemas de inicio de sesión de los usuarios.

Estado de la licencia RDS de Microsoft

Ahora Director muestra el estado de la licencia RDS (Servicios de Escritorio remoto) de Microsoft en el panel “Detalles de la máquina” de la página **Detalles de la máquina** y **Detalles del usuario** para las máquinas de SO de servidor. Se muestra un mensaje que indica el estado de la licencia. Puede pasar el puntero sobre el icono de información para ver más datos. Para obtener más información, consulte la sección Estado de la licencia RDS de Microsoft en Solucionar problemas de máquinas.

Supervisar alertas de hipervisor

Ahora Director muestra alertas para supervisar el estado del hipervisor. Se admiten las alertas provenientes de Citrix Hypervisor y VMware vSphere. Las alertas de hipervisor ayudan a supervisar los siguientes estados o parámetros:

- Uso de CPU
- Uso de memoria

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Uso de la red
- Conexión de hipervisor no disponible.
- Uso del disco (solo vSphere)
- Conexión de host o estado de energía (solo vSphere)

La supervisión de alertas de hipervisor está disponible para los sitios con licencia Premium. Esta función requiere Delivery Controller 7 1811 o posterior. Si está utilizando una versión anterior de Director con la versión más reciente del sitio, solo se muestra el recuento de alertas del hipervisor. Para ver las alertas, actualice Director. Para obtener más información, consulte la sección Supervisar alertas de hipervisor en Alertas y notificaciones.

Datos clave RTOP

Ahora Director muestra datos clave RTOP (RealTime Optimization Pack) 2.6 en el panel HDX de la página **Detalles del usuario**. Lo que ayuda a supervisar el siguiente estado del paquete RTOP para cada usuario:

- Estado (optimizado, respaldo)
- Versión de RTC
- Versión de RTME en el dispositivo de usuario
- Métricas de pérdida de paquetes

Esta función requiere Delivery Controller 7 1811 o posteriores, y VDA 1808 o posteriores.

Acceso al sondeo de aplicaciones a través de Citrix Gateway

Ahora puede usar la función “Sondeo de aplicaciones” de Director para sondear las aplicaciones de Citrix Virtual Apps desde cualquier lugar. Puede usar esta flexibilidad para ejecutar Citrix Application Probe Agent en las máquinas de punto final que están alojadas en otra red. A través de Citrix Gateway, puede acceder al sitio que quiera sondear. Para ello, cuando configure Citrix Application Probe Agent, escriba la URL de Citrix Gateway en el campo de la URL de StoreFront. Citrix Gateway enruta automáticamente la solicitud a la URL de StoreFront del sitio correspondiente. Esta función está disponible para Citrix Gateway 12.1 o posterior, y Delivery Controllers 1811 o posterior. Para obtener más información sobre el sondeo de aplicaciones, consulte Sondeo de aplicaciones.

Agentes Virtual Delivery Agent (VDA) 1811

La versión 1811 de VDA para SO de servidor Windows y VDA para SO de escritorio Windows presenta las siguientes mejoras (además de los elementos de instalación y actualización de VDA mencionados anteriormente):

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Indicador de estado de gráficos

El indicador del estado de gráficos se ha actualizado para reemplazar a la directiva “Mostrar indicador de calidad sin pérdida”.

Este parámetro definirá el indicador del estado de gráficos que se va a ejecutar en la sesión del usuario. Permite ver datos sobre el modo de gráficos en uso, incluido el proveedor de gráficos, el codificador, la codificación por hardware, la calidad de imagen, el estado de pantalla progresiva y la compresión sin pérdida de texto.

De forma predeterminada, la directiva del estado de gráficos está inhabilitada. Reemplaza a la directiva Mostrar indicador de calidad sin pérdida presente en las versiones anteriores, que estaba habilitada de forma predeterminada.

Para obtener más información, consulte Indicador del estado de gráficos.

Correspondencia de PPP en Windows 10

La correspondencia de PPP permite que la sesión de escritorio Windows 10 coincida con los PPP del punto final cuando se usa la aplicación Citrix Workspace para Windows.

> **Nota:**
>
> Esta configuración está desactivada de forma predeterminada. La correspondencia de PPP se habilita cuando la configuración Ajustar escala de PPP se **desactiva**. Cuando se usan aplicaciones alojadas en máquinas virtuales, la escala de PPP se establece en 100% de forma predeterminada.

Mejoras en el rendimiento de la asignación de unidades del cliente

Ahora la asignación de unidades del cliente admite la transferencia de datos desde el host al cliente como un flujo. Esta mejora garantiza que la transferencia de archivos se adapte a las condiciones cambiantes de rendimiento de la red. También utiliza cualquier ancho de banda adicional disponible para ampliar la velocidad de la transferencia de datos. De manera predeterminada, esta función está habilitada. Estas mejoras requieren la aplicación Citrix Workspace 1811 para Windows o posterior.

Para inhabilitar esta función, configure la siguiente clave de Registro y reinicie el servidor:

HKEY_LOCAL_MACHINE\System\Currentcontrolset\services\picadm\Parameters

Nombre: DisableFullStreamWrite

Tipo: REG_DWORD

Valor:

0x01 (inhabilita)

0 o eliminar (habilita)

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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.

Esta función solo se admite en la aplicación Citrix Workspace para Windows 1811 o posterior.

> **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. Este nuevo comportamiento requiere tanto la versión 1811 de VDA (o una posterior) como la aplicación Citrix Workspace 1811 para Windows (o una versión posterior). No está disponible en implementaciones con versiones anteriores del VDA o del cliente. Para estas implementaciones más antiguas, consulte Optimizar el ancho de banda de HDX en conexiones de latencia alta para obtener información sobre la configuración manual de los búferes de salida.

Diseño de pantalla virtual

Esta función permite definir un diseño de monitor virtual que se aplica al escritorio remoto. Asimismo, permite dividir virtualmente un solo monitor de cliente en hasta ocho monitores en el escritorio remoto. Puede configurar los monitores virtuales en la ficha “Diseño del monitor” en el visor de escritorio. Allí, puede dibujar líneas horizontales o verticales para separar la pantalla en monitores virtuales; la pantalla se divide en función de los porcentajes especificados de la resolución del monitor del cliente.

Puede establecer PPP en los monitores virtuales que se utilizarán para el ajuste de escala de PPP o la correspondencia de PPP. Después de aplicar un diseño de monitor virtual, cambie el tamaño o vuelva a conectarse a la sesión.

Esta configuración se aplica a todas las conexiones aplicables posteriores de este cliente, solo a las sesiones de escritorio de un solo monitor en pantalla completa, y no afecta a ninguna aplicación publicada.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Citrix Licensing 11.15

Citrix Licensing 11.15 contiene funciones nuevas, así como problemas resueltos y problemas conocidos.

Compatibilidad con la corroboración del inicio de sesión en el Servicio de autenticación federada

Ahora el Servicio de autenticación federada (FAS) puede recibir la corroboración de inicios de sesión transferida desde Citrix Gateway y StoreFront. Esa corroboración se puede validar para garantizar que fue emitida por un proveedor de identidades (IdP) de confianza. Se ofrece un nuevo FAS Assertion SDK para admitir esta función. Para obtener más información sobre la función de corroboración del inicio de sesión, consulte Introducción a la corroboración de inicio de sesión en el Servicio de autenticación federada de Citrix.

Nuevos nombres de producto

Si lleva siendo cliente o socio de Citrix desde hace algún tiempo, verá nombres nuevos en nuestros productos y en la documentación de esos productos. Si es nuevo en este producto Citrix, es posible que vea diferentes nombres para un producto o componente.

Los nuevos nombres de productos y componentes derivan de una gama de productos y una estrategia de nube que están ambas en plena expansión. En los artículos de esta documentación de producto se usan los siguientes nombres.

- **Citrix Virtual Apps and Desktops:** Ofrece una solución de aplicaciones y escritorios virtuales, como servicio de nube o producto local, que da a los empleados la libertad de trabajar desde cualquier ubicación y con cualquier dispositivo, al tiempo que contribuye a reducir los costes de la infraestructura de TI. Puede entregar aplicaciones Windows, Linux, Web y SaaS o escritorios virtuales completos desde cualquier tipo de nube: pública, local o híbrida. Citrix Virtual Apps and Desktops eran anteriormente XenApp y XenDesktop respectivamente.
- **Aplicación Citrix Workspace:** La aplicación Citrix Workspace incorpora la tecnología existente de Citrix Receiver y las demás tecnologías de cliente de Citrix Workspace. Se ha mejorado para ofrecer capacidades adicionales con las que ofrecer a los usuarios finales una experiencia unificada y contextual donde pueden interactuar con todas las aplicaciones de trabajo, los archivos y los dispositivos que necesitan para desempeñar su trabajo de la manera más eficiente. Para obtener más información, consulte esta entrada del blog.
- **Citrix SD-WAN:** NetScaler SD-WAN, una tecnología crucial para nuestros clientes y socios que transforma sus redes de sucursales y redes WAN con tecnología en la nube, ha pasado a llamarse Citrix SD-WAN.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Citrix Secure Web Gateway:** A medida que se amplían los productos de Citrix Networking, nos enorgullece ofrecer nuestro robusto servicio Citrix Secure Web Gateway, anteriormente conocido como NetScaler Secure Web Gateway.
- **Citrix Gateway:** Nuestro sólido NetScaler Unified Gateway, que permite un acceso seguro y contextual a las aplicaciones y a los datos que usted necesita para hacer mejor su trabajo, ahora se llama Citrix Gateway.
- **Citrix Content Collaboration** y **Citrix Files para Windows:** Las funciones avanzadas de acceso, colaboración, flujos de trabajo, administración de derechos e integración de ShareFile ahora están disponibles en el componente Citrix Content Collaboration ubicado en nuestro espacio de trabajo seguro, contextual e integrado Citrix Workspace. Citrix Files para Windows permite acceder a los archivos de Content Collaboration directamente a través de una unidad asignada, con lo que ofrece una experiencia nativa de Windows Explorer.
- **Citrix Hypervisor:** La tecnología de XenServer para la infraestructura de virtualización, basada en el hipervisor de XenProject, ahora ha pasado a ser Citrix Hypervisor.

A continuación dispone de un resumen rápido:

Es	Era
Citrix Virtual Apps and Desktops	XenApp y XenDesktop
Aplicación Citrix Workspace	Incorpora Citrix Receiver y amplias mejoras
Citrix SD-WAN	NetScaler SD-WAN
Citrix Secure Web Gateway	NetScaler Secure Web Gateway
Citrix Gateway	NetScaler Unified Gateway
Citrix Content Collaboration	ShareFile
Citrix Files para Windows	Aplicación de escritorio ShareFile, ShareFile Sync, ShareFile Drive Mapper
Citrix Hypervisor	XenServer
Citrix Provisioning	Citrix Provisioning Services

La implementación de esta transición en nuestros productos y en su documentación es un proceso continuo.

- Con lo que el contenido del producto aún puede contener los nombres anteriores. Por ejemplo, puede que vea instancias de nombres anteriores en texto de la consola, los mensajes y los nombres de directorios o archivos.
- Es posible que algunos elementos (como los comandos y los MSI conserven los nombres anteriores para que los scripts existentes de cliente sigan funcionando).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Asimismo, la documentación de producto y otros recursos relacionados (como vídeos y entradas de blog) que se incluyan como enlaces en la documentación de este producto pueden contener todavía los nombres anteriores.
- En el caso de Citrix Hypervisor, el nuevo nombre se utilizará en el sitio Web de Citrix y en el material informativo del producto a partir de septiembre de 2018. También se verá el nuevo nombre en las consolas de administración de algunos productos Citrix, como Citrix Virtual Apps and Desktops. En la versión del producto XenServer y en el material de la documentación técnica, se seguirá utilizando XenServer 7.x hasta principios de 2019.

Agradecemos su comprensión durante esta transición. Para obtener más información sobre los nuevos nombres de nuestros productos, consulte https://www.citrix.com/about/citrix-product-guide/.

Nuevos números de versión de productos y componentes

En esta versión, los números de versión de productos y componentes se muestran en el formato: **7 *YYMM.c.m.b***.

- *AAMM* = Año y mes en que se lanzó el producto o componente. Por ejemplo, una versión publicada en septiembre de 2018 aparece como 1809.
- *c* = número de versión de Citrix Cloud para el mes.
- *m:* Versión de mantenimiento (si corresponde).
- *b* = número de compilación (build number). Este campo se muestra solo en la página "Acerca de" del producto y en la función del sistema operativo para eliminar o cambiar programas.

Por ejemplo, **Citrix Virtual Apps and Desktops 7 1809.1.0** indica que la versión del producto se publicó en septiembre de 2018, está asociada a la versión 1 de Citrix Cloud de ese mes y no es una versión de mantenimiento. En algunas pantallas solo se muestran el año y el mes de la versión; por ejemplo, **Citrix Virtual Apps and Desktops 7 1809**.

En versiones anteriores de este producto (XenApp y XenDesktop 7.18 y versiones anteriores), los números de versión se mostraban en el formato: 7.*versión*, donde el valor *versión* aumentaba de uno en uno con cada versión. Por ejemplo, la publicación que seguía a 7.17 era 7.18. Esas publicaciones anteriores no se actualizarán al nuevo formato de numeración.

Problemas resueltos

March 14, 2019

Los siguientes problemas se han corregido a partir de 1808.2:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Citrix Director

- Es posible que un administrador delegado con un rol personalizado no pueda eliminar la asignación de usuario existente en un escritorio utilizando Citrix Studio, PowerShell o Citrix Director. El problema se produce cuando los administradores personalizados tienen permisos para realizar las operaciones en los grupos de entrega, pero no tienen permisos en los catálogos de máquinas. [LC8174]
- En Citrix Director, el consumo de la CPU por parte del proceso w3wp.exe puede ser muy alto. [LC9222]
- Es posible que el valor ExportCsvDrilldownLimit no se aplique a informes personalizados en Citrix Director. [LD0004]
- Puede que los administradores personalizados no puedan obtener los detalles de la sesión desde un VDA 7.15 cuando Citrix Director esté conectado a un Delivery Controller 7.6. [LD0134]

Directiva de Citrix

- Puede que no se inicien las aplicaciones App-V en el modo Administración única desde agentes VDA. El problema ocurre cuando la clave de Registro llamada **ApplicationStartDetails** está vacía o le faltan datos de la aplicación. [LC8798]
- Cuando se aplica la directiva de bucle invertido en el modo de fusión a un VDA y se agrega la URL de StoreFront a un grupo de entrega del VDA en Citrix Studio, pueden aparecer iconos duplicados de las aplicaciones publicadas. [LC8889]
- Cuando se ejecuta la herramienta Resultados de directivas de grupo desde la Consola de administración de directivas de grupo en una máquina con VDA 7.15.2000, aparece el mensaje de error: **An error occurred while generating report: Not Found (Se produjo un error al generar el informe: No encontrado)**. [LC9825]
- Puede que el servicio Citrix Print Manager Service (cpsvc.exe) se cierre inesperadamente. El problema se da cuando hay entradas inservibles en la clave de Registro de impresión que está conectada a un objeto de directiva de grupo (GPO). [LC9921]
- El motor de directivas de grupo puede no insertar todos los valores en la clave de Registro **ApplicationStartDetails**. Por eso, puede que las aplicaciones App-V no se inicien. [LC9942]
- Cuando intenta realizar una copia de seguridad de una directiva de grupo y luego la importa con la Consola de administración de directivas de grupo (GPMC; gpmc.msc) 3.1.2, la GPMC puede dejar de responder. Sin embargo, la directiva se importa. [LD0173]
- Los intentos de usar la Consola de administración de directivas de grupo (GPMC; gpmc.msc) para copiar un objeto de directiva de grupo (GPO) que contenga configuraciones de directivas

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Citrix pueden provocar errores y apuntar a GpmcInterop.dll. La consola de administración Microsoft Management Console (MMC) se cierra inesperadamente. [LD0322]

Citrix Provisioning

Citrix Studio

- Citrix Studio no muestra la opción **Inicio**. En consecuencia, el PC remoto no se enciende. [LC9702]
- En un entorno grande donde se usan muchos grupos de aplicaciones, al hacer clic en la ficha "Aplicaciones" en Studio, se agota el tiempo de espera de la sesión mientras se obtiene el resultado de **Get-BrokerApplicationGroup**. Como resultado, aparece la siguiente excepción:

  Database could not be connected (No se ha podido establecer conexión con la base de datos).

  Antes de indicar la excepción, Studio deja de responder mientras enumera los grupos de aplicaciones. [LD0012]
- En Citrix Studio, cuando intenta aplicar una directiva Citrix a una unidad organizativa (OU) haciendo clic en "Examinar" en la ventana "Asignar directiva", puede aparecer este mensaje de error: **Ocurrió un error desconocido**.

  Aparece la siguiente excepción:

  Collection was modified; enumeration operation may not execute (La colección se ha modificado; puede que la operación de enumeración no se ejecute). [STUD-3847, LD0044]
- Cuando inicia sesión en un escritorio dedicado, puede ocurrir un error de inicio de sesión y el proceso de cierre de sesión puede bloquearse. Citrix Studio muestra la sesión como conectada, pero esa sesión no se puede cerrar hasta que se reinicie manualmente la máquina. [LD0199]
- La conexión de alojamiento de Citrix Studio puede mostrar un mensaje de advertencia donde se insta a utilizar HTTPS para las conexiones de alojamiento de XenServer a pesar de que las conexiones HTTPS no se admitan. [LD0210]

Controller

- Cuando hay licencias de varios tipos para grupos de entrega, podría extraerse un tipo de licencia incorrecto que no esté configurado para un grupo de entrega. [LC9086]
- El consumo de memoria por parte de Citrix High Availability Service (HighAvailabilityService.exe) puede superar los 2 GB. [LC9446]

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- De forma predeterminada, el ID de Amazon Web Services (AWS) para la máquina aprovisionada de Machine Creation Services (MCS) no se conserva. Esta situación podría causar que las acciones de administración de energía de la máquina virtual fallen en AWS.

  Para que el ID de AWS se conserve, use una de estas opciones:

  - Para que el ID de AWS se conserve, establezca el campo **Conexión** en la conexión de host a CreateNewInstanceOnReset=false en la página "Avanzado".
  - Para que el ID de AWS no se conserve, establezca el campo **Conexión** de la conexión de host en CreateNewInstanceOnReset=true en la página "Avanzado" o elimine esa opción.

  Para que el cambio surta efecto, espere 10 segundos. [LC9960]

- En ciertos casos, intentar crear una aplicación mediante el comando **New-BrokerApplication** con el parámetro -AdminFolder podría no crear la carpeta especificada. [LC9982]
- Los intentos de recrear la función "Caché de host local" con un nombre de grupo de entrega que contiene caracteres especiales pueden fallar con un **ID de evento 505**. [LD0068]
- Cuando actualiza un único Delivery Controller en un entorno de varios Delivery Controllers, el informe de prueba del sitio puede contener una versión de base de datos no coincidente. [LD0073]
- En XenApp y XenDesktop 7.18, puede que no se cree un catálogo de máquinas cuando intente crearlo. Este error puede ocurrir si **"Seguridad de los registros" se establece en "Impedir cambios en la configuración si la base de datos no está disponible".**
  [LD0133]
- Cuando se utiliza el comando **get-brokericon -filename** de PowerShell con el parámetro -servername, el comando devuelve un mensaje de error. [LD0324]
- Las aplicaciones publicadas de Citrix Virtual Apps pueden no enumerarse de forma intermitente. Como resultado, aparece una pantalla vacía después de que se inicie la sesión o de que las aplicaciones no se inicien. El servidor SQL puede experimentar un alto consumo de la CPU y SQL Monitor puede mostrar procesos bloqueados y costosos. [LD0336]
- Cuando vCenter Server se reinicia manualmente, el estado de las máquinas virtuales con energía administrada que residen en el hipervisor VMware puede pasar a ser **desconocido**. Ese estado se convierte en desconocido porque la conexión de host no está disponible. Una vez que se complete el reinicio de vCenter Server, el estado de energía de la máquina virtual sigue siendo desconocido, en lugar de restaurarse automáticamente. [LD0355]

© 1999-2019 Citrix Systems, Inc. All rights reserved.

HDX RealTime Optimization Pack

Licencias

Linux VDA

Profile Management

StoreFront

Universal Print Server

Cliente

- El servicio Print Spooler puede cerrarse inesperadamente. El problema ocurre cuando **CRawStreamHeaderWriter::EndPage** y **CRawStreamHeaderWriter::StartPage** intentan acceder a un objeto nulo. [LC7893]
- Después de instalar un VDA, es posible que los puertos de impresora ya no aparezcan en las propiedades de una impresora de red asignada. [LD0166]

Servidor

- Un intento de acceso no autorizado en **CPTStream::ThisStream** puede hacer que el servicio Print Spooler deje de responder. [LC8856]
- Las funciones avanzadas de impresión del controlador de impresión universal (UPD) de Citrix (como el grapado y el origen del papel), pueden mostrar menús vacíos. [LC9711]

VDA para SO de escritorio

Sesión/Conexión

- Una aplicación publicada puede cerrarse de forma intermitente inmediatamente después de iniciarla. El problema se da como consecuencia de un error inesperado al obtener información sobre procesos activos. [LC9167, LC9661]
- Cuando se utiliza el VDA 7.15.1000, puede haber una cantidad anómala de instrucciones de la CPU que pasan por el proceso Winlogon.exe, originadas en twi3.dll. [LC9450]
- Es posible que los VDA dejen de responder después de instalar XenApp y XenDesktop 7.15 LTSR Cumulative Update 2. [LC9701]

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Después de inhabilitar algunos conjuntos de cifrado a través del Registro de Microsoft HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers, es posible que TLS no se habilite. [LC9743]
- Si accede a una estación de trabajo Windows a través una sesión de acceso con Remote PC y se desconecta de la sesión, es posible que la estación de trabajo no se bloquee. Por lo tanto, la estación de trabajo será accesible a cualquier persona que se encuentre físicamente cerca de ella. [LC9812]
- La redirección de vídeo HTML5 puede activarse en sesiones que no la admiten. [LC9935]
- Cuando se procesa una transacción de tarjeta de crédito a través de un dispositivo de usuario, la aplicación y el dispositivo de usuario pueden dejar de responder o puede que solo se reciba un subconjunto de los datos. [LD0152]
- Cuando usuarios anónimos acceden a datos de un miembro de un grupo de entrega Citrix, puede aparecer una interfaz de inicio de sesión incorrecta con el mensaje **Conexión restaurada** después de que se agote el tiempo de espera del protocolo CGP. El mensaje correcto debería ser: **No se pudo reconectar**. [LD0363]
- Esta corrección soluciona un problema de pérdida de memoria que se da cuando la directiva **Conectar automáticamente las unidades del cliente** está inhabilitada. [LD0370]
- La multidifusión no muestra el vídeo cuando se usa un Citrix Receiver para Windows más reciente que la versión 4.6. El sonido sí funciona. [HDX-10055 adaptador de cable]

Excepciones del sistema

- Microsoft Windows Server 2008 R2 podría experimentar una excepción irrecuperable y mostrar una pantalla azul con el código de comprobación de errores **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (0x1000007E)**. [LC9849]
- Los VDA pueden experimentar una excepción irrecuperable en picavc.sys y mostrar una pantalla azul con el código de comprobación de errores **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)**. [LD0006]
- Los VDA pueden experimentar una excepción irrecuperable y mostrar una pantalla azul en wdica.sys con el código de comprobación de errores 0x3b (SYSTEM_SERVICE_EXCEPTION). [LD0089]
- Los VDA pueden experimentar una excepción irrecuperable y mostrar una pantalla azul en picadm.sys con el código de comprobación de errores 0x22. [LD0119]
- Aparece intermitentemente un error de detención (pantalla azul) durante la instalación de un VDA 7.16 en un Surface Pro 3 o 4. Durante la instalación, el controlador igdkmd64 de Intel deja

© 1999-2019 Citrix Systems, Inc. All rights reserved.

de responder. Este es un problema de terceros que afecta las GPU de Intel: Intel 5000 HD e Intel Iris 530. [HDX-12662]

Experiencia de usuario

- Cuando cambia el tamaño de una aplicación publicada e intenta moverla de un monitor a otro, puede aparecer un borde blanco alrededor de la aplicación. [LC9570]
- Un cliente de Microsoft Windows 10 podría aumentar la escala de monitor de alta resolución del cliente cuya escala DPI está establecida en 100. [LD0131]
- Cuando pase el puntero sobre un elemento, la ventana emergente del texto de ayuda puede desaparecer y la aplicación deja de estar en primer plano. [LD0365]

Interfaz de usuario

- Cuando inicia una aplicación alojada en una máquina virtual mientras intenta volver a conectarse a una sesión desconectada, se muestran todas las aplicaciones que están presentes en la sesión, salvo aquellas en las que haya hecho clic más recientemente. [LD0189]

VDA para SO de servidor

Sesión/Conexión

- Una aplicación publicada puede cerrarse de forma intermitente inmediatamente después de iniciarla. El problema se da como consecuencia de un error inesperado al obtener información sobre procesos activos. [LC9167, LC9661]
- Cuando se utiliza el VDA 7.15.1000, puede haber una cantidad anómala de instrucciones de la CPU que pasan por el proceso Winlogon.exe, originadas en twi3.dll. [LC9450]
- Es posible que los VDA dejen de responder después de instalar XenApp y XenDesktop 7.15 LTSR Cumulative Update 2. [LC9701]
- Después de inhabilitar algunos conjuntos de cifrado a través del Registro de Microsoft HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers, es posible que TLS no se habilite. [LC9743]
- La redirección de vídeo HTML5 puede activarse en sesiones que no la admiten. [LC9935]
- El proceso wfshell.exe puede cerrarse inesperadamente. Como resultado, las aplicaciones publicadas no se inician. [LD0102]

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Cuando se procesa una transacción de tarjeta de crédito a través de un dispositivo de usuario, la aplicación y el dispositivo de usuario pueden dejar de responder o puede que solo se reciba un subconjunto de los datos. [LD0152]
- Cuando usuarios anónimos acceden a datos de un miembro de un grupo de entrega Citrix, puede aparecer una interfaz de inicio de sesión incorrecta con el mensaje **Conexión restaurada** después de que se agote el tiempo de espera del protocolo CGP. El mensaje correcto debería ser: **No se pudo reconectar**. [LD0363]
- Esta corrección soluciona un problema de pérdida de memoria que se da cuando la directiva **Conectar automáticamente las unidades del cliente** está inhabilitada. [LD0370]
- Después de actualizar el VDA a la versión 7.15 Cumulative Update 2 o actualizar de la versión 7.15 Cumulative Update 1 a Cumulative Update 2, los valores configurados **AnonymousUserIdleTime** y **MaxAnonymousUsers** en la clave de Registro HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Co pueden eliminarse. [LD0378]
- La multidifusión no muestra el vídeo cuando se usa un Citrix Receiver para Windows más reciente que la versión 4.6. El sonido sí funciona. [HDX-10055 adaptador de cable]

Excepciones del sistema

- Microsoft Windows Server 2008 R2 podría experimentar una excepción irrecuperable y mostrar una pantalla azul con el código de comprobación de errores **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (0x1000007E)**. [LC9849]
- Los VDA pueden experimentar una excepción irrecuperable en picavc.sys y mostrar una pantalla azul con el código de comprobación de errores **SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e)**. [LD0006]
- Los VDA pueden experimentar una excepción irrecuperable y mostrar una pantalla azul en wdica.sys con el código de comprobación de errores 0x3b (SYSTEM_SERVICE_EXCEPTION). [LD0089]
- Los VDA pueden experimentar una excepción irrecuperable y mostrar una pantalla azul en picadm.sys con el código de comprobación de errores 0x22. [LD0119]
- Aparece intermitentemente un error de detención (pantalla azul) durante la instalación de un VDA 7.16 en un Surface Pro 3 o 4. Durante la instalación, el controlador igdkmd64 de Intel deja de responder. Este es un problema de terceros que afecta las GPU de Intel: Intel 5000 HD e Intel Iris 530.[HDX-12662]

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Experiencia de usuario

- Cuando cambia el tamaño de una aplicación publicada e intenta moverla de un monitor a otro, puede aparecer un borde blanco alrededor de la aplicación. [LC9570]
- Cuando pase el puntero sobre un elemento, la ventana emergente del texto de ayuda puede desaparecer y la aplicación deja de estar en primer plano. [LD0365]

Interfaz de usuario

- Cuando intenta iniciar una aplicación publicada, la pantalla de Citrix Receiver para Windows puede aparecer en la esquina inferior derecha. [LC9817]
- Cuando inicia una aplicación alojada en una máquina virtual mientras intenta volver a conectarse a una sesión desconectada, se muestran todas las aplicaciones que están presentes en la sesión, salvo aquellas en las que haya hecho clic más recientemente. [LD0189]

Componentes de escritorio virtual: Otros

- El desbordamiento de caché en la optimización del almacenamiento de Machine Creation Services (Machine Creation Services Storage Optimization o MCSIO) puede resultar en un bajo rendimiento de las máquinas virtuales XenServer. [LC9351]
- Pueden fallar los intentos de ejecutar varias instancias de la misma aplicación App-V en la misma sesión. El problema ocurre cuando el proceso que se está ejecutando difiere del proceso definido en el archivo de manifiesto. [LC9652]
- Puede iniciarse una aplicación incorrecta de un paquete de App-V cuando el nombre de la aplicación esté en un idioma que no sea el inglés. [LD0222]

Citrix Ready Workspace Hub

Se han solucionado los siguientes problemas en la versión 1812:

- Al ejecutar el archivo `wshcollect.sh` en la imagen de Stratodesk, los datos no se muestran correctamente. [WH-1619]
- Las acciones del ratón y del teclado pueden causar anomalías en la pantalla, como que deje de responder o que la pantalla de inicio entre en bucle. [WH-1662, WH-1609, WH-1608]
- El proceso `controlservice` no deja de ejecutarse después de salir de la pantalla de inicio en un nuevo sistema operativo Raspbian Stretch. El Workspace Hub no se puede iniciar. [WH-1586]

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Después de actualizar al sistema operativo Raspbian Stretch, es posible que no pueda detener la proyección de sesiones en un dispositivo Android. [WH-1547]
- Cuando se utiliza la aplicación Citrix Workspace para Linux en la sesión de VDA, las reservas de Outlook muestran un horario que está una hora por delante de la hora de Workspace Hub. [WH-1511]
- El mouse puede saltar a la mitad de la pantalla cuando sale del modo extendido para la proyección de pantalla en un dispositivo Windows. [WH-1402]
- Hay líneas negras inesperadas en el escritorio de sesión de Microsoft Windows 10. [WH-860]

Problemas conocidos

January 29, 2019

La versión 7 1811 de Citrix Virtual Apps and Desktops presenta los siguientes problemas. (Los componentes y las funciones que se documentan por separado tienen sus propios artículos de problemas conocidos.)

Esta advertencia se aplica a cualquier solución temporal que sugiera cambiar una entrada del Registro:

> **ADVERTENCIA**
>
> Si se modifica el Registro de forma incorrecta, se pueden generar problemas graves que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Instalar y actualizar

- Cuando instale un Controller, si selecciona **Quiero conectar con Smart Tools y Call Home** en la página **Smart Tools** del Asistente de instalación, no se puede habilitar Call Home. Como solución temporal, utilice la función de programación en Citrix Scout o habilite Call Home mediante PowerShell. [CAM-9907]
- Mensaje de error después de una actualización parcial de 1808.2: después de actualizar un Controller que también tiene Studio instalado (antes de que los demás Controllers se hayan actualizado), Studio puede mostrar el mensaje “Se produjo un error inesperado” cuando un administrador solicite información sobre catálogos de máquinas o grupos de entrega. Una vez actualizados todos los Controllers, el mensaje no aparece. [BRK-2652]

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Si se produce una excepción de tiempo de espera agotado durante una actualización de StoreFront desde el instalador de Citrix Virtual Apps and Desktops, antes de reiniciar la actualización:
  - Compruebe que cumple los Requisitos de hardware de Citrix Virtual Apps and Desktops y los Requisitos del sistema de StoreFront.
  - Reinicie la máquina virtual que aloja la instalación. [STF-3379]

General

- Cuando se inicia una aplicación desde StoreFront, no se inicia en primer plano o está en primer plano, pero no tiene el foco. Como solución temporal, haga clic en el icono de la aplicación situado en la barra de tareas para traerla al primer plano o en la pantalla de la aplicación para situar el foco en ella. [HDX-10126]
- Después de instalar el complemento de la aplicación Web de Skype Empresarial, puede que las cámaras Web no se enumeren y las páginas de reuniones en Firefox no se actualicen automáticamente. [HDX-13288]
- Cuando instala un dispositivo de audio en el cliente y habilita la redirección de audio e inicia una sesión RDS: Es posible que los archivos de audio no se reproduzcan y aparezca un mensaje de error. Como solución alternativa, agregue esta clave al Registro en la máquina RDS y reiníciela:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SCMConfig

  Nombre: EnableSvchostMitigationPolicy

  Tipo: REG_DWORD

  Datos: 0 [HDX-15791]
- Cuando se conecta a una nueva sesión, se desconecta y luego se vuelve a conectar a la misma sesión, los iconos de su escritorio podrían parpadear. Como solución temporal, restablezca el perfil de usuario, cierre sesión y vuelva a iniciar sesión. [HDX-15926, UPM-1362]
- Pueden fallar las extracciones de archivos comprimidos. Este error puede darse cuando se use la utilidad de extracción de Microsoft en el VDA para extraer un archivo ZIP del cliente en el mismo directorio en ese cliente. Dispone de las siguientes soluciones temporales:
  - Extraer el archivo a un directorio que no sea donde se encuentra el archivo ZIP.
  - Usar otra utilidad de extracción, como WinZip. [HDX-17052]
- Faltan los archivos ubicados en C:\Archivos de programa\Citrix\PowerShell SDK después de una actualización. Este problema se produce porque la versión CDF que utiliza Citrix Provisioning no coincide con la versión que utilizan otros componentes asociados a Citrix Virtual Apps and Desktops. Por eso, los archivos CDF más recientes tienen un número de versión inferior a los anteriores. Este problema no afecta a la funcionalidad de importar colecciones de dispositivos CPV a catálogos de máquinas. Para solucionar este problema:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

1. Cierre Citrix Studio.
2. Monte la nueva ISO de Citrix Virtual Apps and Desktops.
3. En la ISO montada, vaya a \x64\DesktopStudio.
4. Haga clic con el botón secundario en **Citrix Provisioning PowerShell SDK x64** para ver un menú contextual.
5. Seleccione **Reparar**.
6. Ejecute la opción de reparación. La instalación agrega los dos archivos CDF. [PVS-4009]

Director

- En Director, puede que el estado de la licencia RDS aparezca erróneamente como "licencia disponible" cuando el servidor de licencias está configurado correctamente pero la máquina se encuentra en un período de gracia. [BRK-2499]

Studio

- Citrix Studio no se actualiza o muestra el siguiente mensaje de advertencia en el panel inferior de la ficha **Detalles**: "Este catálogo de máquinas tiene las siguientes advertencias: La comprobación de licencias de Escritorio remoto de Microsoft notificó el problema siguiente: no se ha configurado un tipo de licencia". Tenga en cuenta los siguientes dos casos:
  - Cuando el servidor de licencias se configura incorrectamente durante la creación del catálogo de máquinas, aparece el mensaje de advertencia. Sin embargo, después de corregir la configuración del servidor de licencias y actualizar Citrix Studio, sigue apareciendo el mensaje de advertencia.
  - Cuando el servidor de licencias se configura correctamente durante la creación del catálogo de máquinas, no aparece el mensaje de advertencia. Sin embargo, si se realizan cambios en el agente VDA de Server OS que resultan en errores de configuración de licencia, Citrix Studio no muestra el mensaje de advertencia.

  Este problema se produce porque Citrix Studio solo consulta el estado de la licencia RDS durante la creación del catálogo de máquinas. [STUD-4318]

Gráficos

- Cuando se usa Windows 10 1607, desconectarse de la sesión podría no funcionar correctamente. [HDX-13448]
- Cuando se usa Windows 10 1809 LTSC, las dependencias VCLibs no se instalan. [HDX-16754]
- Es posible que los contadores de rendimiento no se muestren en la lista "Contadores disponibles" durante una sesión. [HDX-17017]

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Cuando se utiliza el VDA de Windows 10 1809 Enterprise, es posible que el botón de desconexión no funcione correctamente. [HDX-17150]
- La consola de XenCenter puede mostrar una pantalla vacía después de desconectar una sesión de XenDesktop. Como solución temporal, envíe CTLR + ALT + SUPR a la consola de XenCenter para que aparezca la pantalla de la consola. [HDX-17261]
- Es posible que los PPP no correspondan durante una sesión que se ejecuta en Server OS 2016 o 2019 cuando se cambia el DPI en el cliente y se vuelve a conectar la sesión. Como solución alternativa, cambie el tamaño de la ventana de la sesión para que coincida con los PPP. [HDX-17313]

Impresión

- Las impresoras de Universal Print Server seleccionadas en el escritorio virtual no aparecen en la ventana **Dispositivos e impresoras** del Panel de control de Windows. No obstante, cuando los usuarios trabajan en las aplicaciones, pueden imprimir con esas impresoras. Este problema se produce solamente en plataformas Windows Server 2012, Windows 10 y Windows 8. Para obtener más información, consulte el artículo CTX213540 en Knowledge Center. [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]

Problemas de terceros

- Debido a un cambio reciente en una configuración predeterminada de Microsoft, los dispositivos de almacenamiento masivo USB cifrados de hardware y redirigidos usando un USB genérico en entornos RDS pueden fallar para cuentas que no sean de administrador. Puede cambiar este comportamiento; para ello, modifique la configuración de directiva local en el VDA. Utilice el Editor de directivas de grupo local para seleccionar **Configuración del equipo > Plantillas administrativas > Sistema > Acceso de almacenamiento extraíble** y habilite la directiva **All Removable Storage: Allow direct access in remote sessions** (Todo el almacenamiento extraíble: permitir el acceso directo en sesiones remotas). [HDX-16480 adaptador de cable]
- Cuando un servidor o estación de trabajo tienen poco más de 2000 sesiones desconectadas antes de reiniciarse, el servidor no le permite volver a conectarse. Este problema también se produce si utiliza el Host de sesión de Escritorio remoto (RDSH) o Remote Desktop Protocol (RDP) para conectarse. Este problema se debe a un problema de Windows Server 2019 y Win-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

dows 10 versión 1809. Como solución temporal, reinicie el servidor o la estación de trabajo. [HDX-16186]

- Un VDA que se ejecute en Azure podría congelarse cuando se utiliza Enlightened Data Transport (EDT), lo que requeriría una reconexión a la sesión. Como solución temporal, configure udtMSS en 1400 y OutbufLength en 1400 en los entornos de Azure. Para obtener más información, consulte CTX231821. [HDX-12913]
- En la redirección de contenido del explorador, después de iniciar un vídeo de YouTube con el reproductor de vídeos HTML5 de YouTube, el modo de pantalla completa puede no funcionar. Aunque haga clic en el icono situado en la esquina inferior derecha del vídeo, el vídeo no cambia de tamaño, dejando el fondo negro en toda el área de la página. Como solución temporal, haga clic en el botón de pantalla completa y, a continuación, seleccione el modo de pantalla completa. [HDX-11294]

Citrix Ready Workspace Hub

Se han observado los siguientes problemas en la versión 1812 de Citrix Ready Workspace Hub:

- El cursor del ratón puede moverse lentamente si usa un adaptador de pantalla secundaria. [WH-1664]
- Después de actualizar la versión de WebKitGTK a 2.16 en el sistema operativo Raspbian Stretch, puede observar un rendimiento más lento. Se ha enviado una solicitud para para pasar la imagen a la versión 2.09 a Stratodesk. [WH-1665]
- En el sistema operativo Raspbian Stretch actualizado, el micrófono USB falla al iniciar llamadas de audio para el Optimization Pack. [WH-1647]
- Es posible que la pantalla de inicio se cierre inesperadamente y aparezca la página de inicio de sesión del concentrador. [WH-1371]
- Un subproceso del mouse DisplayConnector podría terminarse inesperadamente durante el inicio de sesión desde un panel Xiaomi Mi. [WH-1419]

Avisos de terceros

December 11, 2018

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)

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Software de terceros de FlexNet Publisher Documentation Supplement y software Open Source utilizados en FlexNet Publisher 11.15.0 (Descargar PDF)

Obsolescencia

March 14, 2019

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 pueden no contener todas las funciones o características obsoletas.
Para obtener información detallada acerca del ciclo de vida útil admitido del producto, consulte el artículo Product Lifecycle Support Policy.

Elementos eliminados y obsoletos

En la siguiente tabla, se muestran las plataformas, las funciones y los productos Citrix que están obsoletos o se han eliminado.Los elementos *obsoletos* no se eliminan inmediatamente. Citrix sigue admitiéndolos en la presente versión, pero se quitarán de la versión futura.Los elementos *eliminados* se quitan (o ya no se admiten) en Citrix Virtual Apps and Desktops (antes XenApp y XenDesktop).

> Compatibilidad con la redirección de contenido en el navegador Internet Explorer 11
>
> Se admite la redirección de contenido en Internet Explorer 11 y ya no está obsoleta. El carácter obsoleto anunciado por primera vez en Citrix Virtual Apps and Desktops 7 1808 se ha eliminado de la siguiente tabla.

Elemento	Obsolescencia anunciada en	Eliminado en	Alternativa
Acceso a escritorios en sitios de Desktop Appliance para usuarios de StoreFront	**1811**		Use Desktop Lock para casos de uso que no pertenezcan a ningún dominio.
Compatibilidad con la tecnología de pantalla remota Framehawk	**1811**		Utilice Thinwire con el transporte adaptable habilitado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Elemento	Obsolescencia anunciada en	Eliminado en	Alternativa
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		Utilice la función administración de energía en Studio.
Citrix StoreFront, Citrix VDA, Citrix Studio, Citrix Director y Citrix Delivery Controller respaldan 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 posterior. (El instalador instala automáticamente .NET Framework 4.7.1 si aún no está instalado.)
Compatibilidad con Linux VDA en Red Hat Enterprise Linux 7.3.	7.18	1808	Instale Linux VDA en una versión posterior de Red Hat Enterprise Linux.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Elemento	Obsolescencia anunciada en	Eliminado en	Alternativa
Compatibilidad de StoreFront con los protocolos TLS 1.0 y TLS 1.1 entre Citrix Virtual Apps and Desktops (antes XenApp y XenDesktop), Citrix Receiver y Workspace Hub.	7.17		Actualice los Citrix Receiver a una aplicación Citrix Workspace que admita el protocolo TLS 1.2. Para obtener más información sobre la aplicación Citrix Workspace, consulte https://docs.citrix.com/es-es/citrix-workspace-app.
Compatibilidad de VDA con la configuración de directiva “Instalación automática de controladores de impresora”.	7.16	7.16	Ninguno. Configuración de directiva que se admitía solo para agentes VDA en sistemas operativos anteriores (Windows 7, Windows Server 2012 R2 y versiones anteriores).
Compatibilidad de Linux VDA con SUSE Linux Enterprise Server 11 Service Pack 4.	7.16	7.16	Instale Linux VDA en una versión respaldada 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Elemento	Obsolescencia anunciada en	Eliminado en	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.
Agentes VDA en Windows 10 versión 1511 (Threshold 2) y versiones anteriores de SO de escritorio 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 escritorio 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.
Redirección de composición del escritorio (anteriormente conocida como DirectX Command Remoting o DCR)	7.15 LTSR	7.16	Use Thinwire.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Elemento	Obsolescencia anunciada en	Eliminado en	Alternativa
Experiencia clásica en Citrix Receiver para Web (interfaz de usuario “burbujas verdes”).	7.15 LTSR (y StoreFront 3.12)		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.
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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Elemento	Obsolescencia anunciada en	Eliminado en	Alternativa
Redirección de Flash	7.15 LTSR		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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Elemento	Obsolescencia anunciada en	Eliminado en	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.
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. Para obtener más información, consulte la sección “Funciones eliminadas” en la documentación de XenApp y XenDesktop 7.13.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Elemento	Obsolescencia anunciada en	Eliminado en	Alternativa
La funcionalidad parcial para manipular datos de iconos, proporcionada por los cmdlets *-CtxIcon.	7.13	7.13	Ahora la proporcionan los cmdlets *-BrokerIcon en el servicio Broker.
Modo antiguo de Thinwire	7.12	7.16	Use 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Elemento	Obsolescencia anunciada en	Eliminado en	Alternativa
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).
Instalar componentes principales en máquinas de 32 bits: Delivery Controller, Director, StoreFront y el servidor de licencias.	7.12	7.16	Use máquinas de 64 bits.
Concesión de conexiones	7.12	7.16	Use Caché de host local.
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.
Conexiones a CloudPlatform.	7.12		Use un hipervisor o servicio de nube compatibles.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Elemento	Obsolescencia anunciada en	Eliminado en	Alternativa
Conexiones Azure Classic (también conocido como Administración de servicios de Azure).	7.12		Use Azure Resource Manager.
Funcionalidad de AppDisks (y la integración de AppDNA en Studio que la admite)*	7.13		Consulte “Citrix App Layering”.
Funcionalidad Personal vDisk*	7.13		

* La opción de servicio Long Term Service Release (LTSR) no lo cubre.

Requisitos del sistema

March 14, 2019

> **Nota:**
>
> Puede obtener información sobre los cambios en los nombres de producto aquí.

Introducción

Los requisitos del sistema descritos en este documento son válidos en el momento de la publicación de la presente versión de producto. Las actualizaciones se realizan periódicamente. Aquellos componentes de los requisitos del sistema que no se incluyen aquí (por ejemplo, sistemas host, la aplicación Citrix Workspace y Citrix Provisioning) se describen en su documentación respectiva.

> **IMPORTANTE:**
>
> Consulte el artículo Antes de instalar para prepararse.

A menos que se indique lo contrario, el instalador de componentes implementa automáticamente los requisitos previos de software (por ejemplo, los paquetes .NET y C++) si no se han detectado las versiones correspondientes en la máquina. Los medios de instalación de Citrix también contienen algunos de estos programas de requisitos previos.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 CTX119253.

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 variará según la configuración. Esto incluye las funciones que utilice y la cantidad de usuarios, entre otros factores. Utilizar solo lo mínimo puede derivar en un rendimiento lento.

En la siguiente tabla, se muestran los requisitos mínimos para los componentes principales.

Componente	Mínimo
Todos los componentes principales en un servidor, solo para un entorno de evaluación, no una implementación de producción.	5 GB de RAM
Todos los componentes principales en un servidor, para una implementación de prueba o un entorno de producción pequeño.	12 GB de RAM
Delivery Controller (se necesita más espacio en disco para la Caché de host local).	5 GB de RAM, 800 MB de disco duro, base de datos; consulte 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	2 GB de RAM; consulte la documentación sobre licencias para conocer las recomendaciones de disco.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 (excepto para la memoria RAM, porque necesitará más memoria RAM para aplicaciones que consuman más).

Para obtener más información:

- El Manual y prácticas recomendadas para Citrix VDI contiene directrices sobre el tamaño de los VDA.
- La escalabilidad de un solo servidor para Citrix Virtual Apps and Desktops analiza cuántos usuarios o máquinas virtuales puede contener un único host físico.

Versiones del runtime de Microsoft Visual C++

Instalar Microsoft Visual C + + 2017 Runtime en un equipo que tiene instalado Microsoft Visual C + + 2015 Runtime puede dar lugar a la eliminación automática del tiempo de ejecuciónde Visual C + + 2015. Esta es la forma en que está diseñada.

Si ya ha instalado componentes de Citrix que instalan automáticamente Visual C++ 2015 Runtime, dichos componentes seguirán funcionando correctamente con la versión de Visual C++ 2017.

Para obtener más información, consulte el artículo de Microsoft https://developercommunity.visualstudio.com/content/problem/332815/visual-c-redistributable-2017-install-removes-visu.html.

Delivery Controller

Sistemas operativos compatibles:

- Windows Server 2019, ediciones Standard y Datacenter, y con la opción Server Core
- Windows Server 2016, ediciones Standard y Datacenter, y con opción Server Core
- Windows Server 2012 R2, ediciones Standard y Datacenter, y Server Core para Windows Server 2012 R2

Requisitos:

- Microsoft .NET Framework 4.7.1 (o una versión posterior) se instala automáticamente si no está instalado.
- Microsoft Internet Information Services (se instala automáticamente; utilizado por una función actualmente en desarrollo que se instala mediante Citrix Orchestration Service).
- Windows PowerShell 3.0 o una versión posterior.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Bibliotecas de tiempo de ejecución de Microsoft Visual C++ 2015 (de 32 y 64 bits).

Bases de datos

Versiones compatibles de Microsoft SQL Server para la configuración del sitio, el registro de configuración y la base de datos de supervisión:

- SQL Server 2017, ediciones Express, Standard y Enterprise.
- SQL Server 2016 SP1 y SP2, ediciones Express, Standard y Enterprise.
- SQL Server 2014 desde SP1 hasta SP3, ediciones Express, Standard y Enterprise. De forma predeterminada y si no se detecta ninguna instalación compatible de SQL Server, se instala SQL Server 2014 SP2 Express durante la instalación del Controller.
- SQL Server 2012 hasta SP4, ediciones Express, Standard y Enterprise.
- SQL Server 2008 R2 SP2 y SP3, ediciones Express, Standard, Enterprise y Datacenter.

Se admiten las siguientes soluciones de alta disponibilidad de base de datos (excepto SQL Server Express, que solo admite el modo autónomo):

- Instancias en clúster de conmutación por error de AlwaysOn de SQL Server
- Grupos de disponibilidad AlwaysOn de SQL Server (incluidos los grupos de disponibilidad básica)
- Crear reflejo de SQL Server

Se requiere la autenticación de Windows para las conexiones entre el Controller y la base de datos de SQL Server del sitio.

Al instalar un Controller, se instala de manera predeterminada una base de datos de SQL Server Express para usarla 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.

Para obtener más información, consulte estos artículos:

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

Citrix Studio

Sistemas operativos compatibles:

- Windows Server 2019, Standard y Datacenter Edition
- Windows Server 2012 R2, Standard y Datacenter Edition
- Windows Server 2016, Standard y Datacenter Edition

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Windows 10

Requisitos:

- Microsoft .NET Framework 4.7.1 (o una versión posterior) se instala automáticamente si no está instalado.
- Microsoft Management Console 3.0 (se incluye con todos los sistemas operativos compatibles)
- Windows PowerShell 3.0 o una versión posterior.

Citrix Director

Sistemas operativos compatibles:

- Windows Server 2019, ediciones Standard y Datacenter, y con la opción Server Core
- Windows Server 2016, ediciones Standard y Datacenter, y con opción Server Core
- Windows Server 2012 R2, ediciones Standard y Datacenter, y Server Core para Windows Server 2012 R2

Requisitos:

- Microsoft .NET Framework 4.7.1 (o una versión posterior) se instala automáticamente si no está instalado.
- Microsoft Internet Information Services (IIS) 7.0 y ASP.NET 2.0. Asegúrese de que el rol de servidor IIS tiene instalado el servicio de rol de contenido estático. Si estos componentes aún no están instalados, se le solicitará que introduzca los medios de instalación de Windows Server y, a continuación, se instalarán.

Citrix User Profile Manager

- Asegúrese de que Citrix User Profile Manager y Citrix User Profile Manager WMI Plugin estén instalados en el VDA (sección 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):

- Windows Server 2012 R2
- System Center 2012 R2 Operations Manager

Exploradores compatibles para ver Director:

- Internet Explorer 11 (Solo puede usar Internet Explorer 10 en máquinas Windows Server 2012 R2.) Internet Explorer no admite el modo de compatibilidad. Utilice la configuración recomendada del explorador para acceder a Director. Al instalar Internet Explorer, acepte el valor predeterminado para usar la configuración de compatibilidad y seguridad recomendada. Si ya ha instalado el explorador y eligió no usar la configuración recomendada, vaya a **Herramientas > Opciones de Internet > Opciones avanzadas > Restablecer**, y siga las instrucciones.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Microsoft Edge
- Firefox ESR (Extended Support Release; versión de asistencia extendida).
- Chrome

La resolución de pantalla recomendada para ver Director es de 1366 x 1024.

Virtual Delivery Agent (VDA) para sistemas operativos de escritorio

Sistemas operativos compatibles:

- Windows 10, versión mínima 1607.
  - Para obtener información sobre las ediciones compatibles, consulte CTX224843.
  - Para conocer los problemas conocidos de Citrix con la versión 1709, consulte CTX229052.

Requisitos:

- Microsoft .NET Framework 4.7.1 (o una versión posterior) se instala automáticamente si no está instalado.
- Bibliotecas de tiempo de ejecución de Microsoft Visual C++ 2013 y 2015 (de 32 y 64 bits)

El acceso con Remote PC usa este VDA, que se instala en equipos físicos de oficina. Este VDA admite el arranque seguro (Secure Boot) para el acceso con Remote PC de Citrix Virtual Desktops en Windows 10.

Algunas funciones de aceleración multimedia (como la Redirección de Windows Media de HDX MediaStream) requieren que Microsoft Media Foundation esté instalado en la máquina donde desea instalar el VDA. Si la máquina no tiene instalado Media Foundation, las funciones de aceleración multimedia no se instalarán y no funcionarán. 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 ediciones de SO de escritorio Windows compatibles, la compatibilidad para 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 escritorio en una máquina de Windows Server 2019 o Windows Server 2016. Consulte VDI de servidor para obtener instrucciones.

Para obtener información sobre cómo instalar un VDA en una máquina con Windows 7, consulte Sistemas operativos anteriores.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Virtual Delivery Agent (VDA) para sistemas operativos de servidor

Sistemas operativos compatibles:

- Windows Server 2019, Standard y Datacenter Edition
- Windows Server 2016, Standard y Datacenter Edition
- Windows Server 2012 R2, Standard y Datacenter Edition

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

- Microsoft .NET Framework 4.7.1 (o una versión posterior) se instala automáticamente si no está instalado.
- Bibliotecas de tiempo de ejecución de Microsoft Visual C++ 2013 y 2015 (de 32 y 64 bits)

El instalador automáticamente instala y habilita los servicios de rol de los Servicios de Escritorio remoto si aún no están instalados y habilitados.

Algunas funciones de aceleración multimedia (como la Redirección de HDX MediaStream para Windows Media) requieren que Microsoft Media Foundation esté instalado en la máquina donde desea instalar el VDA. Si la máquina no tiene instalado Media Foundation, las funciones de aceleración multimedia no se instalarán y no funcionarán. 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 características multimedia no funcionarán:

- Redirección de Flash
- Redirección de Windows Media
- Redirección de vídeo HTML5
- Redirección de cámara Web 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

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

La función Wake on LAN del acceso con Remote PC requiere Microsoft System Center Configuration Manager, mínimo 2012.

> **IMPORTANTE:**
>
> Se admiten las siguientes versiones *superior.inferior*, incluidas las actualizaciones de esas versiones. CTX131239 contiene la información de versión más reciente de hipervisor, además de enlaces a los problemas conocidos.

XenServer

- XenServer 7.6
- XenServer 7.1 LTSR (solo con CU2)

Microsoft Azure Resource Manager

VMware vSphere (vCenter + ESXi)

- VMware vSphere 6.7
- VMware vSphere 6.5
- VMware vSphere 6.0
- VMware vSphere 5.5
- Dispositivo VMware vCenter 5.5, 6 y 6.5

No se admite la operación “Linked Mode” de vSphere vCenter.

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.

- System Center Virtual Machine Manager 2016
- System Center Virtual Machine Manager 2012 R2
- System Center Virtual Machine Manager 2012 SP1
- System Center Virtual Machine Manager 2012

Nutanix Acropolis

- Cuando se usa PVS: 4.5 (o versiones posteriores compatibles)
- Cuando se usa MCS: 4.6.1 (o versiones posteriores compatibles)

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Amazon Web Services (AWS)

- Puede aprovisionar aplicaciones y escritorios en sistemas operativos Windows Server compatibles.
- Citrix no admite el Servicio de base de datos relacional (RDS) de AWS. Sin embargo, AWS ha completado las pruebas de verificación de Citrix Ready. Los clientes pueden intentar usar AWS RDS bajo su propio riesgo y con la asistencia de AWS. Si los clientes de Citrix experimentan dificultades técnicas, Citrix puede requerir que el cliente reproduzca el problema en un RDMS compatible.
- Consulte Citrix XenDesktop en Amazon Web Services para obtener información adicional.

CloudPlatform

Este tipo de host está obsoleto.

Microsoft Azure (clásico)

Este tipo de host está obsoleto.

Niveles funcionales de Active Directory

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

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008

HDX

Sonido

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 a continuación 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 escritorio Windows detectará la presencia de hardware GPU en tiempo de ejecución.

La máquina física o virtual que aloja la aplicación puede usar GPU PassThrough o GPU virtual (vGPU):

- GPU PassThrough está disponible con: Citrix XenServer, Nutanix AHV, VMware vSphere y VMware ESX, donde se conoce como aceleración virtual directa de gráficos (vDGA); y con Microsoft Hyper-V en Windows Server 2016, donde se conoce como asignación de dispositivos diferenciados (DDA).
- vGPU está disponible con Citrix XenServer, Nutanix AHV y VMware vSphere; consulte https://www.citrix.com/products/xenapp-xendesktop/hdx-3d-pro.html. HDX 3D Pro también se admite con instancias Cloud en la serie NV de Microsoft Azure y las ofertas Amazon AWS EC2 G3.

Citrix recomienda que el equipo host tenga, como mínimo, 4 GB de RAM y cuatro CPU virtuales con una velocidad de reloj de 2,3 GHz o más.

Unidad de procesamiento de gráficos (GPU):

- Para la compresión basada en CPU (incluida la compresión sin pérdida), HDX 3D Pro admite cualquier adaptador de pantalla en el equipo host que sea compatible con la aplicación que se entrega.
- Para la aceleración de gráficos virtualizados mediante NVIDIA GRID API, HDX 3D Pro puede utilizarse con tarjetas NVIDIA GRID compatibles (consulte NVIDIA GRID). NVIDIA GRID ofrece una alta velocidad de fotogramas, lo que resulta en una experiencia de usuario altamente interactiva.
- La aceleración de gráficos virtualizados se admite en la familia de procesadores Intel Xeon E3 de la plataforma de gráficos para el centro de datos. Para obtener más información, consulte

© 1999-2019 Citrix Systems, Inc. All rights reserved.

https://www.citrix.com/intel y https://www.intel.com/content/www/us/en/servers/data-center-graphics.html.

- La aceleración de gráficos virtualizados se admite con AMD RapidFire en las tarjetas de servidor de la serie S FirePro de AMD. Consulte AMD Virtualization Solution.

Dispositivo del usuario:

- HDX 3D Pro admite todas las resoluciones de monitor que admite la GPU en el equipo host. No obstante, para alcanzar un rendimiento óptimo con las especificaciones mínimas sugeridas para dispositivos de usuario y GPU, Citrix recomienda utilizar una resolución de monitor máxima para los dispositivos de usuario de 1920 x 1200 píxeles en conexiones LAN, y de 1280 x 1024 píxeles en conexiones WAN.
- Citrix también recomienda que la especificación de los dispositivos de usuario tenga, como mínimo, 1 GB de RAM y una CPU con una velocidad de reloj de 1,6 GHz o más. El uso del códec predeterminado de compresión profunda, necesario en conexiones con poco ancho de banda, requiere una CPU más eficaz a menos que la descodificación se realice en hardware. Para alcanzar un rendimiento óptimo, Citrix recomienda que los dispositivos de usuario tengan 2 GB de RAM y una CPU de doble núcleo, como mínimo, con una velocidad de reloj de 3 GHz o más.
- Para el acceso multimonitor, Citrix recomienda dispositivos de usuario con unidades CPU de cuatro núcleos.
- Los dispositivos de usuario no necesitan una GPU para acceder a los escritorios o aplicaciones entregados con HDX 3D Pro.
- La aplicación Citrix Workspace debe estar instalada.

Para obtener más información, consulte los artículos de HDX 3D Pro y www.citrix.com/xenapp/3d.

HDX y los requisitos de las conferencias de vídeo para la compresión de vídeo de cámaras web

Clientes compatibles: La aplicación Citrix Workspace para Windows, la aplicación Citrix Workspace para Mac, la aplicación Citrix Workspace para Chrome y la aplicación Citrix Workspace para Linux.

Aplicaciones de conferencias de vídeo admitidas:

- Adobe Connect
- Cisco Webex y Webex Teams
- GoToMeeting
- Google Hangouts y Hangouts Meet
- IBM Sametime
- Aplicaciones de vídeo basadas en Media Foundation en Windows 8.x o posterior, Windows Server 2012 R2 y posterior
- Microsoft Lync 2010 y 2013
- Microsoft Skype Empresarial 2015
- Microsoft Skype 7 o posterior

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para usar Skype en un cliente Windows, modifique el Registro en el cliente y en el servidor:

- Clave del Registro de cliente HKEY_CURRENT_USER\Software\Citrix\HdxRealTime
  - Nombre: DefaultHeight, tipo: REG_DWORD, datos: 240
  - Nombre: DefaultWidth, Tipo: REG_DWORD, Datos: 320
- Clave del Registro de servidor HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Vd3d\Compatibility
  - Nombre: skype.exe, tipo: REG_DWORD, datos: Establecido en 0

Otros requisitos del dispositivo de usuario:

- Hardware adecuado para reproducir sonido.
- Cámara Web compatible con DirectShow (use la configuración predeterminada de la cámara Web). Las cámaras web que pueden codificar hardware reducen el consumo de la CPU en el lado del cliente.
- Controladores de cámara web, obtenidos del fabricante de la cámara, cuando sea posible.

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 UPServer 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 2016
- Windows Server 2012 R2

Requisito: Microsoft Visual C++ 2013 en ejecución (de 32 y 64 bits)

En caso de VDA para SO de servidor Windows, 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

Al usar Citrix Provisioning (antes Provisioning Services) con esta versión, la versión mínima admitida de Provisioning Services es la versión 7.0.

Solo se admite Citrix License Server 11.15.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

La Consola de administración de directivas de grupo (GPMC) de Microsoft es necesaria si quiere almacenar la información sobre directivas 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 instalada la biblioteca de tiempo de ejecución de Visual Studio 2015. Para obtener más información, consulte la documentación de Microsoft.

Se admiten varias tarjetas de interfaz de red.

De forma predeterminada, no se instala la aplicación Citrix Workspace para Windows al instalar un VDA actual. Para obtener más información, consulte la documentación más reciente de la aplicación Citrix Workspace para Windows.

Consulte App-V para conocer las versiones compatibles de Microsoft App-V.

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

Sistemas operativos que admiten la redirección de carpetas de cliente:

- Servidor: Windows Server 2012 R2 y Windows Server 2016
- Cliente (con la versión más reciente de la aplicación Citrix Workspace para Windows): Windows 7, Windows 8 y Windows 8.1

Resoluciones mixtas con varios monitores. No se admiten PPP diferentes de un monitor a otro en entornos de Citrix Virtual Apps and Desktops. Puede verificar los ppp (ajuste de escala en %) desde el Panel de control de Windows > Opciones de pantalla. Si utiliza un dispositivo cliente con Windows 8.1 o Windows 10, habilite la opción **Dejarme elegir un nivel de ajuste de escala para todas mis pantallas** del Panel de control de Windows > Opciones de pantalla configurará los monitores correspondientemente. Para obtener más información, consulte CTX201696.

Esta versión de Citrix Virtual Apps and Desktops no es compatible con AppDNA 7.8 ni AppDNA 7.9. Citrix recomienda usar la versión actual de AppDNA.

Información técnica general

March 14, 2019

> **Nota:**
>
> Puede obtener información sobre los cambios en los nombres de producto aquí.

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:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

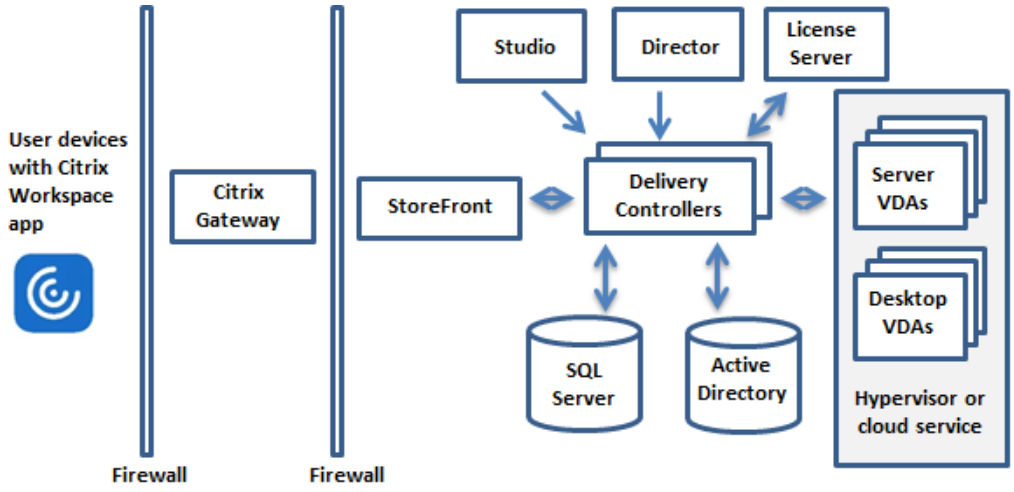
- Los usuarios finales pueden ejecutar aplicaciones y escritorios independientemente de la interfaz y el sistema operativo del dispositivo que estén utilizando.
- Los administradores pueden administrar la red y controlar el acceso desde dispositivos seleccionados o desde todos los dispositivos.
- Los 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 and Desktops desde un único sitio.

Componentes principales

Este artículo es de gran ayuda si acaba de comenzar a utilizar Citrix Virtual Apps and Desktops. Si tiene una comunidad de XenApp 6.x o una versión anterior, o un sitio de XenDesktop 5.6 o una versión anterior, también debería consultar Cambios en 7.x.

En esta imagen, se muestran los componentes principales de una implementación típica, que se denomina “sitio”.



Delivery Controller

El Delivery Controller es el componente de administración central de un sitio. Cada sitio tiene uno o varios Delivery Controllers. Se instala en al menos un servidor del centro de datos. Para la fiabilidad y la disponibilidad del sitio, los Controllers deben instalarse en más de un servidor. Si la implementación incluye un hipervisor o un servicio de nube, los servicios de Controller se comunican con él para distribuir aplicaciones y escritorios, autenticar y administrar el acceso de los usuarios, actuar como intermediario en las conexiones entre los usuarios y sus aplicaciones y escritorios, optimizar y equilibrar las conexiones de los usuarios.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Broker Service del Controller realiza un seguimiento de los usuarios que han iniciado sesión, dónde lo han hecho y qué recursos tienen, y si los usuarios necesitan reconectarse a aplicaciones existentes. Broker Service ejecuta cmdlets de PowerShell y se comunica con el Broker Agent en el VDA a través del puerto TCP 80. No tiene la opción de usar el puerto TCP 443.

Monitor Service recopila datos históricos y los coloca en la base de datos de supervisión. Este servicio utiliza el puerto TCP 80 o 443.

Los datos de los servicios del Controller se almacenan en la base de datos del sitio.

El Controller administra el estado de los escritorios, iniciándolos y deteniéndolos, según la demanda existente y la configuración administrativa. En algunas ediciones, el Controller permite instalar Profile Management para administrar los parámetros de personalización de los usuarios en entornos virtualizados o físicos de Windows.

Base de datos

Se necesita al menos una base de datos Microsoft SQL Server en cada sitio para almacenar la información de configuración y sesiones. Esta base de datos almacena los datos recopilados y administrados por los distintos servicios que conforman el Controller. Instale la base de datos en su centro de datos y asegúrese de que haya una conexión persistente con el Controller.

El sitio también usa una base de datos de registros de configuración y una base de datos de supervisión. De forma predeterminada, estas bases de datos se instalan en la misma ubicación que la base de datos del sitio; este aspecto se puede modificar.

Virtual Delivery Agent (VDA)

El VDA se instala en cada máquina física o virtual del sitio que quiera poner a disposición de los usuarios. Esas máquinas entregan aplicaciones o escritorios. Permite que la máquina se registre en el Controller, que, a su vez, permite que la máquina y sus recursos alojados estén disponibles para los usuarios. Los VDA establecen y administran la conexión entre la máquina y el dispositivo del usuario. Los VDA también verifican que haya una licencia de Citrix disponible para el usuario o la sesión, y aplican las directivas que se hayan configurado para la sesión.

El VDA comunica la información de la sesión al Broker Service en el Controller a través del Broker Agent incluido en el VDA. El agente de broker aloja varios plugins y recopila datos en tiempo real. Se comunica con el Controller a través del puerto TCP 80.

La palabra “VDA” se utiliza a menudo para hacer referencia tanto al agente en sí como a la máquina donde está instalado.

Existen agentes VDA disponibles para sistemas operativos de servidor y de escritorio Windows. Los VDA para sistemas operativos de servidor Windows permiten que varios usuarios se conecten al servi-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

dor al mismo tiempo. Los VDA para SO de escritorio 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 tiendas de escritorios y aplicaciones a los que acceden los usuarios. Puede alojar la tienda 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 seguimiento 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 Software como servicio (SaaS). Para los dispositivos donde no se puede instalar el software de la aplicación Citrix Workspace específico del dispositivo, la aplicación Citrix Workspace para HTML5 ofrece una conexión a través de un explorador Web compatible con HTML5.

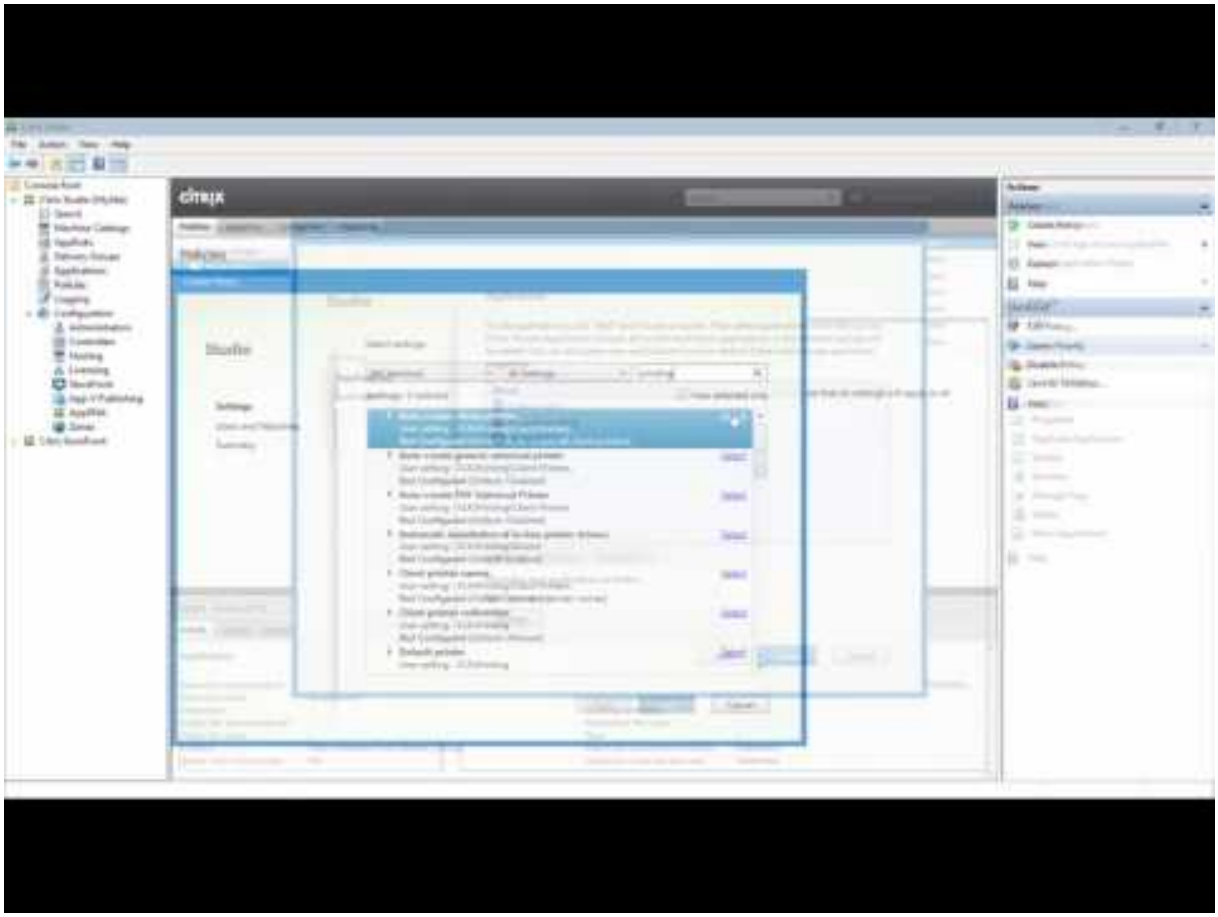
Citrix Studio

Studio es la consola de administración desde la que configurar y administrar la implementación de Citrix Virtual Apps and Desktops. Studio elimina la necesidad de consolas de administración independientes para administrar la entrega de aplicaciones y escritorios. Studio incluye asistentes que le guían para la configuración del entorno, la creación de cargas de trabajo para alojar escritorios y aplicaciones, y la asignación de éstos a los usuarios. También puede usar Studio para asignar licencias de Citrix y realizar un seguimiento de las mismas en el sitio.

La información mostrada en Studio se obtiene del Broker Service que hay en el Controller; se comunica a través del puerto TCP 80.

Aquí dispone de información general sobre Studio.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



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 and 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 utilizando la Asistencia remota de Windows.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Citrix License Server

El servidor de licencias administra las licencias de los productos Citrix. Se comunica con el Controller para administrar las licencias para cada sesión de usuario, y con Studio, para asignar los archivos de licencias. Un sitio debe tener al menos un servidor de licencias para almacenar y administrar los archivos de licencias.

Hipervisor o servicio de nube

El servicio de nube o hipervisor aloja las máquinas virtuales del sitio. Estas pueden ser las máquinas virtuales que se usen para alojar aplicaciones y escritorios, así como las máquinas virtuales que se usen para alojar los componentes de Citrix Virtual Apps and Desktops. Un hipervisor se instala en un host dedicado enteramente a ejecutar el hipervisor y alojar máquinas virtuales.

Citrix Virtual Apps and Desktops admiten varios hipervisores y servicios de nube.

Aunque muchas implementaciones requieren un hipervisor, no lo necesita para proporcionar acceso con Remote PC. Tampoco necesita un hipervisor cuando usa Provisioning Services (PVS) para aprovisionar las máquinas virtuales.

Para obtener más información, consulte:

- Puertos de red.
- Bases de datos.
- Servicios Windows en los componentes de Citrix Virtual Apps and Desktops: Configurar derechos de usuario.
- Hipervisores y servicios de nube respaldados: Requisitos del sistema.

Componentes adicionales

Los siguientes componentes adicionales, no incluidos en la imagen anterior, también pueden incluirse en las implementaciones de Citrix Virtual Apps and Desktops. Para obtener más información, consulte la documentación correspondiente.

Citrix Provisioning

Citrix Provisioning (anteriormente conocido como Provisioning Services) es un componente opcional que está disponible con algunas ediciones. Proporciona una alternativa a MCS para aprovisionar las máquinas virtuales. Mientras que MCS crea copias de una imagen maestra, Provisioning Services distribuye la imagen maestra por streaming a los dispositivos de usuario. Provisioning Services no requiere un hipervisor para hacerlo, por lo tanto, se puede usar para alojar máquinas físicas. Provisioning Services se comunica con el Controller para proporcionar recursos a los usuarios.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Citrix Gateway

Cuando los usuarios se conectan desde fuera del firewall de la empresa, Citrix Virtual Apps and Desktops pueden usar la tecnología de Citrix Gateway (antes llamado Access Gateway y NetScaler Gateway) para proteger esas conexiones con TLS. El dispositivo virtual Citrix Gateway o VPX es un dispositivo de SSL VPN que se implementa en la zona desmilitarizada (DMZ). Proporciona un punto de acceso único y seguro a través del firewall corporativo.

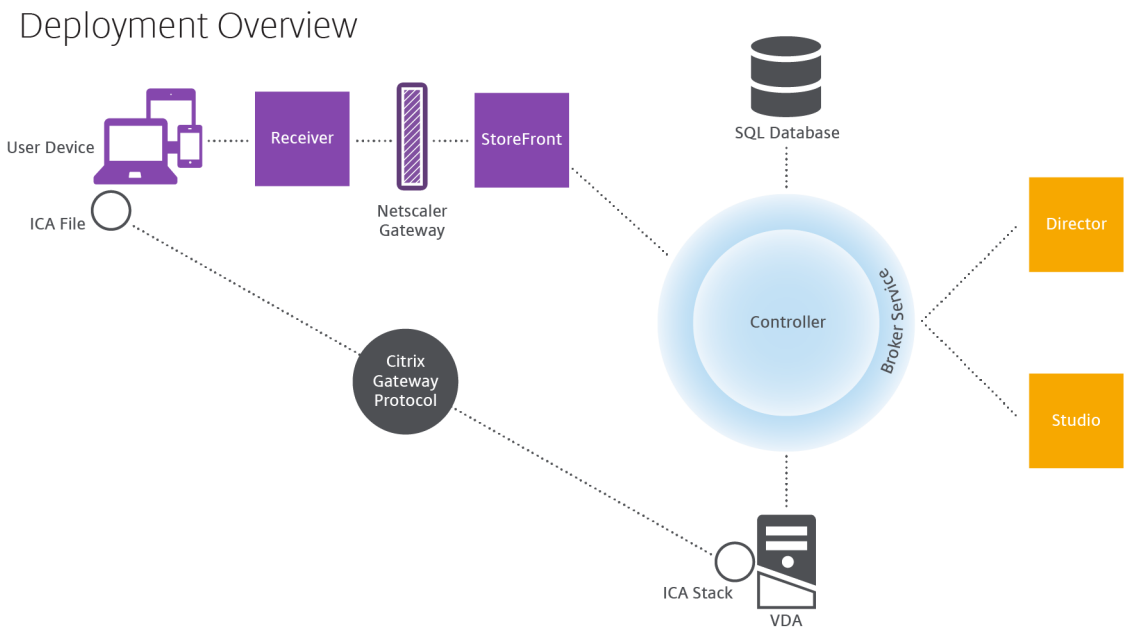
Citrix SD-WAN

En las implementaciones donde se entregan escritorios virtuales a usuarios de ubicaciones remotas, como sucursales de oficina, se puede emplear la tecnología de Citrix SD-WAN para optimizar el rendimiento. Los repetidores aceleran el rendimiento en redes amplias. Con repetidores presentes en la red, los usuarios de la sucursal experimentan un rendimiento similar al de una LAN a través de la WAN. Citrix SD-WAN puede dar prioridad a diferentes partes de la experiencia de usuario de modo que esta experiencia no empeore en la sucursal cuando, por ejemplo, se envíe un archivo de gran tamaño o un trabajo de impresión por la red. La optimización HDX de WAN ofrece compresión por token y 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 características 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



El VDA permite a los usuarios conectarse a escritorios y aplicaciones. Para la mayoría de los métodos de entrega, el VDA se instala en máquinas de servidor o de escritorio, aunque también se puede instalar en PC físicos para el acceso con Remote PC.

El Controller se compone de servicios Windows independientes que administran los recursos, las aplicaciones y los escritorios, y optimizan y equilibran la carga de conexiones de usuarios. Cada sitio tiene uno o varios Delivery Controllers. Como las sesiones dependen de la latencia, el ancho de banda y la fiabilidad de la red, lo ideal es que todos los Controllers se encuentren en la misma LAN.

Los usuarios nunca acceden directamente al Controller. El VDA funciona como intermediario entre los usuarios y el Controller. Cuando los usuarios inician sesión usando 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.

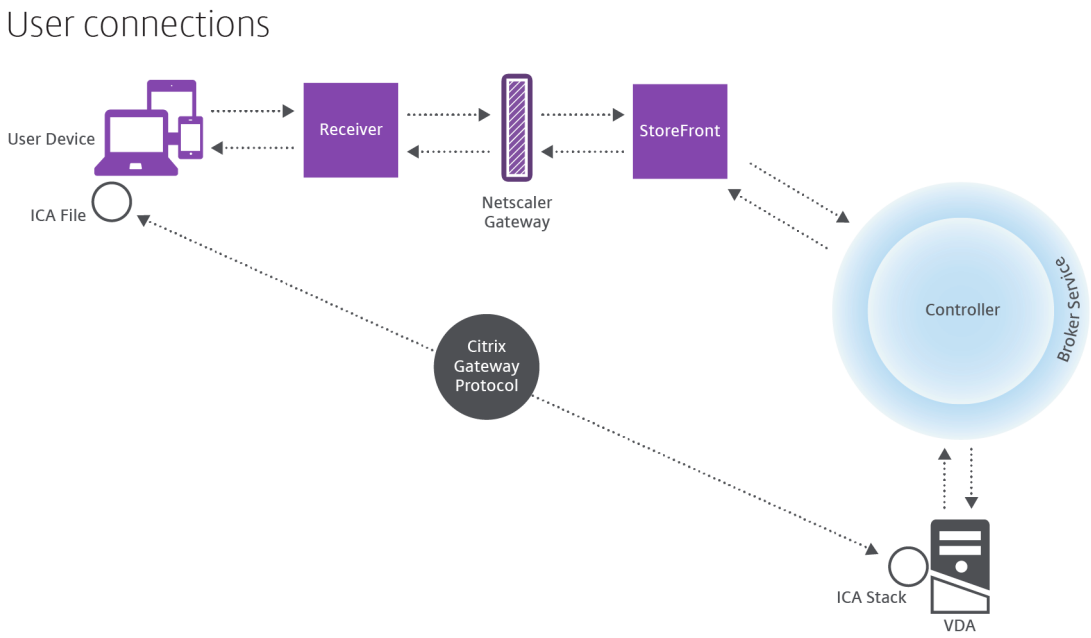
¿Cómo se gestionan las conexiones de usuario?

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



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.

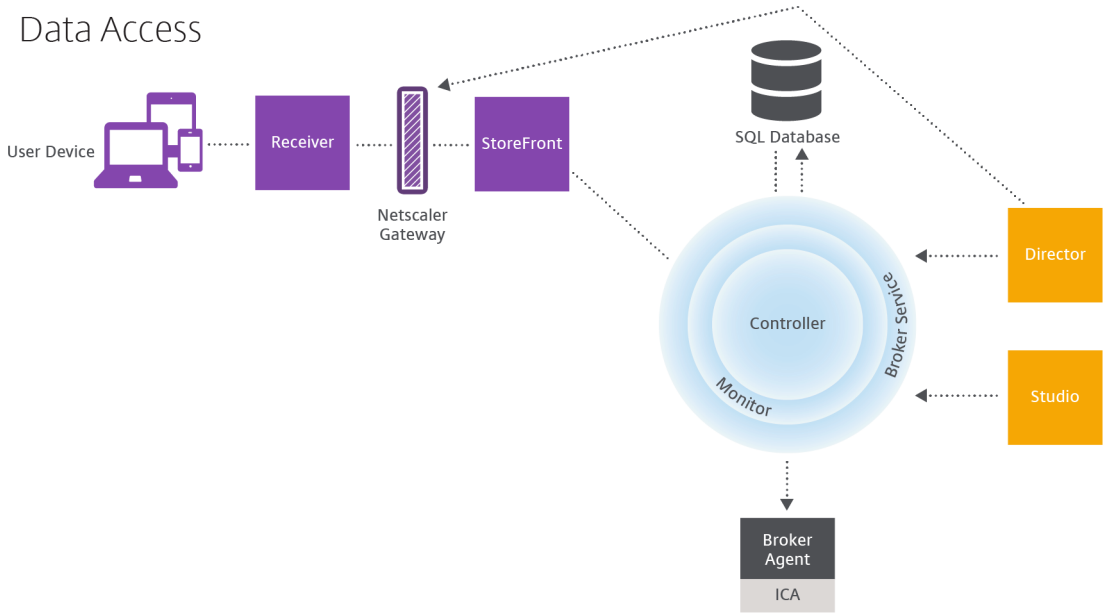
Una vez que el cliente se conecta al VDA, el VDA notifica al Controller que el usuario ha iniciado sesión. El Controller envía esta información a la base de datos del sitio y comienza a registrar datos en la base

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 seguimiento de los datos en tiempo real y lo almacena como datos históricos en la base de datos de supervisión.

Studio solo se comunica con el Broker Service; por lo tanto, solo tiene acceso a datos en tiempo real. Director se comunica con el Broker Service (a través de un plugin de Broker Agent) para tener acceso a la base de datos del sitio.

Director también puede acceder a Citrix Gateway para obtener información sobre los datos HDX.

Entregar escritorios y aplicaciones

Configure las máquinas que van a entregar aplicaciones y escritorios con los catálogos de máquinas. Luego, cree grupos de entrega que especifiquen las aplicaciones y los escritorios que estarán

© 1999-2019 Citrix Systems, Inc. All rights reserved.

disponibles (a través de las máquinas de los catálogos) y qué usuarios pueden acceder a ellos. De forma opcional, 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:

- **Máquinas con sistema operativo de servidor:** Máquinas virtuales o físicas con un sistema operativo de servidor. 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.
- **Máquinas con sistema operativo de escritorio:** Máquinas virtuales o físicas con un sistema operativo de escritorio. Se utilizan para entregar escritorios VDI (escritorios que ejecutan sistemas operativos de escritorio que pueden personalizarse), aplicaciones alojadas en VM (aplicaciones de sistemas operativos de escritorio) 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 blanca.

Para obtener más información, consulte Administración de imágenes de Citrix Virtual Apps and Desktops y Crear catálogos de máquinas.

Grupos de entrega

Los grupos de entrega especifican los usuarios que pueden acceder a las aplicaciones y/o los escritorios y las máquinas que se pueden utilizar para ello. Los grupos de entrega contienen máquinas del

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 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 máquinas adicionales. La restricción de etiqueta puede entenderse como una subdivisión (o partición) de las máquinas de un grupo de entrega. Usar grupos de aplicaciones puede ser útil para aislar un subconjunto de las máquinas de un grupo de entrega y solucionar los problemas que presentan.

Para obtener más información, consulte Crear grupos de aplicaciones.

Más información

Diagramas de Citrix Virtual Apps and Desktops

Active Directory

January 29, 2019

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 se debe ejecutar en las versiones desde Windows Server 2003 a Windows Server 2012 R2; esto no afecta al nivel funcional del dominio.

Este producto respalda 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 respalda 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.

> **Sugerencia:**
>
> No cambie el nombre de equipo ni la pertenencia al dominio de un Controller una vez configurado el sitio.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Implementación en un entorno de Active Directory de varios bosques

Esta información se aplica a XenDesktop 7.1 y XenApp 7.5 (versiones mínimas). No se aplica a versiones anteriores de XenDesktop o XenApp.

En un entorno de Active Directory con varios bosques, si hay confianza unidireccional o bidireccional, se pueden usar reenviadores DNS 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. La clave SupportMultipleForest solo es necesaria en el VDA. Use la información siguiente para agregar la clave de Registro:

> **Precaución:**
>
> Si modifica el Registro de forma incorrecta, pueden producirse problemas graves, que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

HKEY_LOCAL_MACHINE \ Software \ Citrix \ VirtualDesktopAgent \ SupportMultipleForest

- Nombre: SupportMultipleForest
- Tipo: REG_DWORD
- Datos: 0x00000001 (1)

Es posible que sea necesaria la configuración de DNS inversa si el espacio de nombres DNS es diferente del de Active Directory.

Si existen confianzas externas durante la instalación, se necesita la clave del Registro ListOfSIDs. La clave del Registro ListOfSIDs también es necesaria si el FQDN de Active Directory difiere del FQDN de DNS o si el dominio que contiene el controlador de dominio tiene un nombre de NetBIOS que difiere del FQDN de Active Directory. Para agregar la clave del Registro, utilice la siguiente información:

Para un 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

En caso de que haya relaciones de confianza con elementos externos, realice los siguientes cambios en el VDA:

1. Busque el archivo Archivos de programa\Citrix\Virtual Desktop Agent\brokeragentconfig.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 el texto allowNtlm="false" y cámbielo a allowNtlm="true".
5. Guarde el archivo.

Después de agregar la clave del Registro ListOfSIDs y de modificar el archivo brokeragent.exe.config, reinicie Citrix Desktop Service para aplicar los cambios.

La siguiente tabla muestra los tipos de confianza admitidos:

Tipo de confianza	Transitividad	Dirección	Se admite en esta versión
Elemento primario y secundario	Transitiva	Bidireccional	Sí
Raíz del árbol	Transitiva	Bidireccional	Sí
Externa	No transitiva	Unidireccional o bidireccional	Sí
Bosque	Transitiva	Unidireccional o bidireccional	Sí
Acceso directo	Transitiva	Unidireccional o bidireccional	Sí
Dominio	Transitiva o no transitiva	Unidireccional o bidireccional	No

Para obtener más información sobre entornos de Active Directory complejos, consulte CTX134971.

Bases de datos

March 8, 2019

Un sitio de Citrix Virtual Apps o Citrix Virtual Desktops usa tres bases de datos de SQL Server:

- **Sitio:** También conocida como Configuración del sitio, esta base de datos almacena la configuración activa del sitio, el estado actual de la sesión y la información de conexión.
- **Registro de configuración:** También conocida como Registro, esta base de datos almacena información acerca de actividades de tipo administrativo y los cambios de configuración en el

© 1999-2019 Citrix Systems, Inc. All rights reserved.

sitio. Esta base de datos se usa cuando la función Registro de configuración está habilitada (opción predeterminada).
- **Supervisión:** Esta base de datos almacena los datos que utiliza Director, como la información de conexión y de sesión.

Cada Delivery Controller se comunica con la base de datos del sitio. Se requiere la autenticación de Windows entre el Controller y las bases de datos. Un Controller se puede desconectar o apagar sin que esta acción afecte a los otros Controllers del sitio. No obstante, esto significa que la base de datos del sitio representa un punto único de fallo. Si el servidor de base de datos da error, las conexiones existentes seguirán funcionando hasta que el usuario cierre sesión o se desconecte. Para obtener información sobre el comportamiento de las conexiones cuando la base de datos del sitio no está disponible, consulte Caché de host local.

Citrix recomienda realizar una copia de seguridad de las bases de datos periódicamente para poder restaurarla a partir de esa copia si el servidor de base de datos falla. La estrategia de copia de respaldo para cada base de datos puede ser distinta. Para obtener instrucciones, consulte CTX135207.

Si el sitio contiene más de una zona, la zona principal siempre debe contener la base de datos del sitio. Los Controllers de cada zona se comunicarán con esa base de datos.

Alta disponibilidad

Existen varias soluciones de alta disponibilidad que es conveniente tener en cuenta para garantizar la conmutación por error automática:

- **Grupos de disponibilidad AlwaysOn (incluidos los grupos de disponibilidad básica):** Esta solución de alta disponibilidad y recuperación ante desastres para empresas introducida en SQL Server 2012 permite maximizar la disponibilidad de una o varias bases de datos. Los grupos de disponibilidad AlwaysOn requieren que las instancias de SQL Server residan en los nodos de clústeres de conmutación por error de Windows Server (WSFC). Para obtener más información, consulte https://msdn.microsoft.com/en-us/library/hh510230.
- **Crear imágenes reflejo de la base de datos de SQL Server:** Reflejar la base de datos garantiza que, si se pierde la conexión con el servidor de base de datos activo, el proceso automático de conmutación por error se produzca rápidamente (en cuestión de segundos) para que los usuarios en general no resulten afectados. No obstante, este método es más costoso que las soluciones alternativas, ya que se requieren licencias de SQL Server completas en cada servidor de base de datos; tenga en cuenta que no se puede usar SQL Server Express en un entorno reflejado.
- **Agrupación en clústeres de SQL:** La tecnología de agrupación en clústeres de SQL de Microsoft se puede usar para permitir automáticamente que un servidor tome el control de las tareas y las responsabilidades de otro servidor que ha fallado. No obstante, la instalación de esta solución

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 de alta disponibilidad de SQL Server porque permite a los usuarios conectarse varias veces a los últimos escritorios y aplicaciones que han utilizado, incluso cuando la base de datos del sitio no está disponible. Para obtener más información, consulte Caché de host local.

Si se producen fallos en todos los Delivery Controllers de un sitio, es posible configurar los agentes VDA de modo que funcionen en el modo de alta disponibilidad y, así, los usuarios puedan seguir accediendo y utilizando sus escritorios y aplicaciones. En el modo de alta disponibilidad, el VDA acepta conexiones ICA directas de los usuarios en lugar de conexiones con el Controller como intermediario (broker). Utilice esta función solo en el caso poco corriente de que falle la comunicación con todos los Controllers; no es una alternativa a otras soluciones de alta disponibilidad. Para obtener más información, consulte CTX 127564.

> **Nota:**
>
> No se admite la instalación de Controller en un nodo de clúster de SQL o de instalación duplicada (mirroring) de SQL.

Instalar software de base de datos

De forma predeterminada y si no se detecta ninguna otra instancia de SQL Server en ese servidor, se instala SQL Server Express Edition al instalar el primer Delivery Controller. Por lo general, esa acción predeterminada es suficiente para implementaciones piloto o de pruebas de concepto. Sin embargo, SQL Server Express no admite características de alta disponibilidad de Microsoft.

La instalación predeterminada usa las cuentas y los permisos predeterminados del servicio de Windows. Consulte la documentación de Microsoft para ver información detallada de estos valores predeterminados, incluida la incorporación de cuentas de servicio Windows en el rol de sysadmin. Controller usa la cuenta de Servicio de red en esta configuración. Controller no necesita permisos ni roles adicionales de SQL Server.

Si es necesario, puede seleccionar **Ocultar instancia** para la instancia de la base de datos. Al configurar la dirección de la base de datos en Studio, introduzca el número de puerto estático de la instancia,

© 1999-2019 Citrix Systems, Inc. All rights reserved.

en lugar de su nombre. Consulte la documentación de Microsoft para obtener información más detallada sobre cómo ocultar una instancia del motor de base de datos de SQL Server.

Por lo tanto, la mayoría de las implementaciones de producción y cualquier implementación que use funciones de alta disponibilidad de Microsoft, debe instalar otras ediciones de SQL Server admitidas (que no sean Express) en máquinas que no sean el servidor donde está instalado el primer Controller. En el artículo Requisitos del sistema, se ofrece una lista de las versiones admitidas de SQL Server. Las bases de datos pueden residir en una o varias máquinas.

Antes de crear un sitio, compruebe que el software de SQL Server está instalado. No es necesario crear la base de datos pero, si la crea, debe estar vacía. También se recomienda configurar las tecnologías de alta disponibilidad de Microsoft.

Use Windows Update para mantener SQL Server actualizado.

Configurar bases de datos desde el asistente para la creación de sitios

Especifique los nombres de las bases de datos y sus direcciones (ubicación) en la página **Bases de datos** del asistente para la creación de sitios. (Consulte Formatos de direcciones de bases de datos.) Para evitar posibles errores cuando Director consulte Monitor Service, no use espacios en blanco en el nombre de la base de datos de supervisión.

La página **Bases de datos** ofrece dos opciones para configurar bases de datos: automáticamente o mediante scripts. Por lo general, puede usar la opción automática si usted (como usuario de Studio y administrador Citrix) tiene los privilegios de base de datos pertinentes. (Consulte Permisos necesarios para configurar bases de datos.)

Puede cambiar la ubicación de la base de datos de registros de configuración y supervisión más adelante, después de crear el sitio. Consulte Cambiar ubicaciones de base de datos.

Para que un sitio utilice una base de datos reflejada, complete lo siguiente y continúe con el procedimiento de configuración automática o por script.

1. Instale el software de SQL Server en dos servidores, A y B.
2. En el servidor A, cree la base de datos que se utilizará como principal. Haga una copia de seguridad de la base de datos ubicada en el servidor A y, a continuación, cópiela al servidor B.
3. En el servidor B, restaure el archivo de copia de seguridad.
4. Inicie la creación de reflejo en el servidor A.

Para verificar la creación de la base de datos reflejada después de crear el sitio, ejecute el cmdlet `get-configdbconnection` de PowerShell para asegurarse de que el socio de conmutación por error se ha definido en la cadena de conexión para la base de datos reflejada.

Si más adelante quiere agregar, mover o quitar un Delivery Controller de un entorno de base de datos reflejada, consulte [Delivery Controllers](/es-es/citrix-virtual-apps-desktops/manage-deployment/delivery-controllers.html.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configuración automática

Si tiene los privilegios de base de datos necesarios, seleccione la opción “Crear y configurar bases de datos desde Studio” en la página **Bases de datos** del asistente para la creación de sitios. A continuación, especifique los nombres y las direcciones de las bases de datos principales.

Si ya existe una base de datos en una dirección que especifique, esta debe estar vacía. Si no existen bases de datos en la dirección especificada, se le informa que no se ha podido encontrar ninguna base de datos y se le solicita crear una. Tras confirmar esa acción, Studio crea automáticamente las bases de datos y aplica los scripts de inicialización a las bases de datos principales y de réplica.

Configuración por script

Si no tiene los privilegios necesarios de bases de datos, deberá pedir ayuda a alguien con esos privilegios, como a un administrador de base de datos. Aquí se presenta el orden de pasos a seguir:

1. En el asistente para la creación de sitios, seleccione la opción **Generar scripts**. Esta acción genera seis scripts: dos para cada una de las tres bases de datos (una para cada base de datos principal y otra para cada réplica). Puede indicar dónde almacenar los scripts.
2. Facilite esos scripts al administrador de base de datos. El asistente para la creación de sitios se detiene automáticamente en este punto y se le pedirá continuar con la creación de sitios cuando vuelva de nuevo al asistente.

El administrador de base de datos crea la base de datos. Cada base de datos debe tener las siguientes características:

- Usar una intercalación que termine con “_CI_AS_KS”. Citrix recomienda usar una intercalación que termine con “_100_CI_AS_KS”.
- Para un rendimiento óptimo, habilite la instantánea de lectura confirmada de SQL Server. Para obtener más información, consulte CTX 137161.
- Funciones de alta disponibilidad configuradas, si se quiere.
- Para configurar la creación de reflejo, primero debe configurar la base de datos para que use el modelo de recuperación completa (a diferencia del modelo simple, que es el valor predeterminado). Haga una copia de seguridad de la base de datos principal en un archivo y cópielo al servidor reflejado. En la base de datos reflejada, restaure el archivo de copia de seguridad para el servidor reflejado. A continuación, inicie la creación de reflejo en el servidor principal.

El administrador de base de datos usa la herramienta de línea de comandos SQLCMD o SQL Server Management Studio en modo SQLCMD para ejecutar cada script de xxx_Replica.sql en las instancias de alta disponibilidad de base de datos de SQL Server (si se ha configurado la alta disponibilidad) y para ejecutar luego cada script de xxx_Principal.sql en las instancias de base de datos principal de SQL Server. Consulte la documentación de Microsoft para obtener información más detallada acerca de SQLCMD.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Cuando todos los scripts finalizan correctamente, el administrador de base de datos facilita al administrador Citrix las tres direcciones de bases de datos principales.

En Studio, se le solicitará continuar con la creación de sitios y se volverá a la página **Bases de datos**. Escriba las direcciones. Si no se puede establecer contacto con alguno de los servidores que alojan una base de datos, aparecerá un mensaje de error.

Permisos necesarios para configurar bases de datos

Debe ser un administrador local y un usuario de dominio para crear e inicializar bases de datos (o cambiar la ubicación de estas). También debe tener ciertos permisos de SQL Server. Los siguientes permisos se pueden configurar explícitamente o se pueden adquirir por la pertenencia a grupos de Active Directory. Si las credenciales de usuario de Studio no incluyen estos permisos, se le solicitarán las credenciales de usuario de SQL Server.

Operación	Propósito	Rol del servidor	Rol de la base de datos
Crear una base de datos	Crear una base de datos vacía adecuada	dbcreator	
Crea un esquema	Crear los esquemas de cada servicio y agregar el primer Controller al sitio	securityadmin*	db_owner
Agregar un Controller	Agregar un Controller (aparte del primero) al sitio	securityadmin*	db_owner
Agregar un Controller (servidor reflejado)	Agregar un inicio de sesión de Controller al servidor de la base de datos que se encuentra actualmente en el rol de espejo de la base de datos reflejada	securityadmin*	
Actualizar un esquema	Aplicar revisiones hotfix o actualizaciones a esquemas		db_owner

© 1999-2019 Citrix Systems, Inc. All rights reserved.

* Aunque sea técnicamente más restrictivo, en la práctica, el rol de servidor securityadmin debe tratarse como equivalente al rol de servidor sysadmin.

Cuando se utiliza Studio para realizar estas operaciones, la cuenta de usuario debe formar parte del rol de servidor sysadmin.

Formatos de direcciones de bases de datos

Puede especificar una dirección de base de datos de una de las siguientes formas:

- `ServerName`
- `ServerName\\InstanceName`
- `ServerName,PortNumber`

Para un grupo de disponibilidad AlwaysOn, especifique el servidor de escucha del grupo en el campo de ubicación.

Cambiar ubicaciones de base de datos

Después de crear un sitio, puede cambiar la ubicación de las bases de datos de registros de configuración y supervisión. (No se puede cambiar la ubicación de la base de datos del sitio.) Al cambiar la ubicación de una base de datos:

- Los datos de la base de datos anterior no se importarán en la nueva base de datos.
- Los registros no pueden combinarse desde ambas bases de datos al consultarlos.
- La primera entrada del registro en la nueva base de datos indica que se ha producido un cambio en la base de datos, pero no identifica la base de datos anterior.

No es posible cambiar la ubicación de la base de datos de registros de configuración cuando está habilitado el registro obligatorio.

Para cambiar la ubicación de una base de datos:

1. Compruebe que haya instalada una versión admitida de Microsoft SQL Server en el servidor donde residirá la base de datos. Configure las funciones de alta disponibilidad, si fuera necesario.
2. Seleccione **Configuración** en el panel de navegación de Studio.
3. Seleccione la base de datos para la que quiere especificar una nueva ubicación y, a continuación, seleccione **Cambiar base de datos** en el panel **Acciones**.
4. Especifique la nueva ubicación y el nombre de la base de datos.
5. Si quiere que Studio cree la base de datos y si tiene los permisos adecuados, haga clic en **Aceptar**. Cuando se le solicite, haga clic en **Aceptar** y Studio creará automáticamente la base de datos. Studio intenta acceder a la base de datos utilizando las credenciales. Si no puede, el sistema pedirá las credenciales del usuario de la base de datos. Studio carga el esquema de base

© 1999-2019 Citrix Systems, Inc. All rights reserved.

de datos en la base de datos. Las credenciales se conservan solo durante el periodo de creación de la base de datos.

6. Si no quiere que Studio cree la base de datos o no dispone de los permisos necesarios, haga clic en **Generar script**. Los scripts generados incluyen instrucciones para crear manualmente la base de datos y una base de datos reflejada, si es necesario. Antes de cargar el esquema, compruebe que la base de datos está vacía y de que al menos un usuario tiene permiso para acceder a ella y cambiarla.

Más información

- Herramienta para calcular el tamaño de la base de datos.
- Tamaño de la base de datos del sitio y Configurar las cadenas de conexión cuando se utilizan soluciones de alta disponibilidad de SQL Server.

Métodos de entrega

December 4, 2018

Puede resultar complicado satisfacer las necesidades de cada usuario de la organización a partir de una única implementación de virtualización. Citrix Virtual Apps and Desktops permiten a los administradores personalizar la experiencia del usuario con una variedad de métodos.

Esta colección de métodos de entrega (cada uno con sus propias ventajas y desventajas) ofrecen la mejor experiencia de usuario en cualquier caso de uso.

Adaptar las aplicaciones Windows a dispositivos móviles

Los dispositivos de pantalla táctil, tales como smartphones y tabletas, son ahora el estándar de movilidad informática. Estos dispositivos pueden ocasionar problemas cuando se ejecutan en ellos aplicaciones Windows que normalmente usan pantallas de tamaño completo y requieren clics con el botón secundario del mouse para aprovechar toda su funcionalidad.

Citrix Virtual Apps, junto con la aplicación Citrix Workspace, ofrece una solución segura que permite a los usuarios de dispositivos móviles acceder a toda la funcionalidad de sus aplicaciones basadas en Windows, sin necesidad de incurrir en el coste de reescribir esas aplicaciones para adaptarlas a las plataformas móviles.

El método de entrega para aplicaciones publicadas de Citrix Virtual Apps usa tecnología HDX Mobile, que resuelve los problemas asociados con la adaptación de aplicaciones Windows a dispositivos móviles. Este método permite refactorizar las aplicaciones Windows para usarlas en un entorno táctil, al tiempo que mantiene características como los gestos multitoque, los controles de menú nativos,

© 1999-2019 Citrix Systems, Inc. All rights reserved.

las funciones de GPS y la cámara. Muchas funciones táctiles están disponibles de forma nativa en Citrix Virtual Apps and Desktops, y no requieren ningún cambio en el código fuente de la aplicación para activarlas.

Estas funciones incluyen:

- Presentación automática del teclado cuando un campo de edición está activo
- Mayor control de selector para reemplazar el control de cuadro combinado de Windows
- Gestos multitoque, como el pellizco y el zoom
- Desplazamiento por inercia
- Navegación directa con puntero o por panel táctil

Reducir el coste de actualización de los PC

La actualización de equipos físicos es una tarea complicada que muchos negocios afrontan cada 3-5 años, especialmente si el negocio necesita mantener sus sistemas operativos y aplicaciones al día. Los negocios en crecimiento también se enfrentan con grandes costes cuando tienen que agregar nuevos equipos a su red.

El método de entrega VDI con Personal vDisk ofrece un sistema operativo de escritorio totalmente personalizado a cada usuario, en cualquier equipo o cliente ligero, usando recursos de servidor. Los administradores pueden crear máquinas virtuales cuyos recursos (como el procesamiento, la memoria y el almacenamiento) se guardan en el centro de datos de la red.

Esto permite extender el ciclo de vida de máquinas antiguas, mantener el software actualizado y reducir el tiempo de indisponibilidad durante las actualizaciones.

Acceso seguro a aplicaciones y escritorios virtuales para contratistas y socios

La seguridad en la red es un problema creciente, especialmente cuando se trabaja con contratistas, socios y otros trabajadores temporales externos, que necesitan acceso a las aplicaciones y los datos de la empresa. Además, los trabajadores pueden necesitar pedir prestados portátiles u otros dispositivos, lo que puede incrementar costes.

Los datos, las aplicaciones y los escritorios se guardan detrás del firewall de la red segura con Citrix Virtual Apps and Desktops, por lo que lo único que transmite el usuario final son acciones de entrada y salida del dispositivo del usuario, tales como pulsaciones en el teclado, acciones del mouse, audio y actualizaciones de pantalla. Al mantener estos recursos en un centro de datos, Citrix Virtual Apps and Desktops ofrecen una solución de acceso remoto más segura que la configuración típica de red privada virtual (VPN) con SSL.

Con una implementación de VDI con Personal vDisk, los administradores pueden utilizar clientes ligeros o los dispositivos personales de los usuarios, creando una máquina virtual en un servidor

© 1999-2019 Citrix Systems, Inc. All rights reserved.

de red y proporcionando un sistema operativo de escritorio de usuario único. Con ello, el departamento de TI puede mantener la seguridad con trabajadores externos sin necesidad de comprar equipamiento costoso.

Acelerar la migración

Al cambiar a un nuevo sistema operativo, el departamento de TI puede encontrarse con dificultades para entregar aplicaciones antiguas e incompatibles.

Con las aplicaciones alojadas en máquinas virtuales, los usuarios pueden ejecutar aplicaciones antiguas a través de la aplicación Citrix Workspace en la máquina virtual actualizada, sin problemas de compatibilidad. Esto da al departamento de TI un tiempo adicional para resolver problemas de compatibilidad, ayudar a los usuarios en la transición y hacer más eficientes las llamadas al Help Desk.

Ventajas adicionales de usar XenDesktop durante la migración:

- Reducción de la complejidad de los escritorios
- Mejora del control de TI
- Mayor flexibilidad para los usuarios finales en cuanto a uso de dispositivos y ubicación del área de trabajo

Aplicaciones de gráficos 3D profesionales virtualizadas para diseñadores e ingenieros

Muchos fabricantes y empresas de diseño basan su trabajo en aplicaciones de gráficos 3D profesionales. Estas compañías tienen presiones financieras derivadas de los altos costes de hardware necesarios para dar soporte a este tipo de software y se enfrentan también a problemas de logística derivados de la necesidad de compartir archivos de diseños de gran tamaño a través de FTP, correo electrónico y otros métodos similares.

El método de entrega de escritorios físicos alojados ofrece una única imagen de escritorio a las estaciones de trabajo y los servidores Blade sin necesidad de que los hipervisores ejecuten aplicaciones de gráficos 3D en un sistema operativo nativo.

Todos los archivos se guardan en el centro de datos de la red, por lo tanto, el uso compartido de archivos de gran tamaño entre múltiples usuarios en la red es más rápido y más seguro, ya que los archivos no se transfieren desde una estación de trabajo a otra.

Transformar los centros de llamadas

Las empresas que cuentan con centros de llamadas de atención al cliente a gran escala se enfrentan con el difícil reto de mantener un nivel de personal adecuado durante los períodos de mayor uso, al

© 1999-2019 Citrix Systems, Inc. All rights reserved.

tiempo que deben asegurarse de no aprovisionar máquinas en exceso durante los periodos de menor actividad.

El método de entrega de VDI agrupados ofrece a múltiples usuarios el acceso dinámico a un escritorio estándar, por un coste mínimo, cuando se quiere aprovisionar escritorios a muchos usuarios. Las máquinas agrupadas se asignan por sesión y a medida que los usuarios las solicitan.

La necesidad de administrar diariamente estas máquinas es menor, porque los cambios que se hacen en ellas durante la sesión se descartan cuando el usuario cierra la sesión. Esto también aumenta la seguridad.

El método de entrega de escritorios alojados es otra opción viable para transformar los centros de llamadas. Este método aloja varios escritorios de usuario en un mismo sistema operativo de servidor.

Este es un método más eficiente desde el punto de vista de costes que el método de VDI agrupados pero, con los escritorios alojados, los usuarios no pueden instalar aplicaciones, cambiar los parámetros del sistema ni reiniciar el servidor.

Aplicaciones y escritorios publicados de Citrix Virtual Apps

October 3, 2018

Use máquinas de SO de servidor para entregar aplicaciones publicadas de Citrix Virtual Apps y escritorios publicados de Citrix Virtual Apps.

Caso de uso

- Quiere una entrega de recursos basada en servidores, que no sea muy costosa, para minimizar el costo de entregar aplicaciones a un gran número de 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 y 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 manera centralizada y los usuarios no pueden modificar la aplicación, lo que proporciona una experiencia de usuario coherente, segura y fiable.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- 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, desde su menú Inicio, o con una dirección URL que le ha 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.

Procesar, alojar y entregar 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 de SO de servidor.
- 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 de SO de servidor admiten grupos de entrega que alojan o aplicaciones o escritorios, o ambos.

Asignar y administrar sesiones

- Las máquinas de SO de servidor 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 dentro de 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 usando 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para entregar aplicaciones y escritorios publicados de Citrix Virtual Apps:

1. Instale las aplicaciones que desea entregar en una imagen maestra que ejecute un sistema operativo compatible de servidor Windows.
2. Cree un catálogo de máquinas para esta imagen maestra o actualice un catálogo existente con esta imagen maestra.
3. Cree un grupo de entrega para entregar aplicaciones y escritorios a los usuarios. Si entrega aplicaciones, seleccione las que quiere entregar.

Consulte los artículos de instalación y configuración para obtener información más detallada.

Aplicaciones alojadas en VM

October 3, 2018

Use máquinas de SO de escritorio 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 una gran cantidad de usuarios por servidor host (o hipervisor), al tiempo que ofrece 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, ofreciendo así una solución de entrega de aplicaciones más rentable.
- Cuando el usuario inicia una sesión, se le puede asignar aleatoriamente a 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- La ejecución de sesiones múltiples no está respaldada en máquinas de SO de escritorio. 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 discos virtuales personales (Personal vDisk) de los usuarios.

Experiencia de usuario

La misma experiencia de aplicación integrada que tiene lugar con las aplicaciones alojadas compartidas en máquinas con SO de servidor.

Procesamiento, alojamiento y entrega de aplicaciones

Lo mismo que con máquinas de SO del servidor, excepto que son máquinas virtuales de SO de escritorio.

Asignar y administrar sesiones

- Las máquinas con SO de escritorio 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.

Para entregar aplicaciones alojadas en VM:

1. Instale las aplicaciones que desea entregar en una imagen maestra que ejecute un sistema operativo compatible de escritorio Windows.
2. Cree un catálogo de máquinas para esta imagen maestra o actualice un catálogo existente con esta imagen maestra.
3. Al definir la experiencia del escritorio para el catálogo, decida si quiere que los usuarios se conecten a la misma VM o a una nueva cada vez que inicien sesión.
4. Cree un grupo de entrega para entregar la aplicación a los usuarios.
5. En la lista de las aplicaciones instaladas, seleccione la aplicación que quiere entregar.

Consulte los artículos de instalación y configuración para obtener información más detallada.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Escritorios VDI

October 3, 2018

Use máquinas con SO de escritorio para entregar escritorios VDI.

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 de Citrix Virtual Apps, pero no es necesario que las aplicaciones instaladas en ellos respalden sistemas operativos de servidor. Además, según el tipo de escritorio VDI que elija, estos escritorios se pueden asignar a usuarios individuales y permitirles un alto grado de personalización del escritorio.

Al crear un catálogo de máquinas para escritorios VDI, hay que crear uno de estos tipos de escritorios:

- **Escritorios aleatorios no persistentes**, también conocidos como escritorios VDI agrupados. Cada vez que un usuario inicia sesión para usar uno de estos escritorios, se conecta a un escritorio seleccionado de forma dinámica de un grupo de escritorios basado en una imagen maestra. Todos los cambios realizados en el escritorio se pierden tras reiniciarse la máquina.
- **Escritorio estático no persistente**. La primera vez que un usuario inicia sesión para usar uno de estos escritorios, se le asigna un escritorio proveniente de un grupo de escritorios basados en una imagen maestra. Después del primer uso, cada vez que el usuario inicia sesión para usar uno de estos escritorios, el usuario se conecta 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**, también conocido como VDI con Personal vDisk. A diferencia de otros tipos de escritorios VDI, los usuarios pueden personalizar completamente estos escritorios. La primera vez que un usuario inicia sesión para usar uno de estos escritorios, se le asigna un escritorio proveniente de un grupo de escritorios basados en una imagen maestra. Las siguientes conexiones del usuario se establecen con el mismo escritorio que se asignó la primera vez. Los cambios en el escritorio se conservan cuando la máquina se reinicia porque están almacenados en un disco Personal vDisk.

Para entregar escritorios VDI:

1. Cree una imagen maestra que ejecute un sistema operativo compatible de escritorio Windows.
2. Cree un catálogo de máquinas para esta imagen maestra o actualice un catálogo existente con esta imagen maestra. Al definir la experiencia del escritorio para el catálogo de máquinas, decida si quiere que los usuarios se conecten a una nueva VM cada vez que inicien sesión o que se conecten a la misma máquina cada vez que inicien sesión. Si los usuarios se conectan a la misma máquina, puede especificar cómo se conservan los cambios realizados en el escritorio.
3. Cree un grupo de entrega para entregar escritorios a los usuarios.

Consulte los artículos de instalación y configuración para obtener información más detallada.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Puertos de red

November 29, 2018

En las tablas siguientes se indican los puertos de red predeterminados que utilizan los Delivery Controllers, los VDA de Windows, Director y Citrix License Server. Cuando se instalan los componentes de Citrix, el firewall host del sistema operativo también se actualiza, de manera predeterminada, para coincidir con estos puertos de red predeterminados.

Para ver una descripción general de los puertos de comunicación utilizados en otras tecnologías y componentes de Citrix, consulte CTX101810.

Puede llegar a necesitar esta información de puertos:

- Con fines de cumplimiento de normativas.
- Si hay un firewall de red entre estos componentes y otros productos o componentes de Citrix, para poder configurar el firewall adecuadamente.
- Si utiliza un firewall host de terceros, como el que se suministra con un paquete antimalware, en lugar de utilizar el firewall host del sistema operativo.
- Si modifica la configuración del firewall host en estos componentes (normalmente Windows Firewall Service).
- Si reconfigura cualquiera de las funciones de estos componentes para que utilicen un puerto o un intervalo de puertos diferente, y luego quiere inhabilitar o bloquear puertos no utilizados en su configuración. Consulte la documentación del componente para encontrar más información.
- Para obtener información acerca de puertos de otros componentes, como StoreFront y Citrix Provisioning (antes Provisioning Services), consulte el artículo actual “Requisitos del sistema” del componente en cuestión.

En las tablas solo se indican los puertos de entrada. Los puertos de salida vienen determinados normalmente por el sistema operativo y usan números no relacionados. La información sobre puertos de salida normalmente no es necesaria con los fines descritos más arriba.

Algunos de estos puertos están registrados en la autoridad de números asignados de Internet o IANA (Internet Assigned Numbers Authority). Dispone de información detallada sobre estas asignaciones en http://www.iana.org/assignments/port-numbers. Sin embargo, la información descriptiva que indica IANA no siempre refleja el uso actual.

Además, el sistema operativo en el VDA y el Delivery Controller requiere puertos de entrada para su propio uso. Para obtener información más detallada, consulte la documentación de Microsoft Windows.

VDA, Delivery Controller y Director

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Componente	Uso	Protocolo	Puerto de entrada predeterminado	Notas
VDA	ICA/HDX	TCP, UDP	1494	El protocolo de transporte de datos más ligero (EDT) requiere que 1494 esté abierto para UDP. Consulte Configuraciones de directiva de ICA.
VDA	ICA/HDX con fiabilidad de la sesión	TCP, UDP	2598	El protocolo de transporte de datos más ligero (EDT) requiere que 2598 esté abierto para UDP. Consulte Configuraciones de directiva de ICA.
VDA	ICA/HDX sobre TLS	TCP	443	Todas las aplicaciones Citrix Workspace
VDA	ICA/HDX sobre WebSocket	TCP	8008	La aplicación Citrix Workspace para HTML5 y la aplicación Citrix Workspace para Chrome 1.6 y versiones anteriores solamente

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Componente	Uso	Protocolo	Puerto de entrada predeterminado	Notas
VDA	Transporte de audio en tiempo real ICA/HDX por UDP	UDP	De 16500 a 16509	
VDA	ICA/HDX Framehawk	UDP	De 3224 a 3324	
VDA	ICA/Universal Print Server	TCP	7229	Utilizado por al agente de escucha del flujo de datos de impresión de Universal Print Server CGP (Common Gateway Protocol).
VDA	ICA/Universal Print Server	TCP	8080	Utilizado por el agente de escucha de Universal Print Server para solicitudes HTTP/SOAP entrantes.
VDA	Wake On LAN	UDP	9	Administración de energía de Acceso con Remote PC
VDA	Proxy de reactivación	TCP	135	Administración de energía de Acceso con Remote PC
VDA	Delivery Controller	TCP	80	

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Componente	Uso	Protocolo	Puerto de entrada predeterminado	Notas
Delivery Controller	VDA, StoreFront, Director, Studio	TCP	80	
Delivery Controller	StoreFront, Director, Studio por TLS	TCP	443	
Delivery Controller	Delivery Controller, VDA	TCP	89	Caché de host local (Este uso del puerto 89 podría cambiar en versiones posteriores.)
Delivery Controller	Orchestration	TCP	9095	Orchestration
Director	Delivery Controller	TCP	80, 443	

Citrix Licensing

Los siguientes puertos se utilizan para Citrix Licensing.

Componente	Uso	Protocolo	Puerto de entrada predeterminado
Servidor de licencias	Servidor de licencias	TCP	27 000
Servidor de licencias	License Server para Citrix (demonio de proveedor)	TCP	7279
Servidor de licencias	License Administration Console	TCP	8082
Servidor de licencias	Web Services for Licensing	TCP	8083

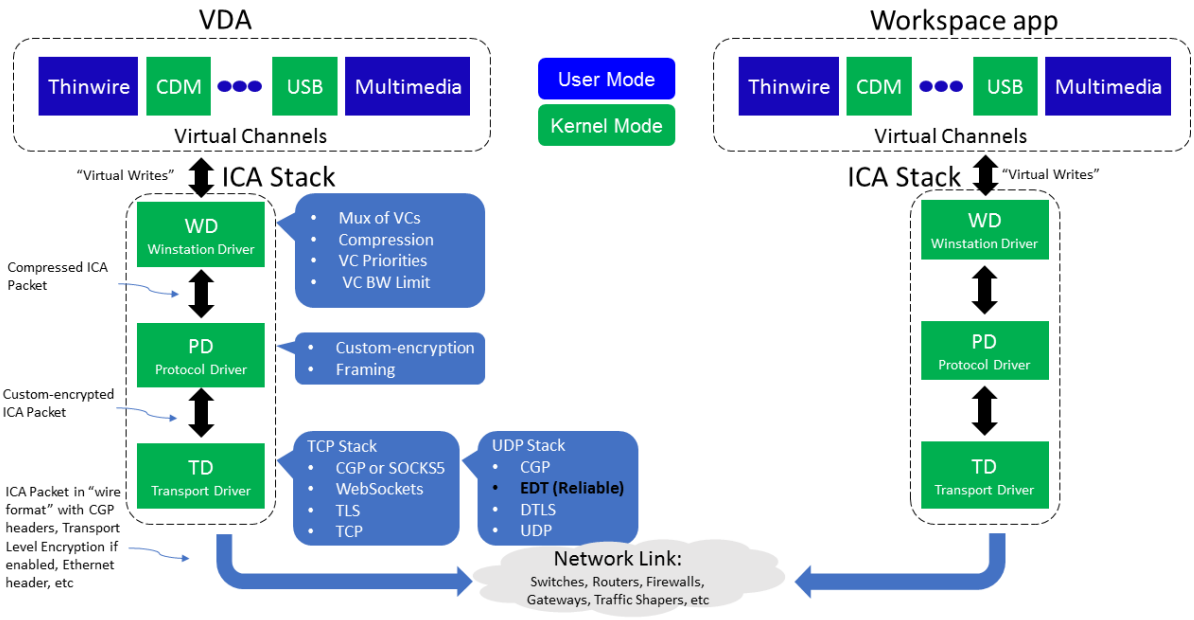
© 1999-2019 Citrix Systems, Inc. All rights reserved.

HDX

March 8, 2019

> **Advertencia**
>
> Si se modifica el Registro de forma incorrecta, se pueden generar problemas graves que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Citrix HDX ofrece 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 adaptativa
- Evitar solapamiento de datos

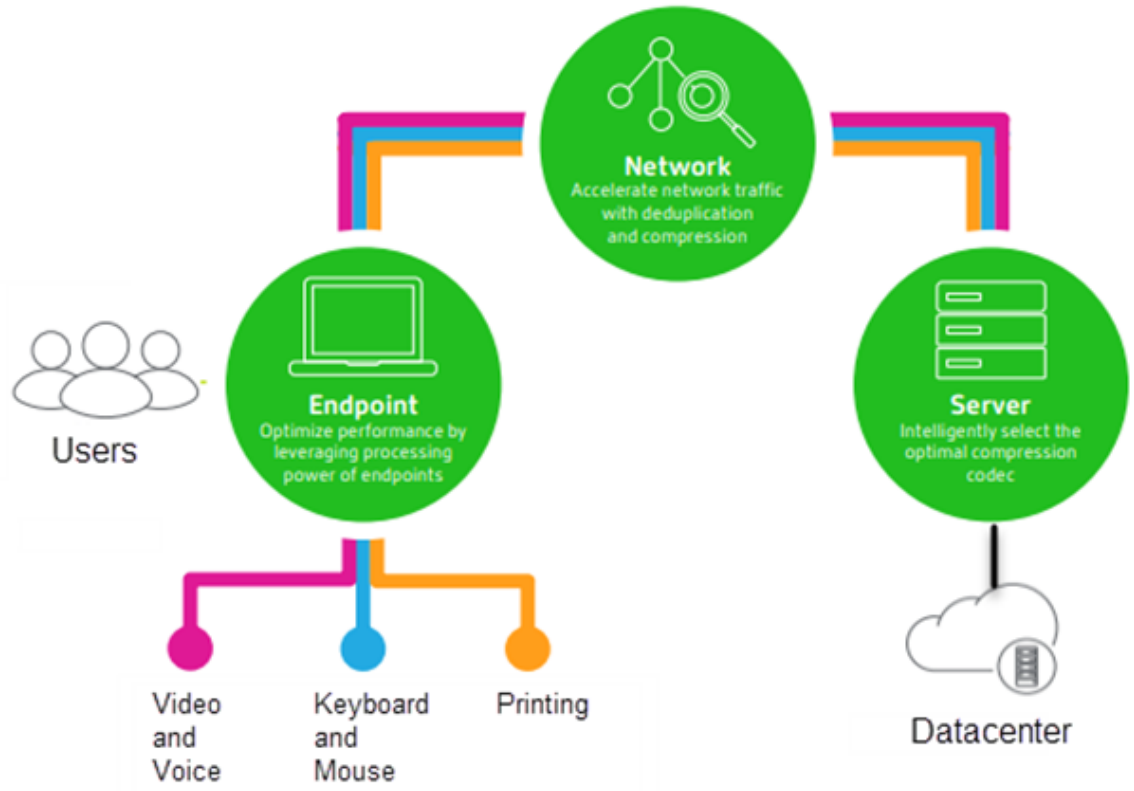
Aplicados en diferentes combinaciones, optimizan la TI y la experiencia del usuario, disminuyen el consumo de ancho de banda y aumentan la densidad de usuarios por servidor host.

- **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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

aplicación. La representación puede ocurrir en el dispositivo de punto final o en el servidor de alojamiento.

- **Compresión adaptativa** - La compresión adaptativa permite que se entreguen pantallas con muchos contenidos multimedia en conexiones de red débiles. HDX primero evalúa varias 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

En el dispositivo

HDX usa la capacidad de computación de los dispositivos de usuario para mejorar y optimizar la experiencia del usuario. La tecnología HDX garantiza que los usuarios tengan una experiencia de contenido multimedia integrada y fruida en sus aplicaciones y escritorios virtuales. El control del área de trabajo permite a los usuarios poner en pausa sus aplicaciones y escritorios virtuales y reanudar su trabajo desde otro dispositivo, retomando la sesión en el mismo punto donde la dejaron.

En la red

HDX incorpora capacidades avanzadas de optimización y aceleración para conseguir el mejor rendimiento sobre cualquier tipo de red, incluidas las conexiones WAN con poco ancho de banda y alta latencia.

Las funciones de HDX se adaptan a los cambios en el entorno. Las funciones están diseñadas para buscar el equilibrio entre el rendimiento y el consumo del ancho de banda. Las funciones de HDX aplican la mejor tecnología aplicable para cada caso de uso, independientemente de si se accede al escritorio o la aplicación localmente dentro de la red de la empresa o si se accede de manera remota desde fuera del firewall de la empresa.

En el centro de datos

HDX usa la capacidad de procesamiento y la escalabilidad de los servidores para ofrecer un rendimiento avanzado de gráficos, independientemente de la capacidad del dispositivo cliente.

La supervisión del canal HDX, proporcionada por Citrix Director, muestra el estado de los canales HDX conectados en los dispositivos de usuario.

HDX Insight

HDX Insight es la integración de NetScaler Network Inspector y Performance Manager en Director. Captura datos sobre el tráfico ICA y ofrece una vista panel de datos en tiempo real e históricos. Esta 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.

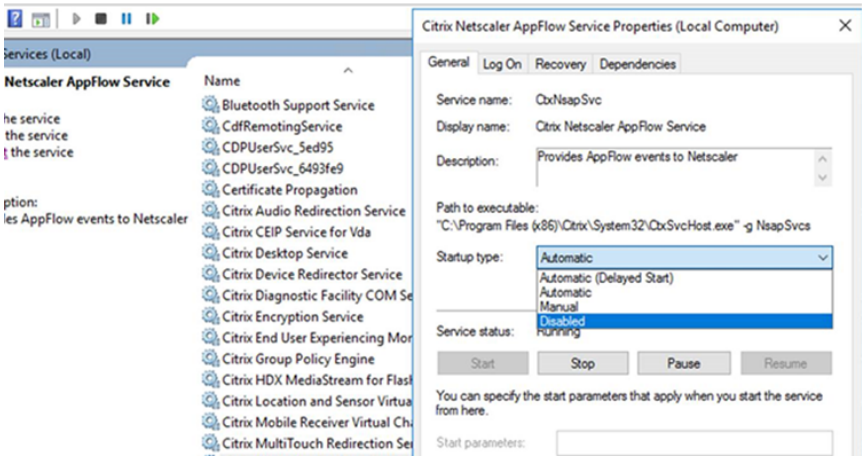
Requisitos mínimos:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Citrix Virtual Apps and Desktops 7 1808
- XenApp y XenDesktop 7.17
- NetScaler 12.0 compilación 57.x
- Aplicación Citrix Workspace para Windows 1808
- Citrix Receiver para Windows 4.10
- Aplicación Citrix Workspace para Mac 1808
- Citrix Receiver para Mac 12.8

Habilitar o inhabilitar el canal virtual HDX Insight

Para inhabilitar esta función, inhabilite las propiedades del servicio Citrix NetScaler Application Flow. Para habilitarla, establezca el servicio en Automático. En ambos casos, le recomendamos que reinicie la máquina del servidor después de cambiar estas propiedades. Este servicio está habilitado (Automático) de forma predeterminada.



Experimentar con las capacidades HDX en su escritorio virtual

- Para ver cómo la redirección de contenido de exploradores (una de las cuatro tecnologías HDX de redirección multimedia) acelera la entrega de contenido multimedia HTML 5 y WenRTC:
  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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- 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 usando un reproductor de audio digital (como iTunes) en el escritorio.

HDX ofrece una experiencia de alta calidad de gráficos y vídeo para la mayoría de los usuarios de manera predeterminada, sin necesidad de realizar configuración alguna. Las configuraciones de directivas Citrix que ofrecen la mejor experiencia integrada para la mayoría de los casos de uso están habilitadas de manera predeterminada.

- HDX selecciona automáticamente el mejor método de entrega basándose en el cliente, la plataforma, la aplicación y el ancho de banda de la red, y luego hace los ajustes necesarios automáticamente según cambien las condiciones de la conexión.
- HDX optimiza el rendimiento de gráficos 2D y 3D y vídeo.
- HDX permite que los dispositivos de usuario reciban archivos multimedia por streaming directamente desde el proveedor de origen en Internet o en la intranet, en lugar de hacerlo a través del servidor host. Si no se cumplen los requisitos para la obtención de contenido del lado del cliente, la entrega de elementos multimedia recurre a la obtención de contenido del lado del servidor y la redirección multimedia. Por lo general, no es necesario ajustar las directivas para la redirección de elementos multimedia.
- HDX entrega, a los escritorios virtuales, contenido sofisticado de vídeo generado en el servidor cuando la redirección multimedia no está disponible: consulte un vídeo de un sitio Web que contiene vídeos de alta definición, como http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/.

Conviene tener en cuenta lo siguiente:

- 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 respaldados de servidor Windows y escritorio 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 lo modifica de forma incorrecta, pueden producirse problemas graves que pueden derivar en la necesidad de instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 utilizando 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:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **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.

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Límite de memoria de presentación. Especifica el tamaño máximo de búfer para vídeos de la sesión en kilobytes (la opción predeterminada es 65536 KB). Para las conexiones que requieran mayor profundidad de color y mayor resolución, aumente el límite. Puede calcular la memoria máxima necesaria.

Mejorar el rendimiento de videoconferencia

Se han optimizado varias aplicaciones conocidas de videoconferencia para la entrega con Citrix Virtual Apps and Desktops a través de la redirección multimedia (consulte, por ejemplo, HDX RealTime 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 una sesión de videoconferencia. 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 el respaldo a la redirección USB de HDX Plug-n-Play isócrono, y funciona bien en conexiones WAN.

Los usuarios de la aplicación Citrix Workspace pueden anular este comportamiento predeterminado. Para ello, deben seleccionar el parámetro **No usar mi micrófono ni mi cámara Web** en Micro y cámara Web de Desktop Viewer. Para evitar que los usuarios cambien la compresión de vídeo de cámara Web de HDX, inhabilite la redirección de dispositivos USB desde las configuraciones de directiva de ICA > Dispositivos USB.

La compresión de vídeo de cámara Web de HDX requiere que las siguientes configuraciones de directiva estén habilitadas (están todas habilitadas de forma predeterminada).

- Redirección de sonido del cliente
- Redirección de micrófonos del cliente
- Conferencia multimedia
- Redirección de Windows Media

Si una cámara Web es compatible con la codificación por hardware, la compresión de vídeo de HDX utiliza la codificación por hardware de manera predeterminada. La codificación por hardware puede consumir más ancho de banda que la codificación por software. Para forzar la compresión de software, agregue el siguiente valor de clave DWORD a la clave del Registro HKCU\Software\Citrix\HdxRealTime: DeepCompress_ForceSWEncode=1.

Prioridades del tráfico de red

Se asignan prioridades al tráfico de red en varias conexiones para una sesión con enrutadores que use QoS (calidad de servicio). Existen cuatro secuencias TCP y dos secuencias UDP que están disponibles para transportar el tráfico ICA entre el dispositivo de usuario y el servidor:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Secuencias TCP: en tiempo real, interactivo, de fondo y en masa
- Secuencias UDP: voz y pantallas remotas de Framehawk

Cada canal virtual se asocia con 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 característica de calidad de servicio (QoS) solo recibe respaldo 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 multisecuencias (multistream) ICA. Dentro de una red interna de la empresa, no se respaldan 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 respaldo para multisecuencia en el entorno, no es necesario definir esta configuración. Defina esta configuración de directiva cuando esté usando enrutadores externos o versiones antiguas de Branch Repeater para conseguir el nivel de Calidad de servicio (QoS) que necesite.
- Configuración de usuario para multisecuencia: Esta configuración está inhabilitada de forma predeterminada.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 característica 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 característica de la barra de idioma por parte del cliente desde el VDA:

1. En el editor de Registro, vaya a HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\T
2. Cree una clave de valor DWORD, SeamlessFlags, y configúrela en 0x40000.

Asignar teclado Unicode

Los Citrix Receiver que no sean Windows usa la distribución del teclado local (Unicode). Si un usuario cambia la distribución del teclado local y la distribución del teclado de servidor (código de escaneo), puede que ambos teclados se desincronicen y el resultado de la salida de caracteres sea incorrecto. Por ejemplo, Usuario 1 cambia la distribución del teclado local de inglés a alemán. A continuación, Usuario 1 cambia el teclado del servidor a alemán. Aunque las distribuciones de ambos teclados sean en alemán, puede que no estén sincronizados, lo que provoca una salida incorrecta de caracteres.

Habilitar o inhabilitar la asignación de distribución de teclado Unicode:

De forma predeterminada, la función está inhabilitada en el lado del agente VDA. Para habilitar la función, debe activarla desde el editor del Registro regedit en el VDA.
En HKEY_LOCAL_MACHINE/SOFTWARE/Citrix, cree la clave CtxKlMap.
Establezca el valor DWORD de EnableKlMap en 1.

Para inhabilitar esta función, establezca el valor DWORD de 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

pueden vincular. Para mantener la compatibilidad, puede cambiar la función al modo compatible para admitir esas aplicaciones no vinculadas.

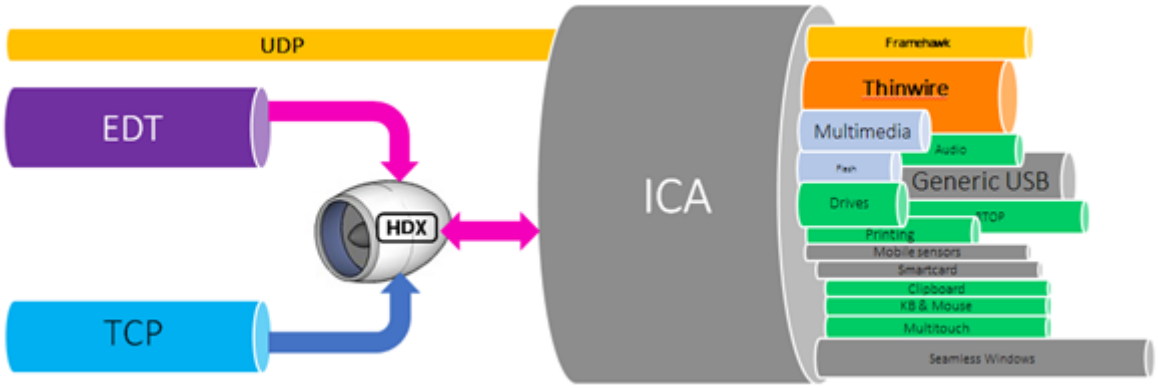
1. En la clave HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap, establezca el valor DWORD DisableWindowHook en 1.
2. Para usar la asignación de distribución de teclado Unicode normal, establezca el valor DWORD de DisableWindowHook en 0.

Transporte adaptable

March 8, 2019

Introducción

El transporte adaptable es un mecanismo de transporte de datos para Citrix Virtual Apps and Desktops. Es más rápido y escalable, mejora la interactividad de las aplicaciones y es más interactivo en conexiones de Internet y WAN difíciles de largo recorrido. El transporte adaptable mantiene la alta escalabilidad de servidores y un uso eficiente del ancho de banda. Al usar el transporte adaptable, los canales virtuales ICA responden automáticamente a las cambiantes condiciones de red. Cambian de forma inteligente el protocolo subyacente entre el protocolo de Citrix (denominado Enlightened Data Transport o EDT) y TCP para conseguir el mejor rendimiento. Mejora el rendimiento de datos en todos los canales virtuales ICA, incluida la tecnología de pantallas remotas Thinwire, la transferencia de archivos (asignación de unidades del cliente), la impresión y la redirección multimedia. Se aplica la misma configuración a las condiciones de WAN y LAN.



Si se establece en **Preferido**, los datos se transportan por EDT siempre que es posible (cuando no sea posible, se recurre a TCP). Con la aplicación Citrix Workspace para Windows (versión mínima 1808) o Citrix Receiver para Windows (versión mínima 4.10) y la fiabilidad de la sesión habilitada, se intenta utilizar EDT y TCP en paralelo durante la conexión inicial, la reconexión de fiabilidad de la sesión y la reconexión automática de clientes. Al hacerlo, se reduce el tiempo de conexión si EDT es **Preferido**,

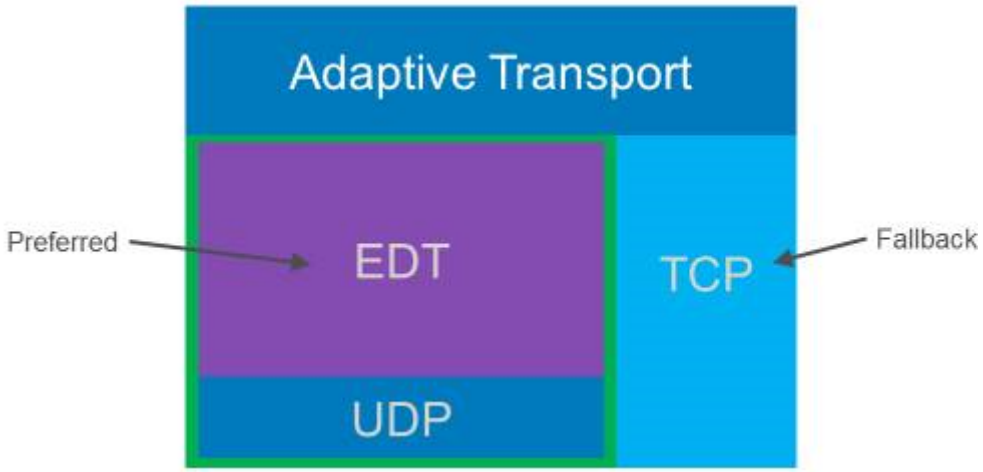
© 1999-2019 Citrix Systems, Inc. All rights reserved.

pero el transporte UDP subyacente requerido no está disponible y se debe usar TCP. De forma predeterminada, después de recurrir a TCP, el transporte adaptable vuelve a intentar utilizar EDT cada cinco minutos.

> **Importante**
>
> EDT y TCP en paralelo requieren:
>
> - La aplicación Citrix Workspace para Windows: versión mínima 1808 y la fiabilidad de la sesión.
> - Citrix Receiver para Windows: versión mínima 4.10 y la fiabilidad de la sesión.
> - La aplicación Citrix Workspace para Mac: versión mínima 1808 y la fiabilidad de la sesión.
> - Citrix Receiver para Mac: versión mínima 12.8 y la fiabilidad de la sesión.

De forma predeterminada, el transporte adaptable está habilitado (**Preferido**), y se usa EDT cuando sea posible (cuando no sea posible, se recurre a TCP).

Para realizar pruebas, se puede establecer el **Modo de diagnóstico**, en cuyo caso solo se usa EDT y se inhabilita la opción de recurrir a TCP.



Interoperabilidad con la optimización WAN de Citrix SD-WAN

La optimización WAN de Citrix SD-WAN (WANOP) ofrece la compresión por tokens entre sesiones (desduplicación de datos), incluido el almacenamiento en caché de vídeo basado en URL. WANOP ofrece una reducción significativa del ancho de banda si dos o varias personas ubicadas en la oficina miran el mismo vídeo obtenido en el cliente, o si transfieren o imprimen partes significativas del mismo archivo o documento. Además, al ejecutar los procesos de reducción de datos ICA y compresión de trabajos de impresión en el dispositivo de la sucursal, WANOP ofrece la descarga de la CPU del servidor VDA y permite una mayor escalabilidad del servidor Citrix Virtual Apps and Desktops.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> **Importante**
>
> Cuando se usa TCP como protocolo de transporte de datos, Citrix WANOP admite las optimizaciones descritas en el párrafo anterior. Cuando use Citrix WANOP en las conexiones de red, elija TCP e inhabilite EDT. Gracias al control de flujo y al control de la congestión que ofrece TCP, WANOP garantiza una interactividad equivalente a EDT con una alta latencia y una pérdida moderada de paquetes.

Requisitos y consideraciones

- Citrix Virtual Apps and Desktops: versión mínima 7 1808.
- XenApp y XenDesktop: versión mínima 7.13.
- VDA para SO de escritorio: versión mínima 7.13.
- VDA para SO de servidor: versión mínima 7.13.
- StoreFront: versión mínima 3.9.
- Aplicación Citrix Workspace para Windows 1808 (versión mínima)
- Citrix Receiver para Windows: versión mínima 4.7 (EDT y TCP en paralelo requieren 4.10 como versión mínima y la Fiabilidad de la sesión).
- Aplicación Citrix Workspace para Mac: versión mínima 1808
- Citrix Receiver para Mac: versión mínima 12.5 (EDT y TCP en paralelo requieren 12.8 como versión mínima y la Fiabilidad de la sesión).
- Aplicación Citrix Workspace para iOS: versión mínima 1808
- Citrix Receiver para iOS: versión mínima 7.2.
- Aplicación Citrix Workspace para Linux: versión mínima 1808
- Citrix Receiver para Linux: versión mínima 13.6 para solamente conexiones directas de VDA, y versión mínima 13.7 para admitir DTLS cuando se usa NetScaler Gateway (o DTLS para conexiones directas de VDA).
- Aplicación Citrix Workspace para Android: versión mínima 1808
- Citrix Receiver para Android: versión mínima 3.12.3 para solamente conexiones directas de VDA.
- Solo agentes VDA IPv4. No se admiten configuraciones de IPv6 ni mixtas (de IPv4 e IPv6).
- Citrix Gateway: versión mínima 1808
- NetScaler: versiones mínimas 11.1 compilación 51.21, 12.0 compilación 35.6. Recomendamos las versiones mínimas 11.1 compilación 55.10 o 12.0 compilación 53.6, ya que estas versiones incluyen importantes soluciones de fragmentación para DTLS. Para obtener más información sobre la configuración de NetScaler, consulte este artículo.

Configuración

1. Instale Citrix Virtual Apps and Desktops.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

2. Instale StoreFront. Si utiliza Citrix Gateway, verifique que la Fiabilidad de la sesión está habilitada. Para ello, vaya a **Studio > StoreFront > Administrar NetScaler Gateway > Seleccione su NetScaler > Secure Ticket Authority > Habilitar fiabilidad de la sesión**.
3. Instale el VDA (para SO de escritorio o SO de servidor).
4. Instale la aplicación Citrix Workspace para Windows, la aplicación Citrix Workspace para Mac, la aplicación Citrix Workspace para iOS, la aplicación Citrix Workspace para Android o la aplicación Citrix Workspace para Linux.
5. Si utiliza Citrix Gateway, habilite la Fiabilidad de sesión en la directiva de Studio. Además, habilite DTLS en el servidor virtual front-end de la VPN.
6. En Studio, habilite la configuración de directiva "Transporte adaptable HDX" (inhabilitada de forma predeterminada).
    - Para habilitar esta configuración de directiva, establezca la opción en Preferido y, a continuación, haga clic en **Aceptar**.
        - **Preferido**. Se utiliza el transporte adaptable por EDT cuando sea posible; cuando no lo sea, se recurre a TCP.
        - **Modo de diagnóstico**. Se obliga el uso de EDT y la opción de recurrir a TCP está inhabilitada. Esta configuración se recomienda solamente para la solución de problemas.
        - **No** (desactivado). Se obliga el uso de TCP y EDT está inhabilitado.
7. Haga clic en Siguiente y siga los pasos indicados en el asistente.
8. La directiva surte efecto cuando el usuario se vuelve a conectar a la sesión ICA. Aunque no es imprescindible, puede ejecutar **gpupdate /force** para extraer la configuración de directiva al servidor, aunque el usuario seguirá teniendo que reconectarse a la sesión ICA.
9. Inicie sesión desde una aplicación Citrix Workspace respaldada para establecer conexión mediante el transporte adaptable.
10. Para un acceso externo seguro, configure el cifrado de DTLS en Citrix Gateway. Para obtener más información, consulte este artículo.

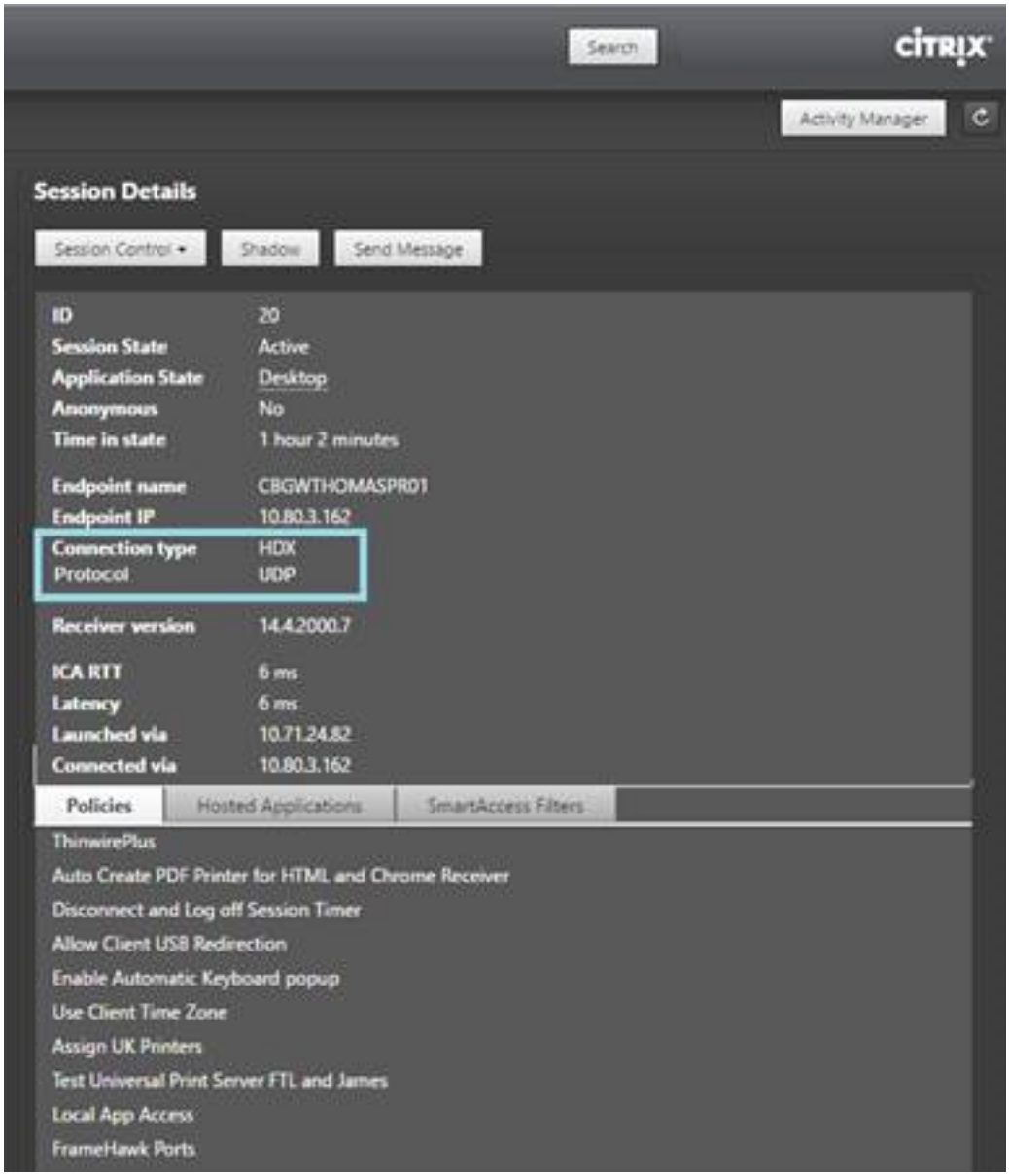
Para confirmar que la configuración de directiva surte efecto:

- Compruebe que los servicios User Datagram Protocol (UDP) de ICA están habilitados en un agente VDA mediante **netstat -a**.
- Compruebe que los canales virtuales se están ejecutando a través de EDT: use **Director** o la utilidad de línea de comandos **CtxSession.exe** disponible en el VDA.

Ejemplo con Director:

En Director, **Detalles de la sesión > Tipo de conexión** muestra las configuraciones de directiva. Busque el tipo de conexión **HDX**. Si el protocolo es **UDP**, EDT está activo para la sesión. Si el protocolo es **TCP**, la sesión está en modo de reserva o predeterminado. Si el tipo de conexión es **RDP**, no se usa ICA y el protocolo es **n/d**. Para obtener más información, consulte Supervisar sesiones.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Ejemplo con CtxSession.exe:

Este ejemplo indica que EDT sobre UDP está activo para la sesión. Escriba CtxSession.exe en la línea de comandos.

C:\Archivos de programa (x86)\Citrix\System32>CtxSession

Protocolos de transporte de sesión 2: UDP > CGP > ICA

Para ver las estadísticas detalladas, use el modificador -v:

```
>CtxSession -v
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Solucionar problemas de conexiones EDT

Requisitos y consideraciones

- VDA para SO de servidor 7.13
- VDA para SO de escritorio 7.13
- Receiver para Windows 4.7 (la versión 4.6 fue experimental)
- Receiver para Linux:
  - 13.6 (conexiones directas)
  - 13.7 (DTLS admitido)
- Receiver para Mac 12.5
- Reciver para iOS 7.2
- Receiver para Android:
  - 3.12.3 (conexiones directas)
  - 3.13 (DTLS admitido)
- StoreFront 3.9
- NSG versión 11.1–51.21 / 12.0.53.6 o posterior

Conexiones paralelas

Receiver para Windows 4.10, Mac 12.8 e iOS 7.5 están programados de forma que pueden intentar una conexión EDT y TCP en paralelo. A EDT se le da una ventaja de 500 milisegundos para favorecer a UDP. Cualquier VDA que admita EDT también admite la conexión paralela.

Para solucionar problemas de conexiones EDT, consulte el siguiente procedimiento:

1. Verifique los requisitos mínimos de versión de producto/componente. Consulte Requisitos y consideraciones.
2. Compruebe que la directiva de Studio **transporte adaptable de HDX** esté en **No configurado** o **Preferido**.

   > Nota:
   >
   > En XenApp y XenDesktop 7.16, se prefiere el transporte adaptable HDX por defecto y no hay un requisito explícito para configurar la directiva de Studio.

3. Comprobar si se utilizan las plantillas administrativas **opcionales** de GPO de Receiver. Si es así, asegúrese de que **Protocolo de transporte** para el valor de Citrix Receiver se establece en **No configurado** o **Preferido** . Las configuraciones laterales de Receiver para Windows son opcionales.
4. No es seguro que los sockets UDP estén escuchando en el VDA. Abra un símbolo del sistema en el VDA y escriba `netstat -a -p udp` . Para más detalles, consulte Cómo confirmar el protocolo hDX Enlightened Data Transport.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

5. Omita NetScaler Gateway: la mejor manera de probar EDT es una ainiciarplicación desde la red interna directamente a StoreFront, sin pasar por NetScaler Gateway. Ejecute `ctxsession` en el símbolo del sistema de VDA y verifique que su sesión esté usando el protocolo UDP. Si eso funciona, su VDA también está listo para conexiones EDT desde el exterior.
6. Inicie una sesión a través de NetScaler Gateway, pero primero inspeccione el archivo ICA. Compruebe que haya una entrada que sea `HDXoverUDP = Preferred`. Si se establece en `Off`, entonces el transporte adaptable HDX no está configurado como **Preferido** en la directiva de Studio, o la actualización de la directiva de grupo aún no se ha aplicado en el VDA. También debe haber una entrada `CGPSecurityTicket=On`, donde CGP es un requisito para que EDT funcione con NetScaler Gateway.
7. En NetScaler Gateway, ejecute `ctxsession` en el símbolo del sistema de VDA y verifique que su sesión esté usando el protocolo UDP. Si está configurado en TCP, puede ser que algo haya ido mal entre Citrix Receiver y el servidor virtual de NetScaler Gateway, y la conexión se haya reducido nuevamente a TCP.
8. Cualquier NetScaler Gateway antes de la versión 12.0.56.20 requiere que DTLS se habilite manualmente en el front-end del servidor virtual VPN.
9. Si está utilizando una VPN como Cisco AnyConnect o cualquier otra solución que altere la MTU en la red, las conexiones EDT pueden fallar. Debe calcular la sobrecarga introducida por el proveedor de VPN y luego modificar la plantilla de archivo ICA en StoreFront para incluir dos entradas más. Además, agregue un cambio en el lado de Citrix Receiver. Para más detalles, ver CTX231821.

Más herramientas para solución de problemas

- **Wireshark**: Para solucionar problemas cuando no puede identificar el problema, use un seguimiento de Wireshark en NetScaler Gateway. Los disectores Wireshark pueden malinterpretar EDT como `QUIC`. Puede utilizar la función `Decode As` en Wireshark para decodificar QUIC como DTLS.
- **NMAP**: Utilizar el `nmap -sU -p 443 <IP Address of your NSG>` para probar si los paquetes UDP están llegando al servidor virtual.
  Ver un seguimiento que funciona y otro que no funciona:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

```
nmap -sU -p 443 23.29.[redacted]

Starting Nmap 7.60 ( https://nmap.org ) at 2017-12-03 22:50 Eastern Standard Time
Nmap scan report for 23.29.[redacted]
Host is up (0.018s latency).

PORT    STATE SERVICE
443/udp open  https

Nmap done: 1 IP address (1 host up) scanned in 9.62 seconds
```

```
nmap -sU -p 443 47.187.[redacted]

Starting Nmap 7.60 ( https://nmap.org ) at 2017-12-03 22:49 Eastern Standard Time
Nmap scan report for 47.187.[redacted]
Host is up (0.047s latency).

PORT    STATE  SERVICE
443/udp closed https

Nmap done: 1 IP address (1 host up) scanned in 9.86 seconds
```

- **Director**: Además, puede consultar **Citrix Director> Detalles de la sesión> Protocolo> UDP** .
- **Seguimientos CDF**: Es posible que deba verificar la lógica EDT en los componentes XenApp y XenDesktop, y generar seguimientos CDF al reproducir el problema.

Server CDF Traces

Module	Applies to
ICA Service	XenDesktop only
MF_DLL_WSXICA	RPM on XenApp only
MF_Driver_Wdica	Both
Portica_Driver_Picadd	Only needed for MSI
Portica_Driver_Td	This also includes traces from EDT, CGP, TLS/DTLS, HTML5, SOCKS (if HTML5 or TLS port, and CGP is not used)
CitrixServicesManager_Service	XenApp Only
StackControl_Agent_ToStack	XenApp Only
Broker Agent	Both

Receiver CDF Traces

Module	
IcaClient_Engine_Wfica_CtlGuid	
IcaClient_UDT	

Instalar y configurar

January 25, 2019

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> **Nota:**
>
> Puede obtener información sobre los cambios en los nombres de producto aquí.

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, características, diferencias de versiones anteriores, requisitos del sistema y bases de datos.
- Consideraciones al decidir dónde instalar los componentes principales.
- Permisos y requisitos de Active Directory.
- Información sobre los instaladores, las herramientas y las interfaces disponibles.

Instalar componentes principales

Instale Delivery Controller, Citrix Studio, Citrix Director, el servidor de licencias y Citrix StoreFront. Para obtener más información, consulte Instalación de componentes principales o Instalación mediante línea de comandos.

Crear un sitio

Después de instalar los componentes principales e iniciar Studio, se le dirigirá automáticamente a crear un sitio.

Instalar uno o varios agentes VDA (Virtual Delivery Agent)

Instale un VDA en una máquina que ejecute un sistema operativo Windows, ya sea en una imagen maestra o directamente en cada máquina. Consulte Instalar agentes VDA o Instalar mediante la línea de comandos. Se ofrecen scripts de ejemplo si quiere instalar agentes VDA a través de Active Directory.

Para máquinas con un sistema operativo Linux, siga las instrucciones que aparecen en Linux Virtual Delivery Agent.

Para implementaciones de acceso con Remote PC, instale un VDA para SO de escritorio en cada PC de la oficina. Si necesita solamente los servicios principales del agente VDA, utilice el programa de instalación independiente VDAWorkstationCoreSetup.exe y sus métodos existentes de distribución

© 1999-2019 Citrix Systems, Inc. All rights reserved.

electrónica de software (ESD). (Antes de la instalación contiene información completa sobre los programas de instalación de VDA disponibles.)

Instalar componentes opcionales

Si va a usar el servidor Citrix Universal Print Server, instale su componente de servidor correspondiente en los servidores de impresión. Consulte Instalar componentes principales o Instalar mediante línea de comandos.

Para permitir que StoreFront use opciones de autenticación tales como aserciones SAML, instale el Servicio de autenticación federada de Citrix.

Para que los usuarios finales tengan un mayor control sobre sus cuentas de usuario, instale el Autoservicio de restablecimiento de contraseñas.

Si lo prefiere, puede integrar otros componentes de Citrix en la implementación de Citrix Virtual Apps and Desktops.

- Citrix Provisioning es un componente optativo que aprovisiona máquinas transmitiendo por streaming una imagen maestra a los dispositivos de destino.
- Citrix Gateway es una solución de acceso seguro a aplicaciones, que ofrece a los administradores un control más preciso de las acciones y las directivas al nivel de aplicación, para proteger el acceso a las aplicaciones y los datos.
- Citrix SD-WAN es un conjunto de dispositivos que optimizan el rendimiento en WAN.

Crear un catálogo de máquinas

Después de crear un sitio en Studio, se le dirigirá a crear un catálogo de máquinas.

Un catálogo puede contener máquinas físicas o virtuales (VM). Las máquinas virtuales se pueden crear a partir de una imagen maestra. Si usa un hipervisor o un servicio de nube para proporcionar máquinas virtuales, primero debe crear una imagen maestra en ese host. A continuación, al crear el catálogo, debe especificar esa imagen, que se usará para crear máquinas virtuales.

Crear un grupo de entrega

Después de crear el primer catálogo de máquinas en Studio, se le dirigirá a crear un grupo de entrega.

Un grupo de entrega especifica los usuarios que pueden acceder a las máquinas de un catálogo de máquinas concreto y las aplicaciones disponibles para esos usuarios.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Crear un grupo de aplicaciones (optativo)

Después de crear un grupo de entrega, si quiere puede crear un grupo de aplicaciones. Puede crear grupos de aplicaciones para las aplicaciones compartidas entre varios grupos de entrega o que son utilizadas por un subconjunto de usuarios dentro de un grupo de entrega.

Antes de instalar

December 4, 2018

> **Nota:**
>
> Puede obtener información sobre los cambios en los nombres de producto aquí.

La implementación de Citrix Virtual Apps and Desktops comienza con la instalación de los siguientes componentes. Este proceso prepara la entrega de aplicaciones y escritorios a los usuarios dentro del firewall.

- Uno o varios Delivery Controllers
- Citrix Studio
- Citrix Director
- Citrix StoreFront
- Citrix License Server
- Uno o varios agentes VDA (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, por ejemplo, Citrix Gateway. Para ver una introducción, consulte Integrar Citrix Virtual Apps and Desktops con Citrix Gateway.

Puede usar el instalador de producto completo, incluido en el archivo ISO, para implementar muchos de los componentes y las tecnologías. También puede usar el instalador independiente de VDA para instalar los VDA. Todos los instaladores ofrecen interfaces gráficas y de línea de comandos. Consulte Instaladores.

Las ISO de producto contienen scripts de ejemplo para instalar, actualizar o quitar los agentes Virtual Delivery Agent de máquinas en Active Directory. También puede usar los scripts para administrar las imágenes maestras que utilicen Machine Creation Services (MCS) y Citrix Provisioning (antes Provisioning Services). Para obtener más información, consulte Instalar agentes VDA mediante scripts.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Información a revisar antes de la instalación

- Información técnica general: Si no conoce el producto ni sus componentes.
- Cambios en 7.x: Si tiene una implementación de XenApp 6.x o XenDesktop 5.6, y va a migrar o actualizar a la versión actual.
- Seguridad: Cuando planifique el entorno de la implementación.
- Problemas conocidos: Los problemas que pueden aparecer en esta versión.
- Bases de datos: Si quiere obtener información sobre las bases de datos del sistema y cómo configurarlas. Durante la instalación de Controllers, puede instalar SQL Server Express para usarlo como la base de datos del sitio. Puede configurar la mayor parte de la información de la base de datos al crear un sitio, después de instalar los componentes principales.
- Acceso con Remote PC: Si implementa un entorno que permite a los usuarios acceder remotamente a sus equipos físicos en la oficina.
- Conexiones y recursos: Si usa un hipervisor o servicio de nube para alojar o aprovisionar máquinas virtuales para aplicaciones y escritorios. Puede configurar la primera conexión cuando cree un sitio, después de instalar los componentes principales. También puede configurar el entorno de virtualización en cualquier momento anterior.
- Microsoft System Center Configuration Manager: Si usa Configuration Manager para administrar el acceso a las aplicaciones y los escritorios, o bien si usa la funcionalidad Wake on LAN con el acceso con Remote PC.

Dónde instalar los componentes

Revise Requisitos del sistema para conocer las versiones, las plataformas y los sistemas operativos respaldados. Los requisitos previos de los componentes se instalan automáticamente; las excepciones se indican. Consulte la documentación de Citrix StoreFront y del servidor de licencias de Citrix 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.

Puede instalar un Delivery Controller y un agente VDA para SO de servidor 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 al agente de entrega virtual (VDA) para el sistema operativo del servidor.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Compruebe que cada sistema operativo tiene las actualizaciones más recientes. Por ejemplo, si no se instala la actualización KB2919355 de Windows, se detiene la instalación de un Controller o un VDA en Windows Server 2012 R2.

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

Dispone de directrices de optimización para máquinas con Windows 10 en CTX216252.

Donde NO instalar los componentes:

- No instale componentes en controladores de dominio de Active Directory.
- No se admite la instalación de un Controller en un nodo de una instalación en clúster de SQL Server ni en una instalación reflejada de SQL Server ni en un servidor con Hyper-V.
- No instale Studio en servidores que ejecutan XenApp 6.5 Feature Pack 2 para Windows Server 2008 R2 o versiones anteriores de XenApp.

Si intenta instalar (o actualizar) un Windows VDA en un sistema operativo que no admite esta versión del producto, aparece un mensaje que le guiará un artículo Citrix que describe las opciones de que dispone.

Permisos y requisitos de Active Directory

Debe ser un usuario de dominio y un administrador local en las máquinas donde instale los componentes.

Para usar el instalador independiente de VDA, debe tener privilegios administrativos elevados, o bien, debe usar **Ejecutar como administrador**.

Configure su dominio de Active Directory antes de comenzar la instalación.

- Requisitos del sistema ofrece una lista de los niveles funcionales respaldados de Active Directory. En Active Directory, se ofrece información adicional.
- Debe tener al menos un controlador de dominio que ejecute los Servicios de dominio de Active Directory.
- No instale ningún componente de Citrix Virtual Apps and Desktops en un controlador de dominio.
- No use barras diagonales (/) cuando indique nombres de unidades organizativas en Studio.

La cuenta de usuario de Windows que se utilizó para instalar el servidor de licencias de Citrix se configura automáticamente como una cuenta de administrador total de Administración delegada en el servidor de licencias.

Para obtener más información:

- Recomendaciones referentes a la seguridad

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- 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

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 análisis de Citrix 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 (como Smart Tools), 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 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 inhabilita la recopilación y la carga.

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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 StoreFront. Consulte la documentación de StoreFront.

El servicio Print Spooler Service está habilitado de forma predeterminada en servidores Windows admitidos. Si inhabilita este servicio, no podrá instalar un VDA para SO de servidor Windows, así que compruebe que este servicio está habilitado antes de instalar un VDA.

La mayoría de las ediciones Windows admitidas vienen con Microsoft Media Foundation ya instalado. Si la máquina donde quiere instalar el VDA no tiene instalado Media Foundation (como las ediciones N), algunas funciones multimedia no se instalarán y no funcionarán. Puede aceptar la limitación o finalizar la instalación del VDA y reiniciar la máquina más tarde, después de instalar Media Foundation. En la interfaz gráfica, se presenta esta opción en un mensaje. En la línea de comandos, puede usar la opción /no_mediafoundation_ack para aceptar la limitación.

Si Media Foundation no está presente en la máquina del VDA, estas características multimedia no funcionarán:

- Redirección de Flash
- Redirección de Windows Media
- Redirección de vídeo HTML5
- Redirección de cámara Web HDX RealTime

Cuando se instala el VDA, se crea automáticamente un nuevo grupo de usuarios locales llamado Usuarios con acceso directo. En un VDA para SO de escritorio, este grupo solo se aplica a conexiones RDP. En un VDA para SO de servidor, este grupo se aplica a conexiones RDP e ICA.

El VDA debe tener direcciones válidas de Controller para comunicarse. De lo contrario, las sesiones no se pueden establecer. Puede especificar direcciones de Controller en el momento de instalar el VDA, o más adelante; pero recuerde que tiene que hacerlo.

Herramientas de compatibilidad para VDA

Todos los instaladores de VDA incluyen un MSI de compatibilidad. Este MSI contiene herramientas de Citrix para verificar el rendimiento del VDA (es decir, su estado general y la calidad de las conexiones). Puede habilitar o inhabilitar la instalación de ese MSI desde la página **Componentes adicionales** de la interfaz gráfica del instalador del 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:\Archivos de programa (x86)\Citrix\Supportability Tools\. Puede cambiar esta ubicación desde la página **Componentes** de la interfaz gráfica del instalador del 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Herramientas disponibles actualmente en el MSI de compatibilidad:

- Citrix Health Assistant: Para obtener información, consulte CTX207624.
- Utilidad de limpieza del VDA: Para obtener información, consulte CTX209255.

Si no instala las herramientas de compatibilidad cuando instala el VDA, el artículo de CTX contiene un enlace al paquete de descarga actual.

Reinicios durante y después de la instalación de VDA

Se necesita reiniciar el sistema una vez al final de la instalación del VDA. Dicho reinicio se produce automáticamente de forma predeterminada.

Para minimizar la cantidad de reinicios necesarios durante la instalación de VDA:

- Compruebe que haya una versión compatible de .NET Framework instalada antes de iniciar la instalación del agente VDA.
- Para máquinas de SO de servidor Windows, instale y habilite los servicios de rol de Servicios de escritorio remoto (RDS) antes de instalar el agente VDA.

Si no instala esos requisitos previos antes de instalar el VDA:

- La máquina se reiniciará automáticamente después de instalar cada requisito previo si usa la interfaz gráfica o la interfaz de línea de comandos sin la opción /noreboot.
- Si utiliza la interfaz de línea de comandos con la opción /noreboot, deberá iniciar el proceso de reinicio.

Después de cada reinicio, la instalación del VDA continúa. (Si está instalando desde la línea de comandos, puede evitar los reinicios con la opción /noresume.)

Nota:

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

Instaladores

Instalador de producto completo

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

- Instalar, actualizar o quitar los componentes principales: Delivery Controller, Studio, Director, StoreFront, License Server.
- Instalar o actualizar agentes VDA para Windows en sistemas operativos de servidor o de escritorio.
- Instalar el componente UpsServer de Universal Print Server en los servidores de impresión.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Instalar el Servicio de autenticación federada.
- Instalar el Autoservicio de restablecimiento de contraseñas.

Para entregar un escritorio desde un sistema operativo de servidor a un solo usuario (por ejemplo, para tareas de desarrollo Web), use la interfaz de línea de comandos del instalador de producto completo. Para obtener más información, consulte VDI de servidor.

Instaladores independientes de VDA

Los instaladores independientes de VDA están disponibles en las páginas de descarga de Citrix. Los instaladores independientes de VDA son mucho más pequeños que la imagen ISO del producto completo. Se acomodan más fácilmente a las implementaciones que:

- Utilizan paquetes ESD (Electronic Software Distribution) que se almacenan provisionalmente o se copian localmente
- Tienen máquinas físicas
- Tienen oficinas remotas

De forma predeterminada, los archivos autoextraíbles que contiene el paquete independiente de VDA se extraen en la carpeta Temp. Se necesita más espacio de disco en la máquina al extraer los archivos a la carpeta Temp que cuando se usa el instalador de producto completo. Sin embargo, los archivos que se extraen en la carpeta Temp se eliminan automáticamente después de que se complete la instalación. De forma alternativa, puede usar el comando /extract con una ruta absoluta.

Dispone de tres instaladores independientes de VDA para la descarga.

VDAServerSetup.exe:

Instala un VDA para SO de servidor. Admite todas las opciones del VDA para SO de servidor que están disponibles con el instalador de producto completo.

VDAWorkstationSetup.exe:

Instala un VDA para SO de escritorio. Admite todas las opciones del VDA para SO de escritorio que están disponibles con el instalador de producto completo.

VDAWorkstationCoreSetup.exe:

Instala un VDA para SO de escritorio, optimizado para implementaciones de acceso con Remote PC o instalaciones básicas de VDI. El acceso con Remote PC usa máquinas físicas. Las instalaciones básicas de VDI son máquinas virtuales que no se utilizan como imagen maestra. Solo instala los servicios básicos necesarios para las conexiones de VDA de estas implementaciones. Por lo tanto, solo respalda un subconjunto de las opciones que son válidas con el instalador de producto completo (o VDAWorkstationSetup).

Este instalador no instala ni contiene los componentes utilizados para:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- App-V.
- Profile Management. Excluir Citrix Profile Manager de la instalación afecta a Director. Para obtener más información, consulte Instalar agentes VDA.
- Machine Identity Service.
- Personal vDisk o AppDisk.
- Citrix Supportability Tools.
- Citrix Files para Windows.

El instalador VDAWorkstationCoreSetup.exe no instala ni contiene la aplicación Citrix Workspace para Windows.

Utilizar VDAWorkstationCoreSetup.exe equivale a usar VDAWorkstationSetup o el instalador de producto completo para instalar un VDA de SO de escritorio y:

- En la interfaz gráfica: Marcar la opción Acceso con Remote PC en la página **Entorno**.
- En la interfaz de línea de comandos: Especificar la opción /remotepc.
- En la interfaz de línea de comandos: Especificar /components vda y /exclude “Citrix Personalization for App-V - VDA” “Personal vDisk” “Machine Identity Service” “Citrix User Profile Manager” “Citrix User Profile Manager WMI Plugin” “Citrix Supportability Tools” “Citrix Files for Windows”.

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

Códigos de retorno en la instalación de Citrix

El registro de instalación contiene el resultado de las instalaciones de los componentes en el formato de un código de retorno Citrix, no como un valor de Microsoft.

- 0 = Success (Operación correcta)
- 1 = Failed (Operación fallida)
- 2 = PartialSuccess (Operación parcialmente correcta)
- 3 = PartialSuccessAndRebootNeeded (Operación parcialmente correcta, reinicio necesario)
- 4 = FailureAndRebootNeeded (Fallo, reinicio necesario)
- 5 = UserCanceled (Operación cancelada por el usuario)
- 6 = MissingCommandLineArgument (Argumento de línea de comando que falta)
- 7 = NewerVersionFound (Versión más reciente encontrada)

Por ejemplo, cuando se usan herramientas como Microsoft System Center Configuration Manager, una instalación por scripts de VDA puede aparecer como fallida cuando el registro de instalación contiene el código de retorno 3. Puede ocurrir cuando el instalador VDA espera un reinicio que usted debe iniciar (por ejemplo, después de una instalación de requisitos previos del rol de Servicios de Escritorio remoto en un servidor). Una instalación de VDA se considera correcta únicamente después de

© 1999-2019 Citrix Systems, Inc. All rights reserved.

que todos los requisitos previos y los componentes seleccionados se hayan instalado y la máquina se reinicie después de la instalación.

Como alternativa, puede empaquetar la instalación en scripts CMD (que devuelven códigos de Microsoft) o cambiar los códigos de operación correcta en el paquete de Configuration Manager.

Entornos de virtualización de Microsoft Azure Resource Manager

March 8, 2019

Siga estas instrucciones si usa Azure Resource Manager para aprovisionar máquinas virtuales en su entorno.

Debe conocer lo siguiente:

- Azure Active Directory: https://azure.microsoft.com/en-us/documentation/articles/active-directory-howto-tenant/
- Marco de consentimiento: https://azure.microsoft.com/en-us/documentation/articles/active-directory-integrating-applications/
- Entidad principal de servicio: https://azure.microsoft.com/en-us/documentation/articles/active-directory-application-objects/

Azure Disk Encryption no se admite cuando se utiliza Machine Creation Services.

Aprovisionamiento a demanda de Azure

Cuando se usa MCS para crear catálogos de máquinas en Azure Resource Manager, la función de aprovisionamiento a demanda de Azure:

- Reduce los costes de almacenamiento
- Proporciona una creación de catálogos más rápida
- Proporciona unas operaciones de energía más rápidas para las máquinas virtuales (VM)

Para el administrador, el aprovisionamiento a demanda no conlleva diferencias entre los procedimientos de Studio para crear conexiones de host o catálogos de máquinas de Machine Creation Services. Las diferencias consisten en cómo y cuándo se crean y se administran los recursos en Azure, así como en la visibilidad de las VM en el portal de Azure.

Antes de que se utilizara el aprovisionamiento a demanda de Azure con Citrix Virtual Apps and Desktops, cuando MCS creaba un catálogo, las máquinas virtuales se creaban en Azure durante el proceso de aprovisionamiento.

Con el aprovisionamiento a demanda de Azure, las máquinas virtuales se crean solo cuando Citrix Virtual Apps and Desktops inicia una acción de encendido, después de completarse el aprovision-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

amiento. Una máquina virtual solo aparece en el portal de Azure cuando se está ejecutando. (En Studio, las máquinas virtuales aparecen tanto si se están ejecutando como si no.)

Cuando se crea un catálogo con Machine Creation Services, el portal de Azure muestra los grupos de recursos, el grupo de seguridad de red, las cuentas de almacenamiento, las interfaces de red, las imágenes base y los discos de identidad. El portal de Azure no muestra ninguna máquina virtual hasta que Citrix Virtual Apps and Desktops inicie una acción de encendido en ella. (En ese momento, el estado de la máquina virtual en Studio cambia a encendido.)

- Para una máquina agrupada, el disco del sistema operativo y la caché de reescritura solo existen cuando existe la máquina virtual. Eso puede resultar en un ahorro considerable del espacio de almacenamiento si apaga frecuentemente las máquinas (por ejemplo, fuera del horario de trabajo).
- Para una máquina dedicada, el disco del sistema operativo se crea la primera vez que se encienda la máquina virtual. Almacena datos hasta que se elimina la máquina.

Cuando Citrix Virtual Apps and Desktops inicia una acción de apagado de una VM, esa VM se elimina de Azure y ya no aparece en el portal de Azure. (En Studio, el estado de la máquina virtual cambia a apagado.)

Catálogos creados antes del aprovisionamiento a demanda

Si dispone de catálogos de máquinas creados antes de que Citrix Virtual Apps and Desktops respaldara el aprovisionamiento a demanda de Azure (mediados de 2017), las máquinas de esos catálogos aparecerán en el portal de Azure independientemente de si se están ejecutando o no. No se puede convertir esas máquinas virtuales en máquinas a demanda.

Para aprovechar las mejoras de rendimiento y los ahorros en costes de almacenamiento que ofrece el aprovisionamiento a demanda, cree catálogos nuevos con MCS.

Azure Managed Disks

Azure Managed Disks es un sistema de almacenamiento de disco elástico que puede usar con los catálogos de máquinas creados por MCS, como alternativa al uso de cuentas de almacenamiento convencionales.

La característica de discos administrados Managed Disks oculta la complejidad de crear y administrar cuentas de almacenamiento, y proporciona una solución simple, escalable y de alta disponibilidad para crear y administrar discos. Puede usar discos administrados como imágenes maestras, así como máquinas virtuales. El uso de discos administrados puede mejorar la creación de catálogos de máquinas y el tiempo de actualización. (Para obtener más información, consulte Learn about Managed Disks.)

© 1999-2019 Citrix Systems, Inc. All rights reserved.

De manera predeterminada, un catálogo de máquinas usa discos administrados. Cuando cree un catálogo, puede anular este valor predeterminado.

Cuando se configura la optimización de E/S (que usa tres discos por cada VM), puede aprovisionar hasta 3333 máquinas virtuales por suscripción. Cuando no se configura la optimización de E/S (que usa dos discos por máquina VM), puede aprovisionar hasta 5000 discos de máquinas virtuales por suscripción. (La función de Managed Disks permite crear hasta 10 000 discos de VM en una suscripción).

Usar discos administrados

Cuando se crea un catálogo de máquinas en Studio, la página **Imagen maestra** del asistente de creación de catálogos ofrece una lista de los discos administrados de Managed Disks, así como las VM y los discos VHD. (No todas las regiones de Azure admiten la función Managed Disks para discos administrados. Los discos administrados deben aparecer en la lista de cualquier región que sea visible para la conexión de host del catálogo.)

El tiempo de creación del catálogo se optimiza cuando la imagen y el catálogo se encuentran en la misma región.

La función Managed Disks no respalda actualmente la copia de discos entre regiones de Azure. Si selecciona una imagen en una región que no sea donde MCS proporcionará el catálogo, la imagen se copia en un VHD en una cuenta de almacenamiento convencional de la región del catálogo y luego se convierte a un disco administrado de Managed Disk.

En la página **Almacenamiento y tipos de licencia** del asistente de creación de catálogos, puede seleccionar una casilla de verificación para usar cuentas de almacenamiento convencionales en lugar de discos administrados. (Esta casilla de verificación no se puede seleccionar cuando se está aprovisionando en una región de Azure que no admite discos administrados).

Crear una conexión a Azure Resource Manager

Consulte el artículo Conexiones y recursos para obtener información sobre los asistentes que crean conexiones. En los siguientes artículos, se describen datos específicos de las conexiones con Azure Resource Manager.

Consideraciones:

- Las entidades de servicio deben contar con el rol Colaborador para la suscripción.
- Al crear la primera conexión, Azure pide conceder a ese rol los permisos necesarios. Para conexiones futuras, aún deberá autenticarse, pero Azure recuerda su consentimiento anterior y no vuelve a mostrar la solicitud.
- Las cuentas utilizadas para la autenticación deben ser de un coadministrador de la suscripción.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- La cuenta utilizada para la autenticación debe ser un miembro del directorio de suscripción. Hay dos tipos de cuentas a tener en cuenta: cuenta profesional o educativa y cuenta personal de Microsoft. Consulte CTX219211 para obtener más información.
- Puede 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. Una manera de rectificarlo es quitar los recursos del directorio y volver a agregarlos explícitamente. Sin embargo, use esta opción con cuidado, ya que puede tener 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, esto ocurre con las cuentas de directorio antiguas establecidas. Solución: agregue una nueva 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 todos 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.

Existen dos métodos para establecer una conexión de host a Azure Resource Manager:

- Autenticarse en Azure Resource Manager para crear una nueva entidad de servicio.
- Usar la información de una entidad de servicio anterior para conectarse a Azure Resource Manager.

Autenticarse en Azure Resource Manager para crear una nueva entidad de servicio

Antes de comenzar, compruebe que:

- Tiene una cuenta de usuario en el inquilino de su suscripción de Azure Active Directory.
- Con la cuenta de usuario de Azure AD, también se coadministra la suscripción de Azure que quiera usar para aprovisionar recursos.

En la instalación del sitio o en el asistente Agregar conexión y recursos:

1. En la página **Conexión**, seleccione el tipo de conexión **Microsoft Azure**. Luego, seleccione su entorno Azure Cloud.
2. En la página **Detalles de conexión**, escriba su ID de suscripción de Azure y un nombre para la conexión. El nombre de conexión puede contener de 1 a 64 caracteres, y no puede contener solo espacios en blanco ni caracteres no alfanuméricos. Después de introducir el ID de suscripción y el nombre de la conexión, se habilita el botón **Crear nueva**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

3. Escriba el nombre de usuario y la contraseña de la cuenta de Azure Active Directory.
4. Haga clic en **Iniciar sesión**.
5. Haga clic en **Aceptar** para conceder a Citrix Virtual Apps and Desktops los permisos mostrados. Citrix Virtual Apps and Desktops crea una entidad de servicio que le permite administrar los recursos de Azure Resource Manager en nombre del usuario especificado.
6. Después de hacer clic en **Aceptar**, volverá a la página **Conexión** en Studio. Tenga en cuenta que, cuando se autentica correctamente en Azure, los botones **Crear nueva** y **Usar existente** se reemplazan por **Conectado** y una marca de verificación verde indica una conexión establecida a la suscripción de Azure.
7. Indique las herramientas a utilizar para crear las máquinas virtuales y, a continuación, haga clic en **Siguiente**. No puede pasar de esta página del asistente hasta que se autentique correctamente en Azure y acepte conceder los permisos necesarios.
8. Los recursos constituyen la región y la red. En la página **Región**, seleccione una región. En la página **Red**,
    - Escriba un nombre de recursos de 1 a 64 caracteres para identificar más fácilmente la combinación de región y red en Studio. Un nombre de recurso no puede contener solo espacios en blanco ni caracteres no alfanuméricos.
    - Seleccione una combinación de red virtual y recurso de grupo. Dado que puede tener más de una red virtual con el mismo nombre, emparejar un nombre de red con un grupo de recursos ofrece combinaciones únicas. Si ha seleccionado una región que no tiene redes virtuales en la página anterior, deberá volver a esa página y seleccionar una región que las tenga.
9. Complete el asistente.

Usar la información de una entidad de servicio anterior para conectarse a Azure Resource Manager

Para crear manualmente una entidad de servicio, conéctese a su suscripción de Azure Resource Manager y use los siguientes cmdlets de PowerShell.

Requisitos previos:

- $SubscriptionId: ID de suscripción de Azure Resource Manager perteneciente a la suscripción donde quiere aprovisionar los agentes VDA.
- $AADUser: Cuenta de usuario de Azure AD perteneciente al inquilino de su suscripción de AD.
- Convierta al usuario $AADUser en el coadministrador de su suscripción.
- $ApplicationName: Nombre de la aplicación que se creará en Azure AD.
- $ApplicationPassword: Contraseña de la aplicación. Usará esta contraseña como secreto de la aplicación cuando cree la conexión de host.

Para crear una entidad de servicio:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

1. Conéctese a su suscripción de Azure Resource Manager.

   ```
   Login-AzureRmAccount
   ```

2. Seleccione la suscripción de Azure Resource Manager donde crear la entidad principal de servicio.

   ```
   Select-AzureRmSubscription -SubscriptionID $SubscriptionId
   ```

3. Cree la aplicación en su inquilino de AD.

   ```
   $AzureADApplication = New-AzureRmADApplication -DisplayName $ApplicationName
    -HomePage "https://localhost/$ApplicationName"-IdentifierUris https://
   $ApplicationName -Password $ApplicationPassword
   ```

4. Cree una entidad principal de servicio.

   ```
   New-AzureRmADServicePrincipal -ApplicationId $AzureADApplication.
   ApplicationId
   ```

5. Asigne un rol a la entidad principal de servicio.

   ```
   New-AzureRmRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName
    $AzureADApplication.ApplicationId -scope /subscriptions/$SubscriptionId
   ```

6. En la ventana de resultados de la consola de PowerShell, anote el ID de aplicación (ApplicationId). Deberá proporcionar ese ID cuando cree la conexión de host.

En la instalación del sitio o en el asistente Agregar conexión y recursos:

1. En la página **Conexión**, seleccione el tipo de conexión **Microsoft Azure** y su entorno de Azure.
2. En la página **Detalles de conexión**, escriba su ID de suscripción de Azure y un nombre para la conexión. (El nombre de conexión puede contener de 1 a 64 caracteres, y no puede contener solo espacios en blanco ni caracteres no alfanuméricos.
3. Haga clic en **Usar existente**. Introduzca el ID de suscripción, el nombre de suscripción, la URL de autenticación, la URL de administración, el sufijo de almacenamiento, el ID de Active Directory o el ID del inquilino, el ID de aplicación y el secreto de aplicación para la entidad de servicio existente. Después de introducir la información, se habilitará el botón **Aceptar**. Haga clic en **Aceptar**.
4. Indique las herramientas a utilizar para crear las máquinas virtuales y, a continuación, haga clic en **Siguiente**. Se utilizará la información que haya proporcionado sobre la entidad de servicio para conectarse a su suscripción de Azure. (No puede pasar de esta página del asistente hasta que proporcione información válida para la opción Usar existente).
5. Los recursos constituyen la región y la red. En la página **Región**, seleccione una región. En la página **Red**:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Escriba un nombre de recurso de 1 a 64 caracteres para identificar más fácilmente la combinación de región y red en Studio. Un nombre de recurso no puede contener solo espacios en blanco ni caracteres no alfanuméricos.
- Seleccione una combinación de red virtual y recurso de grupo. Dado que puede tener más de una red virtual con el mismo nombre, emparejar un nombre de red con un grupo de recursos ofrece combinaciones únicas. Si ha seleccionado una región que no tiene redes virtuales en la página anterior, deberá volver a esa página y seleccionar una región que las tenga.

6. Complete el asistente.

Crear un catálogo de máquinas a partir de una imagen maestra de Azure Resource Manager

Esta información complementa a las instrucciones del artículo Crear catálogos de máquinas.

Una imagen maestra es la plantilla que se usará para crear las máquinas virtuales en un catálogo de máquinas. Antes de crear el catálogo de máquinas, cree una imagen maestra en Azure Resource Manager. Para obtener información acerca de las imágenes maestras en general, consulte el artículo Creación de catálogos de máquinas.

Al crear un catálogo de máquinas en Studio:

- Las páginas **Sistema operativo** y **Administración de máquinas** no contienen información específica de Azure. Siga las instrucciones indicadas en el artículo “Crear catálogos de máquinas”.
- En la página **Imagen maestra**, seleccione un grupo de recursos y, a continuación, vaya a (explore en profundidad) los contenedores del disco duro virtual (VHD) de Azure que quiere usar como imagen maestra. El VHD debe tener instalado un VDA de Citrix. Si el VHD está asignado a una VM, la VM debe estar detenida.
- La página **Tipos de licencia y almacenamiento** solo aparecerá cuando se use una imagen maestra de Azure Resource Manager.

  Seleccione un tipo de almacenamiento: Estándar o Premium. El tipo de almacenamiento influye en los tamaños de las máquinas que se ofrecen en la página Máquinas virtuales del asistente. Ambos tipos de almacenamiento realizan varias copias sincrónicas de los datos en un único centro de datos. Para obtener más información acerca de los tipos de almacenamiento y la replicación de almacenamiento de Azure, consulte lo siguiente:

  - https://azure.microsoft.com/en-us/documentation/articles/storage-introduction/
  - https://azure.microsoft.com/en-us/documentation/articles/storage-premium-storage/
  - https://azure.microsoft.com/en-us/documentation/articles/storage-redundancy/

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Seleccione si utilizar o no las licencias locales (“on-premises”) existentes de Windows Server. Utilizarlas al mismo tiempo que se utilizan las imágenes locales (“on-premises”) existentes de Windows Server usa Azure Hybrid Use Benefits (HUB). Dispone de más detalles en https://azure.microsoft.com/pricing/hybrid-use-benefit/

HUB reduce los costes de ejecución de máquinas virtuales en Azure a la ratio de procesamiento básica, ya que dispensa del precio de licencias adicionales de Windows Server de la galería de Azure. Debe traer sus imágenes locales de Windows Server a Azure para usar HUB. No se respaldan las imágenes de la galería de Azure. Las licencias locales de clientes Windows no reciben respaldo en este momento. Consulte https://blogs.msdn.microsoft.com/azureedu/2016/04/13/how-can-i-use-the-hybrid-use-benefit-in-azure/

Para verificar que las máquinas virtuales aprovisionadas utilizan HUB, ejecute el comando `Get-AzureRmVM -ResourceGroup MyResourceGroup -Name MyVM` de PowerShell y compruebe que el tipo de licencia es Windows_Server. Dispone de instrucciones adicionales en https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-windows-hybrid-use-benefit-licensing/

- En la página **Máquinas virtuales**, indique la cantidad de máquinas virtuales que quiere crear; debe especificar al menos una. Seleccione un tamaño de máquina. Después de crear un catálogo de máquinas, no se puede cambiar el tamaño de máquina. Si, más adelante, quiere otro tamaño, elimine el catálogo y cree uno nuevo que utilice la misma imagen maestra; especifique entonces el tamaño de máquina pertinente.

  Los nombres de máquina virtual no pueden contener caracteres no ASCII o ni caracteres especiales.

- (Cuando se usa Machine Creation Services) En la página **Grupos de recursos**, elija si quiere crear grupos de recursos nuevos o usar los grupos existentes.

  Si opta por crear grupos de recursos nuevos, haga clic en **Siguiente**.

  Si decide utilizar los grupos de recursos existentes, seleccione esos grupos en la lista **Grupos de recursos de aprovisionamiento disponibles**. Debe seleccionar grupos suficientes para las máquinas que está creando en el catálogo. Studio muestra un mensaje si selecciona demasiado pocas. Puede seleccionar más del mínimo requerido de máquinas si va a agregar más máquinas al catálogo más tarde. No se puede agregar más grupos de recursos a un catálogo una vez creado el catálogo.

  Para obtener más información, consulte el apartado Grupos de recursos de Azure más adelante en este artículo.

- Las páginas **Tarjetas de red**, **Cuentas de equipo** y **Resumen** no contienen información específica de Azure. Siga las instrucciones indicadas en el artículo “Crear catálogos de máquinas”.

Complete el asistente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Eliminar catálogos de máquinas

Cuando se elimina un catálogo de máquinas de Azure Resource Manager, las máquinas y los grupos de recursos asociados se eliminan de Azure, incluso aunque indique que deben conservarse.

Grupos de recursos de Azure

Los grupos de recursos de aprovisionamiento de Azure ofrecen una manera de aprovisionar las VM que proporcionan escritorios y aplicaciones a los usuarios. Puede agregar los grupos de recursos de Azure vacíos existentes cuando cree un catálogo de máquinas con MCS en Studio. También puede decidir que se creen nuevos grupos de recursos para usted.

Para obtener información acerca de los grupos de recursos de Azure, consulte Información general sobre Azure Resource Manager.

Requisitos

- Cada grupo de recursos puede contener 240 máquinas virtuales como máximo. Debe haber suficientes grupos de recursos vacíos disponibles en la región donde está creando el catálogo. Si quiere utilizar los grupos de recursos existentes cuando cree un catálogo de máquinas, debe seleccionar suficientes grupos disponibles para admitir la cantidad de máquinas que se van a crear en el catálogo. Por ejemplo, si especifica 500 máquinas en el asistente de creación de catálogos, seleccione al menos tres grupos de recursos de aprovisionamiento disponibles.

  No se puede agregar grupos de recursos a un catálogo de máquinas una vez creado el catálogo. Sin embargo, puede agregar los grupos de recursos suficientes como para admitir las máquinas que pueda agregar al catálogo más tarde.
- Cree grupos de recursos vacíos en la misma región que su conexión de host.
- Si quiere que se creen grupos de recursos nuevos para cada catálogo de MCS, la entidad de servicio Azure asociada a la conexión de host debe tener permiso para crear y eliminar grupos de recursos. Si quiere que se utilicen los grupos de recursos vacíos existentes, la entidad de servicio Azure asociada a la conexión de host debe tener el permiso Colaborador en esos grupos de recursos vacíos.
- Cuando crea una conexión de host en Studio utilizando la opción **Crear nuevo**, la entidad principal de servicio creada tiene los permisos de colaborador con el ámbito de suscripción. Como alternativa, puede usar la opción **Usar existente** para crear la conexión y proporcionar los datos de una entidad principal de servicio existente con el ámbito de suscripción. Si usa la opción **Crear nuevo** y crea la entidad de servicio en Studio, esta tiene los permisos necesarios para crear y eliminar grupos de recursos nuevos o aprovisionar grupos de recursos vacíos existentes.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Las entidades de servicio con ámbito restringido deben crearse mediante PowerShell. Además, cuando se usa a una entidad de servicio con ámbito restringido, debe usar PowerShell o el portal de Azure para crear grupos de recursos vacíos destinados a cada catálogo donde MCS aprovisionará las máquinas virtuales. Para obtener instrucciones, consulte la entrada del blog https://www.citrix.com/blogs/2016/11/09/azure-role-based-access-control-in-xenapp-xendesktop/.)

  Si utiliza una entidad de servicio con un ámbito restringido para la conexión de host, pero el grupo de recursos de la imagen maestra no aparece en la página **Imagen maestra** del asistente de creación de catálogos, probablemente es porque esa entidad no tiene el permiso "Microsoft.Resources/subscriptions/resourceGroups/read" para poder mostrar el grupo de recursos de la imagen maestra. Cierre el asistente, actualice la entidad de servicio para concederle el permiso (consulte la entrada del blog para obtener instrucciones) y, a continuación, reinicie el asistente. (En Azure, la actualización puede tardar hasta 10 minutos en aparecer en Studio.)

Configurar grupos de recursos para un catálogo de máquinas en Studio

En la página "Grupos de recursos" del asistente de creación de catálogos, puede elegir si crear grupos de recursos nuevos o usar los existentes. Consulte la sección en este artículo: *Crear un catálogo de máquinas con una imagen maestra de Azure Resource Manager*.

Qué ocurre con los grupos de recursos cuando se elimina un catálogo de máquinas:

- Si permite que Citrix Virtual Apps and Desktops cree grupos de recursos cuando usted crea el catálogo de máquinas y, posteriormente, elimina ese catálogo, esos grupos de recursos y todos los recursos en esos grupos también se eliminan.
- Si usa grupos de recursos existentes cuando cree el catálogo de máquinas y, posteriormente, elimina ese catálogo, todos los recursos en esos grupos de recursos se eliminan, pero los grupos en sí se conservan.

Consideraciones, limitaciones y solución de problemas

Cuando se usan grupos de recursos existentes, la lista de los grupos de recursos disponibles en la página "Grupos de recursos" del asistente de creación de catálogos no se actualiza automáticamente. Por lo tanto, si tiene abierta esa página del asistente mientras crea o agrega permisos a los grupos de recursos en Azure, esos cambios no se reflejan en la lista del asistente. Para ver los cambios más recientes, dispone de dos opciones: volver a la página "Administración de máquinas" del asistente y volver a seleccionar los recursos asociados a la conexión de host, o cerrar y reiniciar el asistente. Pueden pasar hasta 10 minutos hasta que los cambios realizados en Azure aparezcan en Studio.

Un grupo de recursos debería utilizarse en un solo catálogo de máquinas. No obstante, esto no se aplica. Por ejemplo, se seleccionan 10 grupos de recursos al crear un catálogo, pero solo se crea una

© 1999-2019 Citrix Systems, Inc. All rights reserved.

máquina en el catálogo. Nueve de los grupos de recursos seleccionados permanecen vacíos una vez creado el catálogo. Puede que tenga la intención de usarlos para expandir su capacidad en el futuro, por lo que permanecen asociados a ese catálogo. No se puede agregar grupos de recursos a un catálogo una vez creado el catálogo, así que es sensato planificar para el futuro durante la creación del catálogo. Sin embargo, si se crea otro catálogo, esos nueve grupos de recursos aparecerán en la lista de grupos disponibles. Actualmente Citrix Virtual Apps and Desktops no realiza ningún seguimiento de qué grupos de recursos se asignan a qué catálogos. Supervisar esa asignación recae sobre usted.

Si la conexión utiliza una entidad de servicio que puede acceder a los grupos de recursos vacíos que se encuentran en varias regiones, todos aparecerán en la lista de grupos disponibles. Debe seleccionar los grupos de recursos de la misma región donde crea el catálogo de máquinas.

Solucionar problemas:

- Los grupos de recursos no aparecen en la lista de la página “Grupos de recursos” en el asistente de creación de catálogos.

  La entidad de servicio debe tener los permisos adecuados aplicados a los grupos de recursos que quiera que aparezcan en la lista. Consulte la sección anterior de requisitos.

- Al agregar máquinas a un catálogo de máquinas creado previamente, no se aprovisionan todas las máquinas.

  Después de crear un catálogo, cuando más adelante agregué máquinas a ese catálogo, no exceda la capacidad de máquinas por grupo de recursos originalmente seleccionada para el catálogo (240 por grupo). No se puede agregar grupos de recursos una vez creado el catálogo. Si intenta agregar más máquinas de las que pueden admitir los grupos de recursos existentes, el aprovisionamiento falla.

  Por ejemplo, crea un catálogo de máquinas con 300 VM y 2 grupos de recursos. Los grupos de recursos pueden admitir hasta 480 máquinas virtuales (240 multiplicado por 2). Si más adelante intenta agregar 200 VM al catálogo, lo que supera la capacidad de los grupos de recursos (300 VM actuales + 200 VM nuevas = 500, pero los grupos de recursos pueden contener solo 480 VM).

Más información

- Conexiones y recursos
- Crear catálogos de máquinas
- CTX219211: Configurar una cuenta de Microsoft Azure Active Directory
- CTX219243: Conceder a XenApp y XenDesktop acceso a la suscripción de Azure
- CTX219271: Implementar nube híbrida usando VPN de sitio a sitio

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Entornos de virtualización de Microsoft System Center Virtual Machine Manager

March 8, 2019

Si quiere utilizar Hyper-V con Microsoft System Center Virtual Machine Manager (VMM) para proporcionar máquinas virtuales, siga estas instrucciones.

Esta versión admite las versiones de VMM que figuran en el artículo Requisitos del sistema.

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

- Máquinas virtuales de SO de servidor o escritorio de 1ª generación
- Máquinas virtuales Windows Server 2012 R2, Windows Server 2016 y Windows 10 (con o sin Secure Boot) de 2ª generación

Instalar y configurar un hipervisor

1. Instale Microsoft Hyper-V Server y VMM en los servidores. Todos los Delivery Controllers deben estar en el mismo bosque que los servidores de VMM.
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 un miembro del grupo de seguridad de administradores local en cada uno de los servidores Hyper-V para dar respaldo a la administración del ciclo de vida de las VM (creación, actualización y eliminación de VM).

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

Crear una VM maestra

1. Instale un agente Virtual Desktop Agent en la VM maestra y seleccione la opción de optimizar el escritorio. Esto mejora el rendimiento.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

2. Tome una instantánea de la VM maestra para usarla como copia de seguridad.

Crear escritorios virtuales

Si utiliza MCS para crear máquinas virtuales, al crear un sitio o una conexión:

1. Seleccione el tipo de host de virtualización Microsoft.
2. Escriba la dirección como el nombre de dominio completo del servidor host.
3. Introduzca las credenciales para la cuenta de administrador que configuró anteriormente y que incluye permisos para crear nuevas VM.
4. En **Detalles del host**, seleccione el clúster o el host independiente que quiere utilizar para crear las VM.

   Busque y seleccione un clúster o un host independiente aunque utilice una implementación de host de Hyper-V único.

MCS en recursos compartidos de archivos SMB 3

En caso de catálogos de máquinas creados a través de MCS en recursos compartidos SMB 3 para el almacenamiento de VM, compruebe que las credenciales cumplen los siguientes requisitos, de modo que las llamadas desde la biblioteca de comunicaciones de hipervisor (HCL) del Controller puedan conectarse al almacenamiento SMB:

- Las credenciales de usuario de VMM deben incluir acceso de escritura y lectura completo al almacenamiento de SMB.
- Las operaciones de disco virtual de almacenamiento durante el ciclo de vida de las máquinas virtuales se realizan a través del servidor Hyper-V usando las credenciales de usuario de VMM.

Si usa SMB como almacenamiento, habilite el proveedor de compatibilidad para seguridad de autenticación de credenciales (CredSSP) desde el Controller a cada máquina de Hyper-V cuando se utilice VMM 2012 SP1 con Hyper-V en Windows Server 2012. Para obtener más información, consulte CTX137465.

Si usa una sesión remota de PowerShell 3 estándar, HCL usa CredSSP para abrir una conexión con la máquina Hyper-V. Esta función pasa las credenciales de usuario cifradas por Kerberos a la máquina Hyper-V. A continuación, los comandos de PowerShell de la sesión en la máquina Hyper-V remota se ejecutan con las credenciales proporcionadas (en este caso, las credenciales del usuario de VMM), de forma que los comandos que se comuniquen al almacenamiento funcionen correctamente.

Las siguientes tareas usan scripts de PowerShell que se originan en la HCL y se envían a la máquina Hyper-V para actuar en el almacenamiento de SMB 3.0.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Consolidar una imagen maestra:** Una imagen maestra crea un nuevo esquema de aprovisionamiento (catálogo de máquinas) de MCS. Clona y deja la VM maestra lista para crear nuevas VM a partir del nuevo disco creado (y quita la dependencia de la VM maestra original).

  ConvertVirtualHardDisk en el espacio de nombres root\virtualization\v2

  Ejemplo:

```
$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.

  La HCL carga la identidad en la máquina Hyper-V mediante el recurso compartido de administrador.

  La máquina Hyper-V copia el disco en el almacenamiento de SMB a través de un script de PowerShell que se ejecuta en la sesión remota de PowerShell. Se crea una carpeta en la máquina Hyper-V y los permisos de la carpeta están bloqueados únicamente para el usuario de VMM (a través de la conexión remota de PowerShell).

  La biblioteca HCL elimina el archivo del recurso compartido de administrador.

  Cuando la biblioteca HCL completa la carga del disco de identidad en la máquina Hyper-V, la sesión remota de PowerShell copia los discos de identidad al almacenamiento de SMB y, después, los elimina de la máquina Hyper-V.

  La carpeta del disco de identidad se vuelve a crear si se elimina para que esté disponible para volver a usarse.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Descargar discos de identidad:** Al igual que con las cargas, los discos de identidad pasan a través de la máquina Hyper-V hasta la HCL. El siguiente proceso crea una carpeta que solo tiene permisos de usuario de VMM en el servidor Hyper-V si no existe.

  La máquina Hyper-V copia el disco desde el almacenamiento de SMB al almacenamiento de Hyper-V local mediante un script de PowerShell que se ejecuta en la sesión remota de PowerShell V3.

  La HCL lee el disco desde el recurso compartido de administrador de la máquina Hyper-V y lo copia en memoria.

  La HCL elimina el archivo del recurso compartido de administrador.

- **Crear discos Personal vDisk:** Si el administrador crea la VM en un catálogo de máquinas de Personal vDisk, usted debe crear un disco vacío (PvD).

  La llamada para crear un disco vacío no requiere acceso directo al almacenamiento. Si tiene discos PvD que residen en un almacenamiento que no sea el disco principal o el del sistema operativo, use PowerShell de forma remota para crear el disco PvD en una carpeta de directorio que tenga el mismo nombre que la VM desde la que se creó. Para CSV o LocalStorage, no use PowerShell de forma remota. Crear el directorio antes de crear un disco vacío evita errores de comando de VMM.

  En la máquina Hyper-V, realice un mkdir en el almacenamiento.

Entornos de virtualización de XenServer

January 29, 2019

Crear una conexión a XenServer

Cuando crea una conexión con XenServer, debe proporcionar las credenciales de un administrador avanzado de VM o de un usuario de nivel superior.

Citrix recomienda utilizar HTTPS para proteger las comunicaciones con 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 XenServer. Citrix recomienda seleccionar todos los servidores de la agrupación (en “Edit High Availability”) para permitir la comunicación con 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 respalda el uso de vGPU. La interfaz indica si la selección tiene recursos de GPU dedicados.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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.)

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 XenDesktop)**. 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**.

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

4. Instale XenServer Tools y los controladores de NVIDIA.
5. Desactive la consola de administración de Virtual Network Computing (VNC) para optimizar el rendimiento y, a continuación, reinicie la VM.
6. Se le solicitará que use RDP. Mediante RDP, instale el VDA y, a continuación, reinicie la VM.
7. Si lo desea, puede crear una instantánea de la VM para establecer un punto de referencia para otras imágenes maestras de GPU.
8. Mediante RDP, instale las aplicaciones específicas del usuario que están configuradas en XenCenter y funcionan con GPU.

Más información

- Conexiones y recursos
- Crear catálogos de máquinas

Entornos de Microsoft System Center Configuration Manager

March 8, 2019

Los sitios que usan Microsoft System Center Configuration Manager (Configuration Manager) para administrar el acceso a las aplicaciones y los escritorios en dispositivos físicos pueden extender ese uso a XenApp o XenDesktop a través de estas opciones de integración.

- **Citrix Connector 3.1:** Citrix Connector es un puente entre Configuration Manager y Citrix Virtual Apps and Desktops. Connector permite unificar las operaciones realizadas diariamente en los entornos físicos que se administran con Configuration Manager y en los entornos virtuales que se administran con Citrix Virtual Apps and Desktops. Para obtener más información, consulte Citrix Connector 3.1.
- **Proxy Wake On LAN de Configuration Manager:** La función Wake on LAN del Acceso con Remote PC requiere Configuration Manager. Consulte Acceso con Remote PC para obtener más información.
- **Propiedades de XenApp y XenDesktop:** Con las propiedades de XenApp y XenDesktop, se pueden identificar escritorios virtuales de Citrix para administrarlos a través de Configuration Manager. (En Configuration Manager se utiliza el antiguo nombre de Citrix Virtual Apps and Desktops: XenApp y XenDesktop.) Citrix Connector utiliza automáticamente estas propiedades, pero también se pueden configurar manualmente, como se describe en la sección siguiente.

Propiedades

Si quiere administrar escritorios virtuales, existen propiedades disponibles para Microsoft System Center Configuration Manager.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Las propiedades de valor booleano que se muestran en Configuration Manager pueden aparecer como 1 ó 0, en lugar de True o False.

Las propiedades están disponibles para la clase Citrix_virtualDesktopInfo en el espacio de nombres Root\Citrix\DesktopInformation. Los nombres de propiedad proceden del proveedor Instrumental de administración de Windows (WMI).

Propiedad	Description
AssignmentType	Establece el valor de IsAssigned. Los valores válidos son: ClientIP, ClientName, None y User (establece IsAssigned en True)
BrokerSiteName	Es un sitio; devuelve el mismo valor que HostIdentifier
DesktopCatalogName	Catálogo de máquinas asociado al escritorio.
DesktopGroupName	Grupo de entrega asociado con el escritorio.
HostIdentifier	Es un sitio; 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, es posible que quiera instalar aplicaciones en la imagen maestra y no en las máquinas aprovisionadas, sobre todo si esas máquinas están limpias como máquinas de arranque. Los valores válidos son: True para una máquina virtual que se usa como una imagen maestra (este valor se establece durante la instalación basada en una selección) o en blanco para una máquina virtual aprovisionada a partir de esa imagen.
IsVirtualMachine	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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Propiedad	Description
PersonalvDiskDriveLetter	Para un escritorio con un disco Personal vDisk, es la letra de unidad que se asigna al mismo.
BrokerSiteName, DesktopCatalogName, DesktopGroupName, HostIdentifier	Se determina cuando el escritorio se registra con el Controller; tienen el valor null en un escritorio que no se ha registrado completamente.

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 pueden incluir espacios o variar levemente con respecto a los nombres de propiedades. Por ejemplo, **BrokerSiteName** puede aparecer 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 usar las propiedades de Microsoft en la clase de Microsoft de CCM_DesktopMachine en el espacio de nombres Root\ccm_vdi. Para obtener más información, consulte la documentación de Microsoft.

Entornos de virtualización de VMware

January 29, 2019

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 característica de explorador del almacén de datos (Datastore Browser) en el servidor vCenter (descrito en https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2101567). Si inhabilita esta característica, MCS no funciona correctamente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Privilegios necesarios

Cree una cuenta de usuario de VMware y uno o varios roles de VMware con un conjunto de los privilegios que se describen a continuación. Base la creación de roles en un nivel específico de granularidad necesaria sobre los permisos del usuario para solicitar las distintas operaciones de Citrix Virtual Apps and Desktops en cualquier momento. Para conceder los permisos específicos de usuario en cualquier momento, asócielos al rol correspondiente, en el nivel DataCenter como mínimo.

En las siguientes tablas, se muestran las asignaciones entre las operaciones de Citrix Virtual Apps and Desktops y los privilegios mínimos requeridos de VMware.

Agregar conexiones y recursos

SDK	Interfaz de usuario
System.Anonymous, System.Read, y System.View	Se agrega automáticamente. Puede usar el rol integrado de solo lectura.

Aprovisionar máquinas (Machine Creation Services)

SDK	Interfaz de usuario
Datastore.AllocateSpace	Almacén de datos > Asignar espacio
Datastore.Browse	Almacén de datos > Examinar almacén de datos
Datastore.FileManagement	Almacén de datos > Operaciones de archivos de bajo nivel
Network.Assign	Red > Asignar red
Resource.AssignVMToPool	Recurso > Asignar máquina virtual a la agrupación de recursos
VirtualMachine.Config.AddExistingDisk	Máquina virtual > Configuración > Agregar disco existente
VirtualMachine.Config.AddNewDisk	Máquina virtual > Configuración > Agregar nuevo disco
VirtualMachine.Config.AdvancedConfig	Máquina virtual > Configuración > Avanzado
VirtualMachine.Config.RemoveDisk	Máquina virtual > Configuración > Quitar disco
VirtualMachine.Interact.PowerOff	Máquina virtual > Interacción > Apagar

© 1999-2019 Citrix Systems, Inc. All rights reserved.

SDK	Interfaz de usuario
VirtualMachine.Interact.PowerOn	Máquina virtual > Interacción > Iniciar
VirtualMachine.Inventory.CreateFromExisting	Máquina virtual > Inventario > Crear a partir de existentes
VirtualMachine.Inventory.Create	Máquina virtual > Inventario > Crear nueva
VirtualMachine.Inventory.Delete	Máquina virtual > Inventario > Quitar
VirtualMachine.Provisioning.Clone	Máquina virtual > Aprovisionamiento > Clonar máquina virtual
VirtualMachine.State.CreateSnapshot	*vSphere 5.0, Update 2 y vSphere 5.1, Update 1:* Virtual machine > State > Create snapshot; *vSphere 5.5:* Virtual machine > Snapshot management > Create snapshot

Si quiere que se etiqueten las VM que vaya a crear, agregue los siguientes permisos a la cuenta de usuario:

Para asegurarse de que usa una imagen base limpia para crear nuevas máquinas virtuales, etiquete las VM creadas con Machine Creation Services para excluirlas de la lista de VM disponibles para usarlas como imágenes base.

SDK	Interfaz de usuario
Global.ManageCustomFields	Global > Administrar atributos personalizados
Global.SetCustomField	Global > Definir atributo personalizado

Aprovisionar máquinas (Citrix Provisioning)

Todos los privilegios 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	Máquina virtual > Configuración > Cambiar recuento de CPU
VirtualMachine.Config.Memory	Máquina virtual > Configuración > Memoria

© 1999-2019 Citrix Systems, Inc. All rights reserved.

SDK	Interfaz de usuario
VirtualMachine.Config.Settings	Máquina virtual > Configuración > Parámetros
VirtualMachine.Provisioning.CloneTemplate	Máquina virtual > Aprovisionamiento > Clonar plantilla
VirtualMachine.Provisioning.DeployTemplate	Máquina virtual > Aprovisionamiento > Implementar plantilla

Administración de energía

SDK	Interfaz de usuario
VirtualMachine.Interact.PowerOff	Máquina virtual > Interacción > Apagar
VirtualMachine.Interact.PowerOn	Máquina virtual > Interacción > Iniciar
VirtualMachine.Interact.Reset	Máquina virtual > Interacción > Restablecer
VirtualMachine.Interact.Suspend	Máquina virtual > Interacción > Suspender

Actualizar y revertir imagen

SDK	Interfaz de usuario
Datastore.AllocateSpace	Almacén de datos > Asignar espacio
Datastore.Browse	Almacén de datos > Examinar almacén de datos
Datastore.FileManagement	Almacén de datos > Operaciones de archivos de bajo nivel
Network.Assign	Red > Asignar red
Resource.AssignVMToPool	Recurso > Asignar máquina virtual a la agrupación de recursos
VirtualMachine.Config.AddExistingDisk	Máquina virtual > Configuración > Agregar disco existente
VirtualMachine.Config.AddNewDisk	Máquina virtual > Configuración > Agregar nuevo disco
VirtualMachine.Config.AdvancedConfig	Máquina virtual > Configuración > Avanzado

© 1999-2019 Citrix Systems, Inc. All rights reserved.

SDK	Interfaz de usuario
VirtualMachine.Config.RemoveDisk	Máquina virtual > Configuración > Quitar disco
VirtualMachine.Interact.PowerOff	Máquina virtual > Interacción > Apagar
VirtualMachine.Interact.PowerOn	Máquina virtual > Interacción > Iniciar
VirtualMachine.Interact.Reset	Máquina virtual > Interacción > Restablecer
VirtualMachine.Inventory.CreateFromExisting	Máquina virtual > Inventario > Crear a partir de existentes
VirtualMachine.Inventory.Create	Máquina virtual > Inventario > Crear nueva
VirtualMachine.Inventory.Delete	Máquina virtual > Inventario > Quitar
VirtualMachine.Provisioning.Clone	Máquina virtual > Aprovisionamiento > Clonar máquina virtual

Eliminar máquinas aprovisionadas

SDK	Interfaz de usuario
Datastore.Browse	Almacén de datos > Examinar almacén de datos
Datastore.FileManagement	Almacén de datos > Operaciones de archivos de bajo nivel
VirtualMachine.Config.RemoveDisk	Máquina virtual > Configuración > Quitar disco
VirtualMachine.Interact.PowerOff	Máquina virtual > Interacción > Apagar
VirtualMachine.Inventory.Delete	Máquina virtual > Inventario > Quitar

Crear AppDisks

Válido para VMware vSphere 5.5, como mínimo, y XenApp y XenDesktop 7.8, como mínimo.

SDK	Interfaz de usuario
Datastore.AllocateSpace	Almacén de datos > Asignar espacio
Datastore.Browse	Almacén de datos > Examinar almacén de datos

© 1999-2019 Citrix Systems, Inc. All rights reserved.

SDK	Interfaz de usuario
Datastore.FileManagement	Almacén de datos > Operaciones de archivos de bajo nivel
VirtualMachine.Config.AddExistingDisk	Máquina virtual > Configuración > Agregar disco existente
VirtualMachine.Config.AddNewDisk	Máquina virtual > Configuración > Agregar nuevo disco
VirtualMachine.Config.AdvancedConfig	Máquina virtual > Configuración > Avanzado
VirtualMachine.Config.EditDevice	Máquina virtual > Configuración > Modificar parámetros de dispositivo
VirtualMachine.Config.RemoveDisk	Máquina virtual > Configuración > Quitar disco
VirtualMachine.Interact.PowerOff	Máquina virtual > Interacción > Apagar
VirtualMachine.Interact.PowerOn	Máquina virtual > Interacción > Iniciar

Eliminar AppDisks

Válido para VMware vSphere 5.5, como mínimo, y XenApp y XenDesktop 7.8, como mínimo.

SDK	Interfaz de usuario
Datastore.Browse	Almacén de datos > Examinar almacén de datos
Datastore.FileManagement	Almacén de datos > Operaciones de archivos de bajo nivel
VirtualMachine.Config.RemoveDisk	Máquina virtual > Configuración > Quitar disco
VirtualMachine.Interact.PowerOff	Máquina virtual > Interacción > Apagar

Obtener e importar un certificado

Para proteger las comunicaciones de vSphere, Citrix recomienda utilizar HTTPS en lugar de HTTP. HTTPS requiere certificados digitales. Citrix recomienda utilizar un certificado digital emitido por una autoridad de certificación en función de la directiva de seguridad de la organización.

Si no puede utilizar un certificado digital emitido por una entidad de certificación y las directivas de seguridad de la organización lo permiten, puede utilizar el certificado autofirmado instalado por

© 1999-2019 Citrix Systems, Inc. All rights reserved.

VMware. Agregue el certificado de VMware vCenter a cada Delivery Controller.

1. Agregue el nombre de dominio completo (FQDN) del equipo que ejecuta vCenter Server al archivo hosts de ese servidor, ubicado en %SystemRoot%/WINDOWS/system32/Drivers/etc/. Este paso solo es necesario si el nombre FQDN del equipo que ejecuta vCenter Server aún no está presente en el sistema de nombres de dominio.
2. Obtenga el certificado de vCenter con alguno de los tres métodos siguientes:

   Desde el servidor vCenter.

   a) Copie el archivo rui.crt desde el servidor vCenter a una ubicación accesible en los Delivery Controllers.
   b) En Controller, vaya a la ubicación donde está el certificado exportado y abra el archivo rui.crt.

   Descargue el certificado usando un explorador Web. Si está usando Internet Explorer, dependiendo de la cuenta de usuario, puede que tenga que hacer clic con el botón secundario en Internet Explorer y elegir **Ejecutar como administrador** para descargar o instalar el certificado.

   a) Abra el explorador Web y establezca una conexión Web segura con el servidor vCenter (por ejemplo https://server1.domain1.com)).
   b) Acepte las advertencias de seguridad.
   c) Haga clic en la barra de dirección donde aparece el error de certificado.
   d) Revise el certificado y haga clic en la ficha Detalles.
   e) Seleccione **Copiar a archivo y exportar en formato CER** y escriba un nombre cuando lo pida el procedimiento.
   f) Guarde el certificado exportado.
   g) Vaya a la ubicación del certificado exportado y abra el archivo CER.

   Impórtelo directamente desde Internet Explorer ejecutado como administrador.

   - Abra el explorador Web y establezca una conexión Web segura con el servidor vCenter (por ejemplo https://server1.domain1.com)).
   - Acepte las advertencias de seguridad.
   - Haga clic en la barra de dirección donde aparece el error de certificado.
   - Vea el certificado.

3. Importe el certificado en el almacén de certificados de cada uno de los Controllers.

   a) Haga clic en **Instalar certificado**, seleccione **Máquina local** y, a continuación, haga clic en **Siguiente**.
   b) Seleccione **Colocar todos los certificados en el siguiente almacén** y, a continuación, haga clic en **Examinar**. Seleccione **Personas de confianza** y haga clic en **Aceptar**. Haga clic en **Siguiente** y, a continuación, en **Finalizar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Si cambia el nombre del servidor vSphere después de la instalación, debe generar un certificado autofirmado nuevo en ese servidor antes de importar el certificado nuevo.

Consideraciones sobre la configuración

Crear una VM maestra:

Use una VM maestra para proporcionar las aplicaciones y los escritorios de los usuarios en un catálogo de máquinas. En el hipervisor:

1. Instale el VDA en la VM maestra y seleccione la opción de optimizar el escritorio, lo que mejora el rendimiento.
2. Tome una instantánea de la VM maestra para usarla como copia de seguridad.

Crear una conexión:

En el asistente para la creación de conexiones:

- Seleccione el tipo de conexión VMware.
- Especifique la dirección del punto de acceso para el SDK de vCenter.
- Especifique las credenciales de la cuenta de usuario VMware que ha configurado y que incluye permisos para crear nuevas VM. Especifique el nombre de usuario en el formato dominio/nombre_de_usuario.

Huella digital SSL de VMware

La funcionalidad huella digital SSL de VMware resuelve un error frecuente que se daba al crear una conexión de host a un hipervisor VMware vSphere. Anteriormente, los administradores tenían que crear manualmente una relación de confianza entre los Delivery Controllers del sitio y el certificado del hipervisor antes de crear una conexión. La función huella digital SSL de VMware elimina ese requisito manual: la huella digital del certificado que no es de confianza se almacena en la base de datos del sitio, de modo que el hipervisor puede identificarse continuamente como hipervisor de confianza por Citrix Virtual Apps and Desktops o, incluso si no es por ellos, por los Controllers.

Al crear una conexión de host de vSphere en Studio, un cuadro de diálogo le permite ver el certificado de la máquina a la que se está conectando. Por lo que puede elegir si quiere confiar en ella.

Entornos de virtualización de Nutanix

March 8, 2019

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:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Instalar y registrar el plug-in de Nutanix en el entorno de Citrix Virtual Apps and Desktops.
- Crear una conexión con el hipervisor Nutanix Acropolis.
- Crear un catálogo de máquinas que usa una instantánea de la imagen maestra que se ha creado en el hipervisor Nutanix.

Para obtener más información, consulte la guía de instalación de plug-ins MCS de Nutanix Acropolis, disponible en el portal de asistencia de Nutanix.

Prepare la instalación del plug-in MCS de Nutanix para Citrix Cloud Connector

Los requisitos previos para la integración de Nutanix Acropolis en el Delivery Controller de Citrix Virtual Apps and Desktops incluyen lo siguiente:

- Los usuarios con el plug-in MCS de AHV para el instalador de Citrix Cloud Connector deben tener privilegios de administrador en la VM de Citrix Cloud Connector.
- Registre la VM de Citrix Cloud Connector con una ubicación de recursos en el arrendatario de Citrix Cloud.
- Instale el plug-in MCS de AHV para Citrix Cloud Connector en todos los Cloud Connectors registrados con el arrendatario de Citrix Cloud. Realice esta instalación aunque los Connectors comuniquen una ubicación de recursos sin AHV.

Instalar y registrar el plug-in de Nutanix

Después de instalar los componentes de Citrix Virtual Apps and Desktops, complete el siguiente procedimiento para instalar y registrar el plug-in de Nutanix en los Delivery Controllers. Entonces, podrá usar Studio para crear una conexión con el hipervisor Nutanix y, a continuación, crear un catálogo de máquinas que use una instantánea de la imagen maestra que creó en el entorno de Nutanix.

1. Obtenga el plug-in de Nutanix, e instálelo en los Delivery Controllers.
2. Compruebe que se ha creado una carpeta de Nutanix Acropolis en C:\Archivos de programa\Common Files\Citrix\HCLPlugins\CitrixMachineCreation\v1.0.0.0.
3. Ejecute `C:\\Program Files\\Common Files\\Citrix\\HCLPlugins\\RegisterPlugins.exe -PluginsRoot "C:\\Program Files\\Common Files\\Citrix\\HCLPlugins\\CitrixMachineCreation\\v1.0.0.0"`.
4. Reinicie los servicios Citrix Host Service, Citrix Broker Service y Citrix Machine Creation Service.
5. Ejecute los siguientes cmdlets de PowerShell para comprobar que el plug-in de Nutanix Acropolis se ha registrado:

```
Add-PSSnapin Citrix*
Get-HypHypervisorPlugin
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Crear una conexión con Nutanix

Consulte Crear un sitio y Conexiones y recursos para obtener información completa sobre todas las páginas de los asistentes que crean conexiones.

En el asistente "Configuración de sitio" o "Agregar conexión y recursos", seleccione el tipo de conexión **Nutanix** en la página **Conexión** y luego especifique la dirección y las credenciales del hipervisor, así como un nombre para la conexión. En la página **Red**, seleccione una red para la unidad de alojamiento.

Crear un catálogo de máquinas mediante una instantánea de Nutanix

Esta información complementa las instrucciones del artículo Crear catálogos de máquinas. Solo describe los campos que son específicos de Nutanix.

La instantánea que seleccione es la plantilla que se usará para crear las máquinas virtuales del catálogo. Antes de crear el catálogo de máquinas, cree las imágenes y las instantáneas en Nutanix.

- Para obtener información acerca de las imágenes maestras en general, consulte el artículo "Crear catálogos de máquinas".
- Para obtener información sobre los procedimientos de Nutanix para la creación de imágenes y las instantáneas, consulte la documentación de Nutanix a la que se hace referencia.

Las páginas **Sistema operativo** y **Administración de máquinas** no contienen información específica de Nutanix. Siga las instrucciones indicadas en el artículo "Crear catálogos de máquinas".

En la página **Contenedor**, que es específica de Nutanix, seleccione el contenedor donde se colocarán los discos de las VM.

En la página **Imagen maestra**, seleccione la instantánea de la imagen. Los nombres de instantánea de Acropolis deben llevar el prefijo "XD_" para usarse en Citrix Virtual Apps and Desktops. Utilice la consola de Acropolis para cambiar el nombre de las instantáneas, si es necesario. Si cambia el nombre de las instantáneas, reinicie el asistente Crear catálogos para ver una lista con los nombres actualizados.

En la página **Máquinas virtuales**, indique la cantidad de unidades CPU virtuales y la cantidad de núcleos por cada CPU virtual.

Las páginas **Tarjetas de red**, **Cuentas de equipo** y **Resumen** no contienen información específica de Nutanix. Siga las instrucciones indicadas en el artículo "Crear catálogos de máquinas".

Entornos de virtualización de Microsoft Azure

December 11, 2018

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> **Nota:**
>
> Este artículo contiene información sobre Azure (Classic). Para obtener información sobre Azure Resource Manager, consulte Entornos de virtualización para Azure Resource Manager.

Configurar conexión

Cuando se utiliza Studio para crear una conexión de Microsoft Azure, se necesita información del archivo de configuración de publicación de Microsoft Azure. La información de ese archivo XML referente a cada suscripción es similar al ejemplo siguiente (el certificado de administración real será mucho más largo):

```
<Subscription
ServiceManagementUrl="\*address\*"
Id="o1455234-0r10-nb93-at53-21zx6b87aabb7p"
Name="Test1"
ManagementCertificate=";alkjdflaksdjfl;akjsdfl;akjsdfl;
   sdjfklasdfilaskjdfkluqweiopruaiopdfaklsdjfjsdilfasdkl;fjerioup" />
```

En el siguiente procedimiento, se presupone que está creando una conexión desde Studio y ha iniciado el asistente para la creación de sitios o el asistente para la creación de conexiones.

1. En un explorador Web, vaya a https://manage.windowsazure.com/publishsettings/index.
2. Descargue el archivo de configuración de publicación.
3. En Studio, en la página **Conexión** del asistente, después de seleccionar el tipo de conexión de Microsoft Azure, haga clic en **Importar**.
4. Si tiene más de una suscripción, se le pedirá que seleccione la suscripción pertinente.

El identificador y el certificado se importan automática y silenciosamente en Studio.

Las acciones de energía que se llevan a cabo mediante una conexión están sujetas a umbrales. Por lo general, los valores predeterminados son adecuados y no se deben cambiar. Sin embargo, puede modificar una conexión y cambiarlos (no puede, en cambio, cambiar estos valores cuando cree la conexión). Para obtener más información, consulte Modificar parámetros de conexión.

Máquinas virtuales

En Studio, al crear un catálogo de máquinas, la selección del tamaño de cada máquina virtual depende de las opciones que presente Studio, el coste y el rendimiento del tipo seleccionado de instancia de VM, además de la escalabilidad.

Studio presenta todas las opciones de instancia de máquina virtual que Microsoft Azure ofrece en una región seleccionada; Citrix no puede modificar esta presentación. Por lo tanto, debe conocer sus apli-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

caciones y sus CPU, su memoria y sus requisitos de E/S. Dispone de varias opciones de rendimiento a precios diferentes; consulte los siguientes artículos de Microsoft para entenderlas mejor.

- Tamaños de máquinas virtuales y el servicio de nube para Azure: https://msdn.microsoft.com/en-us/library/azure/dn197896.aspx
- Precios de máquinas virtuales: http://azure.microsoft.com/en-us/pricing/details/virtual-machines

Nivel Básico: Las máquinas virtuales que tengan como prefijo “Básico” representan el disco básico. Están limitadas principalmente por el nivel 300 de IOPS que respalda Microsoft. Estos parámetros no se recomiendan para cargas de trabajo de SO de escritorio (VDI) o SO de servidor RDSH (host de sesión de Escritorio remoto).

Nivel estándar: Las VM de nivel estándar aparecen en cuatro series: A, D, DS y G.

Serie	Aparecen en Studio como
A	Muy pequeña, pequeña, mediana, grande, muy grande, A5, A6, A7, A8, A9, A10, A11. Las medianas y grandes se recomiendan para pruebas con cargas de trabajo de SO de escritorio (VDI) o SO de servidor (RDSH), respectivamente.
D	Standard_D1, D2, D3, D4, D11, D12, D13, D14. Estas máquinas virtuales ofrecen SSD para almacenamiento temporal.
DS	Standard_DS1, DS2, DS3, DS4, DS11, DS12, DS13, DS14. Estas máquinas virtuales ofrecen almacenamiento de SSD local para todos los discos.
G	Standard_G1 – G5. Estas máquinas virtuales están diseñadas para informática de alto rendimiento.

Al aprovisionar máquinas en el almacenamiento premium de Azure, debe seleccionar un tamaño de máquinas que se admita en la cuenta de almacenamiento premium.

Coste y rendimiento de tipos de instancias de máquinas virtuales

Para obtener la lista de precios de EE. UU., el coste de cada tipo de instancia de máquina virtual por hora está disponible en http://azure.microsoft.com/en-us/pricing/details/virtual-machines/.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Cuando se trabaja con entornos de nube, es importante entender los requisitos informáticos reales. En pruebas de concepto u otras actividades de prueba, puede ser tentador aprovechar los tipos de instancias de máquinas virtuales de alto rendimiento. También puede resultar tentador utilizar las máquinas virtuales de menor rendimiento para ahorrar costes. Sin embargo, el objetivo es usar una máquina virtual apropiada para la tarea en cuestión. Empezar por las de mayor rendimiento puede no darle los resultados que necesita y será muy caro con el tiempo (en algunos casos, en solo siete días). En caso de tipos de instancias de máquinas virtuales de bajo rendimiento con un coste menor, el rendimiento y la usabilidad pueden no ser adecuados para la tarea.

Para cargas de trabajo de SO de escritorio (VDI) o SO de servidor (RDSH), los resultados de las pruebas con LoginVSI y su carga media de trabajo muestran que los tipos de instancia Mediana (A2) y Grande (A3) ofrecen la mejor relación entre precio y rendimiento.

Los tipos de instancia Mediana (A2) y Grande (A3 o A5) representan la mejor relación entre coste y rendimiento para evaluar cargas de trabajo. No se recomienda nada menor. Una serie de máquinas virtuales con mayores capacidades pueden ofrecer a aplicaciones o usuarios el rendimiento y la usabilidad que estos necesiten. Sin embargo, es mejor usar los tres tipos de instancia mencionados como referencia para determinar si el coste más elevado que implica un tipo de instancia de VM con mayores capacidades se traduce en un valor real.

Escalabilidad

Existen varias restricciones que afectan la escalabilidad de catálogos en una unidad de alojamiento. Algunas restricciones, como la cantidad de núcleos de CPU en una suscripción de Azure, se pueden solventar poniéndose en contacto con el servicio de asistencia de Microsoft Azure para aumentar su valor predeterminado (20). Otros, como la cantidad de máquinas virtuales en una red virtual por suscripción (2048), no se pueden cambiar.

Actualmente, Citrix respalda 40 máquinas virtuales en un catálogo.

Para ampliar la cantidad de máquinas virtuales en un catálogo o un host, póngase en contacto con el servicio de asistencia de Microsoft Azure. Los límites predeterminados de Microsoft Azure impiden la ampliación a más de una cantidad determinada de máquinas virtuales; no obstante, este límite cambia con frecuencia. Consulte la información más reciente en: http://azure.microsoft.com/en-us/documentation/articles/azure-subscription-service-limits/.

Una red virtual de Microsoft Azure admite un máximo de 2048 máquinas virtuales.

Microsoft recomienda un límite de 40 imágenes de VM de disco estándar por servicio de nube. A la hora de realizar ampliaciones de escala, tenga en cuenta la cantidad de servicios de nube necesarios para la cantidad de máquinas virtuales de toda la conexión. Asimismo, tenga en mente la cantidad de máquinas virtuales necesarias para proporcionar las aplicaciones alojadas.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Póngase en contacto con el servicio de asistencia de Microsoft Azure para determinar si se deben aumentar las limitaciones predeterminadas de núcleos de CPU para ajustarse a sus cargas de trabajo.

Instalar componentes principales

March 8, 2019

Los componentes principales son el Delivery Controller, Studio, Director, StoreFront y el servidor de licencias.

> **Importante:**
>
> Antes de comenzar una instalación, consulte Antes de instalar. Además, consulte este artículo antes de iniciar una instalación.

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 Instalar mediante 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.

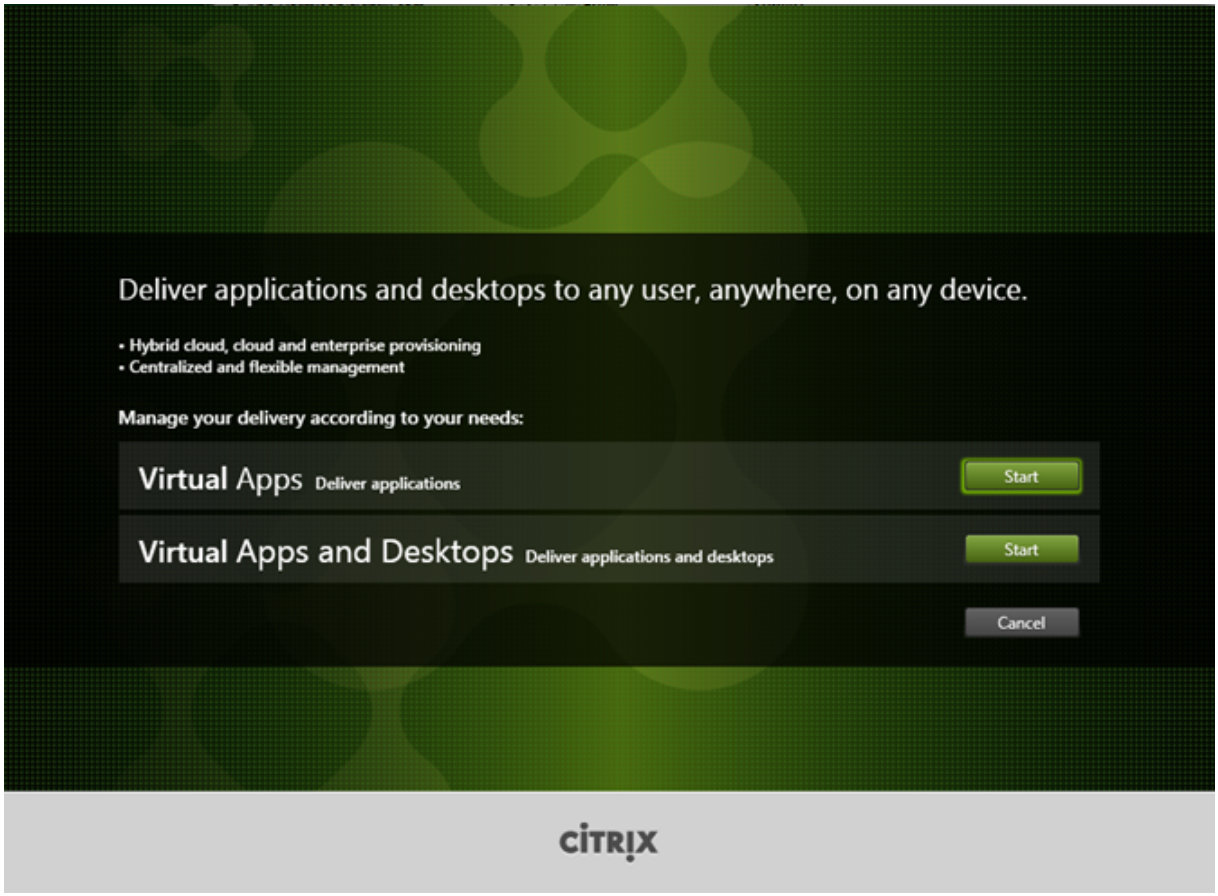
Descomprima el archivo. Si lo desea, puede grabar un DVD del archivo ISO.

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 la imagen ISO. Si el instalador no se inicia automáticamente, haga doble clic en la aplicación **AutoSelect** o la unidad montada.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Paso 2: Elija el producto a instalar



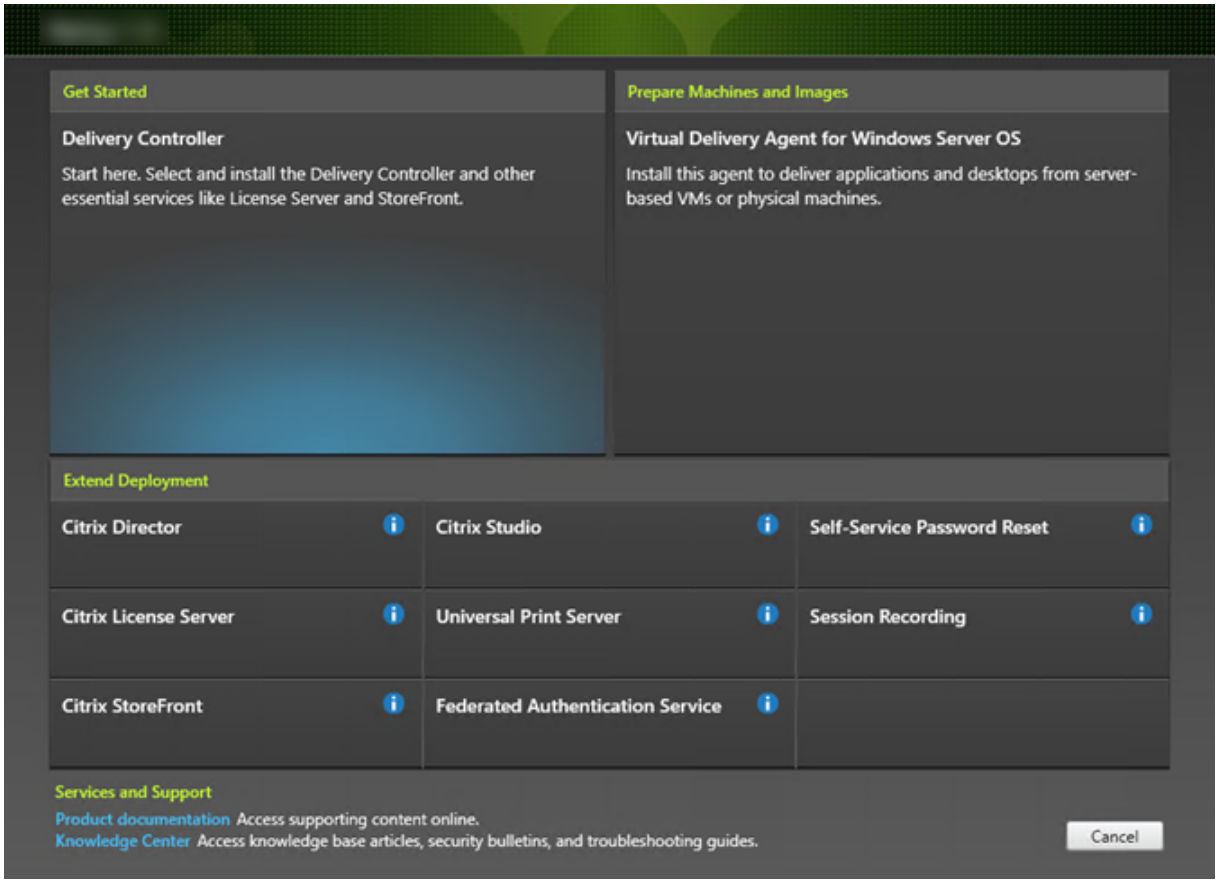
Haga clic en **Iniciar** situado junto al producto a instalar: Virtual Apps o Virtual Apps and Desktops.

(Si la máquina ya tiene instalados componentes de Citrix Virtual Apps and Desktops, esta página no aparecerá.)

Opción de la línea de comandos: /xenapp para instalar Citrix Virtual Apps; se instalan Citrix Virtual Apps and Desktops si se omite la opción

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Paso 3: Elija qué instalar



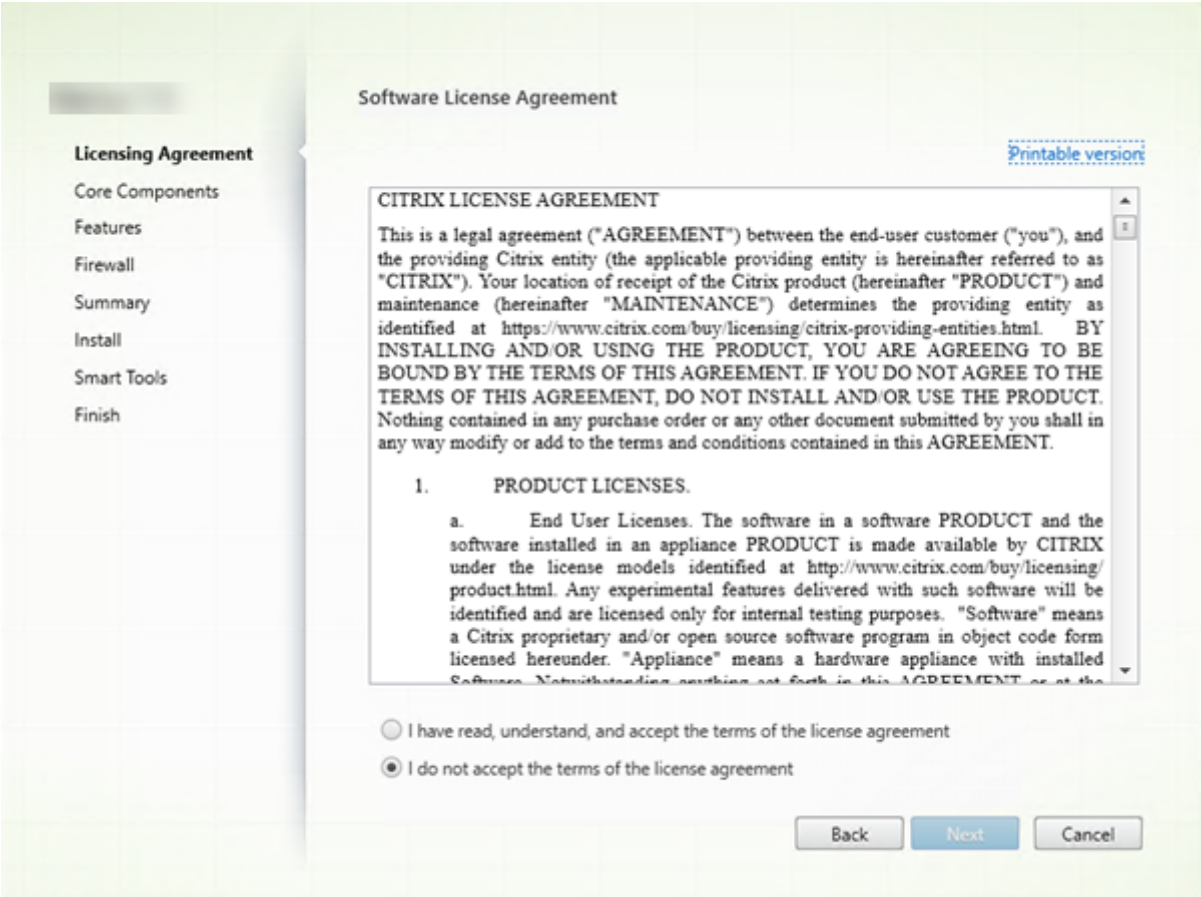
Si acaba de empezar, seleccione **Delivery Controller**. (En una página posterior, seleccionará los componentes concretos que se instalarán en esta máquina.)

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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

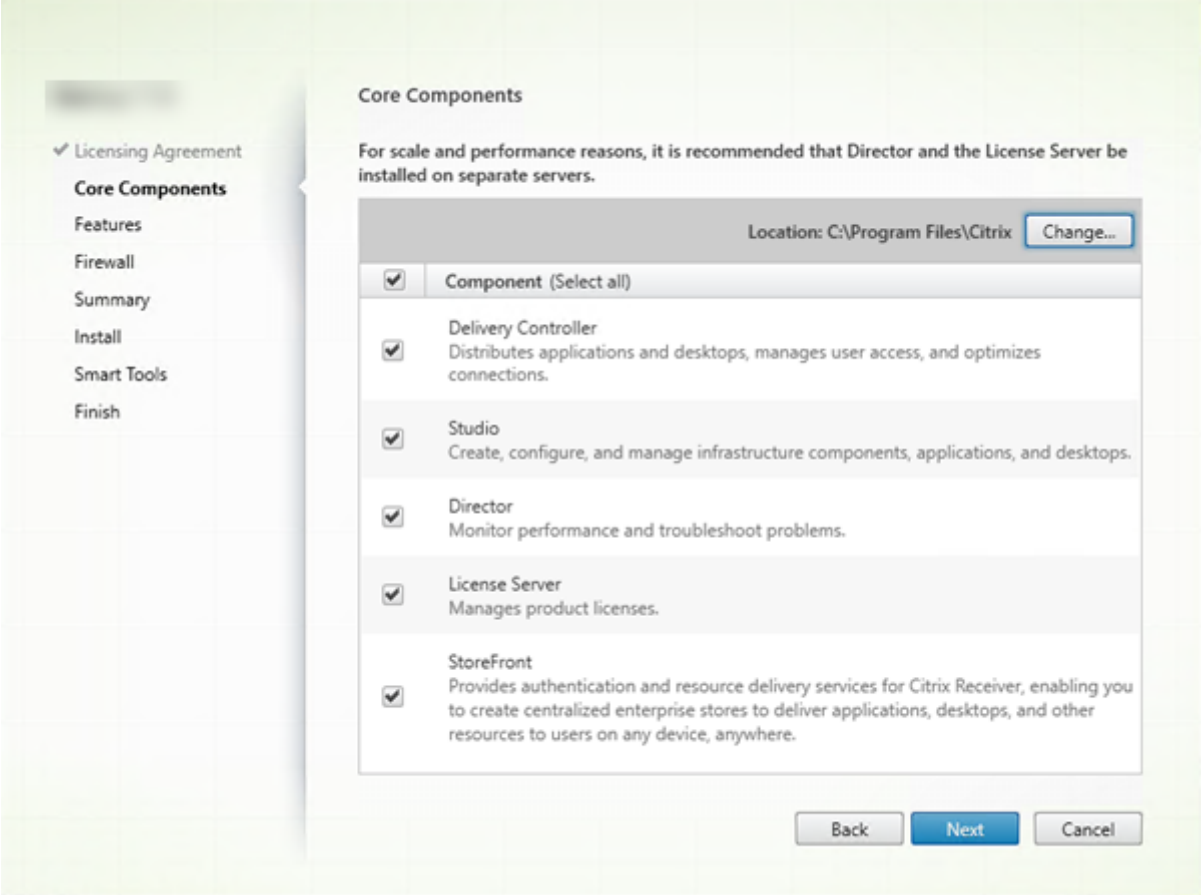
Paso 4: Lea y acepte el contrato de licencia



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**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Paso 5: Seleccione los componentes a instalar y la ubicación de la instalación



En la página **Componentes principales**:

- **Ubicación:** De forma predeterminada, los componentes se instalan en C:\Archivos de programa\Citrix. La opción predeterminada no presenta problemas para la mayoría de las implementaciones. Si indica otra ubicación, esta debe tener permisos de ejecución para el servicio de red.
- **Componentes:** De forma predeterminada, están marcadas las casillas de todos los componentes principales. Instalar todos los componentes principales en un servidor puede servir para pruebas o pruebas de concepto, o bien puede ser útil en implementaciones pequeñas de producción. No obstante, para entornos de producción grandes, Citrix recomienda instalar Director, StoreFront y el servidor de licencias en servidores independientes.

  Indique solo los componentes que quiera instalar en esta máquina. Después de instalar los componentes en esta máquina, podrá ejecutar de nuevo el instalador en otras máquinas para instalar otros componentes.

  Aparecerá un icono para avisarle si decide no instalar un componente principal necesario en esta máquina. Ese aviso le recordará que debe instalar ese componente, aunque no sea nece-

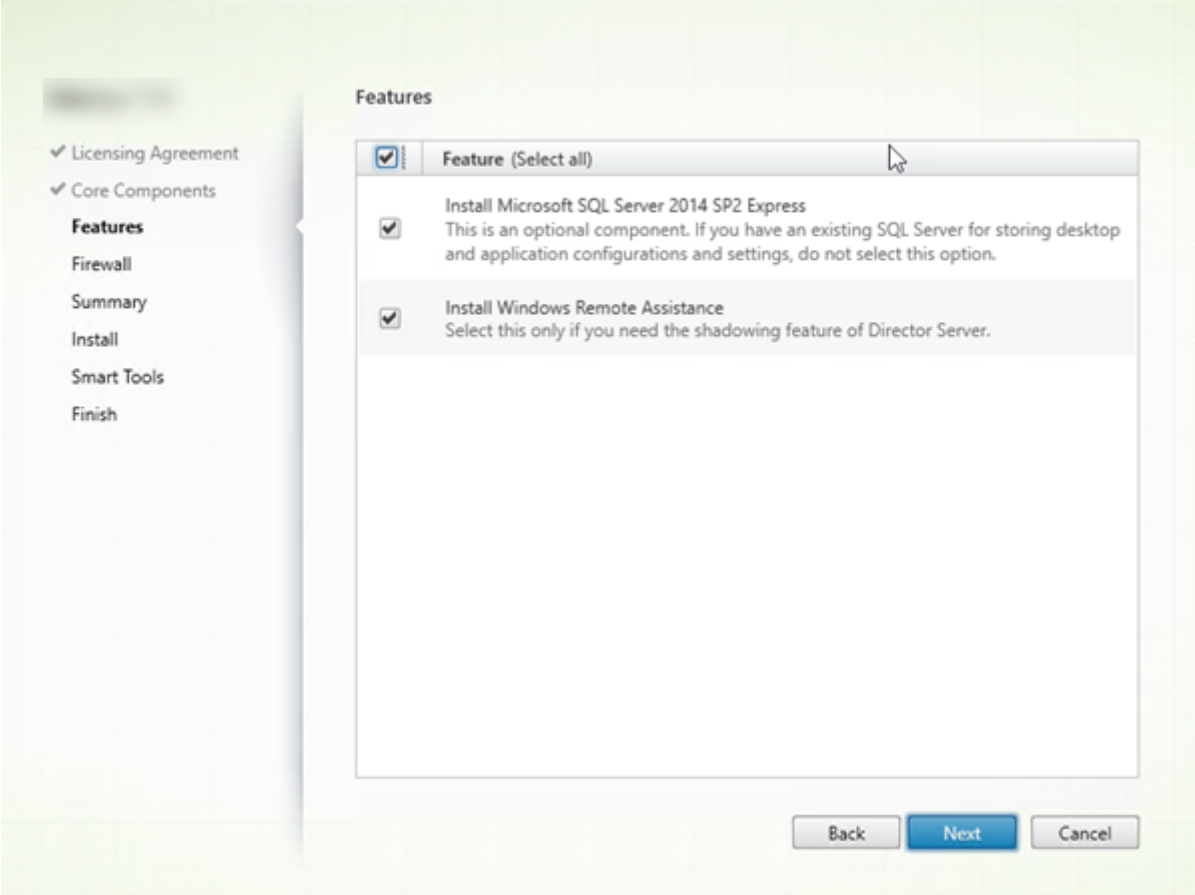
© 1999-2019 Citrix Systems, Inc. All rights reserved.

sariamente en esta máquina.

Haga clic en **Siguiente**.

Opciones de línea de comandos: /installdir, /components, /exclude

Paso 6: Habilite o inhabilite las características



En la página **Características**:

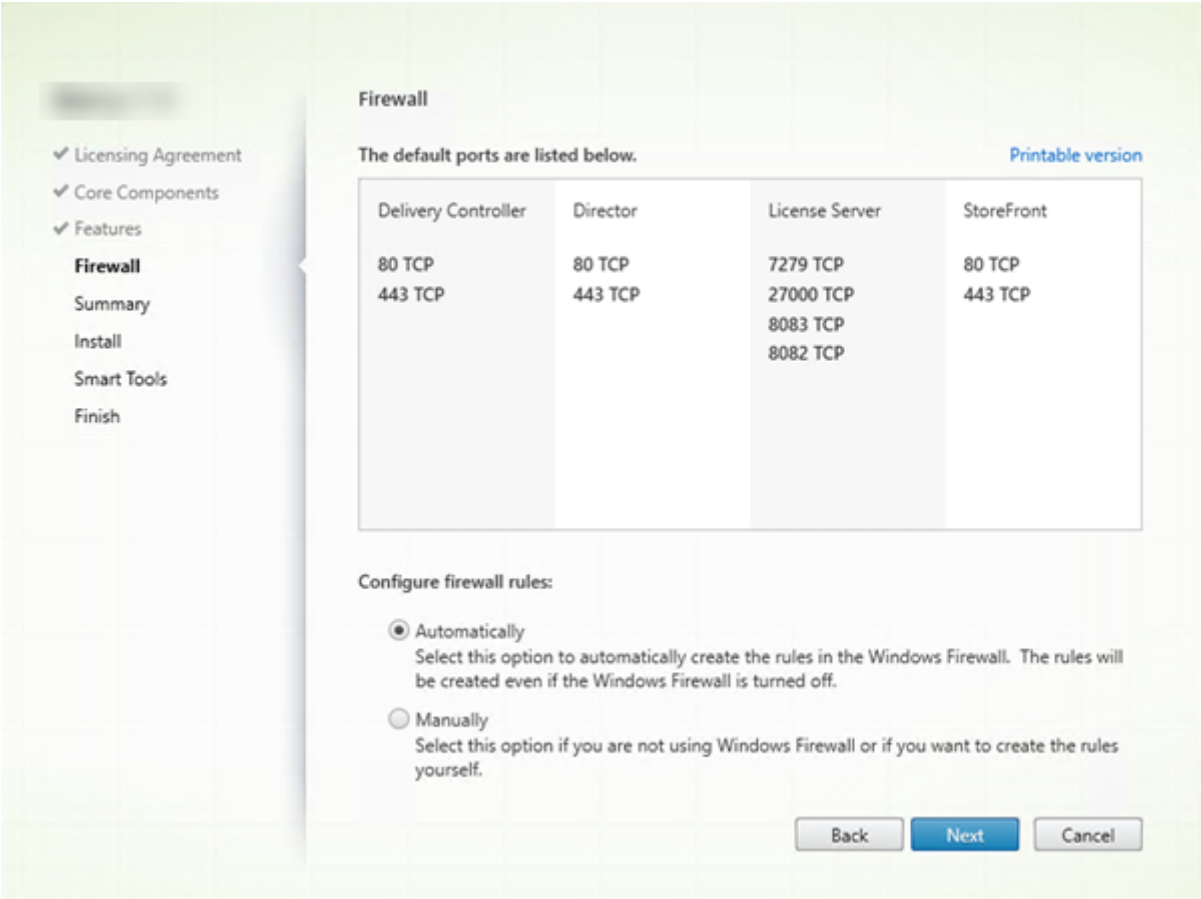
- Seleccione si instalar Microsoft SQL Server Express para usarla como la base de datos del sitio. De forma predeterminada, esta opción está habilitada. Si no conoce las bases de datos de Citrix Virtual Apps and Desktops, consulte Bases de datos.
- Al instalar Director, la Asistencia remota de Windows 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**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Opciones de línea de comandos: /nosql (para impedir la instalación), /no_remote_assistance (para impedir que se habilite)

Paso 7: Abra los puertos del Firewall de Windows



De forma predeterminada, los puertos que aparecen en la página **Firewall** se abren automáticamente si el servicio Firewall de Windows se está ejecutando, incluso aunque el firewall no esté habilitado. La opción predeterminada no presenta problemas para la mayoría de las implementaciones. Para obtener información acerca de los puertos, consulte Puertos de red.

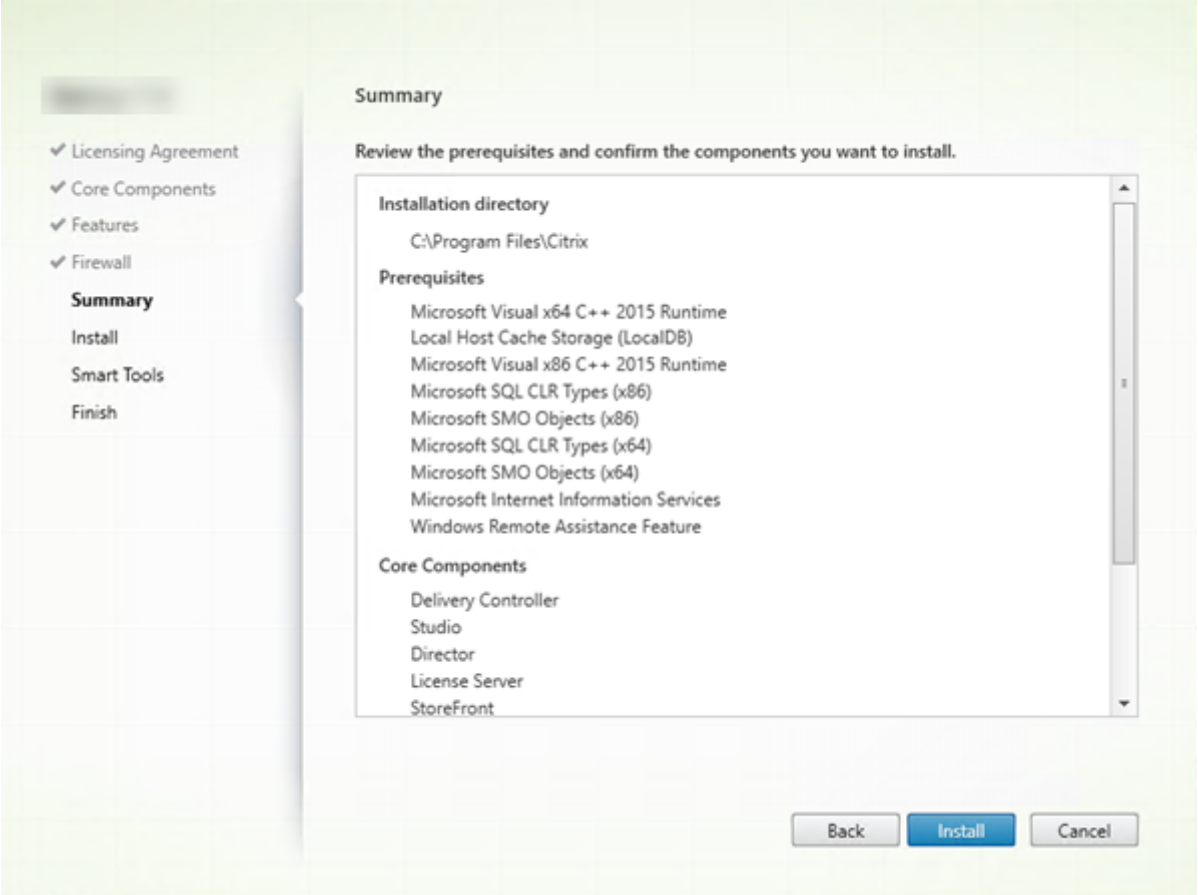
Haga clic en **Siguiente**.

(En el gráfico, se muestran las listas de los puertos que aparecen si se elige instalar todos los componentes principales en esta máquina. Por regla general, este tipo de instalación solo se realiza para las implementaciones de prueba.)

Opción de línea de comandos: /configure_firewall

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Paso 8: Revise los requisitos previos y confirme la instalación

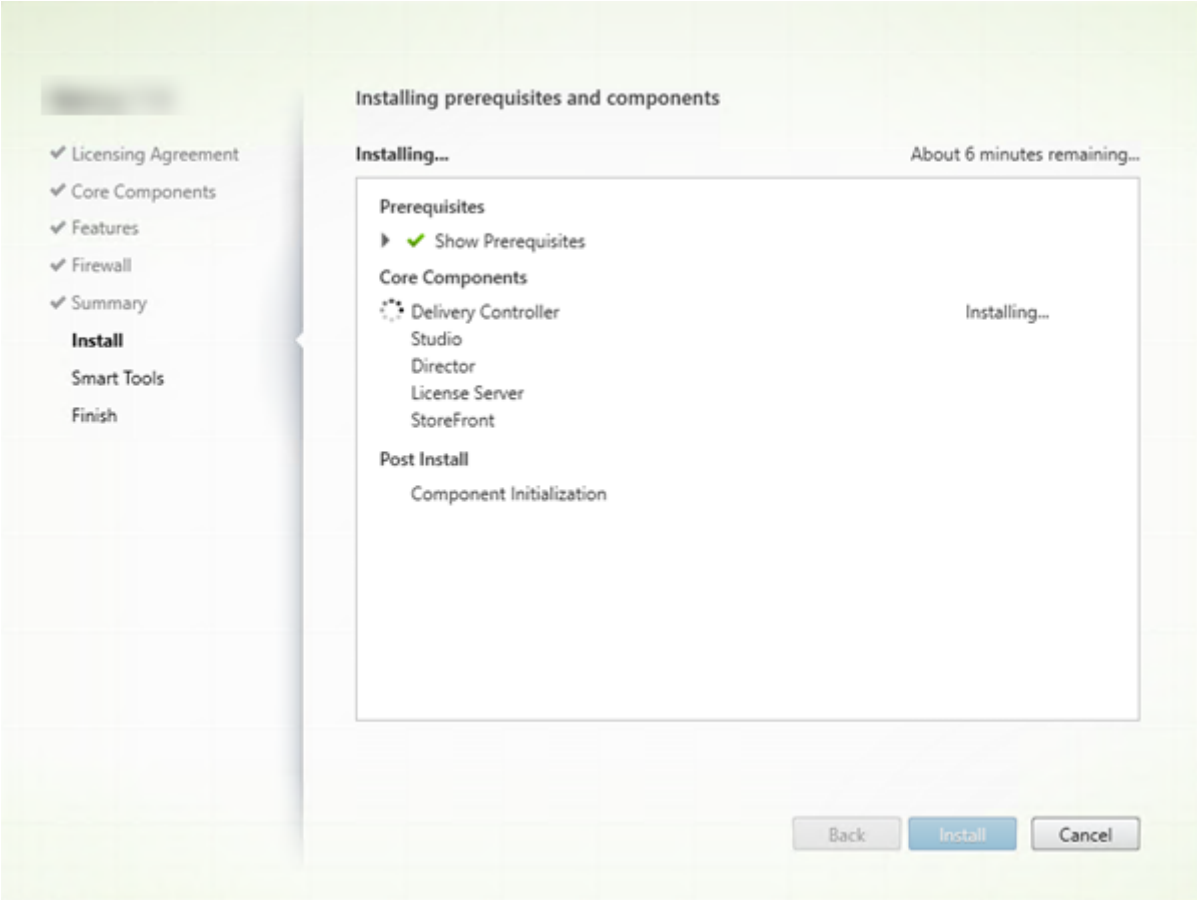


La página **Resumen** muestra lo que se instalará. Si fuera necesario, puede usar el botón Atrás para volver a las páginas anteriores del asistente y cambiar las opciones.

Cuando haya terminado, haga clic en **Instalar**.

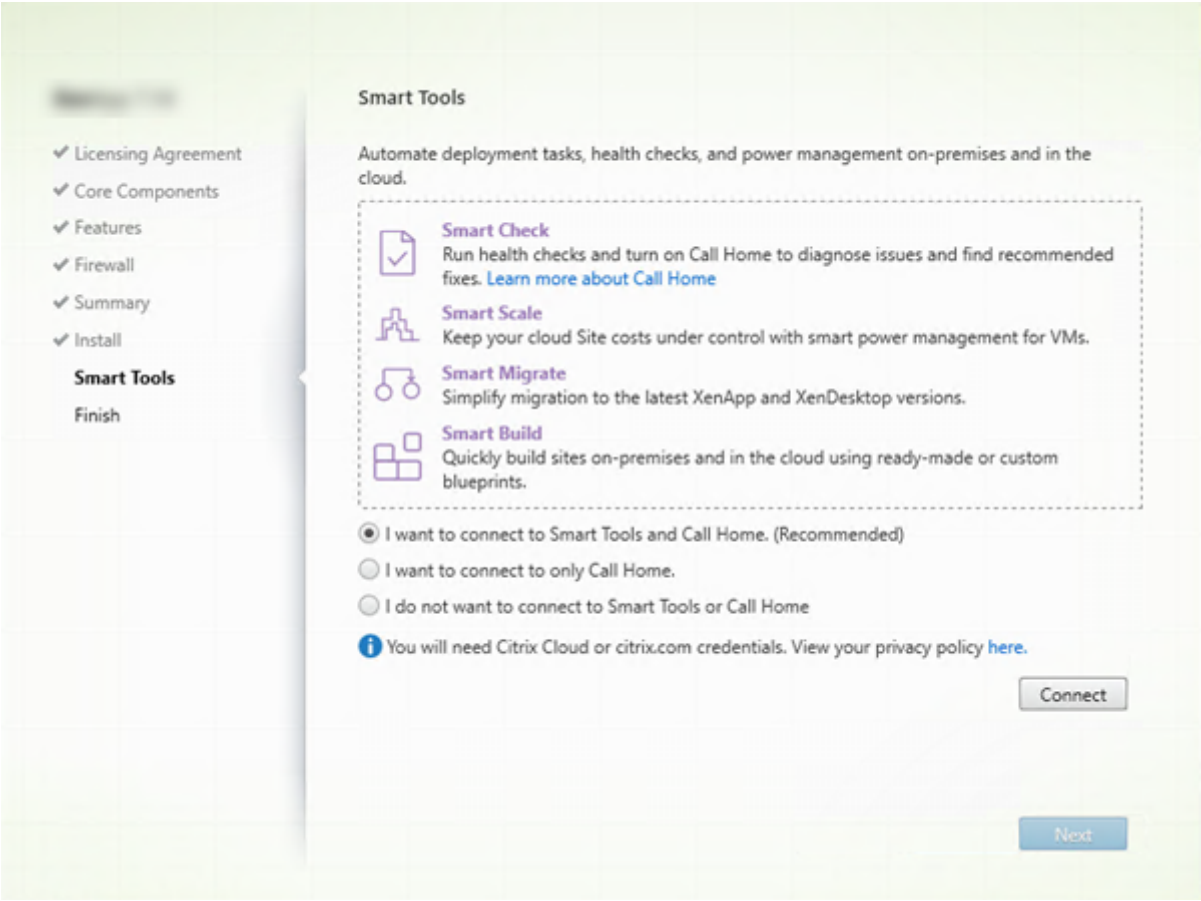
La pantalla muestra el progreso de la instalación.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

Paso 9: Conéctese a Smart Tools y Call Home



Al instalar o actualizar un Delivery Controller, la página del agente de Smart Tools ofrece varias opciones:

- Habilitar conexiones con Smart Tools y Call Home. Ésta es la opción recomendada.
- Habilitar conexiones con Call Home. Durante una actualización, esta opción no aparece si Call Home ya está habilitado o si se produce un error relacionado con el servicio de telemetría de Citrix en el instalador.
- No habilitar conexiones con Smart Tools o Call Home.

Si instala StoreFront (pero no un Controller), el asistente muestra la página **Call Home**, que le permite participar en Call Home. Si instala otros componentes principales (pero no un Controller ni StoreFront), el asistente no mostrará ni la página **Smart Tools** ni **Call Home**.

Si elige una de las opciones que habilitan las conexiones con Smart Tools y/o Call Home:

1. Haga clic en **Conectar**.
2. Proporcione sus credenciales de Citrix o Citrix Cloud.
3. Una vez validadas las credenciales, el proceso descarga un certificado de agente de Smart Tools. Una vez completada la operación, aparece una marca de verificación verde junto al

© 1999-2019 Citrix Systems, Inc. All rights reserved.

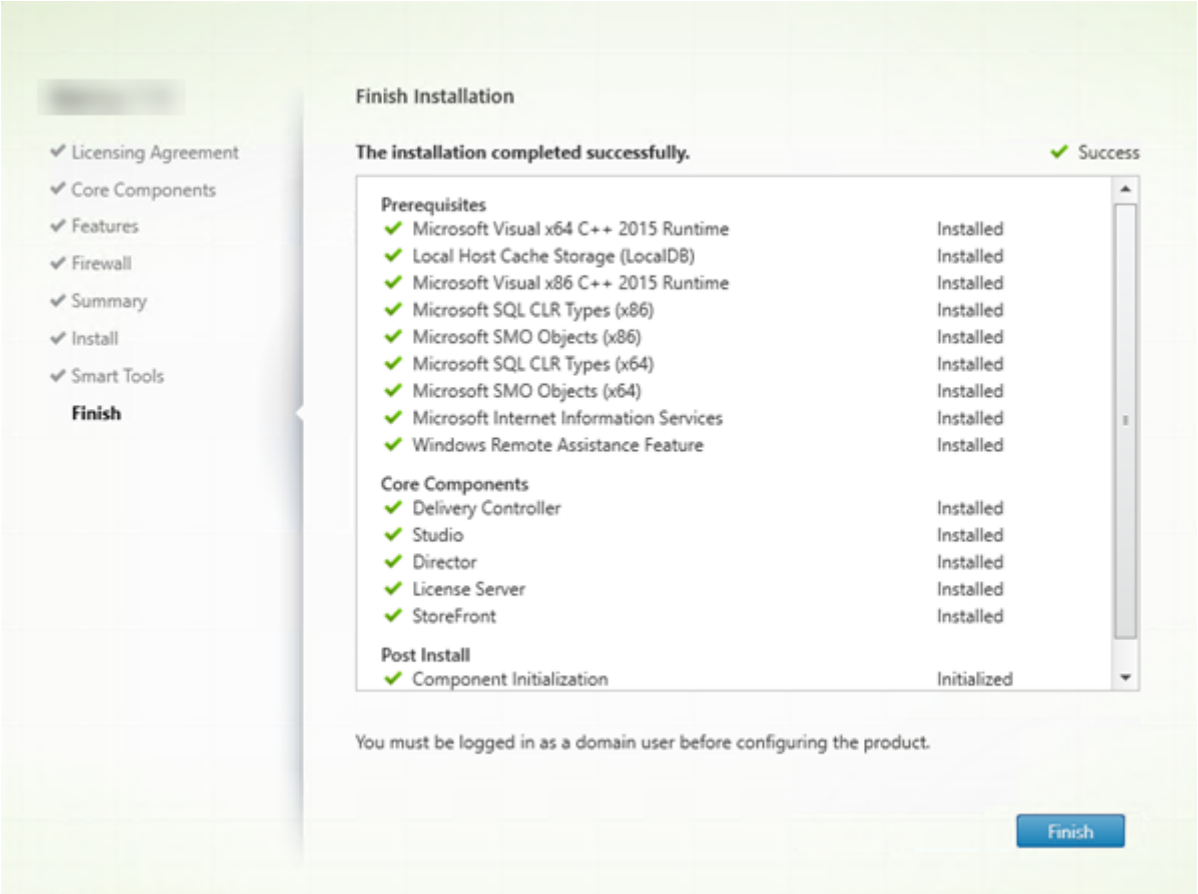
botón **Conectar**. Si ocurre un error durante este proceso, cambie la participación seleccionada (a No quiero…). Puede inscribirse más adelante.

4. Haga clic en **Siguiente** para continuar con el Asistente de instalación.

Si decide no participar, haga clic en **Siguiente**.

Opción de línea de comandos: /exclude “Smart Tools Agent” (para impedir la instalación)

Paso 10: Finalice la instalación



La página **Finalizar** presenta marcas de verificación verdes para todos los requisitos previos y los componentes que se hayan instalado e inicializado correctamente.

Haga clic en **Finish**.

Paso 11: 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 principales. También puede instalar más Controllers en otros servidores.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Siguientes pasos

Después de instalar todos los componentes principales, use Studio para crear un sitio.

Después de crear el sitio, instale agentes VDA.

Puede usar el instalador de producto completo en cualquier momento para ampliar la implementación con los siguientes componentes:

- Componente de servidor Universal Print Server: Inicie el instalador en el servidor de impresión. Seleccione **Universal Print Server** en la sección "Ampliar implementación". Acepte el contrato de licencia y continúe hasta el final del asistente. No hay nada más que especificar o seleccionar. Para instalar este componente desde la línea de comandos, consulte Instalar usando la línea de comandos.
- Servicio de autenticación federada.
- Autoservicio de restablecimiento de contraseñas.
- Grabación de sesiones.

Instalar agentes VDA

March 8, 2019

> Nota:
>
> Puede obtener información sobre los cambios en los nombres de producto aquí.

Existen dos tipos de agentes VDA para máquinas Windows: el agente VDA para SO de servidor y el agente VDA para SO de escritorio. (Para obtener más información acerca de los agentes VDA para máquinas Linux, consulte la documentación de Linux Virtual Delivery Agent.)

> **Importante:**
>
> Antes de comenzar una instalación, consulte Antes de instalar. Por ejemplo, la máquina debe tener las últimas actualizaciones de Windows. Si no están presentes las actualizaciones necesarias (como KB2919355), la instalación falla.

Antes de instalar agentes VDA, debe tener instalados los componentes principales. También puede crear el sitio antes de instalar los agentes VDA.

En este artículo, se describe la secuencia de pasos que se siguen en el asistente de instalación de un VDA. Se ofrecen asimismo los equivalentes de línea de comandos. Para obtener más información, consulte Instalar mediante la línea de comandos.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 desea, puede grabar un DVD del archivo ISO.
2. Use una cuenta de administrador local en la imagen o la máquina donde esté instalando el VDA. Introduzca el DVD en la unidad o monte el archivo ISO. Si el instalador no se inicia automáticamente, haga doble clic en la aplicación **AutoSelect** o la unidad montada.

    Se iniciará el asistente de instalación.

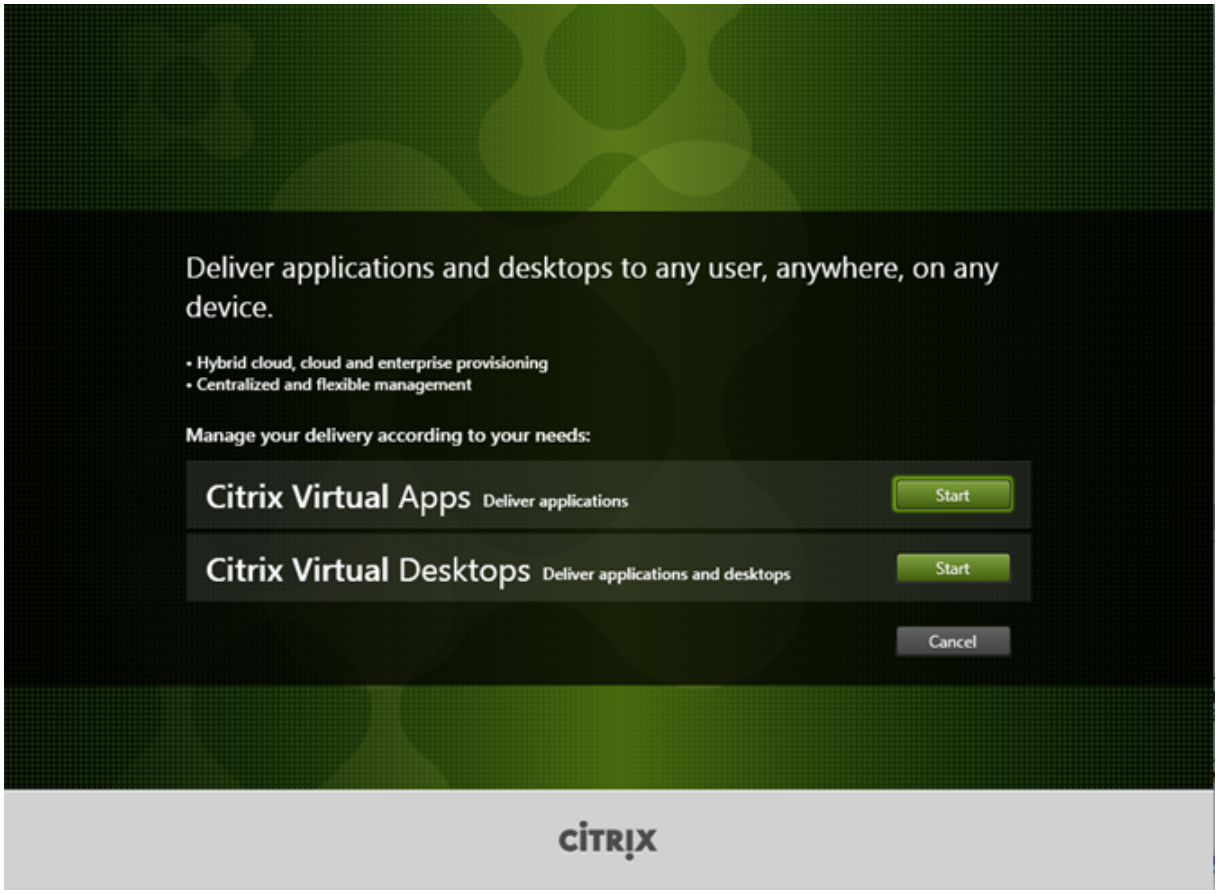
Si usa un paquete independiente:

1. Utilice las credenciales de su cuenta de Citrix para acceder a la página de descargas de Citrix Virtual Apps and Desktops. Descargue el paquete correspondiente:
    - VDAServerSetup.exe: VDA de SO de servidor *versión*
    - VDAWorkstationSetup.exe: VDA de SO de escritorio *versión*
    - VDAWorkstationCoreSetup.exe: VDA de servicios básicos de SO de escritorio *versión*
2. Haga clic con el botón secundario en el paquete que ha descargado y seleccione **Ejecutar como administrador**.

    Se iniciará el asistente de instalación.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Paso 2: Elija el producto a instalar

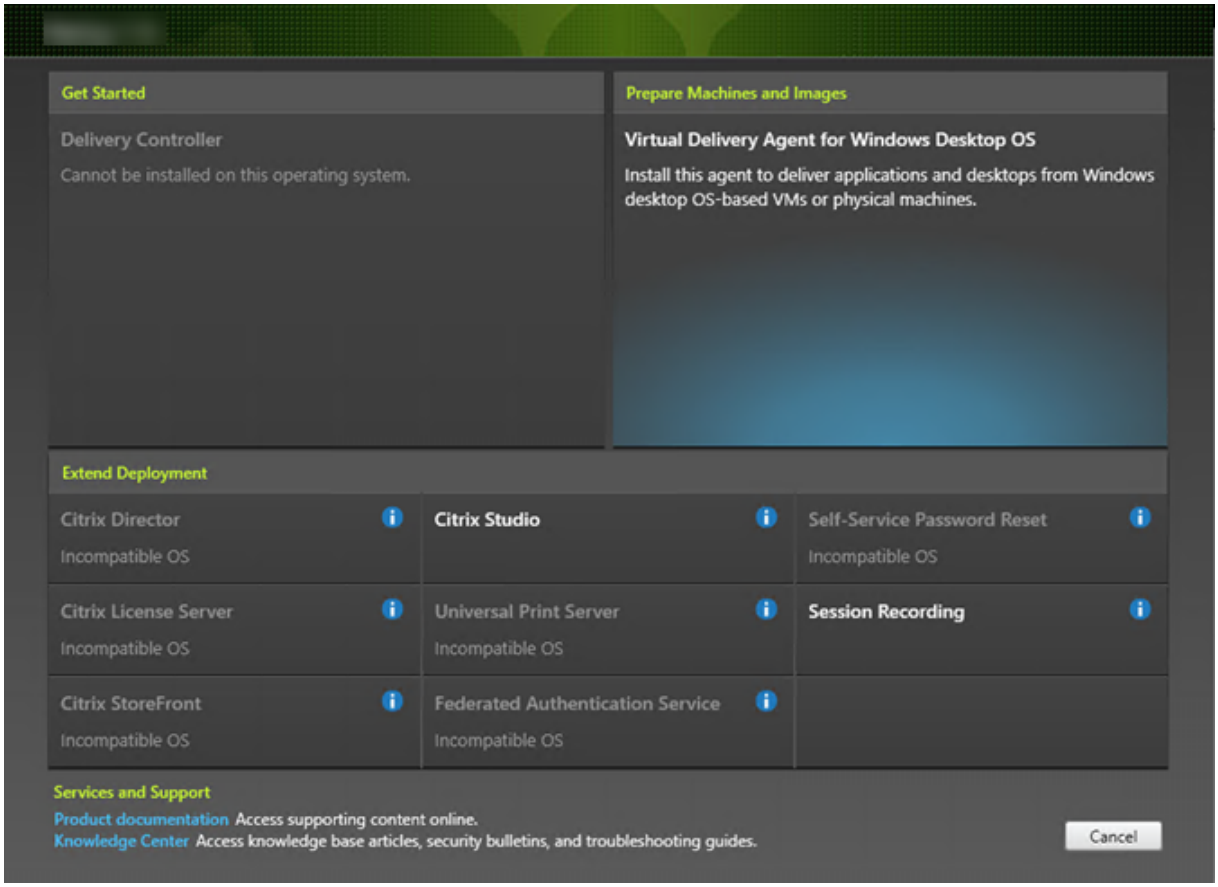


Haga clic en **Iniciar**, situado junto al producto a instalar: Citrix Virtual Apps o Citrix Virtual Desktops. (Si la máquina ya tiene instalados componentes de Citrix Virtual Apps o Citrix Virtual Desktops, esta página no aparecerá.)

Opción de la línea de comandos: /xenapp para instalar Citrix Virtual Apps; se instala Citrix Virtual Desktops si se omite la opción

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Paso 3: Seleccione el VDA



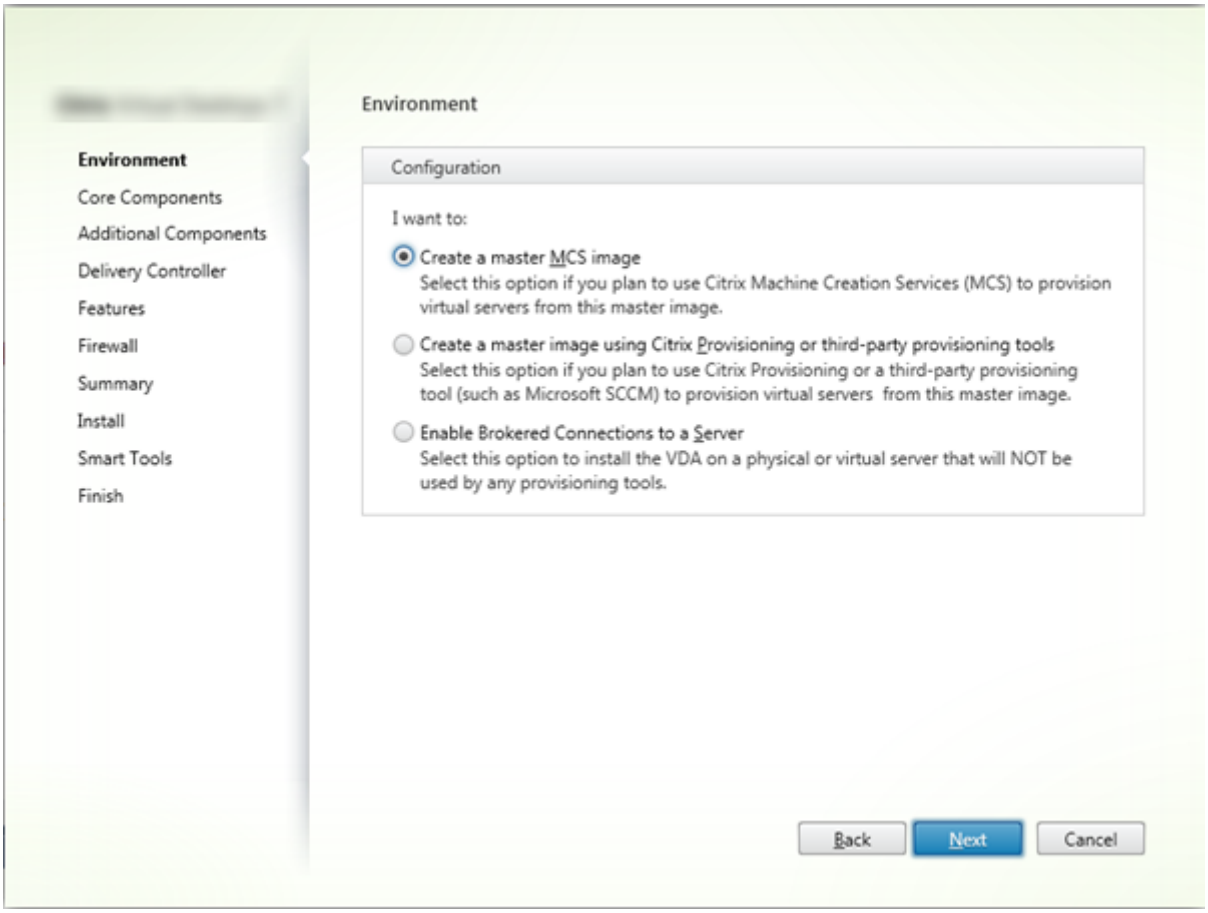
Seleccione la entrada de Virtual Delivery Agent. El instalador detecta si se ejecuta en un SO de escritorio o de servidor, de modo que solo ofrece el tipo de VDA apropiado.

Por ejemplo, si ejecuta el instalador en una máquina Windows 10, se ofrece la opción de VDA para sistema operativo de escritorio. No se ofrece la opción de VDA para sistema operativo de servidor.

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Paso 4: Especifique cómo se usará el VDA



En la página **Entorno**, especifique cómo va a usar el VDA, si usará esta máquina como imagen maestra para aprovisionar máquinas adicionales o no.
La opción que elija afectará a las herramientas de Citrix Provisioning que se instalarán automáticamente (si las hay) y los valores predeterminados en 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 una imagen maestra de VM, si va a usar Machine Creation Services para aprovisionar las máquinas virtuales. Esta es la opción predeterminada. Opción de la línea de comandos: /mastermcsimage o /masterimage
- **Crear una imagen maestra con Citrix Provisioning o herramientas de aprovisionamiento de terceros:** Seleccione esta opción para instalar un VDA en una imagen maestra de VM, si va a usar Citrix Provisioning o herramientas de aprovisionamiento de terceros (como Microsoft System

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Center Configuration Manager) para aprovisionar las máquinas virtuales. Opción de la línea de comandos: /masterpvsimage

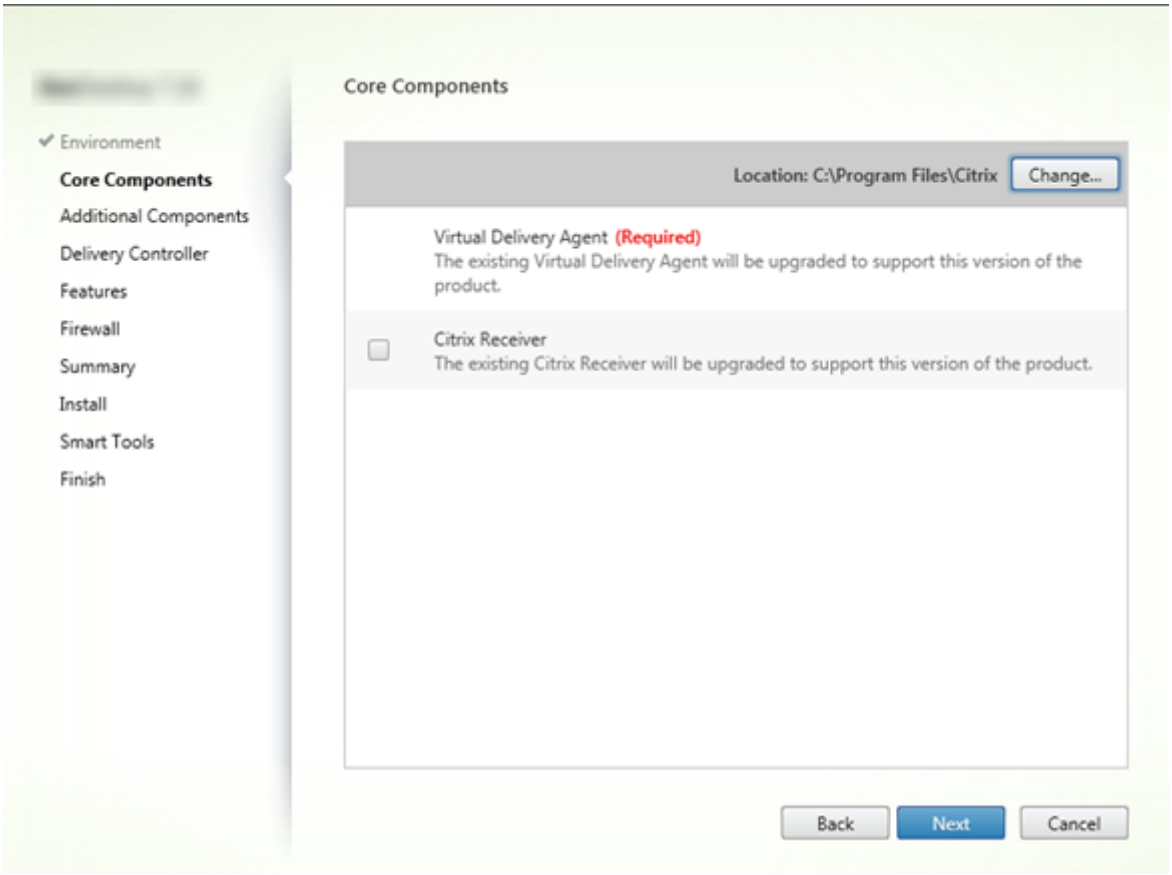
- (Aparece solo en las máquinas con SO de servidor) **Habilitar conexiones de broker con servidores:** Seleccione esta opción para instalar un VDA en una máquina física o virtual que no se utilizará como imagen maestra para aprovisionar otras máquinas. Opciones de la línea de comandos: /remotepc
- (Aparece solo en las máquinas con SO de escritorio) **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. Opciones de la línea de comandos: /remotepc

Haga clic en **Siguiente**.

Esta página no aparecerá:

- Si está actualizando un VDA
- Si está utilizando el instalador VDAWorkstationCoreSetup.exe

Paso 5: Seleccione los componentes a instalar y la ubicación de la instalación



En la página **Componentes principales**:

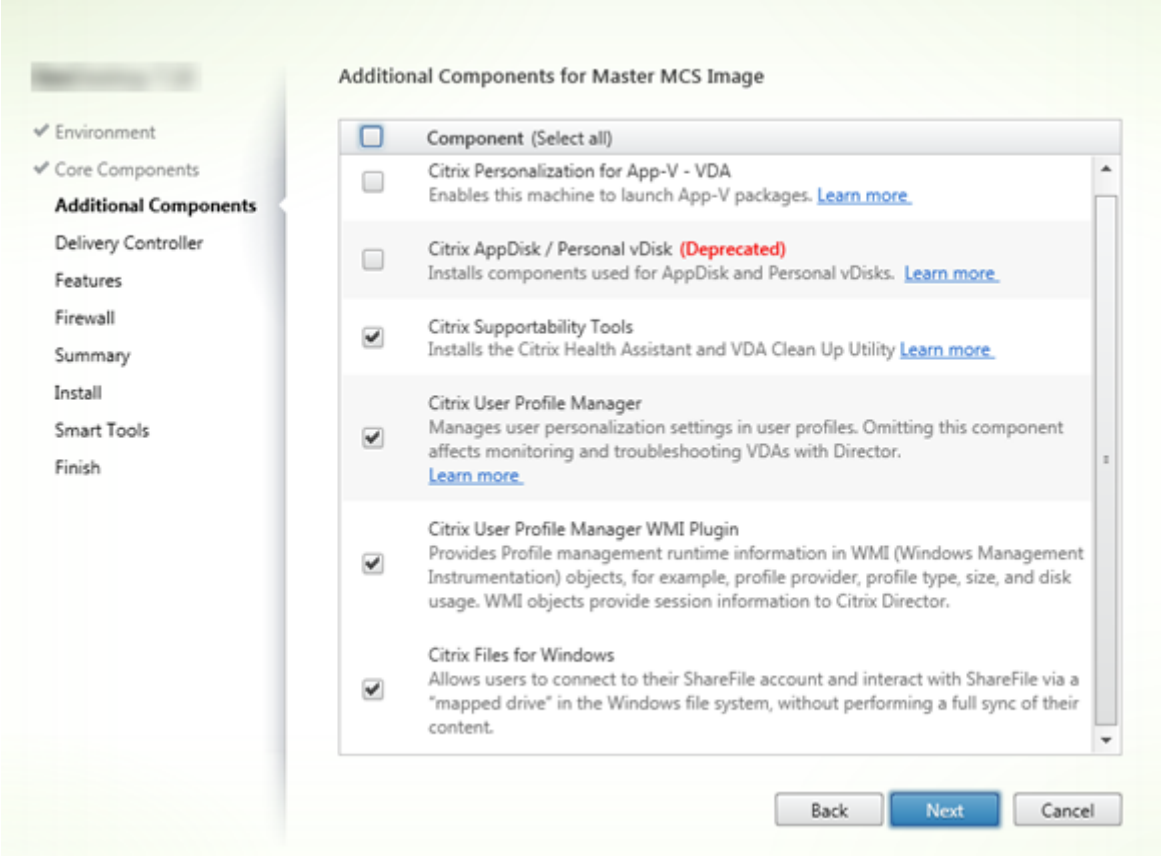
© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Ubicación:** De forma predeterminada, los componentes se instalan en C:\Archivos de programa\Citrix. Esta opción predeterminada no presenta problemas para la mayoría de las implementaciones. Si indica otra ubicación, esta debe tener permisos de ejecución para el servicio de red.
- **Componentes:** De forma predeterminada, no se instala la aplicación Citrix Workspace para Windows con el VDA. Si utiliza el instalador VDAWorkstationCoreSetup.exe, la aplicación Citrix Workspace para Windows no se instala nunca, así que esta casilla no aparece.

Haga clic en **Siguiente**.

Opciones de línea de comandos: /installdir, "/components vda plugin" para instalar el VDA y la aplicación Citrix Workspace para Windows

Paso 6: Instale componentes adicionales



La página **Componentes adicionales** contiene casillas de verificación para habilitar o inhabilitar la instalación de otras funcionalidades y tecnologías con el VDA. En una instalación de línea de comandos, puede usar la opción /exclude o /includeadditional para omitir o incluir expresamente uno o varios de los componentes disponibles.

En la siguiente tabla se indica el parámetro predeterminado de los elementos en esta página. El

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 de servidor) o “Acceso con Remote PC” (para SO de escritorio) seleccionado
Citrix Personalization for App-V	No seleccionado	No seleccionado
Citrix AppDisk o Personal vDisk	No seleccionado	No se muestra porque no es válido para este caso de uso.
Citrix Supportability Tools	Seleccionado	No seleccionado
Citrix User Profile Manager	Seleccionado	No seleccionado
Citrix User Profile Manager WMI Plugin	Seleccionado	No seleccionado
Citrix Files para Windows	No seleccionado	No seleccionado

Esta página no aparecerá si:

- Se usa el instalador VDAWorkstationCoreSetup.exe. Además, las opciones de línea de comandos para los componentes adicionales no son válidas cuando se utilizan junto con ese instalador.
- Actualiza un VDA y todos los componentes adicionales ya están instalados. (Si alguno de los componentes adicionales ya está instalado, la página muestra solo aquellos que no están instalados.)

Marque o desmarque las siguientes casillas de verificación:

- **Personalización de Citrix para App-V:** Instale este componente si va a usar aplicaciones provenientes de paquetes de Microsoft App-V. Para obtener más información, consulte App-V.

  Opción de línea de comandos: /includeadditional “Citrix Personalization for App-V – VDA” para habilitar la instalación del componente, /exclude “Citrix Personalization for App-V – VDA” para impedir la instalación del componente

- **Citrix AppDisk / Personal vDisk:** Estas tecnologías están obsoletas. Válido solamente cuando se instala un VDA para SO de escritorio en una VM. Instala los componentes utilizados para Personal vDisk y AppDisk.

  Opción de línea de comandos: /includeadditional “Personal vDisk” para habilitar la instalación del componente, /exclude “Personal vDisk” para impedir la instalación del componente

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Citrix Supportability Tools:** Instala el MSI que contiene las herramientas de compatibilidad de Citrix, como Citrix Health Assistant.

  Opción de línea de comandos: /includeadditional “Citrix Supportability Tools” para habilitar la instalación del componente, /exclude “Citrix Supportability Tools” para impedir la instalación del componente

- **Citrix User Profile Manager:** Este componente administra los parámetros de personalización de usuario en los perfiles de usuario. Para obtener más detalles, consulte Profile Management.

  Excluir Citrix Profile Management de la instalación afecta a la supervisión y la solución de problemas de los agentes VDA a través de Citrix Cloud. 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 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.

  Opción de línea de comandos: /includeadditional “Citrix User Profile Manager” para habilitar la instalación del componente, /exclude “Citrix User Profile Manager” para impedir la instalación del componente

- **Citrix user Profile Manager WMI Plugin:** Este plug-in ofrece información del tiempo de ejecución de Profile Management en objetos WMI (Windows Management Instrumentation); por ejemplo, el proveedor del perfil, el tipo de perfil, el tamaño y el uso del disco. Los objetos WMI proporcionan información acerca de las sesiones a Citrix Director.

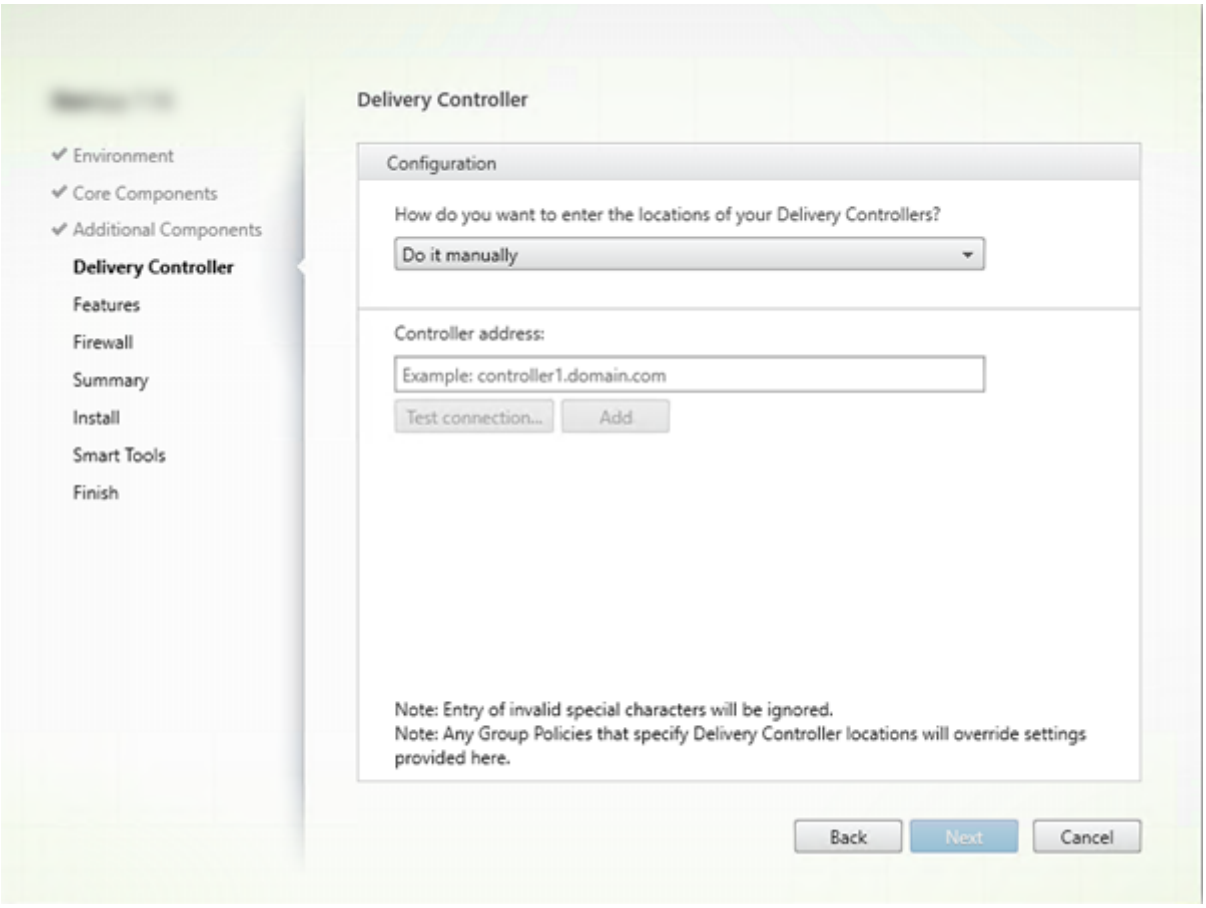
  Opción de línea de comandos: /includeadditional “Citrix User Profile Manager WMI Plugin” para habilitar la instalación del componente, /exclude “Citrix User Profile Manager WMI Plugin” para impedir la instalación del componente

- **Citrix Files para Windows:** Este componente permite a los usuarios conectarse a su cuenta de Citrix Files. Una vez conectados, pueden interactuar con Citrix Files a través de una unidad asignada en el sistema de archivos de Windows (sin requerir una sincronización completa de su contenido).

  Opción de línea de comandos: /includeadditional “Citrix Files for Windows” para habilitar la instalación del componente, /exclude “Citrix Files for Windows” para impedir la instalación del componente

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Paso 7: Direcciones de Delivery Controller



En la página **Delivery Controller**, elija cómo especificar las direcciones de los Controllers instalados. Citrix recomienda especificar las direcciones de los Controllers ahora (“Hacerlo manualmente”), mientras instala el VDA. El VDA no puede registrarse en el Controller sin esta información. Si un VDA no puede registrarse, los usuarios no podrán acceder a las aplicaciones ni a los escritorios que contenga ese VDA.

- **Hacerlo manualmente:** Opción predeterminada. Introduzca el nombre de dominio completo (FQDN) de un Controller instalado y, a continuación, haga clic en **Agregar**. Si ha instalado Controllers adicionales, agregue sus direcciones respectivas.
- **Hacerlo más tarde (Avanzado):** Si elige esta opción, el asistente le solicitará confirmación antes de continuar. Para especificar más adelante esas direcciones, puede volver a ejecutar el instalador más adelante o usar una directiva de grupo de Citrix. El asistente también se lo recordará en la página **Resumen**.
- **Elegir ubicaciones desde Active Directory:** Esta opción es válida solamente cuando la máquina está unida a un dominio y el usuario es un usuario de dominio.
- **Dejar que Machine Creation Services lo haga automáticamente:** Esta opción es válida solamente si utiliza Machine Creation Services (MCS) para aprovisionar máquinas.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

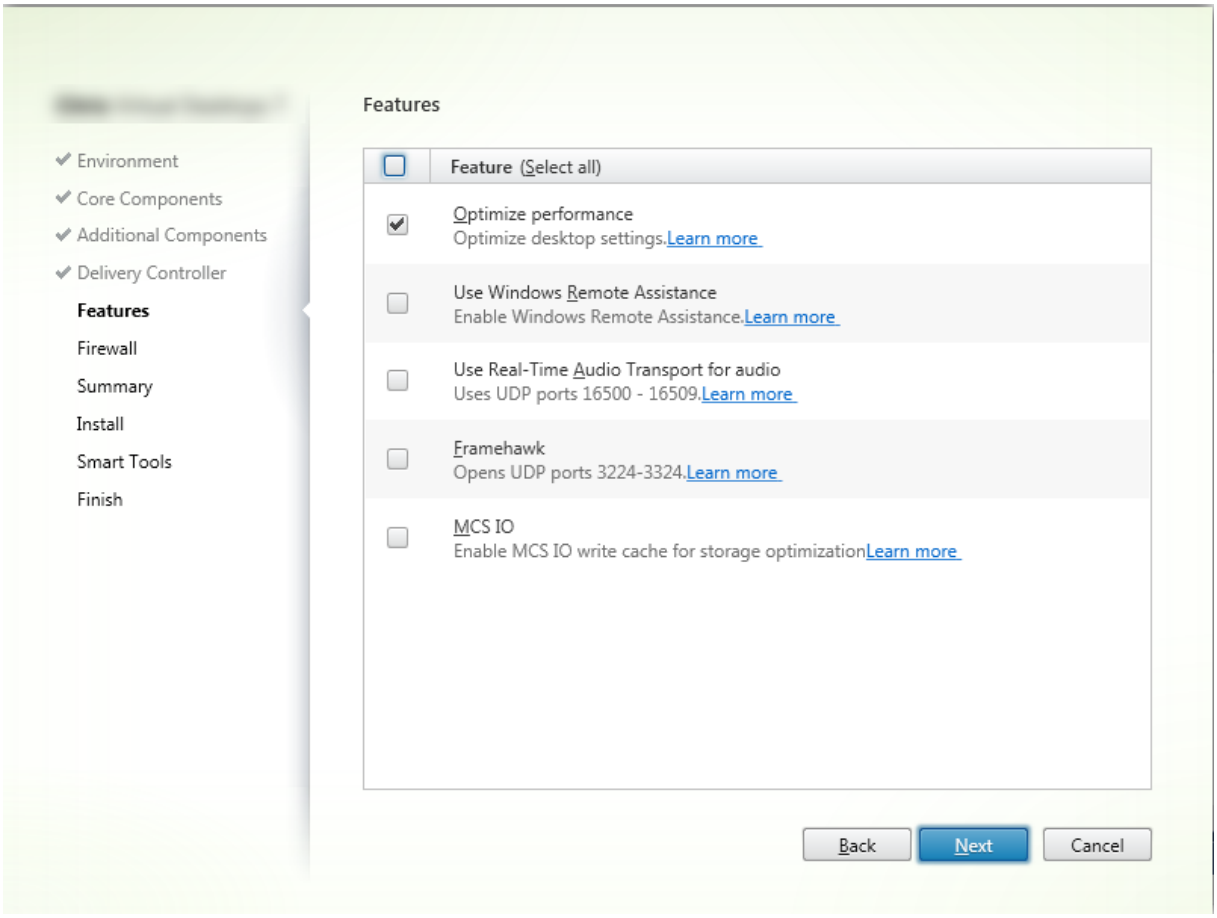
Haga clic en **Siguiente**. Si ha seleccionado la opción “Hacerlo más tarde (avanzado)”, se le pedirá que confirme que especificará las direcciones de Controller más adelante.

Otras consideraciones

- La dirección solo puede contener caracteres alfanuméricos.
- Si especifica direcciones durante la instalación del VDA y en la directiva de grupo, las configuraciones de directiva sobrescribirán las configuraciones que defina durante la instalación.
- Un registro correcto de VDA también requiere que los puertos del firewall que se utilizan para la comunicación con el Controller estén abiertos. Se habilitan de forma predeterminada en la página **Firewall** del asistente.
- Después de especificar las ubicaciones de los Controllers (al instalar el VDA o más adelante), puede usar la funcionalidad de actualización automática para actualizar los VDA cuando se instalen o se quiten Controllers. Para obtener más información sobre cómo los agentes VDA detectan Controllers y se registran en ellos, consulte Registro de VDA.

Opción de línea de comandos: /controllers

Paso 8: Habilite o inhabilite las características



© 1999-2019 Citrix Systems, Inc. All rights reserved.

En la página **Características**, marque o desmarque las casillas de verificación para habilitar o inhabilitar respectivamente las funcionalidades que quiera utilizar.

- **Optimización del rendimiento:** Esta opción solo es válida cuando se instala un VDA en una VM (no en una máquina física). Cuando esta característica está habilitada (opción predeterminada), la herramienta de optimización se usa para los VDA que se ejecutan en una VM que está en un hipervisor. La optimización de VM incluye la inhabilitación de archivos sin conexión, la inhabilitación de la desfragmentación de fondo y la reducción del tamaño del registro de sucesos. Para obtener más información, consulte CTX125874.

  Opción de la línea de comandos: /optimize

  Si utiliza el instalador VDAWorkstationCoreSetup.exe, esta característica no aparecerá en el asistente y la opción de línea de comandos no será válida. Si usa otro instalador en un entorno de acceso con Remote PC, inhabilite esta característica.

- **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 la línea de comandos: /enable_remote_assistance

- **Usar transporte de sonido Real-Time:** Habilite esta característica si en su red se utiliza ampliamente voz sobre IP. Esta característica reduce la latencia y mejora la resistencia del sonido en redes con pérdida. Lo que permite que los datos de sonido se transmitan mediante RTP sobre UDP. Opción inhabilitada de forma predeterminada.

  Opción de la línea de comandos: /enable_real_time_transport

- **Framehawk:** Cuando esta característica está habilitada, se abren los puertos UDP bidireccionales del 3224 al 3324. Opción inhabilitada de forma predeterminada.

  Puede cambiar el intervalo de puertos más tarde con la configuración de directiva de Citrix "Intervalo de puertos del canal de presentación Framehawk". Deberá abrir los puertos del firewall local. Debe haber una ruta de red UDP abierta en cualquiera de los firewalls internos (de VDA a la aplicación Citrix Workspace o de VDA a Citrix Gateway) y externos (de Citrix Gateway a la aplicación Citrix Workspace). Si se implementa Citrix Gateway, los datagramas de Framehawk se cifran mediante el protocolo DTLS (puerto UDP predeterminado: 443). Para obtener más información, consulte Framehawk.

  Opción de la línea de comandos: /enable_framehawk_port

- **AppDisk o Personal vDisk:** Estas tecnologías están obsoletas. Válido solamente cuando se instala un VDA para SO de escritorio en una VM. Esta casilla de verificación está disponible solo si ha marcado la casilla Citrix AppDisk o Personal vDisk en la página **Componentes adicionales**. Si esta casilla de verificación está marcada, se puede usar AppDisks y Personal vDisk.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Opción de la línea de comandos: /baseimage

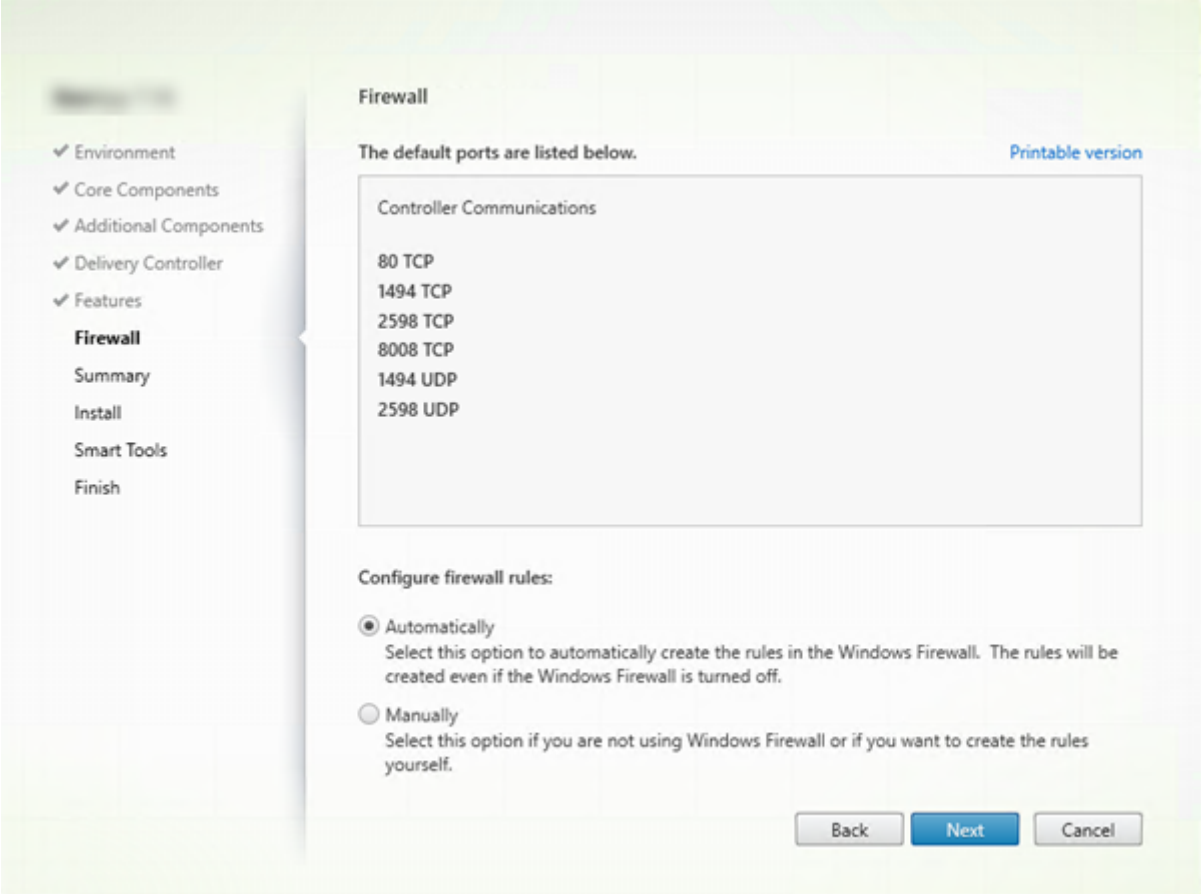
Si utiliza el instalador VDAWorkstationCoreSetup.exe, esta característica no aparecerá en el asistente y la opción de línea de comandos no será válida.

- **E/S de MCS:** Válido solo cuando se usa MCS para aprovisionar las máquinas virtuales. Cuando se selecciona, se instala el controlador de la caché de escritura MCSIO. Para obtener más información, consulte Almacenamiento compartido por los hipervisores y Configurar caché para datos temporales.

  Opción de línea de comandos: /install_mcsio_driver

Haga clic en **Siguiente**.

Paso 9: Puertos de firewall



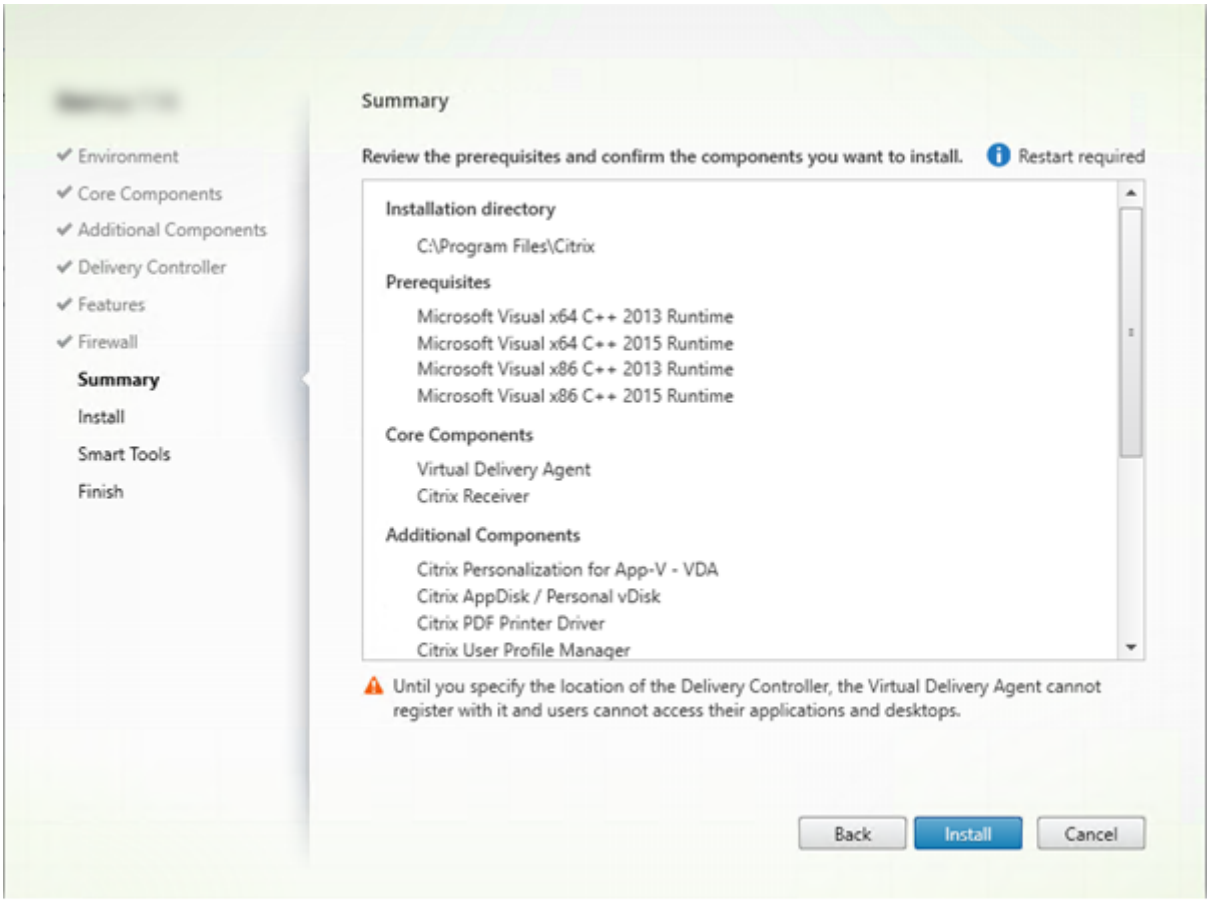
De forma predeterminada, los siguientes puertos se abren automáticamente en la página **Firewall** si el servicio Firewall de Windows se está ejecutando, incluso aunque no esté habilitado. Esta opción predeterminada no presenta problemas para la mayoría de las implementaciones. Para obtener información acerca de los puertos, consulte Puertos de red.

Haga clic en **Siguiente**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Opción de la línea de comandos: /enable_hdx_ports

Paso 10: Revise los requisitos previos y confirme la instalación



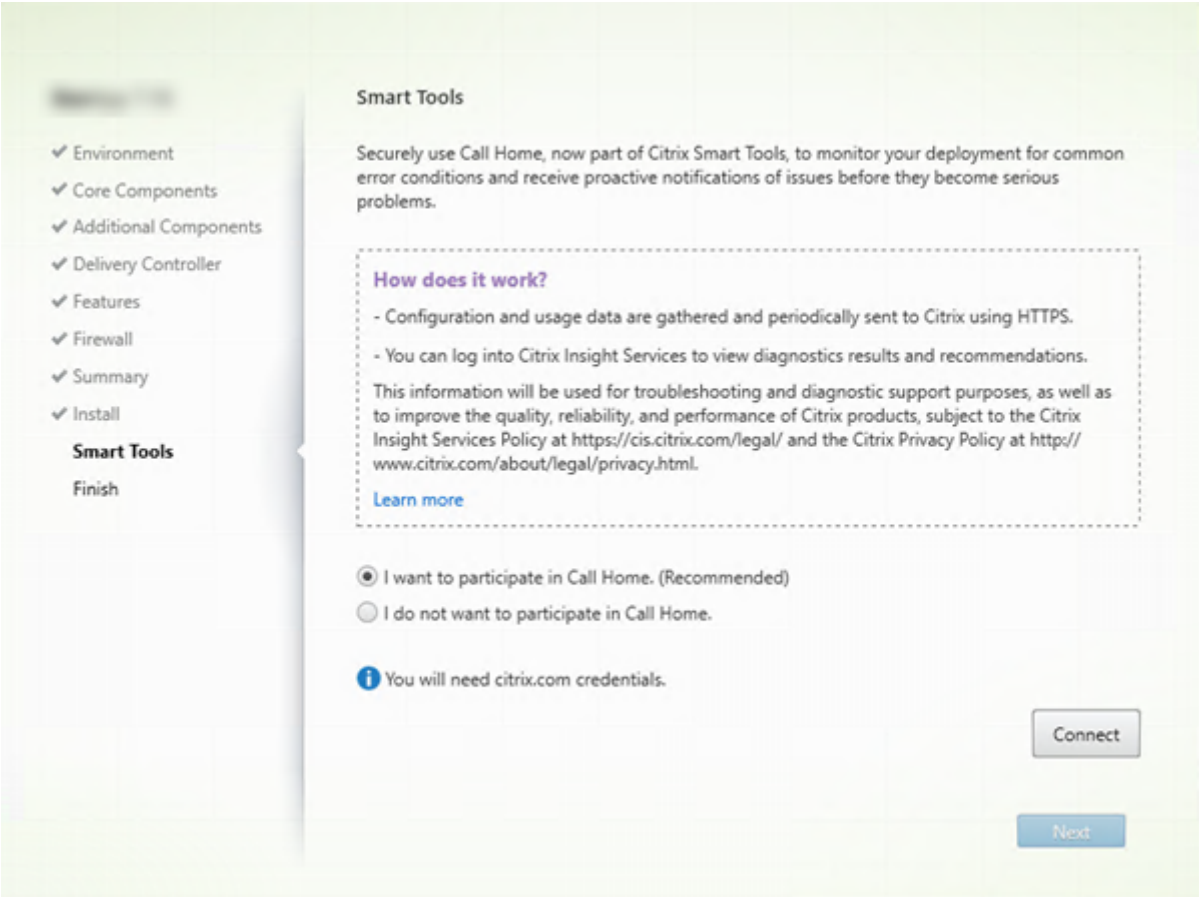
La página **Resumen** muestra lo que se instalará. Puede usar el botón Atrás para volver a las páginas anteriores del asistente y cambiar las opciones.

Cuando haya terminado, haga clic en **Instalar**.

Es posible que la máquina se reinicie una o dos veces si los requisitos previos todavía no están instalados o habilitados. Consulte Antes de instalar.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Paso 11: Participar en Call Home

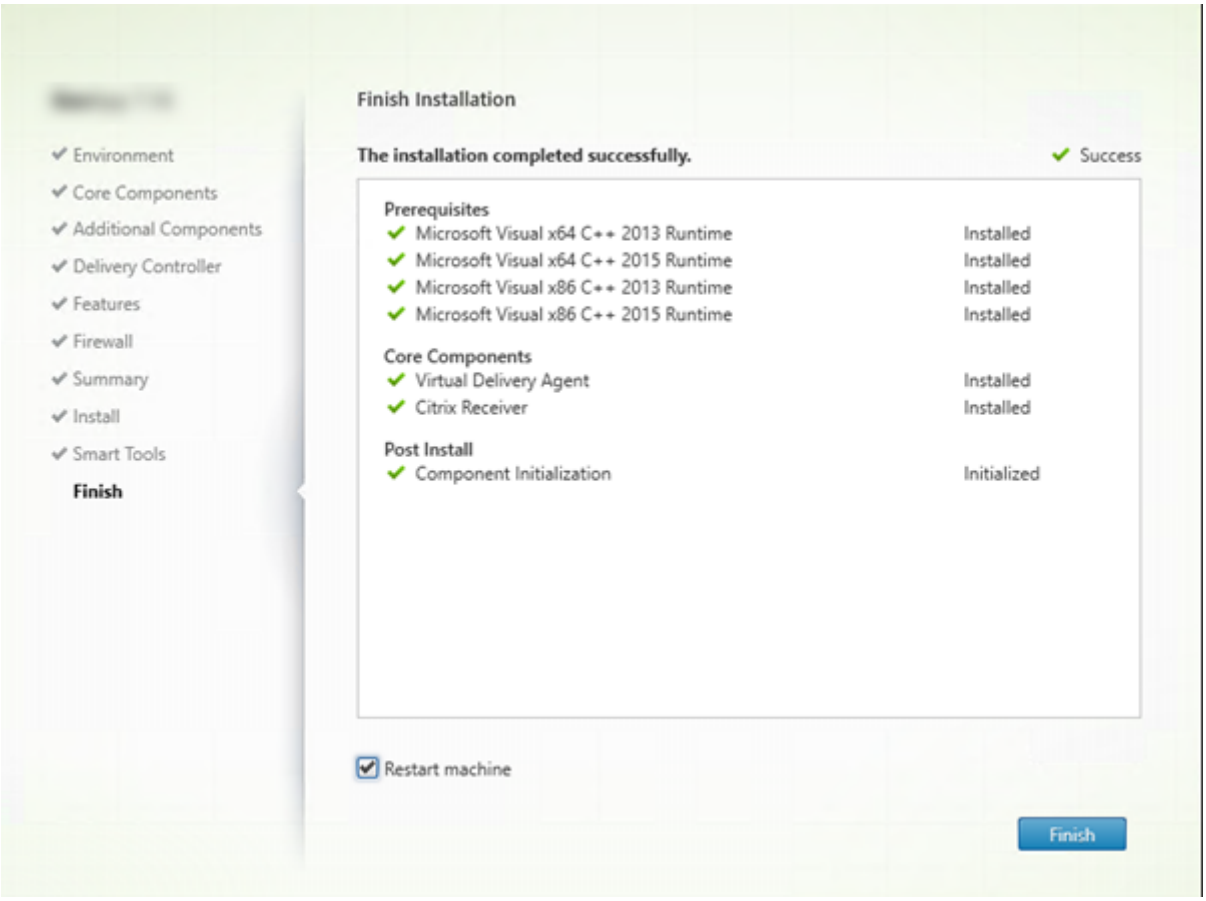


En la página **Smart Tools**, seleccione si quiere participar en Citrix Call Home, que ahora forma parte de Citrix Smart Tools. Si elige participar (opción predeterminada), haga clic en **Conectar**. Cuando se le solicite, introduzca las credenciales de su cuenta de Citrix.

Una vez validadas las credenciales (o si elige no participar), haga clic en **Siguiente**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Paso 12: Finalice la instalación



La página **Finalizar** presenta marcas de verificación verdes para todos los requisitos previos y los componentes que se hayan instalado e inicializado correctamente.

Haga clic en **Finish**. 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Crear grupos de entrega

Personalizar un VDA

Si quiere personalizar un VDA ya instalado:

1. Desde la característica de Windows para quitar o cambiar programas, seleccione **Citrix Virtual Delivery Agent** o **Citrix Remote PC Access/VDA 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 del resultado de la instalación de un componente, consulte Códigos de retorno en la instalación de Citrix.

En Studio, la "versión instalada de VDA" en el panel Detalles referente al grupo de entrega puede no ser la versión real instalada en las máquinas. La pantalla Programas y características de la máquina Windows muestra la versión real del VDA.

Instalar mediante la línea de comandos

March 14, 2019

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 la documentación de Linux Virtual Delivery Agent.

> **Importante:**
>
> 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para complementar el uso de los comandos de instalación directamente, se proporcionan scripts de ejemplo en la imagen ISO del producto. Puede usarlos para instalar, actualizar o quitar máquinas VDA de Active Directory. Para obtener más información, consulte Instalar agentes VDA mediante scripts.

Si intenta instalar (o actualizar) un Windows VDA en un sistema operativo que no admite esta versión del producto, aparece un mensaje que le guiará a la información donde se describen las opciones de que dispone. Esta información también está disponible en Sistemas operativos anteriores.

Para obtener información sobre cómo informa Citrix del resultado de la instalación de un componente, consulte Códigos de retorno en la instalación de Citrix.

Usar el instalador de producto completo

Para acceder a la interfaz de línea de comandos del instalador de producto completo:

1. Descargue el paquete de productos de Citrix. Se necesitan credenciales de cuenta de Citrix para tener acceso al sitio de descargas.
2. Descomprima el archivo. Si lo desea, puede grabar un DVD del archivo ISO.
3. Inicie una sesión en el servidor donde desea instalar los componentes, usando una cuenta de administrador local.
4. Introduzca el DVD en la unidad o monte el ISO archivo.
5. Desde el directorio \x64\XenDesktop Setup de los medios de instalación, ejecute el comando correspondiente.

Para instalar los componentes principales: Ejecute XenDesktopServerSetup.exe con las opciones que aparecen en Opciones de línea de comandos para instalar componentes principales.

Para instalar un VDA: Ejecute XenDesktopVDASetup.exe con las opciones que aparecen en Opciones de línea de comandos para instalar un VDA.

Para instalar el Universal Print Server: Siga las instrucciones indicadas en Instalar Universal Print Server mediante la línea de comandos.

Para instalar el Servicio de autenticación federada: Citrix recomienda usar la interfaz gráfica.

Para instalar el Autoservicio de restablecimiento de contraseñas: Consulte las instrucciones indicadas en Autoservicio de restablecimiento de contraseñas.

Para instalar la Grabación de sesiones: Siga las instrucciones indicadas en Grabación de sesiones.

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**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

1. Descargue el paquete correspondiente de Citrix:
    - Virtual Delivery Agent para sistema operativo de servidor: VDAServerSetup.exe
    - Virtual Delivery Agent para sistema operativo de escritorio: VDAWorkstationSetup.exe
    - Servicios principales de Virtual Delivery Agent para sistema operativo de escritorio: VDAWorkstationCoreSetup.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 instalarlos:
        - Use `/extract` con la ruta de acceso absoluta, por ejemplo `.\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia`. El directorio debe existir. De lo contrario, la extracción falla.
        - A continuación, en un comando aparte, ejecute XenDesktopVdaSetup.exe desde el directorio que contiene el contenido extraído (en el ejemplo anterior, CitrixVDAInstallMedia). Utilice las opciones válidas que aparecen en Opciones de línea de comandos para instalar un VDA.
    - Para ejecutar el paquete descargado, basta con ejecutar su nombre: VDAServerSetup.exe, VDAWorkstationSetup.exe o VDAWorkstationCoreSetup.exe. Utilice las opciones válidas que aparecen en Opciones de línea de comandos para instalar un VDA.

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 componentes principales

Las siguientes opciones son válidas para instalar los componentes principales con el comando XenDesktopServerSetup.exe. Para obtener más información acerca de las opciones, consulte Instalar componentes principales.

- **/components** *componente* [,*componente*] ...

  Lista de los componentes, separados por comas, para instalar o quitar. Los valores válidos son:

    - CONTROLLER: Controller
    - DESKTOPSTUDIO: Studio
    - DESKTOPDIRECTOR: Director
    - LICENSESERVER: Servidor de licencias de Citrix
    - STOREFRONT: StoreFront

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Si se omite esta opción, se instalarán todos los componentes (o se quitarán, si se especifica la opción /remove).

- **/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 Memoria caché del host local. Esta opción no afecta a la instalación o no de SQL Server Express para usarlo como la base de datos del sitio.
  - "Smart Tools Agent": Impide la instalación del agente de Citrix Smart Tools.

- **/help** o **/h**

  Muestra la ayuda del comando.

- **/ignore_site_test_failure**

  Válido solo durante la actualización del Controller. Se ignoran todos los fallos en las pruebas del sitio y la actualización continúa. Si se omite (o se establece en false), una prueba de sitio que haya fallado detiene el instalador, sin realizar la actualización. De forma predeterminada, False.

- **/installdir *directory***

  Directorio vacío existente donde se instalarán los componentes. Valor predeterminado = C:\Archivos de programa\Citrix.

- **/logpath *path***

  Ubicación del archivo de registro. La carpeta especificada debe existir. El instalador no puede crearla. 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **/noreboot**

  Impide que se reinicie el sistema después de la instalación. (Para la mayoría de los componentes principales, el reinicio no está habilitado de forma predeterminada.)

- **/nosql**

  Impide la instalación de Microsoft SQL Server Express en el servidor donde se instala Controller. Si se omite esta opción, se instalará SQL Server Express para usar como la base de datos del sitio. (Esta opción no afecta a la instalación de la LocalDB de SQL Server Express, que se puede utilizar para la Memoria caché del host local.)

- **/quiet** o **/passive**

  No aparece ninguna interfaz de usuario durante la instalación. La única evidencia de que está teniendo lugar el proceso de instalación aparece en el Administrador de tareas de Windows. Si se omite esta opción, se abre la interfaz gráfica.

- **/remove**

  Quita los componentes principales especificados con la opción /components.

- **/removeall**

  Quita todos los componentes principales instalados.

- **/sendexperiencemetrics**

  Envía automáticamente a Citrix los análisis recopilados durante la instalación, la actualización o la eliminación. Si se omite esta opción (o se indica /disableexperiencemetrics), los análisis se recopilan localmente, pero no se envían automáticamente.

- **/tempdir** *directorio*

  Directorio que contiene los archivos temporales durante la instalación. Valor predeterminado = c:\Windows\Temp.

- **/xenapp**

  Instala Citrix Virtual Apps. Si se omite esta opción, se instala Citrix Virtual Apps and Desktops.

Ejemplos de instalación de componentes principales

El siguiente comando instala el Controller de Citrix Virtual Apps and Desktops, Studio, Citrix Licensing y SQL Server Express en un servidor. Los puertos de firewall necesarios para la comunicación entre componentes se abrirán automáticamente.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller,
desktopstudio,licenseserver /configure\\_firewall
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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
```

Opciones de línea de comandos para instalar un VDA

Las siguientes opciones son válidas con uno o más de los comandos: `XenDesktopVDASetup.exe`, `VDAServerSetup.exe`, `VDAWorkstationSetup.exe` o `VDAWorkstationCoreSetup.exe`.

Para obtener más información acerca de las opciones, consulte Instalar agentes VDA.

- **/baseimage**

  Válido solamente cuando se instala un VDA para SO de escritorio en una VM. Habilita el uso de discos Personal vDisk con una imagen maestra. Personal vDisk está obsoleto.

  Esta opción no es válida cuando se usa el instalador VDAWorkstationCoreSetup.exe.

- **/components** *componente*[,*componente*]

  Lista de los componentes, separados por comas, para instalar o quitar. Los valores válidos son:

  - VDA: Virtual Delivery Agent
  - PLUGINS: Aplicación Citrix Workspace para Windows

  Para instalar el VDA y la aplicación Citrix Workspace para Windows, especifique /components vda plugins.

  Si se omite esta opción, solo se instala el VDA (no la aplicación Citrix Workspace).

  Esta opción no es válida cuando se usa el instalador VDAWorkstationCoreSetup.exe. Ese instalador no puede instalar la aplicación Citrix Workspace.

- **/controllers** "*controller* [*controller*]"

  Lista de nombres de dominio completos (FQDN) de Controllers, separados por espacios y entre comillas rectas, con los que se puede comunicar el VDA. No especifique las opciones /site_guid y /controllers a la vez.

- **/disableexperiencemetrics**

  Impide que los análisis recopilados durante la instalación, la actualización o la eliminación se carguen automáticamente en Citrix.

- **/enable_framehawk_port**

  Abre los puertos UDP que usa Framehawk. De forma predeterminada, False.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **/enable_hdx_ports**

  Abre los puertos del Firewall de Windows requeridos por Controller y por las características 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 para comunicarse con el Controller, 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 se requieren para 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 use el VDA para comunicarse con el Controller y las funcionalidades habilitadas, especifique la opción /enable_hdx_ports, además de la opción /enable_hdx_udp_ports.

- **/enable_real_time_transport**

  Habilita o inhabilita el uso de UDP para los paquetes de sonido (Transferencia de sonido en tiempo real para sonido). Habilitar esta función puede mejorar el rendimiento del sonido. 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.

- **/exclude** "*componente*"[,"*componente*"]

  Impide la instalación de uno o varios componentes opcionales, separados por comas y escritos entre comillas rectas. Por ejemplo, instalar o actualizar un VDA en una imagen que no se administra mediante Machine Creation Services no requiere el componente Machine Identity Service. Los valores válidos son:

  - AppDisks VDA Plug-in
  - Personal vDisk
  - Machine Identity Service
  - Citrix User Profile Manager
  - Citrix User Profile Manager WMI Plugin

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Citrix Universal Print Client
- Citrix Telemetry Service
- Citrix Personalization for App-V - VDA
- Citrix Supportability Tools
- Agente de Smart Tools
- Citrix Files para Windows

Excluir Citrix Profile Management de la instalación (con la opción /exclude "Citrix User Profile Manager") afectará a la supervisión y la solución de problemas de los VDA con 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.

Incluso aunque use una solución externa para la administración de perfiles de usuario, Citrix recomienda instalar y ejecutar el servicio Citrix Profile Management. No es necesario habilitar el servicio Citrix Profile Management.

Si va a usar MCS para aprovisionar máquinas virtuales, no excluya Machine Identity Service.

Si especifica /exclude e /includeadditional con el mismo nombre de componente adicional, ese componente no se instala.

Esta opción no es válida cuando se usa el instalador VDAWorkstationCoreSetup.exe. El instalador excluye automáticamente muchos de los elementos.

- **/h** o **/help**

  Muestra la ayuda del comando.

- **/hdxflashv2only**

  Impide la instalación de binarios antiguos de redirección de Flash para mejorar la seguridad.

  Esta opción no está disponible en la interfaz gráfica.

- **/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 componentes adicionales que no están incluidos de manera predeterminada. Los valores válidos son:

  - Personal vDisk
  - Citrix User Profile Manager
  - Citrix User Profile Manager WMI Plugin
  - Citrix Universal Print Client
  - Citrix Telemetry Service
  - Citrix Personalization for App-V - VDA

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Citrix Supportability Tools
- Agente de Smart Tools
- Citrix Files para Windows

Si especifica /exclude e /includeadditional con el mismo nombre de componente adicional, ese componente se excluye de la instalación.

- **/installdir** *directorio*

  Directorio vacío existente donde se instalarán los componentes. Valor predeterminado = C:\Archivos de programa\Citrix.

- **/install_mcsio_driver**

  Habilita la memoria caché de escritura de E/S de MCS para optimizar el almacenamiento.

- **/logpath *path**

  Ubicación del archivo de registro. La carpeta especificada debe existir. El instalador no puede crearla. Predeterminado = "%TEMP%\Citrix\XenDesktop Installer"

  Esta opción no está disponible en la interfaz gráfica.

- **/masterimage**

  Válido solamente cuando se instala un VDA en una VM. Establece el VDA como imagen maestra. Esta opción equivale a /mastermcsimage.

  Esta opción no es válida cuando se usa el instalador VDAWorkstationCoreSetup.exe.

- **/mastermcsimage**

  Especifica que esta máquina se utilizará como imagen maestra con Machine Creation Services para aprovisionar las máquinas virtuales. Esta opción equivale a /masterimage.

- **/masterpvsimage**

  Especifica que esta máquina se utilizará como imagen maestra con Citrix Provisioning o una herramienta de aprovisionamiento de terceros (como Microsoft System Center Configuration Manager) para aprovisionar las máquinas virtuales.

- **/no_mediafoundation_ack**

  Comprueba que Microsoft Media Foundation no está instalado, y algunas funciones de HDX multimedia no se instalarán y no funcionarán. Si se omite esta opción y Media Foundation no está instalado, falla la instalación de VDA. La mayoría de las ediciones Windows admitidas vienen con Microsoft Media Foundation ya instalado, a excepción de las ediciones N.

- **/nodesktopexperience**

  Válido solamente cuando se instala un VDA para SO de servidor. Impide la habilitación de la característica Enhanced Desktop Experience. Esta característica también está controlada por la configuración de directiva de Citrix Enhanced Desktop Experience.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **/noreboot**

  Impide que se reinicie el sistema después de la instalación. El VDA no se puede usar hasta después de reiniciarse.

- **/noresume**

  De forma predeterminada, cuando se necesita reiniciar la máquina durante una instalación, el instalador se reanuda automáticamente después de que se complete el reinicio. Para anular el valor predeterminado, especifique /noresume. Puede ser útil si debe volver a montar el medio o quiere capturar información durante una instalación automatizada.

- **/optimize**

  Válido solamente cuando se instala un VDA en una VM. Habilita la optimización de los agentes VDA que se ejecutan en una VM en un hipervisor. La optimización de VM incluye la inhabilitación de archivos sin conexión, la inhabilitación de la desfragmentación de fondo y la reducción del tamaño del registro de sucesos. No especifique esta opción para implementaciones de acceso con Remote PC. Para obtener más información, consulte CTX125874.

- **/portnumber** *puerto*

  Válido solamente si se especifica la opción /reconfig. Número de puerto para habilitar las comunicaciones entre VDA y Controller. El puerto previamente configurado queda inhabilitado a menos que sea el puerto 80.

- **/quiet** o **/passive**

  No aparece ninguna interfaz de usuario durante la instalación. La única prueba de que está teniendo lugar el proceso de instalación y configuración aparece en el Administrador de tareas de Windows. Si se omite esta opción, se abre la interfaz gráfica.

- **/reconfigure**

  Personaliza los parámetros de VDA configurados anteriormente cuando se usa con las opciones /portnumber, /controllers o /enable_hdx_ports. Si se especifica esta opción sin especificar también la opción /quiet, se abrirá la interfaz gráfica para personalizar VDA.

- **/remotepc**

  Válido solo para implementaciones de acceso con Remote PC (SO de escritorio) o conexiones con broker (SO de servidor). Excluye la instalación de los componentes siguientes en un sistema operativo de escritorio:

  - Citrix Personalization for App-V
  - Citrix User Profile Manager
  - Citrix User Profile Manager WMI Plugin
  - Machine Identity Service
  - Personal vDisk

© 1999-2019 Citrix Systems, Inc. All rights reserved.

  - Citrix Supportability Tools
  - Citrix Files para Windows

  Esta opción no es válida cuando se usa el instalador VDAWorkstationCoreSetup.exe. El instalador excluye la instalación de estos componentes.

- **/remove**

  Quita los componentes especificados con la opción /components.

- **/removeall**

  Quita todos los componentes de VDA instalados.

- **/sendexperiencemetrics**

  Envía automáticamente a Citrix los análisis recopilados durante la instalación, la actualización o la eliminación. Si se omite esta opción (o se indica la opción /disableexperiencemetrics), los análisis se recopilan localmente, pero no se envían automáticamente.

- **/servervdi**

  Instala un VDA para SO de escritorio en un servidor Windows respaldado. Omita esta opción cuando instale un VDA para SO de servidor en un servidor Windows. Antes de usar esta opción, consulte VDI de servidor.

  Esta opción debe usarse solamente con el instalador de VDA completo. Esta opción no está disponible en la interfaz gráfica.

- **/site_guid** *GUID*

  Identificador único global de la unidad organizativa (OU) de Active Directory para el sitio. Esto asocia un escritorio virtual con un sitio cuando se usa Active Directory para el descubrimiento (el método de descubrimiento predeterminado y recomendado es la actualización automática). El GUID del sitio es una de las propiedades del sitio que se muestra en Studio. No especifique las opciones /site_guid y /controllers a la vez.

- **/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 hacen aparecer como equipos físicos.

  Esta opción no está disponible en la interfaz gráfica.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Ejemplos de instalación de un VDA

Instalar un VDA con el instalador de producto completo:

El siguiente comando instala un VDA para SO de escritorio y la aplicación Citrix Workspace en la ubicación predeterminada en una VM. Este VDA se utilizará como imagen maestra y usará MCS para aprovisionar las máquinas virtuales. El VDA se registrará inicialmente en el Controller de un servidor llamado "Contr-Main" en el dominio mydomain. El VDA utilizará la función de optimización y Asistencia remota de Windows.

```
\\x64\\XenDesktop Setup\\XenDesktopVdaSetup.exe /quiet /components vda,
plugins /controllers "Contr-Main.mydomain.local"/enable\\_hdx\\_ports /
optimize /mastermcsimage /enable\\_remote\\_assistance
```

Instalar un VDA de SO de escritorio con el instalador independiente VDAWorkstationCoreSetup:

El siguiente comando instala un VDA con los servicios principales en un SO de escritorio 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 puerto
- /enable_hdx_ports

Instalar Universal Print Server

En cada uno de sus servidores de impresión, instale el siguiente software, en el orden indicado. Este software está disponible en las carpetas especificadas en el medio de instalación completo del producto.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Software	Folder (Carpeta)	Nombre de archivo
Bibliotecas de tiempo de ejecución de Microsoft Visual C++ 2013 (de 32 y 64 bits).	Soporte> VcRedist_2013_RTM	**vcredist_x64.exe** y **vcredist_x86.exe**
Bibliotecas de tiempo de ejecución de Microsoft Visual C++ 2015 (de 32 y 64 bits).	Support > VcRedist_2015	**vc_redist.x64.exe** y **vc_redist.x64.exe**
Citrix Diagnostic Facility	x64> Componentes de escritorio virtual	**cdf_x64.msi**
Componente de servidor de impresión universal (Universal Print Server)	x64 > Universal Print Server	**UpsServer_x64.msi**

Después de instalar el software en los servidores de impresión, configúre el Universal Print Server siguiendo las instrucciones de Aprovisionar impresoras.

Instalar agentes VDA usando scripts

January 22, 2019

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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.

> **Importante:**
>
> Antes de comenzar una instalación, consulte y complete las tareas de Antes de instalar.

Instalar o actualizar agentes VDA usando 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 respaldo de los scripts originales antes de personalizarlos.
2. Edite el script:
   - Especifique la versión del VDA que quiere instalar: `SET DESIREDVERSION`. Por ejemplo, la versión 7 se puede especificar como 7.0. El valor completo se encuentra en los medios de instalación, en el archivo ProductVersion.txt. Sin embargo, no es necesaria una coincidencia completa.
   - Especifique el recurso compartido de red desde donde se invocará al instalador. Indique la raíz de la distribución (el nivel superior del árbol). Cuando se ejecute el script, se invocará automáticamente la versión apropiada del instalador (32 bits o 64 bits). Por ejemplo: `SET DEPLOYSHARE=\\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 Instalar usando 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 sólo 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Eliminar agentes VDA usando 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 respaldo de los scripts originales antes de personalizarlos.
2. Edite el script.
    - Especifique la versión del VDA que quiere quitar: `SET CHECK\\_VDA\\_VERSION`. Por ejemplo, la versión 7 se puede especificar como 7.0. El valor completo se puede encontrar en los medios de instalación, en el archivo ProductVersion.txt (por ejemplo, 7.0.0.3018). Sin embargo, no es necesaria una coincidencia completa.
    - Si lo desea, puede especificar también una ubicación en el recurso compartido de red para guardar los registros centralizados.
3. Mediante la directiva de grupo Scripts de inicio, asigne el script a la unidad organizativa donde se encuentran las máquinas. Esta unidad organizativa debe contener sólo 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_<FechayHora>.log
- VDA_Install_ProcessLog_<FechayHora>.log

Revise el contenido de esos registros para comprobar que el script:

- Se ejecuta según lo previsto.
- Detecta correctamente el sistema operativo de destino.
- Está configurado correctamente para que apunte a la raíz de DEPLOYSHARE (que contiene el archivo AutoSelect.exe).
- Es capaz de autenticarse en los dos puntos compartidos DEPLOYSHARE y LOGSHARE.

Crear un sitio

March 8, 2019

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Un *sitio* es el nombre que se da a una implementación de Citrix Virtual Apps and Desktops. Incluye Delivery Controllers y otros componentes principales, los VDA (Virtual Delivery Agent), las conexiones a hosts (si las hay), además de los catálogos de máquinas y los grupos de entrega. Puede crear el sitio después de instalar los componentes principales, antes de crear el primer catálogo de máquinas y el primer grupo de entrega.

Si el Controller está instalado en Server Core, use los cmdlets de PowerShell en Citrix Virtual Apps and Desktops SDK para crear un sitio.

Cuando se crea un sitio, usted queda inscrito automáticamente en el programa CEIP de mejora de la experiencia del cliente (Citrix Customer Experience Improvement Program). CEIP recopila estadísticas y datos de uso anónimos y, a continuación, los envía a Citrix. El primer paquete de datos se envía a Citrix aproximadamente siete días después de crear el sitio. Puede cambiar su inscripción en cualquier momento después de crear el sitio. Seleccione **Configuración** en el panel de navegación de Studio. A continuación, seleccione la ficha **Asistencia para productos** y siga las instrucciones. Para obtener más información, consulte http://more.citrix.com/XD-CEIP.

El usuario que crea un sitio se convierte en un administrador total; para obtener más información, consulte Administración delegada.

Consulte este artículo antes de crear el sitio, para saber cuál debería ser el procedimiento.

Paso 1: Abra Studio e inicie el Asistente para creación de sitios

Abra Studio, si aún no está abierto. Se le guiará automáticamente a la acción que inicia el Asistente para la creación de sitios. Seleccione esa acción.

Paso 2: Nombre y tipo de sitio

En la página **Introducción**, elija un tipo de sitio:

- **Sitio de entrega de aplicaciones y escritorios**. Cuando crea un sitio de entrega de aplicaciones y escritorios, también puede decidir si crear un sitio de implementación completa (recomendado) o un sitio vacío. Un sitio vacío solo está configurado parcialmente y son los usuarios avanzados los que suelen crearlo.
- **Sitio de acceso con Remote PC**. Un sitio de acceso con Remote PC permite a usuarios designados acceder a sus equipos de oficina de forma remota a través de una conexión segura.

Si crea ahora una implementación de entrega de aplicaciones y escritorios, puede agregar más adelante una implementación de acceso con Remote PC. De igual manera, si ahora crea una implementación de acceso con Remote PC, puede agregar más adelante una implementación completa.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Escriba un nombre para el sitio. Una vez creado el sitio, aparece el nombre de este en la parte superior del panel de navegación de Studio: **Citrix Studio** (*nombre del sitio*).

Paso 3: Bases de datos

La página **Bases de datos** contiene selecciones para configurar la base de datos del sitio, la base de datos de supervisión y la base de datos de registros de configuración. Para obtener más información acerca las opciones y los requisitos de configuración de las bases de datos, consulte Bases de datos.

Si instala SQL Server Express para usarlo como la base de datos del sitio, se producirá un reinicio después de la instalación de ese software. Ese reinicio no se producirá si no instala el software SQL Server Express para usarlo como la base de datos del sitio.

Si no utiliza el software SQL Server Express predeterminado, compruebe que el software de SQL Server está instalado en las máquinas antes de crear el sitio. En Requisitos del sistema, se ofrece una lista de las versiones respaldadas.

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**, indique si usar las licencias existentes o la prueba gratuita de 30 días, que permite agregar archivos de licencia más adelante. Puede agregar o descargar los archivos de licencias desde el asistente para la creación de sitios. Para obtener información más detallada, consulte la documentación de Licencias.

Especifique la dirección del servidor de licencias en el formato *nombre*:[*puerto*]. El nombre debe ser FQDN, NetBIOS o una dirección IP. Se recomienda FQDN. Si se omite el número de puerto, el predeterminado es 27000.

Haga clic en **Conectar**. No se puede pasar a la siguiente página hasta que se establezca una conexión con el servidor de licencias.

Paso 5: Administración de energía (solo para acceso con Remote PC)

Consulte el paso 8. Acceso con Remote PC

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Paso 6: Conexión de host, red y almacenamiento

Si utiliza máquinas virtuales en un hipervisor o servicio de nube para entregar aplicaciones y escritorios, tiene la opción de crear la primera conexión con el host. También puede especificar los recursos de red y almacenamiento para esa conexión. Después de crear el sitio, puede modificar esa conexión y esos recursos; también puede crear más conexiones. Para obtener más información, consulte Conexiones y recursos.

- Para conocer la información que se especifica en la página **Conexión**, consulte Conexiones y recursos.
  - Si no usa máquinas virtuales alojadas en hipervisores ni servicios de nube (o si usa Studio para administrar escritorios alojados en máquinas blade dedicadas), seleccione el tipo de conexión **Ninguno**.
  - Si configura un sitio de acceso con Remote PC y quiere utilizar la función Wake on LAN, seleccione el tipo **Microsoft System Center Configuration Manager**.

  Además del tipo de conexión, especifique si usará las herramientas de Citrix (como Machine Creation Services) u otras herramientas para crear las máquinas virtuales.
- Para conocer la información que se especifica en las páginas **Almacenamiento** y **Red**, consulte Almacenamiento de host, Administrar almacenamiento y Seleccionar almacenamiento.

Paso 7: Características adicionales

En la página **Características adicionales**, puede seleccionar características para personalizar su sitio. Cuando se marca la casilla de verificación de un elemento que requiere información, aparece un cuadro de configuración.

- **Integración de AppDNA:** (Esta característica está obsoleta.) Si usa AppDisks y tiene instalado AppDNA. La integración con AppDNA permite analizar las aplicaciones que contienen los AppDisks. Con esos análisis, puede ver si hay problemas de compatibilidad y llevar a cabo acciones para resolverlos.
- **Publicación App-V:** Seleccione esta funcionalidad si quiere usar aplicaciones de paquetes de Microsoft App-V que se encuentran en servidores App-V. Facilite la URL del servidor de administración de App-V, así como la URL y el número de puerto del servidor de publicación de App-V.

  Si quiere usar aplicaciones procedentes de paquetes de App-V solo en recursos compartidos de red, no es necesario seleccionar esta funcionalidad.

  También puede habilitar, inhabilitar o configurar esta funcionalidad más adelante en Studio. Para obtener más información, consulte App-V.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Paso 8: Acceso con Remote PC

Para obtener información acerca de implementaciones de acceso con Remote PC, consulte Acceso con Remote PC.

Si utiliza la función Wake on LAN, complete los pasos de configuración en System Center Configuration Manager de Microsoft antes de crear el sitio. Para obtener más información, consulte Configuration Manager y Wake on LAN para Acceso con Remote PC.

Al crear un sitio de acceso con Remote PC:

- Si usa la función Wake on LAN, en la página **Administración de energía**, especifique la dirección, las credenciales y la conexión de Microsoft System Center Configuration Manager.
- Especifique los usuarios o los grupos de usuarios en la página **Usuarios**. No hay ninguna acción predeterminada que agregue automáticamente a todos los usuarios. Asimismo, especifique datos sobre cuentas de máquina (dominio y OU) en la página **Cuentas de máquina**.

  Para agregar información de los usuarios, haga clic en **Agregar usuarios**. Seleccione usuarios y grupos de usuarios, y luego haga clic en **Agregar usuarios**.

  Para agregar información sobre cuentas de máquina, haga clic en **Agregar cuentas de máquina**. Seleccione las cuentas de máquina y, a continuación, haga clic en **Agregar cuentas de máquina**. Haga clic en **Agregar unidades organizativas**. Seleccione el dominio y las unidades organizativas, e indique si deben incluirse los elementos de las subcarpetas. Haga clic en **Agregar unidades organizativas**.

Se crea automáticamente un catálogo de máquinas llamado “Cuentas de máquina de usuarios para Remote PC”. Este catálogo contiene todas las cuentas de máquina que se agregaron en el Asistente para la creación de sitios. Se crea automáticamente un grupo de entrega llamado “Escritorios de usuario para Remote PC”. Este grupo contiene a todos los usuarios y los grupos de usuarios que se hayan agregado.

Paso 9: Resumen

La página **Resumen** contiene la información especificada. Utilice el botón **Atrás** si quiere cambiar algo. Cuando haya terminado, haga clic en **Crear** y comenzará la creación del sitio.

Probar la configuración del sitio

Para ejecutar pruebas después de crear un sitio, seleccione **Citrix Studio (Sitio** *nombre-de-sitio***)** en la parte superior del panel de navegación. A continuación, haga clic en **Probar sitio** en el panel central. Puede ver un informe HTML de los resultados de la prueba del sitio.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

La prueba de funcionamiento del sitio puede fallar si hay un Controller instalado en Windows Server 2016. El error se produce cuando una base de datos local SQL Server Express se utiliza como la base de datos del sitio y no se ha iniciado el servicio SQL Server Browser. Para evitar este fallo, complete las tareas siguientes.

1. Habilite el servicio SQL Server Browser (si fuera necesario) e inícielo.
2. Reinicie el servicio SQL Server (SQLEXPRESS).

Las pruebas del sitio se ejecutan automáticamente cuando actualiza una implementación anterior. Para ver información más detallada, consulte Pruebas preliminares en el sitio.

Solucionar problemas

Después de configurar el sitio, puede instalar Studio y agregarlo a través de la consola MMC como un complemento en una máquina remota. Si intenta quitar ese complemento más adelante, la consola MMC puede dejar de responder. Como solución temporal, reinicie MMC.

Crear catálogos de máquinas

March 14, 2019

Las colecciones de máquinas físicas o virtuales se administran como una entidad única, llamada catálogo de máquinas. Todas las máquinas de un catálogo de máquinas tienen el mismo tipo de sistema operativo: servidor o escritorio. Un catálogo de máquinas de SO de servidor puede contener máquinas Windows o Linux, pero no ambos.

Studio le guiará para crear el primer catálogo de máquinas después de crear el sitio. Después de crear el primer catálogo de máquinas, Studio le guiará para crear su primer grupo de entrega. Posteriormente, puede cambiar el catálogo que haya creado y crear más catálogos.

Información general

Cuando crea un catálogo de máquinas virtuales, debe indicar cómo aprovisionarlas. Puede usar herramientas de Citrix, como Machine Creation Services (MCS) o Citrix Provisioning (antes Provisioning Services). O bien, puede utilizar sus propias herramientas para aprovisionar máquinas.

- Si utiliza Citrix Provisioning para crear las máquinas, consulte la documentación de Citrix Provisioning para obtener instrucciones.
- Si elige Machine Creation Services para aprovisionar las máquinas, debe proporcionar una imagen maestra (o una instantánea de ella) para crear máquinas virtuales idénticas en el catálogo. Antes de crear el catálogo, primero debe usar las herramientas en el hipervisor o servicio de

© 1999-2019 Citrix Systems, Inc. All rights reserved.

nube para crear y configurar la imagen maestra. Este proceso incluye instalar un Virtual Delivery Agent (VDA) en la imagen. Después, crea un catálogo de máquinas en Studio. Debe seleccionar esa imagen (o instantánea), especificar la cantidad de máquinas virtuales que se van a crear en el catálogo y configurar información adicional.

- Si las máquinas ya están disponibles (por lo tanto, no necesita imágenes maestras), debe crear uno o varios catálogos para esas máquinas.
- Si crea un catálogo directamente mediante el SDK de PowerShell, puede especificar una plantilla de hipervisor (VMTemplates), en vez de una imagen o una instantánea de la imagen.

Si utiliza Machine Creation Services o Citrix Provisioning para crear el primer catálogo de máquinas, debe usar la conexión de host que ha configurado al crear el sitio. Más adelante, después de crear el primer catálogo de máquinas y el grupo de entrega, podrá cambiar la información de esta conexión o crear conexiones adicionales.

Después de completar el Asistente para la creación de catálogos de máquinas, se ejecutan pruebas automáticamente para garantizar que los catálogos se han configurado correctamente. Una vez completadas las pruebas, generan un informe que podrá ver. Ejecute las pruebas en cualquier momento desde Studio.

> **Nota:**
>
> MCS no es compatible con Windows 10 IoT Core ni Windows 10 IoT Enterprise. Consulte el sitio de Microsoft para obtener más información.

Para obtener detalles técnicos sobre las herramientas de aprovisionamiento de Citrix, consulte Administración de imágenes de Citrix Virtual Apps and Desktops.

Verificar licencias RDS

La creación de un catálogo que contenga máquinas con sistema operativo Windows Server incluye una comprobación automática de las licencias RDS de Microsoft válidas. Studio busca, en el catálogo, una máquina encendida y registrada para llevar a cabo la comprobación.

- Si no encuentra ninguna máquina encendida y registrada, muestra un mensaje de advertencia, donde explica que la comprobación de licencias RDS no se pudo realizar.
- Si encuentra una máquina y detecta un error, Studio muestra un mensaje de advertencia sobre el catálogo que contiene el problema detectado. Para eliminar una advertencia de licencias RDS de un catálogo (para que ya no aparezca en la pantalla de Studio), seleccione el catálogo y haga clic en la opción **Quitar advertencia de licencias de RDS** en el panel **Acciones**. Cuando se le solicite, confirme la acción.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Registro de VDA

El agente VDA debe registrarse en un Delivery Controller (en implementaciones locales) o Cloud Connector (en implementaciones Citrix Cloud) para que se le tenga en cuenta cuando se inicien sesiones con broker. Los VDA no registrados pueden derivar en una 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, Studio proporciona información en el Asistente para la creación de catálogos, y después de agregar máquinas de un catálogo a un grupo de entrega.

En el Asistente para la creación de catálogos de máquinas, después de agregar las máquinas existentes, la lista de nombres de cuenta de equipo indicará si cada máquina es adecuada para agregarla al catálogo. Pase el puntero sobre el icono situado junto a cada máquina para ver un mensaje informativo sobre esa máquina.

Si el mensaje indica una máquina problemática, puede quitarla (mediante el botón **Quitar**) o agregarla. Por ejemplo, si un mensaje indica que no se ha podido obtener información acerca de una máquina (posiblemente porque nunca se registró), agréguela de todos modos.

Para obtener más información, consulte:

- CTX136668 para obtener instrucciones de solución de problemas en el registro de los VDA
- Niveles funcionales y versiones de VDA
- Métodos de registro de los VDA

Resumen de la creación de catálogos con MCS

A continuación, se ofrece un breve resumen de las acciones de MCS predeterminadas después de proporcionar información en el Asistente para la creación de catálogos de máquinas.

- Si seleccionó una imagen maestra (en lugar de una instantánea), MCS crea una instantánea.
- MCS crea una copia completa de la instantánea y la coloca en cada ubicación de almacenamiento definida en la conexión de host.
- MCS agrega las máquinas a Active Directory, lo que crea identidades únicas.
- MCS crea la cantidad de máquinas virtuales especificadas en el asistente, con dos discos definidos para cada máquina virtual. Además de los dos discos por máquina virtual, también se almacena una imagen maestra en la misma ubicación de almacenamiento. Si ha definido varias ubicaciones de almacenamiento, cada una obtiene los siguientes tipos de disco:
  - La copia completa de la instantánea (indicada anteriormente), 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 los escritorios agrupados, se elimina y se crea uno nuevo después de cada reinicio.

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 de copia completa 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 que tener en cuenta al decidir sobre soluciones de almacenamiento, configuraciones y capacidades 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 discos adicionales para satisfacer determinados casos de uso y el consumo de funciones. Por ejemplo:

  - Personal vDisk ofrece a los usuarios finales la capacidad de instalar aplicaciones sin intervención del administrador en un disco aparte, conectado a la máquina virtual.
  - AppDisk ofrece a los usuarios finales la capacidad de adjuntar los discos de sólo aplicaciones a máquinas virtuales, principalmente para catálogos de SO de servidor.
  - Optimización de almacenamiento de MCS crea un disco de estilo de caché de escritura para cada máquina virtual.
  - MCS ha agregado la capacidad de usar clones de copia completa en lugar del caso de uso del disco Delta descrito anteriormente.

  Las funciones del hipervisor también pueden entrar en la ecuación. Por ejemplo:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

  - Citrix XenServer IntelliCache crea un disco de lectura en el almacenamiento local para que cada XenServer guarde en IOPS en la imagen maestra que podría mantenerse en la ubicación compartida de almacenamiento.

- Sobrecarga del hipervisor

  Cada hipervisor utiliza archivos específicos que crean sobrecarga para las máquinas virtuales. Los hipervisores también pueden usar el almacenamiento para operaciones de administración y registro general. Calcular espacio para incluir la sobrecarga de:

  - Archivos de registros
  - Archivos específicos del hipervisor. Por ejemplo:
    * VMware agrega archivos adicionales a la carpeta de **almacenamiento de VM**. Consulte Prácticas recomendadas de VMware.
    * Calcule los requisitos del tamaño total de máquinas virtuales. Tome como ejemplo una máquina virtual con 20 GB para el disco virtual, 16 GB para el archivo de intercambio de máquina virtual (el tamaño de una memoria asignada) y 100 MB para los archivos de registros, o 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 máquinaa un catálogo no requiere copiar el disco base en cada ubicación de almacenamiento. La creación del catálogo varía en función de las funcionalidades seleccionadas. Por lo tanto, un catálogo que emplea un disco personal vDisk o AppDisks necesitará más espacio que un simple catálogo aleatorio agrupado.
  - La actualización del catálogopermite 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 periodo de tiempo.

Consideraciones adicionales:

- **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 capacidades del aprovisionamiento dinámico.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Compatibilidad con el arrendamiento de host AWS dedicado

Puede utilizar MCS para aprovisionar hosts AWS dedicados. Un administrador puede crear un catálogo de máquinas con el arrendamiento del host definido a través de PowerShell.

Un host dedicado Amazon [EC2] es un servidor físico con [EC2]una capacidad de instancia totalmente dedicada, lo que permite utilizar licencias de software por socket o por máquina virtual existente.

Los hosts dedicados tienen una utilización predeterminada basada en el tipo de instancia. Por ejemplo, un único host dedicado asignado de los tipos de instancia C4 Large está limitado a ejecutar 16 instancias. Consulte el sitio de AWS para obtener más información.

Los requisitos para el aprovisionamiento a los hosts AWS son:

- Una imagen (AMI) importada de BYOL (bring your own license). Con hosts dedicados, puede usar y administrar sus licencias existentes.
- Una asignación de hosts dedicados con suficiente utilización para abarcar las solicitudes de aprovisionamiento.
- Habilite **auto-placement**.

Para aprovisionar a un host AWS dedicado mediante PowerShell, utilice el cmdlet **New-ProvScheme** con el parámetro “TenancyType” establecido en *Host*.

Consulte la documentación para desarrolladores de Citrix para obtener más información.

Preparar una imagen maestra en el hipervisor o servicio de nube

Para obtener más información sobre cómo crear conexiones a hipervisores y proveedores en la nube, consulte Conexiones y recursos.

La imagen maestra contiene el sistema operativo, las aplicaciones no virtualizadas, el VDA, y otro software.

Conviene tener en cuenta lo siguiente:

- Una imagen maestra también se conoce como imagen clon, imagen dorada, VM base o imagen base. Los proveedores de host y los proveedores de servicios en la nube usan otros nombres.
- Al usar Citrix Provisioning, se puede usar una imagen maestra o un equipo físico como dispositivo de destino maestro. Citrix Provisioning utiliza una terminología diferente de MCS para referirse a las imágenes. Para obtener información más detallada, consulte la documentación de Citrix Provisioning.
- Compruebe que el hipervisor o el servicio de nube tienen procesadores, memoria y capacidad de almacenamiento suficientes para admitir la cantidad de máquinas creadas.
- Configure la cantidad necesaria de espacio en disco duro para los escritorios y las aplicaciones. Ese valor no se puede cambiar más adelante o en el catálogo de la máquina.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Los catálogos de máquinas para acceso con Remote PC no utilizan imágenes maestras.
- Consideraciones acerca de la activación de KMS de Microsoft al utilizar Machine Creation Services: Si la implementación incluye agentes VDA de la versión 7.x con un host de XenServer 6.1 o 6.2, vSphere o Microsoft System Center Virtual Machine Manager, no tendrá que rearmar manualmente Microsoft Windows o Microsoft Office.

> **Sugerencia:**
>
> El controlador asociado a la optimización de E/S de MCS puede provocar que algunas máquinas virtuales Azure MCS dejen de funcionar. Citrix recomienda inhabilitar la optimización de E/S para catálogos Azure MCS hasta que se publique una nueva versión.

Instale y configure el siguiente software en la imagen maestra:

- Herramientas de integración para el hipervisor (como XenServer 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 App-V. El cliente de App-V está disponible en Microsoft.
- Si utiliza Machine Creation Services y va a localizar Microsoft Windows, instale las configuraciones regionales y los paquetes de idioma. Durante el aprovisionamiento, cuando se crea una instantánea, las máquinas virtuales aprovisionadas usan las configuraciones regionales y los paquetes de idioma instalados.

> **Importante:**
>
> Si utiliza Citrix Provisioning o Machine Creation Services, no debe ejecutar Sysprep en imágenes maestras.

Para preparar una imagen maestra:

1. Mediante la herramienta de administración del hipervisor, cree una imagen maestra y, a continuación, instale el sistema operativo, además de todos los Service Pack y las actualizaciones. Especifique la cantidad de CPU virtuales. También puede especificar el valor de la CPU virtual

© 1999-2019 Citrix Systems, Inc. All rights reserved.

si crea el catálogo de máquinas mediante PowerShell. No se puede especificar la cantidad de CPU virtuales si crea el catálogo con Studio. Configure la cantidad necesaria de espacio en disco duro para los escritorios y las aplicaciones. Ese valor no se puede cambiar más adelante o en el catálogo.

2. Compruebe que el disco duro está conectado a la ubicación de dispositivo 0. La mayoría de las plantillas de imagen maestra estándar configuran esta ubicación de manera predeterminada, pero es posible que no suceda lo mismo con algunas plantillas personalizadas.
3. Instale y configure el software anterior en la imagen maestra.
4. Si utiliza Citrix Provisioning, cree un archivo VHD para el disco vDisk del dispositivo de destino maestro antes de unir el dispositivo de destino maestro a un dominio. Para obtener información más detallada, consulte la documentación de Citrix Provisioning.
5. Si no utiliza Machine Creation Services, debe unir la imagen maestra al dominio al que pertenecen las aplicaciones y los escritorios. Compruebe que la imagen maestra está disponible en el host donde se crearán las máquinas. Si utiliza Machine Creation Services, no es necesario unir la imagen maestra a un dominio. Las máquinas aprovisionadas se unen al dominio especificado en el Asistente para la creación de catálogos.
6. Citrix recomienda que cree y dé nombre a una instantánea de la imagen maestra, para que se pueda identificar más tarde. Si especifica una imagen maestra en lugar de una instantánea al crear un catálogo de máquinas, Studio crea una instantánea pero no se le podrá asignar ningún nombre.

Crear un catálogo de máquinas mediante Studio

Antes de iniciar el asistente de creación de catálogos, revise esta sección.

Si utiliza una imagen maestra, compruebe que hay instalado un VDA en la imagen antes de crear el catálogo de máquinas.

Desde Studio:

- Si ya ha creado un sitio, pero aún no ha creado un catálogo de máquinas, Studio le guiará hacia el punto de partida idóneo para crear un catálogo de máquinas.
- Si ya ha creado un catálogo de máquinas y quiere crear otro, seleccione **Catálogos de máquinas** en el panel de navegación de **Studio**. A continuación, seleccione **Crear catálogo de máquinas** en el panel **Acciones**.

El asistente le guiará a través de los siguientes elementos. Las páginas del asistente pueden variar según las opciones que escoja.

Paso 1: Sistema operativo

Cada catálogo contiene máquinas de un solo tipo. Seleccione uno.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **SO de servidor:** Un catálogo con SO de servidor ofrece aplicaciones y escritorios alojados compartidos. Las máquinas pueden ejecutar versiones respaldadas 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 escritorio:** Un catálogo de SO de escritorio proporciona aplicaciones y escritorios VDI que se pueden asignar a una variedad de 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.

Paso 2: Administración de máquinas

Esta página no aparece cuando se crean catálogos de acceso con Remote PC.

La página **Administración de máquinas** indica cómo se administran las máquinas y con qué herramienta se implementan.

Elija si la administración de energía de las máquinas del catálogo se llevará a cabo a través de Studio.

- Las opciones de energía de las máquinas se administran a través de Studio o se aprovisionan mediante un entorno de nube (por ejemplo, máquinas virtuales o equipos Blade). Esta opción solo está disponible si ya dispone de una conexión configurada a un hipervisor o servicio de nube.
- Las opciones de energía de las máquinas no se administran a través de Studio (por ejemplo, máquinas físicas).

Si ha indicado que las opciones de energía de las máquinas se administran a través de Studio o se aprovisionan mediante un entorno de nube, elija la herramienta que se va a utilizar para crear las máquinas virtuales.

- **Citrix Machine Creation Services (MCS):** Utiliza una imagen maestra para crear y administrar máquinas virtuales. Los catálogos de máquinas en entornos de nube usan MCS. MCS no está disponible para máquinas físicas.
- **Citrix Provisioning:** (Antes Provisioning Services.) Administra los dispositivos de destino como una colección de dispositivos. Un disco vDisk de Citrix Provisioning creado a partir de un dispositivo de destino maestro entrega escritorios y aplicaciones.
- **Otros:** Una herramienta que administra máquinas que ya se encuentran en el centro de datos. Citrix recomienda usar Microsoft System Center Configuration Manager u otra aplicación de terceros para una mayor uniformidad entre las máquinas del catálogo.

Paso 3: Tipos de escritorio (experiencia de escritorio)

Esta página solo aparece cuando se crea un catálogo que contiene máquinas de SO de escritorio.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

La página **Experiencia de escritorio** determina lo que ocurre cada vez que un usuario inicia sesión. Seleccione una de las siguientes opciones:

- Los usuarios se conectan a un escritorio nuevo (aleatorio) cada vez que inician sesión.
- Los usuarios se conectan al mismo escritorio (estático) cada vez que inician sesión.

Si elige la segunda opción y usa Citrix Provisioning para aprovisionar las máquinas, puede definir qué pasará con los cambios que los usuarios realicen en el escritorio:

- Guardar en un disco Personal vDisk aparte los cambios que los usuarios efectúen en el escritorio. (Personal vDisk está obsoleto.)
- Guardar en el disco local los cambios que los usuarios efectúen en el escritorio.
- Descartar los cambios del usuario y limpiar el escritorio virtual cuando el usuario cierre sesión.

Paso 4: Imagen maestra

Esta página solo aparece cuando se utiliza Machine Creation Services para crear máquinas virtuales.

En la página **Imagen maestra**, seleccione la conexión al hipervisor de host o el servicio de nube y, a continuación, seleccione la instantánea o máquina virtual creada anteriormente. Si está creando el primer catálogo de máquinas, la única conexión disponible es la configurada al crear el sitio.

Recuerde:

- Cuando utilice MCS o Citrix Provisioning, no ejecute Sysprep en imágenes maestras.
- Si especifica una imagen maestra en lugar de una instantánea, Studio creará una instantánea pero usted no le podrá asignar ningún nombre.

Para que pueda utilizar las funciones más recientes del producto, compruebe que la imagen maestra tiene instalada la versión más reciente de VDA. No cambie la selección predeterminada de VDA mínimo. No obstante, si debe usar una versión anterior de VDA, consulte Niveles funcionales y versiones de VDA.

Aparecerá un mensaje de error si selecciona una instantánea o máquina virtual que no sea compatible con la tecnología de administración de la máquina que haya seleccionado antes en el asistente.

Paso 5: Entornos de servicios y plataformas de nube

Si utiliza un servicio o una plataforma de nube (como Azure Resource Manager, Nutanix o Amazon Web Services) para alojar máquinas virtuales, el Asistente para la creación de catálogos de máquinas puede contener páginas específicas para ese host.

Para obtener más información, consulte Dónde encontrar información acerca de los tipos de conexión.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Paso 6: Colección de dispositivos

Esta página solo aparece cuando se utiliza Citrix Provisioning para crear máquinas virtuales.

En la página **Colección de dispositivos**, se muestran los conjuntos de dispositivos y aquellos dispositivos que aún no se han agregado a los catálogos.

Seleccione las colecciones de dispositivos que va a usar.

Paso 7: Máquinas

Esta página no aparece cuando se crean catálogos de acceso con Remote PC.

El título de esta página depende de lo seleccionado en la página **Administración de máquinas**: **Máquinas**, **Máquinas virtuales** o **Máquinas virtuales y usuarios**.

Si utiliza MCS:

- Especifique la cantidad de máquinas virtuales que se van a crear.
- Seleccione la cantidad de memoria (en MB) que tendrá cada máquina virtual.
- Cada máquina virtual creada tendrá un disco duro. El tamaño se este se configura en la imagen maestra. No se puede cambiar el tamaño del disco duro en el catálogo.
- Si indicó en la página **Experiencia de escritorio** que los cambios que los usuarios efectúen en los escritorios estáticos deben guardarse en un disco Personal vDisk aparte, especifique el tamaño de este en gigabytes, así como la letra de su unidad.
- Si la implementación contiene más de una zona, puede seleccionar una zona para el catálogo.
- Si quiere crear máquinas virtuales de escritorio estático, seleccione un modo de copia para la máquina virtual. Consulte Modo de copia para la máquina virtual.
- Si quiere crear máquinas virtuales de escritorio aleatorio que no usan discos Personal vDisk, puede configurar una memoria caché que se va a usar para los datos temporales de cada máquina. Consulte Configurar la caché de datos temporales.

Al usar Citrix Provisioning:

La página **Dispositivos** ofrece una lista de las máquinas que hay en la colección de dispositivos que haya seleccionado en la página anterior. No se puede agregar ni quitar máquinas en esta página.

Si utiliza otras herramientas:

Agregue o importe una lista de los nombres de cuentas de máquina de Active Directory. Puede cambiar el nombre de la cuenta de Active Directory que tenga una máquina virtual después de agregarla o importarla. Si indicó máquinas estáticas en la página **Experiencia de escritorio**, puede especificar el nombre de usuario de Active Directory para cada máquina virtual que agregue.

Después de agregar o importar los nombres, puede hacer clic en el botón **Quitar** para eliminar nombres de la lista, sin salir de esta página.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Si utiliza Citrix Provisioning u otras herramientas (pero no MCS):

Un icono y un cuadro de información emergente acerca de cada máquina agregada (o importada o proveniente de una colección de dispositivos de Citrix Provisioning) pueden ayudarle a identificar aquellas máquinas que no sean aptas para ser agregadas al catálogo o no puedan registrarse en un Delivery Controller. Para obtener más información, consulte Niveles funcionales y versiones de VDA.

Modo de copia para la máquina virtual

El modo de copia que especifique en la página **Máquinas** determina si MCS crea clones ligeros (copia rápida) o pesados (copia completa) a partir de la imagen maestra. (La opción predeterminada es clones ligeros.)

- Puede optar por los clones de copia rápida para un uso más eficiente del almacenamiento y una creación de máquinas más rápida.
- En cambio, puede utilizar los clones de copia completa para unas mejores recuperación de datos y 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, es posible que necesite un nuevo VDA. Establecer un nivel funcional permite que todas las funcionalidades introducidas en esa versión (y versiones posteriores, si el nivel funcional no cambia) estén disponibles para las máquinas del catálogo. Sin embargo, las máquinas de ese catálogo que tengan una versión anterior de VDA no podrán registrarse.

Un menú desplegable en la parte inferior de la página **Máquinas** (o **Dispositivos**) permite seleccionar la versión mínima que debe tener un agente VDA para poder registrarse. Esto establece el nivel funcional mínimo del catálogo. De forma predeterminada, el nivel funcional de versión más reciente se selecciona para implementaciones locales. Si sigue la recomendación de Citrix de siempre instalar y actualizar los VDA y los componentes principales a la versión más reciente, no es necesario cambiar esta selección. Sin embargo, si debe seguir usando versiones anteriores de VDA, seleccione el valor correcto.

Una versión de Citrix Virtual Apps and Desktops puede no incluir una nueva versión de VDA, o el nuevo VDA puede no afectar al nivel funcional. En estos casos, el nivel funcional puede indicar una versión de VDA anterior a la versión de los componentes instalados o actualizados. Por ejemplo, aunque la versión 7.17 contiene un VDA 7.17, el nivel funcional predeterminado (“7.9 y versiones posteriores”) sigue siendo el más actual. Por lo tanto, después de instalar o actualizar los componentes desde 7.9-7.16 a 7.17, no es necesario cambiar el nivel funcional predeterminado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

En las implementaciones de Citrix Cloud, Studio usa un nivel funcional predeterminado que puede ser anterior a la versión más reciente.

El nivel funcional seleccionado determina la lista anterior de máquinas. En la lista, un cuadro de información situado junto a cada entrada indica si el VDA de la máquina es compatible con el catálogo en ese nivel funcional.

Aparecen mensajes en la página si el VDA de las máquinas no cumple o excede el nivel funcional mínimo seleccionado. Puede continuar con el asistente. Seguramente las máquinas no podrán registrarse en un Controller. De forma alternativa, puede:

- Quitar de la lista las máquinas que contengan agentes VDA antiguos, actualizar sus VDA y, a continuación, agregarlas de nuevo al catálogo.
- Elija un nivel funcional más bajo, aunque ello impedirá el acceso a las funcionalidades 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 escritorio, o bien, si intenta agregar una máquina de SO de escritorio creada en su momento para la asignación aleatoria a un catálogo de máquinas estáticas.

> **Importante:**
>
> Para la versión 1811, se ha agregado un nivel funcional adicional: **1811 (o posterior)**. Ese nivel está pensado para las funciones futuras de Citrix Virtual Apps and Desktops. La selección **7.9 (o posterior)** sigue siendo la predeterminada. Ese valor predeterminado ahora es válido para todas las implementaciones.
>
> Si selecciona **1811 (o posterior)**, ningún VDA de versión anterior en ese catálogo podrá registrarse en ningún Controller o Cloud Connector. Sin embargo, si el catálogo solo contiene VDA 1811 o versiones posteriores admitidas, todos podrán registrarse.

Configurar la caché de datos temporales

El almacenamiento en caché de datos temporales localmente en la VM es optativo. Puede habilitar el uso de la memoria caché de datos temporal en la máquina cuando se usa MCS para administrar máquinas agrupadas (no dedicadas) en un catálogo. Si el catálogo utiliza una conexión que especifica un espacio de almacenamiento para datos temporales, puede habilitar y configurar la información de caché de datos temporales al crear el catálogo.

Para habilitar el almacenamiento en caché de los datos temporales, el VDA de cada máquina del catálogo debe ser, como mínimo, de la versión 7.9. Esta característica se conoce como MCSIO.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> **Importante:**
>
> Esta función requiere un controlador MCSIO actualizado. La instalación de este controlador es una opción cuando instala o actualiza un VDA. De forma predeterminada, ese controlador no se instala.

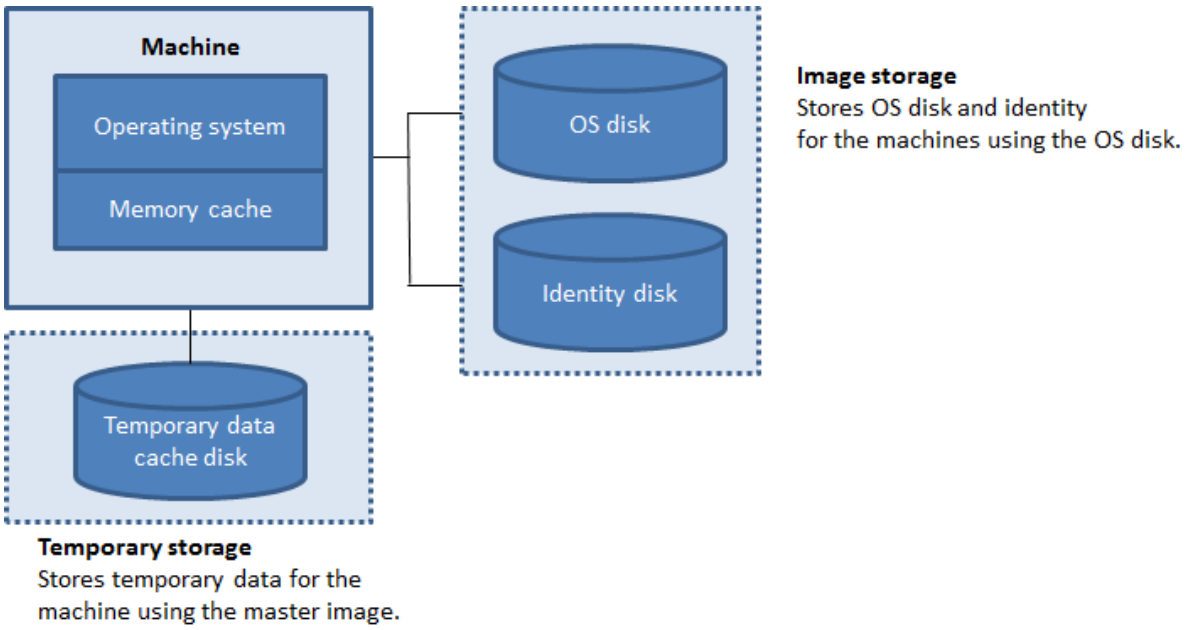
Puede especificar si los datos temporales utilizarán un almacenamiento local o compartido cuando cree la conexión que utilizará el catálogo; para obtener más información, consulte Conexiones y recursos. El proceso de habilitar y configurar la caché temporal en el catálogo incluye dos casillas de verificación y valores: **Memoria asignada para caché** (MB) y **Tamaño de caché de disco** (GB). De forma predeterminada, estas casillas de verificación están desmarcadas. Cuando marca una o ambas casillas, los valores predeterminados difieren según el tipo de conexión. Por lo general, los valores predeterminados son suficientes para la mayoría de los casos, sin embargo, tenga en cuenta el espacio necesario para:

- Archivos de datos temporales creados por Windows, incluido el archivo de paginación de Windows.
- Datos de perfil de usuario.
- Datos de ShareFile que se sincronizan en las sesiones de usuario.
- Datos que pueden crear o copiar los usuarios de las sesiones, o aplicaciones que los usuarios pueden instalar dentro de la sesión.

Windows no permitirá que una sesión use una cantidad de caché de disco que sea mayor que la cantidad de espacio libre en la imagen maestra original desde la cual se aprovisionaron las máquinas de catálogo. Por ejemplo, no se consigue ningún beneficio especificando una caché de disco de 20 GB si solo hay 10 GB de espacio disponible en la imagen maestra.

Si marca la casilla de verificación **Tamaño de caché de disco**, los datos temporales inicialmente se escriben en la memoria caché. Cuando la memoria caché alcanza su límite configurado (el valor de **Memoria asignada para caché**), los datos más antiguos se mueven a la caché del disco de datos temporales.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



La memoria caché está incluida en la cantidad total de memoria en cada máquina; por lo tanto, si marca la casilla **Memoria asignada para caché**, considere la opción de aumentar la memoria total de cada máquina.

Si deja sin marcar la casilla **Memoria asignada para caché** y deja marcada la casilla **Tamaño de caché de disco**, los datos temporales se escriben directamente en la caché de disco usando una cantidad mínima de la memoria caché.

Si se cambia el valor predeterminado del **Tamaño de caché de disco**, el rendimiento puede verse afectado. El tamaño debe coincidir con los requisitos de los usuarios y la carga que se coloca en la máquina.

> **Importante:**
>
> Si el caché de disco se queda sin espacio, la sesión de 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 tenga el tamaño suficiente para contener todos los datos temporales. Esto es factible solo si hay grandes cantidades de RAM disponibles para ser asignadas a cada VM.

Si deja sin marcar ambas casillas, los datos temporales no se almacenan en caché. Se escriben en el disco diferencial (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.

Esta función no está disponible cuando se usa una conexión de host Nutanix.

No puede cambiar los valores de caché en un catálogo de máquinas después de haberlo creado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Paso 8: Tarjetas de interfaz de red (NIC)

Esta página no aparece cuando se crean catálogos de acceso con Remote PC.

En la página **Tarjetas de interfaz de red**, si quiere utilizar varias tarjetas de interfaz de red (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.

Paso 9. Cuentas de máquina

Esta página solo aparece cuando se crean catálogos de acceso con Remote PC.

En la página **Cuentas de máquina**, especifique las cuentas de máquina de Active Directory o unidades organizativas (OU) para agregarlas a usuarios o grupos de usuarios. No use barras diagonales (/) en el nombre de una unidad organizativa.

Puede elegir una conexión de administración de energía que haya configurado previamente o puede optar por no usar la administración de energía. Si quiere usar la administración de energía, pero aún no se ha configurado la conexión correspondiente, puede crear dicha conexión más tarde y posteriormente modificar el catálogo de máquinas para actualizar la configuración de la administración de energía.

Paso 10. Cuentas de equipo

Esta página solo aparece cuando se utiliza Machine Creation Services para crear máquinas virtuales.

Cada máquina del catálogo debe tener una cuenta de equipo de Active Directory correspondiente. En la página **Cuentas de equipo**, indique si se van a crear cuentas o si se van a utilizar cuentas existentes, además de la ubicación de estas.

- Si opta por crear cuentas, debe tener acceso a una cuenta de administrador de dominio para el dominio donde residirá la máquina.

  Especifique el esquema de nombres de cuenta para las máquinas que se van a crear con marcas hash para indicar dónde aparecerán los números o las letras secuenciales. No use barras diagonales (/) en el nombre de una unidad organizativa. Un nombre no puede empezar con un número. Por ejemplo, un esquema de nombres de PC-Ventas-## (con números del 0 al 9 seleccionados) tiene como resultado cuentas de equipo llamadas PC-Ventas-01, PC-Ventas-02, PC-Ventas-03, etc.

- 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:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

```
[ADComputerAccount]
ADcomputeraccountname.domain
...
```

Compruebe que hay cuentas suficientes para las máquinas que está agregando. Como Studio es el responsable de administrar estas cuentas, permita que Studio restablezca las contraseñas de todas las cuentas, o bien especifique la contraseña de la cuenta (que debe ser la misma para todas las cuentas).

Para catálogos que contienen máquinas físicas o máquinas existentes, seleccione o importe las cuentas existentes y asigne cada máquina a una cuenta de equipo de Active Directory y a una cuenta de usuario.

Para máquinas creadas con Citrix Provisioning, las cuentas de equipo de los dispositivos de destino se administran de forma diferente. Para obtener más información al respecto, consulte la documentación de Citrix Provisioning.

Paso 11. Resumen, nombre y descripción

En la página **Resumen**, revise la configuración especificada. Introduzca un nombre y una descripción para el catálogo. Esta información se mostrará en Studio.

Cuando termine, haga clic en **Finalizar** para iniciar la creación del catálogo.

Solucionar problemas

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-ProvServiceConfigurationD -Name ImageManagementPrep_NoAutoShutdown -Value $True`.
4. Cree un nuevo 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`.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Qué hacer a continuación

Si este es el primer catálogo creado, Studio le guiará para crear un grupo de entrega.

Administrar catálogos de máquinas

March 8, 2019

Introducción

Puede agregar o quitar máquinas de un catálogo de máquinas; también puede cambiarlo de nombre, modificar su descripción o administrar sus cuentas de equipo de Active Directory.

Asimismo, el mantenimiento de catálogos puede incluir la comprobación de que cada máquina tenga los últimos cambios de configuración y las actualizaciones más recientes del sistema operativo o del software antivirus.

- Para catálogos que contienen máquinas agrupadas aleatorias creadas con Machine Creation Services (MCS), mantenga las máquinas actualizando primero la imagen maestra utilizada en el catálogo. Después de actualizar la imagen, actualice las máquinas. Este proceso permite actualizar de forma eficiente una gran cantidad de máquinas de usuario.
- Para máquinas creadas con Citrix Provisioning, las actualizaciones a las máquinas se propagan mediante discos Personal vDisk. Para obtener información más detallada, consulte la documentación de Citrix Provisioning.
- Para catálogos que contengan máquinas estáticas asignadas permanentemente y para catálogos de máquinas de acceso con Remote PC, administre las actualizaciones en las máquinas de los usuarios fuera de Studio. Puede hacerlo de forma individual o colectiva mediante herramientas de distribución de software de terceros.

Para obtener información sobre la creación y la administración de conexiones con hosts de hipervisores y servicios de nube, consulte Conexiones y recursos.

> **Nota:**
>
> MCS no es compatible con Windows 10 IoT Core ni Windows 10 IoT Enterprise. Consulte el sitio de Microsoft para obtener más información.

Acerca de las instancias persistentes

Al actualizar un catálogo MCS creado con instancias persistentes o dedicadas, cualquier máquina nueva creada para el catálogo utiliza la imagen actualizada. Las instancias preexistentes continúan

© 1999-2019 Citrix Systems, Inc. All rights reserved.

utilizando la instancia original. El proceso de actualización de una imagen se realiza de la misma manera que cuando se trata de cualquier otro tipo de catálogo. Se deben tener en cuenta las siguientes cuestiones:

- Con catálogos de discos persistentes, las máquinas preexistentes no se actualizan a la nueva imagen. Sin embargo, todas las máquinas nuevas que se agreguen al catálogo utilizan la nueva imagen.
- Para catálogos de discos no persistentes, la imagen de la máquina se actualiza la próxima vez que se restablezca la máquina.
- Con catálogos de máquinas persistentes, actualizar la imagen también implica actualizar las instancias de catálogo que la utilizan.
- En el caso de catálogos no persistentes, si quiere utilizar imágenes diferentes para máquinas diferentes, las imágenes deben residir en catálogos separados.

Agregar máquinas a un catálogo

Antes de comenzar:

- Compruebe que el host de virtualización (hipervisor o proveedor de servicios en la nube) contenga procesadores, memoria y capacidad de almacenamiento suficientes para dar cabida a las máquinas adicionales.
- Compruebe que tiene suficientes cuentas de equipo de Active Directory sin usar. Si utiliza cuentas existentes, tenga en cuenta que la cantidad de máquinas que puede agregar se limita a la cantidad de cuentas disponibles.
- Si usa Studio con el fin de crear cuentas de equipo de Active Directory para las máquinas adicionales, debe tener los permisos de administrador de dominio apropiados.

Para agregar máquinas a un catálogo:

1. Seleccione **Catálogos de máquinas** en el panel de navegación de **Studio**.
2. Seleccione un catálogo de máquinas y, a continuación, seleccione **Agregar máquinas** en el panel **Acciones**.
3. Seleccione la cantidad de máquinas virtuales que se van a agregar.
4. Si no hay suficientes cuentas existentes de Active Directory para la cantidad de máquinas virtuales que quiere agregar, seleccione el dominio y la ubicación donde se crearán las cuentas. Especifique un esquema de nombres de cuenta con marcas hash para indicar dónde aparecerán los números o las letras secuenciales. No use barras diagonales (/) en el nombre de una unidad organizativa. Un nombre no puede empezar con un número. Por ejemplo, un esquema de nombres de PC-Ventas-## (con números del 0 al 9 seleccionados) tiene como resultado cuentas de equipo llamadas PC-Ventas-01, PC-Ventas-02, PC-Ventas-03, etc.
5. Si usa cuentas existentes de Active Directory, vaya a esas cuentas o haga clic en **Importar** y especifique un archivo CSV que contenga los nombres de cuenta. Compruebe que hay cuen-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

tas suficientes para las máquinas que está agregando. Como Studio es el responsable de administrar estas cuentas, permita que Studio restablezca las contraseñas de todas las cuentas o especifique la contraseña de la cuenta (que debe ser la misma para todas las cuentas).

Las máquinas se crean en un proceso en segundo plano, que puede tardar mucho tiempo si se crea una gran cantidad de máquinas. La creación de máquinas continúa aunque se cierre Studio.

Eliminar máquinas de un catálogo

Después de eliminar una máquina de un catálogo, los usuarios ya no podrán acceder a ella. Por eso, antes de eliminar una máquina, compruebe que:

- Existe una copia de seguridad de los datos del usuario, si fueran útiles.
- Todos los usuarios han cerrado la sesión. La activación del modo de mantenimiento impide nuevas conexiones a una máquina.
- Las máquinas se apagan.

Para eliminar máquinas de un catálogo:

1. Seleccione **Catálogos de máquinas** en el panel de navegación de **Studio**.
2. Seleccione un catálogo y, a continuación, seleccione **Ver máquinas** en el panel **Acciones**.
3. Seleccione una o varias máquinas y, a continuación, seleccione **Eliminar** en el panel **Acciones**.

Elija si se eliminarán las máquinas que se van a quitar. Si opta por eliminar máquinas, indique si las cuentas de Active Directory de esas máquinas deben conservarse, inhabilitarse o eliminarse.

Cuando se elimina un catálogo de máquinas de Azure Resource Manager, las máquinas y los grupos de recursos asociados se eliminan de Azure, incluso aunque indique que deben conservarse.

Cambiar la descripción de un catálogo o cambiar la configuración de acceso con Remote PC

1. Seleccione **Catálogos de máquinas** en el panel de navegación de **Studio**.
2. Seleccione un catálogo y, a continuación, seleccione **Modificar catálogo de máquinas** en el panel **Acciones**.
3. (Solo para catálogos de acceso con Remote PC) En la página **Administración de energía**, puede cambiar la configuración de administración de energía y seleccionar una conexión de administración de energía. En la página **Unidades organizativas**, agregue o quite unidades organizativas de Active Directory.
4. En la página **Descripción**, cambie la descripción del catálogo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Cambiar el nombre de un catálogo

1. Seleccione **Catálogos de máquinas** en el panel de navegación de **Studio**.
2. Seleccione un catálogo y, a continuación, seleccione **Cambiar nombre de catálogo de máquinas** en el panel **Acciones**.
3. Introduzca el nuevo nombre.

Mover un catálogo a otra zona

Si la implementación tiene más de una zona, puede mover un catálogo de una zona a otra.

Tenga en cuenta que mover un catálogo a otra zona que el hipervisor o el servicio de nube que contiene las máquinas virtuales de ese catálogo puede afectar el rendimiento.

1. Seleccione **Catálogos de máquinas** en el panel de navegación de **Studio**.
2. Seleccione un catálogo y, a continuación, seleccione **Mover** en el panel **Acciones**.
3. Seleccione la zona a la que quiere mover el catálogo.

Eliminar un catálogo

Antes de eliminar un catálogo, asegúrese de que:

- Todos los usuarios han cerrado sesión y no hay sesiones desconectadas en ejecución.
- El modo de mantenimiento se activa para todas las máquinas del catálogo, de modo que no se pueden establecer conexiones nuevas.
- Todas las máquinas del catálogo se apagan.
- El catálogo no está asociado a ningún grupo de entrega. En otras palabras, el grupo de entrega no contiene máquinas provenientes del catálogo.

Para eliminar un catálogo:

1. Seleccione **Catálogos de máquinas** en el panel de navegación de **Studio**.
2. Seleccione un catálogo y, a continuación, seleccione **Eliminar catálogo de máquinas** en el panel **Acciones**.
3. Indique si las máquinas del catálogo deberían eliminarse. Si opta por eliminar máquinas, indique si las cuentas de equipo de Active Directory de esas máquinas deben conservarse, inhabilitarse o eliminarse.

Administrar cuentas de equipo de Active Directory en un catálogo

Para administrar cuentas de Active Directory en un catálogo de máquinas, puede:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Liberar cuentas de máquina sin utilizar eliminando cuentas de equipo de Active Directory que haya en catálogos de máquinas de SO de servidor y SO de escritorio. Estas cuentas se pueden usar para otras máquinas.
- Agregar cuentas de modo que, cuando se agreguen más máquinas al catálogo, las cuentas de equipo ya estén listas. No use barras diagonales (/) en el nombre de una unidad organizativa.

Para administrar cuentas de Active Directory:

1. Seleccione **Catálogos de máquinas** en el panel de navegación de **Studio**.
2. Seleccione un catálogo y, a continuación, seleccione **Administrar cuentas de AD** en el panel **Acciones**.
3. Elija si desea agregar o eliminar las cuentas de equipo. Si agrega cuentas, deberá especificar qué hacer con las contraseñas de cuenta: restablecerlas todas o escribir una contraseña para todas ellas.

   Puede restablecer contraseñas si no conoce las contraseñas de cuenta actuales. Debe tener permisos específicos para realizar el restablecimiento de contraseñas. Si introduce una contraseña, se cambiará la contraseña en las cuentas a medida que se importan. Si elimina una cuenta, se le solicitará que elija si la cuenta de Active Directory debe mantenerse, inhabilitarse o eliminarse.

También puede indicar si las cuentas de Active Directory se deberían conservar, inhabilitar o eliminar cuando quite máquinas de un catálogo o elimine un catálogo.

Actualizar un catálogo

Citrix recomienda guardar copias o instantáneas de las imágenes maestras antes de actualizar las máquinas de un catálogo. La base de datos conserva un registro histórico de las imágenes maestras utilizadas con cada catálogo de máquinas. Se pueden revertir las máquinas de un catálogo para usar la versión anterior de la imagen maestra si los usuarios detectan 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. Si lo hace, no podrá usarlas para revertir el catálogo.

En caso de catálogos de máquinas que utilizan Citrix Provisioning (antes Provisioning Services), debe publicar un disco Personal vDisk nuevo para aplicar los cambios al catálogo. Para obtener información más detallada, consulte la documentación de Citrix Provisioning.

Una vez actualizada la máquina, se reinicia automáticamente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Actualizar o crear una imagen maestra

Antes de actualizar un catálogo de máquinas, actualice la imagen maestra existente o cree una en el hipervisor de host.

1. En el hipervisor o proveedor del servicio de nube, tome una instantánea de la VM actual y dele un nombre significativo. Esta instantánea se puede usar para revertir (deshacer) los cambios en las máquinas del catálogo, si fuera necesario.
2. Si es necesario, encienda la máquina virtual de la imagen maestra e inicie sesión.
3. Instale las actualizaciones o realice los cambios necesarios en la imagen maestra.
4. Si la imagen maestra usa un disco Personal vDisk, actualice el inventario.
5. Apague la máquina virtual.
6. Tome una instantánea de la VM y dele un nombre significativo fácilmente reconocible cuando el catálogo se actualice en Studio. Aunque Studio puede crear una instantánea, Citrix recomienda crear la instantánea usando la consola de administración del hipervisor y, a continuación, seleccionarla en Studio. Este método le permite asignar un nombre y una descripción significativos para la instantánea, en lugar de recibir un nombre generado automáticamente. Para imágenes maestras de GPU, puede cambiar la imagen maestra solo a través de la consola XenCenter de XenServer.

Actualizar el catálogo

Para preparar y aplicar la actualización a todas las máquinas de un catálogo:

1. Seleccione **Catálogos de máquinas** en el panel de navegación de **Studio**.
2. Seleccione un catálogo y, a continuación, seleccione **Actualizar máquinas** en el panel **Acciones**.
3. En la página **Imagen maestra**, seleccione el host y la imagen que quiere implantar.
4. En la página **Estrategia de implantación**, elija cuándo se actualizarán las máquinas del catálogo a la nueva imagen maestra (en el siguiente apagado o inmediatamente). Consulte los siguientes apartados para obtener información más detallada.
5. En la página **Resumen**, revise la información y haga clic en **Finalizar**. Cada máquina se reiniciará automáticamente después de actualizarse.

Si está actualizando un catálogo directamente mediante el SDK de PowerShell, en lugar de Studio, puede especificar una plantilla de hipervisor (VMTemplates), como alternativa a una imagen o una instantánea de la imagen.

Estrategia de implantación:

La actualización de la imagen se realiza en el siguiente apagado si usa Citrix Connector para System Center Configuration Manager.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Si quiere actualizar la imagen de inmediato, configure una hora concreta para la distribución y las notificaciones pertinentes.

- **Hora de distribución:** Puede optar por actualizar todas las máquinas al mismo tiempo o especificar el periodo total de tiempo durante el que se debe comenzar a actualizar todas las máquinas que contiene el catálogo. Un algoritmo interno determina cuándo se actualiza y se reinicia cada máquina durante ese intervalo.
- **Notificación:** En la lista desplegable "Notificación", situada a la izquierda, elija si mostrar un mensaje de notificación en las máquinas antes de empezar una actualización. De forma predeterminada, no se muestra ningún mensaje. Si elige mostrar un mensaje 15 minutos antes de empezar una actualización, también puede decidir (en la lista desplegable de la derecha) si repetir el mensaje cada cinco minutos después del primer mensaje. De forma predeterminada, el mensaje no se repite. A menos que elija actualizar todas las máquinas a la vez, el mensaje de notificación se mostrará en cada máquina en el momento correspondiente antes de que empiece la actualización, calculada por un algoritmo interno.

Revertir una actualización

Después de aplicar una imagen maestra nueva o actualizada, puede revertirla. Puede ser necesario si surgen problemas con las máquinas recién actualizadas. Cuando revierte una actualización, las máquinas del catálogo vuelven a la última imagen funcional. Las nuevas funciones que requieran la nueva imagen ya no están disponibles. Al igual que en la implantación, la reversión de una máquina implica un reinicio.

1. Seleccione **Catálogos de máquinas** en el panel de navegación de **Studio**.
2. Seleccione el catálogo de máquinas y, a continuación, seleccione **Revertir actualización de máquinas** en el panel **Acciones**.
3. Puede especificar cuándo se aplicará la versión anterior de la imagen maestra a las máquinas de la manera que se describe más arriba, en la operación de implantación.

La reversión solo se aplica a máquinas que deben revertirse. En caso de máquinas que no se hayan actualizado con la imagen maestra nueva o actualizada (por ejemplo, máquinas con usuarios que no han cerrado sesión), los usuarios no reciben mensajes de notificación y no se ven obligados a cerrar sesión.

Actualizar un catálogo o revertir una actualización

Actualice el catálogo de máquinas después de actualizar los VDA de las máquinas a una versión más reciente. Citrix recomienda actualizar todos los VDA a la versión más reciente para permitir el acceso a todas las funciones nuevas.

Antes de actualizar un catálogo de máquinas:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Si utiliza Citrix Provisioning, debe actualizar la versión de VDA en la consola de Citrix Provisioning.
- Inicie las máquinas actualizadas para que se registren con el Controller. Esto permite a Studio determinar si las máquinas del catálogo necesitan actualización.

Para actualizar un catálogo de máquinas:

1. Seleccione **Catálogos de máquinas** en el panel de navegación de **Studio**.
2. Seleccione el catálogo. En la ficha **Detalles** del panel inferior, se muestra la información de versión.
3. Seleccione **Actualizar catálogo**. Si Studio detecta que el catálogo necesita actualización, se le informará mediante un mensaje. Siga las indicaciones. Si una o varias máquinas no se pueden actualizar, aparecerá un mensaje en el que se le explicará el motivo. Citrix recomienda resolver los problemas de máquinas antes de actualizar el catálogo para que todas las máquinas funcionen correctamente.

Después de completar la actualización del catálogo, puede revertir las máquinas a sus versiones anteriores de VDA. Para ello, seleccione el catálogo y, a continuación, seleccione **Deshacer** en el panel **Acciones**.

Solucionar problemas

Para máquinas que presentan un "Estado de energía desconocido", consulte CTX131267 para obtener instrucciones.

Crear grupos de entrega

March 8, 2019

Un grupo de entrega es un conjunto de máquinas seleccionadas de uno o varios catálogos de máquinas. El grupo de entrega especifica los usuarios que pueden usar esas máquinas y las aplicaciones y/o escritorios disponibles para esos usuarios.

Crear un grupo de entrega es el siguiente paso de la configuración de la implementación después de crear un sitio y de crear un catálogo de máquinas. Posteriormente, puede cambiar los parámetros iniciales del primer grupo de entrega y crear otros. Sin embargo, existen funciones y configuraciones que se pueden definir solo cuando se modifica un grupo de entrega, no cuando se crea.

Para el acceso con Remote PC, cuando se crea un sitio, se crea automáticamente un grupo de entrega llamado "Escritorios de acceso con Remote PC".

Para crear un grupo de entrega:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

1. Si ya ha creado un sitio y un catálogo de máquinas, pero aún no ha creado ningún grupo de entrega, Studio le dirige al punto de partida para crear uno. En cambio, si ya ha creado un grupo de entrega y quiere crear otro, seleccione **Grupos de entrega** en el panel de navegación de Studio y, a continuación, seleccione **Crear grupo de entrega** en el panel "Acciones".
2. El asistente Crear grupo de entrega se inicia con la página **Introducción**, que se puede eliminar de futuros inicios de este asistente.
3. El asistente le guiará a través de las páginas que se describen a continuación. Cuando haya terminado en cada página, haga clic en **Siguiente** para llegar a la página final.

Paso 1: Máquinas

En la página **Máquinas**, seleccione un catálogo y especifique la cantidad de máquinas que quiere usar de ese catálogo.

Conviene tener en cuenta lo siguiente:

- Al menos una máquina debe permanecer sin uso en el catálogo de máquinas seleccionado.
- Se puede especificar el mismo catálogo de máquinas en más de un grupo de entrega; sin embargo, una máquina solo se puede usar en un grupo de entrega.
- Un grupo de entrega puede usar más de un catálogo de máquinas. Sin embargo, esos catálogos deben contener los mismos tipos de máquina (SO de servidor, SO de escritorio o acceso con Remote PC). En otras palabras, no se pueden mezclar tipos de máquinas en un grupo de entrega. Del mismo modo, si la implementación contiene catálogos de máquinas Windows y Linux, un grupo de entrega puede contener máquinas de un tipo de sistema operativo, pero no ambos.
- Citrix recomienda instalar o actualizar todas las máquinas a la versión más reciente de VDA y, a continuación, actualizar los catálogos de máquinas y grupos de entrega según sea necesario. Al crear un grupo de entrega, si selecciona máquinas que tienen instaladas versiones diferentes de VDA, el grupo de entrega será compatible con la versión más antigua de VDA. (Esto es el *nivel funcional* del grupo.) Por ejemplo, si una de las máquinas que seleccione tiene instalada la versión 7.1 de VDA y otras máquinas tienen la versión actual, todas las máquinas del grupo podrán usar únicamente las funciones que se admitían en la versión 7.1 de VDA. Esto significa que algunas funcionalidades que requieran de versiones posteriores de VDA podrían no estar disponibles en ese grupo de entrega. Por ejemplo, para usar la funcionalidad AppDisks, los agentes VDA (y, por tanto, el nivel funcional del grupo) debe ser una versión mínima de 7.8.
- Todas las máquinas de un catálogo de acceso con Remote PC se asocian automáticamente a un grupo de entrega. Por eso, al crear un sitio de acceso con Remote PC, se crea automáticamente un catálogo denominado "Máquinas de acceso con Remote PC" y un grupo de entrega llamado "Escritorios de acceso con Remote PC".

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Paso 2: Tipo de entrega

Esta página solo aparece si ha seleccionado un catálogo que contiene máquinas estáticas (asignadas) de SO de escritorio.

Elija **Aplicaciones** o **Escritorios** en la página **Tipo de entrega**. No se puede habilitar ambas opciones.

Si ha seleccionado máquinas de un catálogo de máquinas aleatorias (agrupadas) de SO de servidor o SO de escritorio, se entiende que el tipo de entrega serán aplicaciones y escritorios, por lo que podrá entregar aplicaciones, escritorios o ambos.

Paso 3: AppDisks

AppDisks ha quedado obsoleto.

Para agregar un AppDisk, haga clic en **Agregar**. En el cuadro de diálogo Seleccionar AppDisks, se ofrece una lista de todos los AppDisks disponibles de la columna izquierda. En la columna derecha, se ofrece una lista de las aplicaciones presentes en el AppDisk. Al seleccionar la ficha **Aplicaciones** situada encima de la columna derecha, se muestran aplicaciones en un formato similar al del menú Inicio. Al seleccionar la ficha **Paquetes instalados**, se muestran aplicaciones en un formato similar al de la lista "Programas y características".

Marque una o varias casillas de verificación.

Paso 4: Usuarios

Especifique los usuarios y los grupos de usuarios que pueden utilizar las aplicaciones y los escritorios del grupo de entrega.

Dónde se especifican las listas de usuarios

Las listas de usuarios de Active Directory se especifican al crear o modificar lo siguiente:

- Una lista de acceso de usuarios a un sitio no configurada mediante Studio. La regla predeterminada de la directiva que rige los derechos a las aplicaciones incluye a todos los usuarios. Consulte los cmdlets `BrokerAppEntitlementPolicyRule` de PowerShell SDK 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

aplicación A para un departamento específico, sin restringir innecesariamente el acceso por parte de otros grupos:

- Use la regla predeterminada de directiva de derechos de aplicaciones que incluye a todos los usuarios.
- Configure la lista de usuarios del grupo de entrega para permitir que todos los usuarios de las oficinas centrales usen cualquiera de las aplicaciones especificadas en el grupo de entrega.
- (Si hay grupos de aplicaciones configurados) Configure la lista de usuarios del grupo de aplicaciones para permitir que los miembros de la unidad de negocio de Administración y Finanzas accedan a las aplicaciones con nombres desde la A a la L.
- Configure las propiedades de la aplicación A para restringir su visibilidad únicamente al personal de Cuentas por cobrar en el departamento de Administración y Finanzas.

Usuarios autenticados y no autenticados

Hay dos tipos de usuarios: los autenticados y los no autenticados (también llamados anónimos). Puede configurar uno o ambos tipos en un grupo de entrega.

- **Autenticado:** Para acceder a aplicaciones y escritorios, los usuarios y miembros del grupo cuyo nombre especifique deben introducir credenciales (como la tarjeta inteligente o el nombre de usuario y contraseña) en StoreFront o la aplicación Citrix Workspace. Para grupos de entrega que contengan máquinas de SO de escritorio, puede importar más tarde los datos de usuario (una lista de usuarios), al modificar el grupo de entrega.
- **No autenticado (anónimo):** Para grupos de entrega que contienen máquinas de SO de servidor, puede permitir a los usuarios acceder a sus aplicaciones y escritorios sin presentar credenciales a StoreFront o la aplicación Citrix Workspace. Por ejemplo, en máquinas quiosco, es posible que la aplicación requiera credenciales, mientras que el portal de acceso o las herramientas de Citrix no las requieran. Se crea un grupo de usuarios anónimos al instalar el primer Delivery Controller.

  Para conceder acceso a usuarios no autenticados, cada máquina del grupo de entrega debe tener instalado un VDA para SO de servidor Windows (versión mínima 7.6). Cuando los usuarios no autenticados están habilitados, se debe disponer de una tienda de StoreFront no autenticada.

  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 movilidad entre clientes y el control del espacio de trabajo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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

Conviene tener en cuenta lo siguiente:

- No se pueden agregar aplicaciones a grupos de entrega de acceso con Remote PC.
- De forma predeterminada, las aplicaciones nuevas 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 está agregando. Si rechaza la solicitud, la aplicación se agregará con un sufijo que hará su nombre único en la carpeta de aplicaciones.
- Al agregar una aplicación a más de un grupo de entrega, puede producirse un problema de visibilidad si no dispone de permisos suficientes para ver la aplicación en todos esos grupos de entrega. En tales casos, consulte a un administrador con más permisos o amplíe el ámbito para incluir todos los grupos de entrega a los que se haya agregado la aplicación.
- Si publica dos aplicaciones con el mismo nombre para los mismos usuarios, cambie la propiedad Nombre de la aplicación (para el usuario) en Studio; de lo contrario, los usuarios verán nombres duplicados en la aplicación Citrix Workspace.

Haga clic en **Agregar** para ver los orígenes de aplicación.

- **Desde el menú Inicio**: Se trata de las aplicaciones que se detectan en una máquina creada a partir de la imagen maestra en un catálogo de máquinas seleccionado. Cuando se selecciona este origen, se abre una nueva página con una lista de las aplicaciones detectadas; seleccione las que quiera agregar y, a continuación, haga clic en **Aceptar**.
- **Definidas manualmente**: Se trata de las aplicaciones que se encuentran en el sitio o en la red. Cuando se selecciona este origen, se abre una nueva página donde se escribe la ruta al archivo ejecutable, al directorio de trabajo, los argumentos de línea de comandos opcionales y los nom-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

bres simplificados para administradores y usuarios. Después de introducir la información, haga clic en **Aceptar**.

- **Existentes:** Se trata de aplicaciones agregadas anteriormente al sitio, existentes posiblemente en otro grupo de entrega. Cuando se selecciona este origen, se abre una nueva página con una lista de las aplicaciones detectadas; seleccione las que quiera agregar y, a continuación, haga clic en **Aceptar**.
- **App-V:** Se trata de las aplicaciones presentes en paquetes de App-V. Cuando se selecciona este origen, se abre una nueva página donde se puede seleccionar el servidor App-V o la biblioteca de aplicaciones. Seleccione las aplicaciones que quiera agregar y, a continuación, haga clic en **Aceptar**. Para obtener más información, consulte App-V.

Si una aplicación o su origen no están disponibles o no son válidos, no serán visibles o no se podrán seleccionar. Por ejemplo, el origen **Existentes** no está disponible si no hay aplicaciones que se hayan agregado al sitio. O bien, una aplicación podría no ser compatible con el tipo de sesiones admitidas en las máquinas del catálogo seleccionado.

Paso 6: Escritorios

El título de esta página depende del catálogo de máquinas que haya elegido anteriormente en la página **Máquinas**:

- Si eligió un catálogo que contiene máquinas agrupadas, esta página se llamará **Escritorios**.
- Si eligió un catálogo que contiene máquinas asignadas y especificó "Escritorios" en la página **Tipo de entrega**, esta página se llamará **Asignaciones de usuarios de escritorios**.
- Si eligió un catálogo que contiene máquinas asignadas y especificó "Aplicaciones" en la página **Tipo de entrega**, esta página se llamará **Asignaciones de usuarios de máquinas de aplicaciones**.

Haga clic en **Agregar**. En el cuadro de diálogo:

- En los campos Nombre simplificado y Descripción, escriba la información que se verá en la aplicación Citrix Workspace.
- Para agregar una restricción de etiqueta a un escritorio, elija **Restringir inicios a máquinas con la etiqueta** y, a continuación, seleccione la etiqueta en el menú desplegable. (Para obtener más información, consulte Etiquetas.)
- Mediante los botones de radio, indique quién puede iniciar un escritorio (para grupos con máquinas agrupadas) o a quién se asignará una máquina cuando inicie el escritorio (para grupos con máquinas asignadas). Los usuarios pueden ser todos los usuarios que puedan acceder a ese grupo de entrega, o bien, grupos de usuarios y usuarios específicos.
- Si el grupo contiene máquinas asignadas, especifique la cantidad máxima de escritorios por usuario. Este debe ser un valor de uno o más.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Habilite o inhabilite el escritorio (para máquinas agrupadas) o la regla de asignación de escritorios (para máquinas asignadas). Si inhabilita un escritorio, este deja de entregar escritorios; inhabilitar una regla de asignación de escritorios detiene la asignación automática de escritorios a los usuarios.
- Cuando haya finalizado con el cuadro de diálogo, haga clic en **Aceptar**.

Instancias máximas de un escritorio en un sitio (solo PowerShell)

Para configurar la cantidad máxima de instancias en un escritorio del sitio (solo PowerShell):

- En PowerShell, use el cmdlet BrokerEntitlementPolicyRule adecuado con el parámetro MaxPerEntitlementInstances. Por ejemplo, el siguiente cmdlet modifica la regla "tsvda-desktop" para establecer en dos la cantidad máxima de instancias simultáneas de un escritorio permitidas en el sitio. Cuando hay dos instancias de escritorio en ejecución, se produce un error si un tercer suscriptor intenta iniciar un escritorio.

  ```
  Set-BrokerEntitlementPolicyRule -Name tsvda-desktop -MaxPerEntitlementInstances
   2
  ```

- Para obtener ayuda, use el cmdlet Get-Help. Por ejemplo, `Get-Help Set-BrokerEntitlementPolicyRu -Parameter MaxPerEntitlementInstances`.

Paso 7: Resumen

Escriba un nombre para el grupo de entrega. También puede especificar una descripción (opcional), que aparecerá en Studio y en la aplicación Citrix Workspace.

Revise la información de resumen y, a continuación, haga clic en **Finalizar**. Si no ha seleccionado ninguna aplicación ni ha especificado escritorios a entregar, se le preguntará si quiere continuar.

Administrar grupos de entrega

March 8, 2019

Introducción

En este artículo se describen los procedimientos para administrar los grupos de entrega. 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Consulte el artículo Aplicaciones para obtener información sobre cómo administrar aplicaciones en los grupos de entrega. Ese artículo incluye cómo agregar y eliminar aplicaciones en un grupo de entrega y cómo cambiar las propiedades de una aplicación.

La administración de grupos de entrega requiere los permisos de administración delegada correspondientes al rol integrado de Administrador de grupo de entrega. Para obtener información más detallada, consulte Administración delegada.

Cambiar la configuración de usuario en un grupo de entrega

El nombre de esta página puede aparecer como **Parámetros de usuario** o **Parámetros básicos**.

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en el panel "Acciones".
3. En la página **Parámetros de usuario** (o **Parámetros básicos**), puede cambiar los parámetros de la tabla siguiente.
4. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta. También puede hacer clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

Parámetro	Descripción
Descripción	El texto que utiliza Citrix Workspace (o StoreFront) y que verán los usuarios.
Habilitar grupo de entrega	Indica si el grupo de entrega está habilitado o no.
Zona horaria	
Habilitar Secure ICA	Oculta todas las comunicaciones que tienen lugar desde y hacia las máquinas del grupo de entrega usando la funcionalidad SecureICA, que cifra el protocolo ICA. El nivel predeterminado es 128 bits. Este nivel se puede cambiar usando el SDK. Citrix recomienda el uso de métodos de cifrado adicionales como el cifrado TLS cuando se trabaje en redes públicas. Asimismo, SecureICA no comprueba la integridad de los datos.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Agregar o eliminar usuarios de un grupo de entrega

Para obtener más información acerca de los usuarios, consulte Usuarios.

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en el panel "Acciones".
3. En la página **Usuarios**, para agregar usuarios, haga clic en **Agregar** y especifique los usuarios que quiere agregar. Para quitar usuarios, seleccione uno o varios usuarios y, a continuación, haga clic en **Quitar**. Marque o desmarque la casilla para permitir el acceso a usuarios no autenticados.
4. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta. También puede hacer clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

Importar o exportar listas de usuarios

Para grupos de entrega que contengan máquinas físicas con SO de escritorio, puede importar la información de usuarios desde un archivo CSV después de crear el grupo de entrega. También es posible exportar información de usuarios a un archivo CSV. El archivo CSV puede contener datos de una versión anterior del producto.

La primera línea del archivo CSV debe contener encabezados de columna separados por comas (no necesariamente por orden), que pueden ser: `ADComputerAccount`, `AssignedUser`, `VirtualMachine`, y `HostId`. Las siguientes líneas del archivo deben contener datos separados por comas. Las entradas `ADComputerAccount` pueden ser nombres comunes, direcciones IP, nombres distintivos o pares de nombres de dominios y equipos.

Para importar o exportar la información de usuarios:

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo de entrega y, a continuación, haga clic en **Modificar grupo de entrega** en el panel "Acciones".
3. En la página **Asignación de máquinas**, seleccione el botón **Importar lista** o **Exportar lista** y, a continuación, vaya a la ubicación del archivo.
4. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta. También puede hacer clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en el panel "Acciones".
3. En la página **Tipo de entrega**, seleccione el tipo de entrega que quiere.
4. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta. También puede hacer clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

Cambiar direcciones de StoreFront

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en el panel "Acciones".
3. En la página **StoreFront**, seleccione o agregue direcciones URL de StoreFront que utiliza la aplicación Citrix Workspace instalada en cada máquina del grupo de entrega.
4. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta. También puede hacer clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

También puede especificar la dirección de servidor StoreFront tras seleccionar **Configuración > StoreFront** en el panel de navegación de Studio.

Agregar, modificar o eliminar una restricción de etiqueta para un escritorio

Agregar, modificar o eliminar restricciones de etiqueta puede tener efectos no esperados en los escritorios que se tengan en cuenta para el inicio. Consulte las precauciones y los aspectos a tener en cuenta en Etiquetas.

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en el panel "Acciones".
3. En la página **Escritorios**, seleccione el escritorio y haga clic en **Modificar**.
4. Para agregar una restricción de etiqueta, elija **Restringir inicios a máquinas con la etiqueta** y, a continuación, seleccione la etiqueta.
5. Para cambiar o eliminar una restricción de etiqueta, ya sea:
   - Seleccione otra etiqueta.
   - Puede eliminar la restricción de etiqueta al desmarcar la casilla **Restringir inicios a máquinas con esta etiqueta** .
6. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta. También puede hacer clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Actualizar o revertir la versión de un grupo de entrega

Actualice un grupo de entrega después de actualizar la versión de los VDA de sus máquinas y los catálogos de máquinas que contengan las máquinas que se usan en ese grupo de entrega.

Antes de iniciar la actualización del grupo de entrega:

- Si utiliza Citrix Provisioning (antes Provisioning Services), debe actualizar la versión de VDA en la consola de Citrix Provisioning.
- Inicie las máquinas que contienen el VDA actualizado para que se registren con un Delivery Controller. Este proceso indica a Studio los elementos que necesitan actualización del grupo de entrega.
- Si debe seguir usando versiones anteriores de VDA, es posible que las funciones más recientes del producto no estén disponibles. Para obtener más información, consulte los artículos de actualización de versiones.

Para actualizar un grupo de entrega:

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo de entrega y haga clic en **Actualizar grupo de entrega** en el panel "Acciones". La acción **Actualizar grupo de entrega** aparece solo si Studio detecta agentes VDA actualizados.

Studio le indica qué máquinas, si las hay, no pueden actualizarse y por qué. A continuación, puede cancelar la actualización, resolver los problemas de las máquinas y, luego, iniciar de nuevo el proceso de actualización.

Después de completar la actualización, puede revertir las máquinas a su estado anterior. Para ello, seleccione el grupo de entrega y, a continuación, haga clic en **Deshacer** en el panel "Acciones".

Administrar grupos de entrega de acceso con Remote PC

Si una máquina del catálogo de acceso con Remote PC no está asignada a ningún usuario, Studio la asigna temporalmente a un grupo de entrega asociado a ese catálogo de máquinas. Esta asignación temporal permite que la máquina se asigne más tarde a un usuario.

La asociación de grupo de entrega a catálogo de máquinas tiene un valor de prioridad. La prioridad determina a qué grupo de entrega se asigna la máquina cuando esta se registra en el sistema o cuando un usuario necesita que se le asigne una máquina: cuanto menor sea el valor, mayor será la prioridad. Si un catálogo de máquinas de acceso con Remote PC tiene varias asignaciones de grupos de entrega, el software selecciona la de prioridad más alta. Puede configurar este valor de prioridad con el SDK de PowerShell.

Nada más crearse, los catálogos de máquinas de acceso con Remote PC se asocian a un grupo de entrega. Esto significa que las cuentas de máquina o unidades organizativas que se agreguen al catálogo

© 1999-2019 Citrix Systems, Inc. All rights reserved.

de máquinas más adelante se pueden agregar al grupo de entrega. Esta asociación se puede activar o desactivar.

Para agregar o quitar una asociación de catálogo de máquinas de acceso con Remote PC a un grupo de entrega:

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
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**.

Apagar y reiniciar máquinas en un grupo de entrega

No se admite este procedimiento en las máquinas de acceso con Remote PC.

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo y, a continuación, seleccione **Ver máquinas** en el panel "Acciones".
3. Seleccione la máquina y, a continuación, seleccione una de las siguientes opciones del panel Acciones (es posible que, según el estado de la máquina, algunas opciones no estén disponibles):
    - **Forzar apagado:** Apaga la máquina y actualiza la lista de máquinas.
    - **Reiniciar:** Solicita al sistema operativo que se apague y que, a continuación, vuelva a iniciar la máquina. Si el sistema operativo no puede hacerlo, esta permanece en su estado actual.
    - **Forzar reinicio:** Obliga al sistema operativo a apagarse y, a continuación, reinicia la máquina.
    - **Suspender:** Pausa la máquina sin apagarla y actualiza la lista de máquinas.
    - **Apagar:** Solicita al sistema operativo de la máquina que se apague.

Para acciones no 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 evitar que los usuarios de máquinas de SO de escritorio 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. Consulte Conexiones y recursos.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Administrar la energía de las máquinas de un grupo de entrega

Solo es posible administrar las opciones de energía de las máquinas con SO de escritorios virtuales, no las máquinas físicas (incluidas las máquinas de acceso con Remote PC). Las máquinas de SO de escritorio y con capacidad de GPU no se pueden suspender, por lo que las operaciones de apagado dan error. Para máquinas de SO de servidor, puede crear una programación de reinicios.

En grupos de entrega que contengan máquinas agrupadas, las máquinas virtuales de SO de escritorio 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 de SO de escritorio pueden ser:

- De asignación permanente y en uso
- De asignación permanente y no conectadas (pero listas)
- No asignadas y no conectadas

Durante el uso habitual, los grupos de entrega estáticos normalmente contienen máquinas asignadas de forma permanente y máquinas sin asignar. Al principio, todas las máquinas se presentan sin asignar (excepto las máquinas asignadas manualmente al crearse el grupo de entrega). Cuando los usuarios se conectan, las máquinas pasan a estar asignadas de forma permanente. Puede administrar la totalidad de las opciones de energía de las máquinas sin asignar en esos grupos de entrega. En cambio, la administración de energía de las máquinas de asignación permanente solo es parcial.

- **Agrupaciones y búferes:** Para grupos de entrega agrupados y grupos de entrega estáticos con máquinas sin asignar, una agrupación (en este caso) es un conjunto de máquinas no asignadas o asignadas temporalmente que se mantienen en estado activo y listas para que se conecten los usuarios. El usuario obtiene una máquina inmediatamente después de iniciar sesión. El tamaño de la agrupación (la cantidad de máquinas que se mantienen activas) se puede configurar en función del momento del día. En caso de grupos de entrega estáticos, utilice el SDK para configurar la agrupación.

  Un búfer es un conjunto adicional de máquinas sin asignar que se mantienen en modo de espera. Estas se inician cuando la cantidad de dichas máquinas en la agrupación se encuentra por debajo de un umbral. El umbral es un porcentaje del tamaño del grupo de entrega. Para grupos de entrega grandes, se puede encender una cantidad significativa de máquinas cuando se excede el umbral. Por lo tanto, planifique con cuidado los tamaños del grupo de entrega o use el SDK para ajustar el tamaño predeterminado del búfer.

- **Temporizadores de estado de energía:** Puede usar temporizadores de estado de energía para suspender máquinas después de que los usuarios se hayan desconectado durante un período de tiempo especificado. Por ejemplo, las máquinas se suspenderán automáticamente fuera

© 1999-2019 Citrix Systems, Inc. All rights reserved.

del horario de oficina si los usuarios han estado desconectados durante, al menos, 10 minutos. Las máquinas aleatorias o las máquinas con discos Personal vDisk se apagan automáticamente cuando los usuarios cierran sesión, a menos que se configure la propiedad de grupo de entrega `ShutdownDesktopsAfterUse` en el SDK.

Se pueden configurar temporizadores para los días de la semana y para los fines de semana, para intervalos de horas punta y viceversa.

- **Administración parcial de energía en máquinas de asignación permanente:** En caso de máquinas de asignación permanente, se pueden configurar temporizadores de estado de energía, pero no agrupaciones o búferes. Las máquinas se encienden al comienzo de cada período de mayor actividad (hora punta) y se apagan al comienzo de cada período de actividad normal. De modo que no se tiene un control preciso (como con las máquinas sin asignar) sobre la cantidad de máquinas que pasan a estar disponibles para compensar las máquinas consumidas.

Para administrar la energía de las máquinas con SO de escritorio virtual

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en el panel "Acciones".
3. En la página **Administración de energía**, seleccione **Lunes a Viernes** en la lista desplegable **Administrar energía de las máquinas**. De manera predeterminada, se consideran los días de lunes a viernes como los días de la semana.
4. Para grupos de entrega aleatorios, en **Máquinas para iniciar**, seleccione **Modificar** y especifique el tamaño de la agrupación de lunes a viernes. A continuación, seleccione la cantidad de máquinas que quiere iniciar.
5. En **Horas punta**, establezca las horas punta y las horas normales para cada día.
6. Establezca los temporizadores de estado de energía para las horas punta y las horas normales durante los días de la semana. Para ello, en **Durante horas punta > Cuando está desconectado**, especifique la demora (en minutos) que deben transcurrir antes de suspender una máquina desconectada del grupo de entrega y seleccione **Suspender**. En **Durante horas normales > Cuando está desconectado**, especifique la demora que debe transcurrir antes de apagar una máquina del grupo de entrega con la sesión cerrada y seleccione **Apagar**. Este temporizador no está disponible para grupos de entrega con máquinas aleatorias.
7. Seleccione **Fin de semana** en la lista desplegable **Administrar energía de las máquinas** y, a continuación, configure las horas de mayor actividad y los temporizadores de estado de energía para los fines de semana.
8. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta. También puede hacer clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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.

Para cambiar el porcentaje de agentes VDA en un estado de energía para catálogos

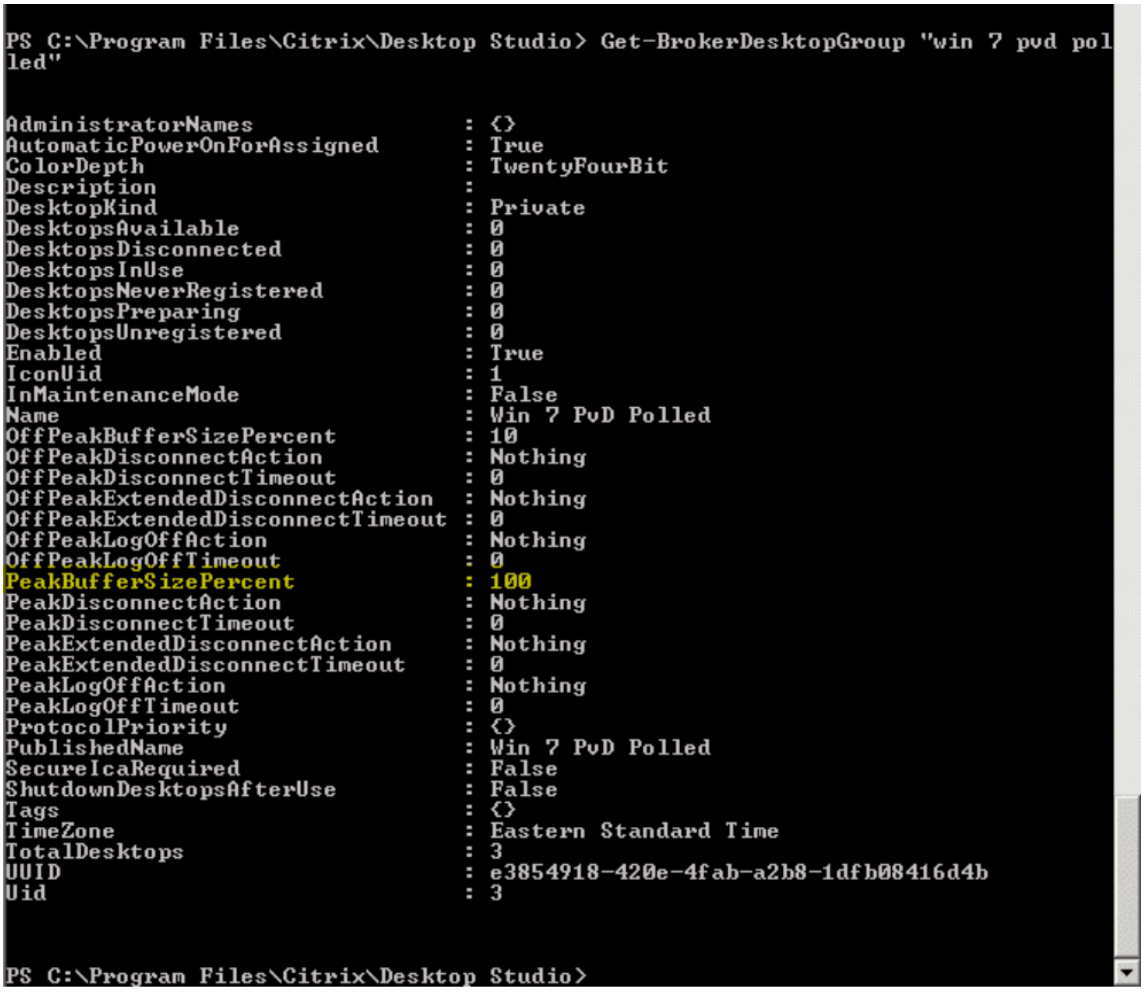
1. Ajuste las horas pico para el grupo de escritorios desde la sección **Administración de energía** para el **grupo de entrega**.
2. Tome nota del nombre del grupo de escritorios.
3. Con privilegios de administrador, inicie PowerShell y ejecute los siguientes comandos. Reemplace “Nombre del grupo de 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”
   ```

© 1999-2019 Citrix Systems, Inc. All rights reserved.



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 pico y que estén disponibles para los usuarios después de cerrar sesión, introduzca:

```
## Set-BrokerDesktopGroup ”Desktop Group Name”-AutomaticPowerOnForAssignedDuringPeak
 $True
```

Crear y administrar programaciones de reinicios para las máquinas de un grupo de entrega

Una programación de reinicios especifica cuándo se reinician periódicamente las máquinas de un grupo de entrega. Puede crear una o varias programaciones para un grupo de entrega. Una programación puede afectar a:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- 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 de etiqueta, porque la etiqueta restringe una acción solo a los elementos (en este caso, máquinas) que tienen la etiqueta.

Por ejemplo: todas las máquinas están en un solo grupo de entrega y quiere reiniciarlas todas al menos una vez por semana, salvo las máquinas que utiliza el departamento de contabilidad, que deben reiniciarse todos los días. Quiere reiniciar todas las máquinas al menos una vez por semana, salvo las máquinas que utiliza el departamento de contabilidad, que deben reiniciarse todos los días. Para ello, configure una programación para todas las máquinas y otra para las máquinas del departamento de contabilidad.

Una programación incluye el día y la hora en que comienza el reinicio, así como la duración de este. La duración es "iniciar todas las máquinas afectadas al mismo tiempo" o el tiempo que debe tardarse en reiniciar todas las máquinas afectadas.

Puede activar o desactivar una programación. Inhabilitar una programación puede ser útil durante la realización de pruebas, durante intervalos especiales o cuando se preparan programaciones antes de necesitarlas.

No puede usar programaciones para el encendido o apagado automáticos desde Studio, solo para reiniciar.

Superposición de programaciones

Es posible que las programaciones se solapen. En el ejemplo anterior, ambas programaciones afectan a las máquinas utilizadas por el equipo de contabilidad. Esas máquinas podrían reiniciarse dos veces el domingo.
Ahora bien, la programación está diseñada para evitar tener que reiniciar la misma máquina con más frecuencia de la necesaria, pero eso no puede garantizarse.

- Si las programaciones se solapan en la hora de inicio y la duración, es más probable que las máquinas se reinicien una sola vez.
- Por tanto, cuanto más difieran las programaciones en la hora de inicio y la duración, más probable será que haya varios reinicios.
- La cantidad de máquinas que se vean afectadas por los reinicios programados también puede influir en las posibilidades de superposición. En el ejemplo, la programación semanal que afecta a todas las máquinas podría iniciar los reinicios mucho más rápidamente que el 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Ver programaciones de reinicios

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en el panel "Acciones".
3. Seleccione la página **Programación de reinicios**.

La página **Programación de reinicios** contiene la siguiente información para cada programación configurada:

- Nombre de la programación.
- Restricción de etiqueta utilizada, si la hay.
- La frecuencia con se producen los reinicios de las máquinas.
- Si los usuarios de la máquina reciben una notificación.
- Si la programación está habilitada. Inhabilitar una programación puede ser útil durante la realización de pruebas, durante intervalos especiales o cuando se preparan programaciones antes de necesitarlas.

Agregar (aplicar) etiquetas

Si configura una programación de reinicios que usa una restricción de etiqueta, compruebe que esa etiqueta se ha agregado (aplicado) a las máquinas a las que esa programación debería afectar. (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.

En el ejemplo anterior, cada una de las máquinas utilizadas por el equipo de contabilidad tendría una etiqueta aplicada.

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione el grupo de entrega que contiene las máquinas a las que afectará la programación.
3. Haga clic en **Ver máquinas** y, a continuación, seleccione las máquinas a las que agregará la etiqueta.
4. Haga clic en **Administrar etiquetas** en el panel "Acciones".
5. Si la etiqueta ya existe, marque la casilla situada junto al nombre de la etiqueta. Si la etiqueta no existe, haga clic en **Crear** y especifique el nombre de la etiqueta. Una vez creada, marque la casilla situada junto al nombre de la etiqueta recién creada.
6. Haga clic en **Guardar** en el cuadro de diálogo **Administrar etiquetas**.

Crear una programación de reinicios

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en el panel "Acciones".
3. En la página **Programación de reinicios**, haga clic en **Agregar**.
4. En la página **Agregar programación de reinicios**:
    - Escriba un nombre y una descripción para la programación.
    - Si utiliza una restricción de etiqueta, seleccione la etiqueta.
    - En **Frecuencia de reinicio**, seleccione la frecuencia con que se produce el reinicio (diariamente, de lunes a viernes, los días del fin de semana o un día concreto cada semana).
    - Con el reloj de 24 horas, especifique la hora del día para comenzar el reinicio.
    - Para la **Duración de reinicio**, elija si todas las máquinas deben reiniciarse al mismo tiempo, o bien elija la franja total del tiempo necesario para empezar a reiniciar todas las máquinas afectadas. Un algoritmo interno determina cuándo se reinicia cada máquina durante ese intervalo.
    - En **Enviar notificación a los usuarios**, elija si mostrar un mensaje de notificación en las máquinas correspondientes antes de empezar un reinicio. De forma predeterminada, no se muestra ningún mensaje.
    - Si elige mostrar un mensaje 15 minutos antes de empezar el reinicio, puede decidir (en "Frecuencia de notificación") si repetir el mensaje cada cinco minutos después del primer mensaje. De forma predeterminada, el mensaje no se repite.
    - Escriba el título y el texto de la notificación. No hay texto predeterminado.

      Si quiere que el mensaje incluya la cantidad de minutos que quedan antes del reinicio, incluya la variable **%m%**. Por ejemplo: "Advertencia: Su equipo se reiniciará automáticamente dentro de %m% minutos". El valor disminuye cinco minutos en cada mensaje repetido. A menos que haya optado por reiniciar todas las máquinas a la vez, el mensaje de notificación se mostrará en cada máquina en el momento correspondiente antes de que empiece el reinicio, calculado por un algoritmo interno.
    - Para habilitar la programación, marque la casilla de verificación. Para inhabilitar la programación, desmarque la casilla de verificación.
5. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta, o bien haga clic en "Aceptar" para aplicar los cambios y cerrar la ventana.

Modificar, quitar, habilitar o inhabilitar una programación de reinicios

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en el panel "Acciones".
3. En la página **Programación de reinicios**, marque la casilla de una programación.
    - Para modificar una programación, haga clic en **Modificar**. Actualice los parámetros de la programación siguiendo las instrucciones indicadas en Crear una programación de reinicios.
    - Para habilitar o inhabilitar una programación, haga clic en **Modificar**. Marque o desmarque la casilla **Habilitar programación de reinicios**.
    - Para eliminar una programación, haga clic en **Quitar**. Confirme la eliminación. (La eliminación de una programación no afecta a las etiquetas aplicadas a las máquinas afectadas.)

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 de SO de servidor está en modo de mantenimiento, los usuarios pueden conectarse a las sesiones existentes, pero no pueden iniciar sesiones nuevas.
- Cuando una máquina de SO de escritorio (o un PC de acceso con Remote PC) está en modo de mantenimiento, los usuarios no pueden conectarse ni volver a conectarse a ella. Las conexiones actuales permanecen conectadas hasta que se desconectan o cierran sesión.

Para activar o desactivar el modo de mantenimiento:

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo.
3. Para activar el modo de mantenimiento en todas las máquinas de un grupo de entrega, seleccione **Activar modo de mantenimiento** en el panel "Acciones". Para activar el modo de mantenimiento en una máquina, seleccione **Ver máquinas** en el panel "Acciones". Seleccione una máquina y, a continuación, seleccione **Activar modo de mantenimiento** en el panel "Acciones".
4. Para desactivar el modo de mantenimiento en una o todas las máquinas de un grupo de entrega, siga las instrucciones anteriores, pero seleccione **Desactivar modo de mantenimiento** en el panel "Acciones".

La configuración de la Conexión a Escritorio remoto (RDC) de Windows también afecta a si una máquina de SO de servidor está en modo de mantenimiento o no. El modo de mantenimiento se activa en cualquiera de las siguientes circunstancias:

- Cuando el modo de mantenimiento se activa, como se ha descrito anteriormente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Cuando la conexión a Escritorio remoto se establece en **No permitir las conexiones a este equipo**.
- Cuando la conexión a Escritorio remoto no se establece en **No permitir las conexiones a este equipo** y el parámetro "Modo de inicio de sesión de usuario en la Configuración de host remoto" es **Permitir reconexiones, pero impedir nuevos inicios de sesión** o **Permitir reconexiones, pero impedir nuevos inicios de sesión hasta que el servidor se reinicie**.

También puede activar o desactivar el modo de mantenimiento de:

- Una conexión, que afecta a las máquinas que usan esa conexión.
- Un catálogo de máquinas, que afecta a las máquinas en ese catálogo.

Cambiar asignaciones de máquinas a usuarios en un grupo de entrega

Puede cambiar las asignaciones de las máquinas de SO de escritorio aprovisionadas con MCS. No puede cambiar las asignaciones para máquinas de SO de servidor o máquinas aprovisionadas con Citrix Provisioning.

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo.
3. Seleccione **Modificar grupo de entrega** en el panel "Acciones". En la página **Escritorios** o **Reglas de asignación de escritorio** (el título de la página depende del tipo de catálogo que utilice el grupo de entrega), especifique los nuevos usuarios.
4. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta. También puede hacer clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

Cambiar la cantidad máxima de máquinas por usuario

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en el panel "Acciones".
3. En la página **Reglas de asignación de escritorio**, establezca los escritorios máximos por usuario.
4. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta. También puede hacer clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

Administrar la carga de las máquinas de un grupo de entrega

Solo puede administrar la carga de las máquinas de SO de servidor.

La Administración de carga mide la carga del servidor y determina el servidor que desea seleccionar en el entorno actual. Esta selección se basa en:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Estado del modo de mantenimiento del servidor:** Una máquina de SO de servidor 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 de servidor. 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). Debe especificar los patrones de carga en la configuración de la directiva de administración de carga.

  Puede supervisar el índice de carga en el SDK, en Director y en la búsqueda de Studio.

  De forma predeterminada, la columna de **índice de carga del servidor** está oculta en Studio. Para que esa columna aparezca, primero seleccione una máquina. A continuación, seleccione con el botón secundario el encabezado de una columna y elija **Seleccionar columna**. En la **Categoría de máquina**, seleccione **Índice de carga**.

  En el SDK, use el cmdlet `Get-BrokerMachine`. Para obtener más información, consulte CTX202150.

  Un índice de carga de servidor de 10000 indica que la carga del servidor es total. Si no hay otros servidores disponibles, es posible que los usuarios reciban un mensaje en el que se les notifica que el escritorio o la aplicación no están disponibles cuando intentan iniciar sesión.
- **Configuración 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 de XenApp anteriores a 7.5.)

  Si todos los servidores se encuentran en, o superan, 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.

Quitar una máquina de un grupo de entrega

Al quitar una máquina, se elimina de un grupo de entrega. No se eliminará del catálogo de máquinas que el grupo de entrega utiliza. Por lo tanto, esa máquina está disponible para la asignación a otro grupo de entrega.

Las máquinas deben estar apagadas antes de poder eliminarlas. Para impedir temporalmente que los usuarios se conecten a una máquina mientras se procede a quitarla, ponga la maquina en modo de mantenimiento antes de apagarla.

Las máquinas pueden contener datos personales, así que actúe con precaución a la hora de asignar una máquina a otro usuario. Considere restablecer la imagen inicial de la máquina.

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

2. Seleccione un grupo y, a continuación, seleccione **Ver máquinas** en el panel "Acciones".
3. Compruebe que la máquina esté apagada.
4. Seleccione **Quitar del grupo de entrega** en el panel "Acciones".

También puede quitar una máquina de un grupo de entrega a través de la conexión que usa la máquina. Para obtener más información, consulte Conexiones y recursos.

Restringir el acceso a máquinas en un grupo de entrega

Todos los cambios que realice para restringir el acceso a las máquinas de un grupo de entrega anulan los parámetros anteriores, independientemente del método que utilice. Puede:

- **Restringir el acceso de los administradores mediante los ámbitos de administración delegada:** Puede crear y asignar un ámbito que permita el acceso de los administradores a todas las aplicaciones, y otro ámbito que conceda acceso solamente a determinadas aplicaciones. Para obtener más información, consulte Administración delegada.
- **Restringir el acceso de los usuarios a través de las expresiones de directiva SmartAccess:** Use las expresiones de la directiva para filtrar las conexiones de usuario realizadas a través de Citrix Gateway.

  1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
  2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en el panel "Acciones".
  3. En la página **Directiva de acceso**, seleccione **Conexiones a través de NetScaler Gateway**.
  4. Para elegir un subconjunto de esas conexiones, seleccione **Conexiones que cumplan cualquiera de estos filtros**. Ahora defina el sitio de Citrix Gateway y agregue, modifique o quite las expresiones de directiva SmartAccess para las situaciones de acceso autorizado de los usuarios. Para obtener información más detallada, consulte la documentación de Citrix Gateway.
  5. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta. También puede hacer clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

- **Restringir el acceso de los usuarios a través de los filtros de exclusión:** Use los filtros de exclusión incluidos en las directivas de acceso que usted estableció en el SDK. Las directivas de acceso se aplican a grupos de entrega para limitar las conexiones. Por ejemplo, puede restringir el acceso a las máquinas por parte de un subconjunto de usuarios. También puede especificar los dispositivos de usuario permitidos. El uso de filtros de exclusión permite definir más detalladamente las directivas de acceso. Por ejemplo, por razones de seguridad, puede negar el acceso a un subconjunto de usuarios o dispositivos. De forma predeterminada, los filtros de exclusión están inhabilitados.

  Por ejemplo: en el caso de un laboratorio escolar ubicado en una subred dentro de la

© 1999-2019 Citrix Systems, Inc. All rights reserved.

red corporativa, para impedir el acceso desde ese laboratorio a un determinado grupo de entrega, independientemente del usuario que utilice las máquinas del laboratorio, use el comando siguiente: `Set-BrokerAccessPolicy -Name VPDesktops_Direct -ExcludedClientIPFilterEnabled $True -`.

Puede utilizar el asterisco (*) como comodín para hacer coincidir todas las etiquetas que comienzan por la misma expresión de directiva. Por ejemplo, si agrega la etiqueta `VPDesktops_Direct` a una máquina y `VPDesktops_Test` a otra, al configurar la etiqueta en el script `Set-BrokerAccessPolicy` como `VPDesktops_*`, se aplica el filtro a las dos máquinas.

Si se conecta mediante un explorador Web o con la funcionalidad de experiencia de usuario de la aplicación Citrix Workspace habilitada en la tienda, no puede usar un filtro de exclusión de nombres de clientes.

Actualizar una máquina en un grupo de entrega

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo y, a continuación, seleccione **Ver máquinas** en el panel "Acciones".
3. Seleccione una máquina y, a continuación, seleccione **Actualizar máquinas** en el panel "Acciones".

Para elegir otra imagen maestra, seleccione **Imagen maestra** y, a continuación, seleccione una instantánea.

Para aplicar cambios y notificar a los usuarios de la máquina, seleccione **Notificación de implantación para usuarios finales**. A continuación, especifique:

- El momento de la actualización de la imagen maestra: ahora o en el próximo reinicio
- La hora de la distribución de reinicios (el tiempo total para comenzar a actualizar todas las máquinas del grupo)
- Si los usuarios serán notificados del reinicio
- El mensaje que los usuarios recibirán

Cerrar una sesión, desconectarla o enviar un mensaje a los usuarios de un grupo de entrega

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo y, a continuación, seleccione **Ver máquinas** en el panel "Acciones".
3. Para cerrar la sesión de un usuario, seleccione la sesión o el escritorio y, a continuación, seleccione **Cerrar sesión** en el panel "Acciones". La sesión se cierra y la máquina queda disponible para otros usuarios, a menos que esté asignada a un usuario concreto.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

4. Para desconectar una sesión, seleccione la sesión o el escritorio y, a continuación, seleccione **Desconectar** en el panel "Acciones". Las aplicaciones siguen ejecutándose y la máquina permanece asignada a ese usuario. El usuario puede volver a conectarse a la misma máquina.
5. Para enviar un mensaje a los usuarios, seleccione la sesión, la máquina o el usuario y, a continuación, seleccione **Enviar mensaje** en el panel "Acciones". Escriba el mensaje.

Puede configurar temporizadores de estado de energía para las máquinas de SO de escritorio a fin de gestionar automáticamente las sesiones que no se estén utilizando. Para obtener información más detallada, consulte Administrar energía de las máquinas.

Configurar el preinicio de sesiones y la persistencia de sesiones en un grupo de entrega

Estas funciones solo se admiten en máquinas con SO de servidor.

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, el preinicio de sesiones y la persistencia de sesiones no se usan: se inicia una sesión cuando un usuario inicia una aplicación, y esta permanece activa hasta que se cierre la última aplicación abierta de la sesión.

Consideraciones:

- El grupo de entrega debe admitir aplicaciones, y las máquinas deben estar ejecutando un VDA para SO de servidor 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, pero solo cuando están conectadas. 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`).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- 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.

  Este parámetro no se puede inhabilitar desde Studio, pero sí se puede en el SDK (con el cmdlet New/Set-BrokerSessionPreLaunch). Si inhabilita el tiempo de espera, este no aparece en la pantalla de Studio 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.

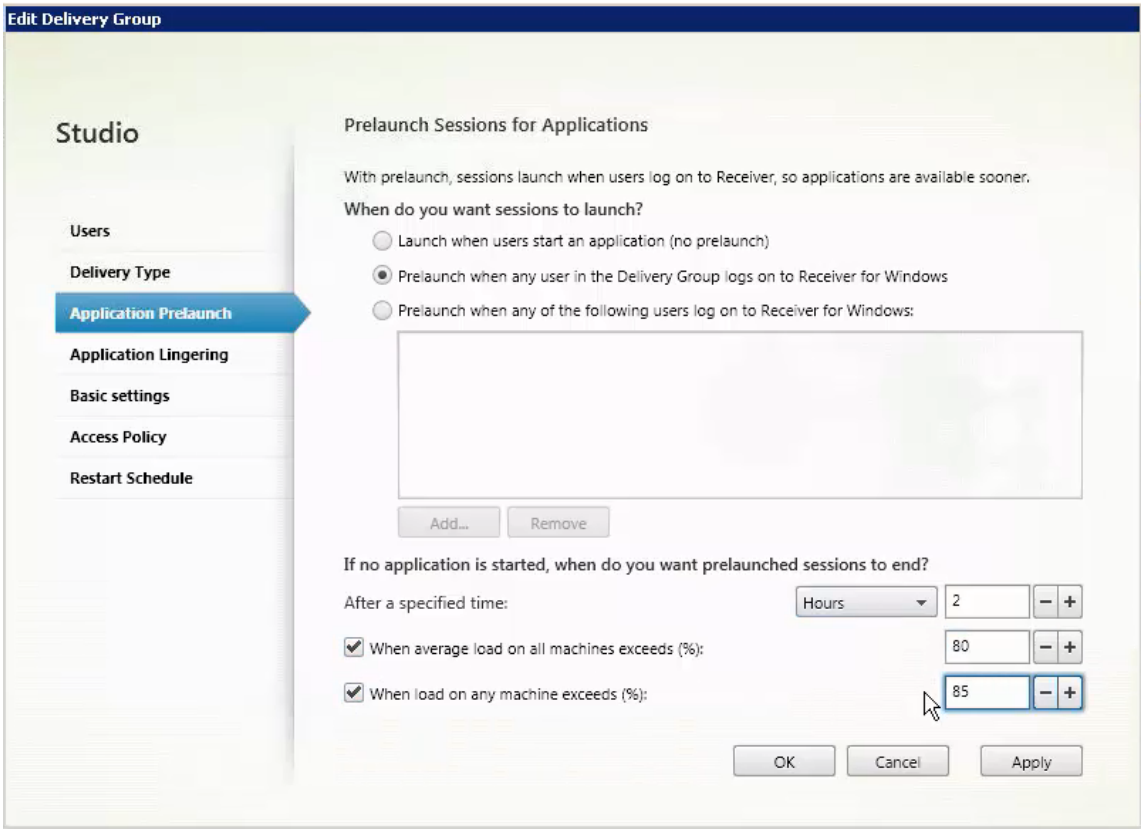
  Puede configurar dos umbrales: el porcentaje medio de carga para todos los servidores del grupo de entrega y el porcentaje máximo de carga para un servidor único del grupo de entrega. Cuando se supera un umbral, se finalizan aquellas sesiones que hayan tenido el estado de preinicio o persistente durante más tiempo. Las sesiones se finalizan una a una con intervalos de minutos entre cada cierre hasta que la carga baje 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para habilitar la función de preinicio de sesiones

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en el panel "Acciones".
3. En la página **Preinicio de aplicaciones**, habilite el preinicio de sesiones. Para ello, elija cuándo deben iniciarse estas:
   - Cuando un usuario inicia una aplicación. Esta es la opción predeterminada. El preinicio de sesiones está inhabilitado.
   - Cuando un usuario del grupo de entrega inicia sesión en la aplicación Citrix Workspace para Windows.
   - Cuando alguien de una lista de usuarios y grupos de usuarios inicia sesión en la aplicación Citrix Workspace para Windows. Si elige esta opción, compruebe que ha especificado también los usuarios o los grupos de usuarios.



4. Una sesión preiniciada se reemplaza por una sesión habitual cuando el usuario inicia una aplicación. Si el usuario no inicia una aplicación (es decir, la sesión preiniciada no se llega a utilizar), la siguiente configuración afecta a la cantidad de tiempo que esta sesión permanece activa.
   - Cuando se agota un intervalo de tiempo especificado. Puede cambiar el intervalo de tiempo (de 1-99 días, de 1-2376 horas, o de 11-42 560 minutos).

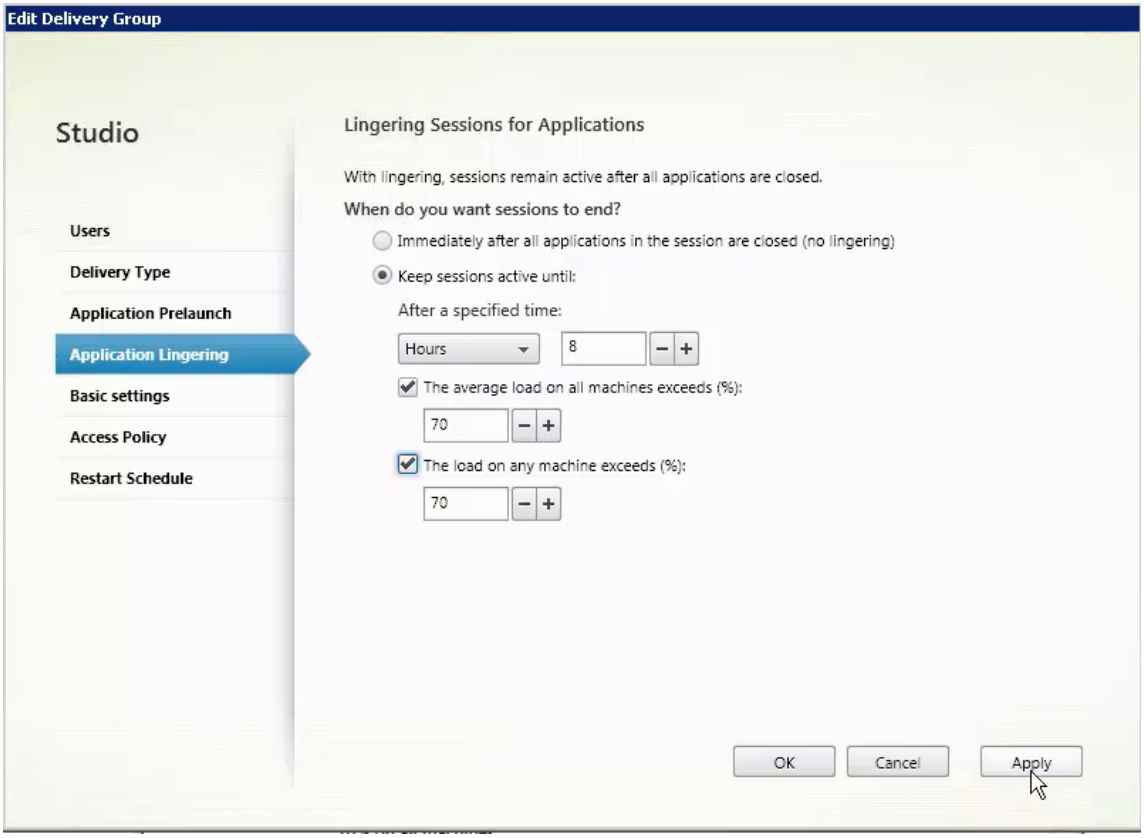
© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Cuando el promedio de carga de todas las máquinas del grupo de entrega supera un porcentaje especificado (del 1-99%).
- Cuando la carga de una máquina del grupo de entrega supera un porcentaje especificado (del 1-99%).

En resumen, una sesión preiniciada permanece activa hasta que se da uno de los siguientes eventos: un usuario inicia una aplicación, se agota el tiempo especificado, o se supera un umbral de carga especificado.

Para habilitar la persistencia de sesiones

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar grupo de entrega** en el panel "Acciones".
3. En la página **Persistencia de aplicaciones**, habilite la persistencia de sesiones seleccionando la opción **Mantener las sesiones activas hasta**.



4. Algunos parámetros influyen en la cantidad de tiempo que las sesiones persistentes pueden permanecer activas si el usuario no inicia otra aplicación.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Cuando se agota un intervalo de tiempo especificado. Puede cambiar el intervalo de tiempo: de 1-99 días, de 1-2376 horas, o de 11-42 560 minutos.
- Cuando el promedio de carga de todas las máquinas del grupo de entrega supera un porcentaje especificado: 1-99%.
- Cuando la carga de una máquina del grupo de entrega supera un porcentaje especificado: del 1-99%.

En resumen, una sesión persistente permanece activa hasta que se da uno de los siguientes eventos: un usuario inicia una aplicación, se agota el tiempo especificado, o se supera un umbral de carga especificado.

Solucionar problemas

- Los VDA que no estén registrados en un Delivery Controller no se tienen en cuenta cuando se inician sesiones con broker, lo que provoca una infrautilización de recursos que podrían estar disponibles. Existen diversos motivos por los que un VDA puede no registrarse, y un administrador puede solucionar muchos de ellos. Para solucionar problemas, Studio proporciona información en el Asistente para la creación de catálogos y después de agregar el catálogo a un grupo 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. 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 "Detalles", porque ahí se ofrecen 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 Studio, la "versión instalada de VDA" en el panel Detalles referente al grupo de entrega puede variar de la versión real instalada en las máquinas. La pantalla Programas y características de la máquina Windows muestra la versión real del VDA.
- Para máquinas que presentan un "Estado de energía desconocido", consulte CTX131267 para obtener instrucciones.

Crear grupos de aplicaciones

March 8, 2019

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Introducción

Los grupos de aplicaciones permiten administrar colecciones de aplicaciones. Puede crear grupos de aplicaciones para las aplicaciones compartidas entre varios grupos de entrega o que son utilizadas por un subconjunto de usuarios dentro de un grupo de entrega. Los grupos de aplicaciones son optativos: ofrecen una alternativa para no tener que agregar las mismas aplicaciones a varios grupos de entrega. Los grupos de entrega se pueden asociar con varios grupos de aplicaciones, y un grupo de aplicaciones puede estar asociado a varios grupos de entrega.

El uso de grupos de aplicaciones puede proporcionar ventajas para la administración de aplicaciones y para el control de los recursos frente a la opción de grupos de entrega:

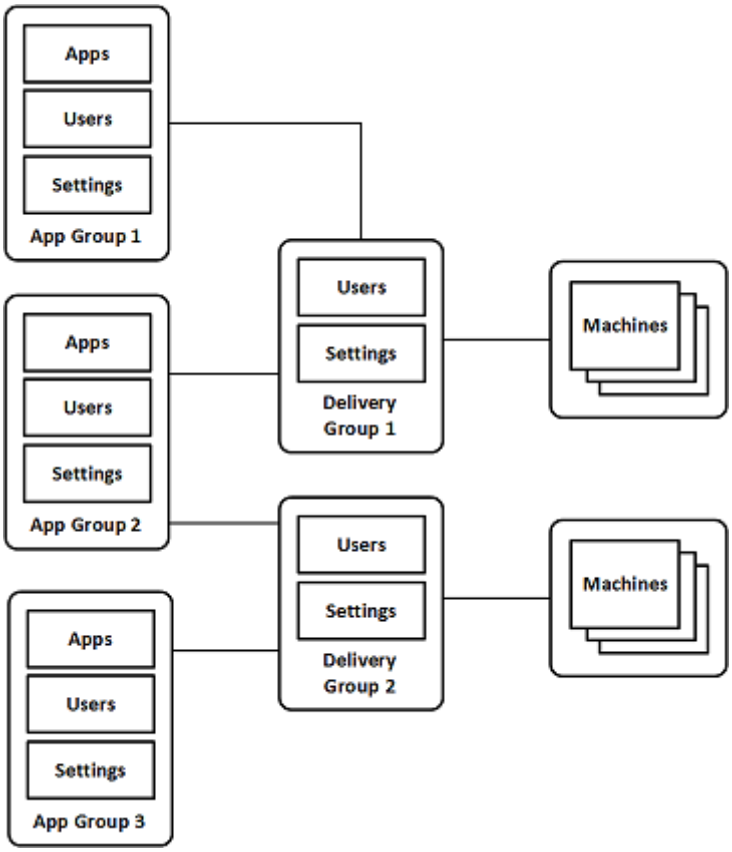
- La agrupación lógica de las aplicaciones y sus parámetros permite administrar esas aplicaciones como una sola unidad. Por ejemplo, no tiene que agregar (publicar) la misma aplicación en grupos de entrega individuales de uno en uno.
- Compartir sesiones entre grupos de aplicaciones puede reducir el consumo de los recursos. En otros casos, la inhabilitación del uso compartido de sesiones entre grupos de aplicaciones puede ser beneficioso.
- Puede usar la función de restricción de etiqueta 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 máquinas adicionales. La restricción de etiqueta puede entenderse como una subdivisión (o partición) de las máquinas de un grupo de entrega. Usar un grupo de aplicaciones o escritorios con una restricción de etiqueta puede ser útil para aislar un subconjunto de las máquinas de un grupo de entrega y solucionar los problemas que presentan.

Ejemplos de configuración

Ejemplo 1:

El gráfico siguiente muestra una implementación de Citrix Virtual Apps and Desktops que incluye grupos de aplicaciones:

© 1999-2019 Citrix Systems, Inc. All rights reserved.



En esta configuración, las aplicaciones se agregan a los grupos de aplicaciones no a los grupos de entrega. Los grupos de entrega especifican qué máquinas se usarán. (Aunque no se muestra, las máquinas se encuentran en catálogos de máquinas.)

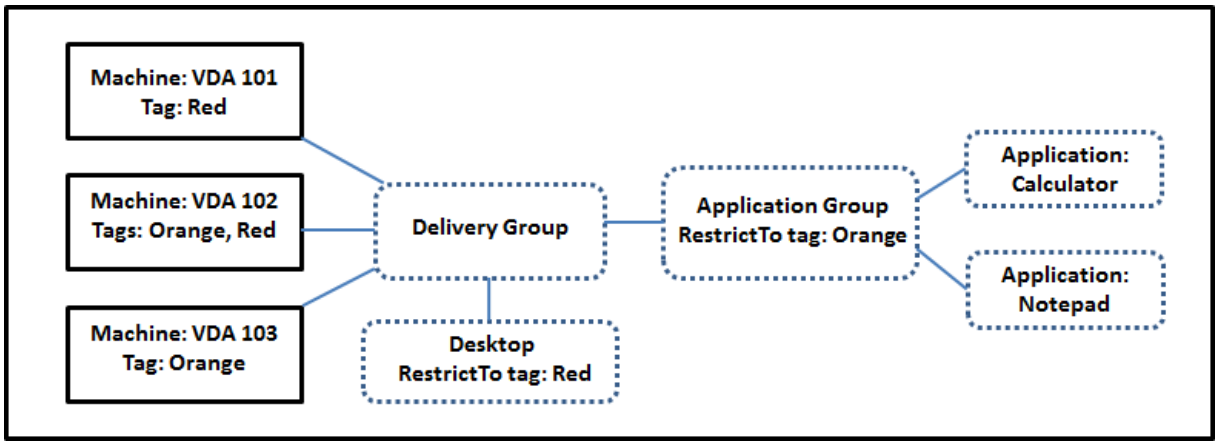
El grupo de aplicaciones 1 está asociado al grupo de entrega 1. A las aplicaciones del Grupo de aplicaciones 1 tienen acceso los usuarios especificados en el Grupo de aplicaciones 1, siempre y cuando también estén en la lista de usuarios del Grupo de entrega 1. Esto es conforme a la recomendación de que la lista de usuarios de un grupo de aplicaciones debe ser un subconjunto (una restricción) de la lista de usuarios del grupo de entrega asociado. Los parámetros del Grupo de aplicaciones 1 (tales como el uso compartido de sesiones entre grupos de aplicaciones y los grupos de entrega asociados) se aplican a las aplicaciones y los usuarios de ese grupo. Los parámetros del Grupo de entrega 1 (tales como el respaldo para usuarios anónimos) se aplican a los usuarios de los grupos de aplicaciones 1 y 2, porque esos grupos de aplicaciones se han asociado a ese grupo de entrega.

El Grupo de aplicaciones 2 está asociado a dos grupos de entrega: 1 y 2. Se puede asignar una prioridad a cada uno de esos grupos de entrega en el Grupo de aplicaciones 2, para indicar el orden en que se comprobarán los grupos de entrega cuando se inicie una aplicación. Si los grupos de entrega tienen la misma prioridad, se les aplica el equilibrio de carga. A las aplicaciones del Grupo de aplicaciones 2 tienen acceso los usuarios especificados en el Grupo de aplicaciones 2, siempre y cuando también estén en la lista de usuarios de los grupos de entrega 1 y 2.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Ejemplo 2:

En esta sencilla distribución, se usan restricciones de etiqueta para limitar las máquinas que se tendrán en cuenta para ciertos inicios de aplicaciones y escritorios. El sitio tiene un grupo de entrega compartido, un escritorio publicado, y un grupo de aplicaciones configurado con dos aplicaciones.



Se han agregado etiquetas a cada una de las tres máquinas (VDA 101, 102 y 103).

El grupo de aplicaciones se creó con la restricción de etiqueta “Naranja”, por lo que cada una de sus aplicaciones (Calculadora y Bloc de notas) solo se pueden iniciar en las máquinas de ese grupo de entrega que tengan la etiqueta “Naranja”: VDA 102 y 103.

Para ver instrucciones y ejemplos más detallados sobre cómo usar las restricciones de etiqueta en los grupos de aplicaciones (y escritorios), consulte Etiquetas.

Información orientativa y consideraciones

Citrix recomienda agregar aplicaciones a grupos de aplicaciones o grupos de entrega, pero no a ambos. De lo contrario, la complejidad de tener las aplicaciones asignadas a dos tipos de grupos puede complicar la administración de las mismas.

De forma predeterminada, hay un grupo de aplicaciones habilitado. Después de crear un grupo de aplicaciones, puede modificar el grupo para cambiar este parámetro. Consulte Administrar grupos de aplicaciones.

De forma predeterminada, se pueden compartir sesiones entre grupos de aplicaciones. Consulte Compartir sesiones entre grupos de aplicaciones.

Citrix recomienda que los grupos de entrega se actualicen a la versión actual. Eso requiere:

1. Actualizar los VDA de las máquinas utilizadas en el grupo de entrega.
2. Actualizar los catálogos que contienen esas máquinas.
3. Actualizar el grupo de entrega.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 grupo de entrega. Para obtener información más detallada, consulte Administración delegada.

Este artículo se refiere a la "asociación" de una aplicación con varios grupos de aplicaciones para diferenciarla de la acción de agregar una nueva instancia de esa aplicación desde algún origen disponible. Del mismo modo, los grupos de entrega se asocian con grupos de aplicaciones (y viceversa), en lugar de ser agregados como componentes unos de otros.

Compartir sesiones con grupos de aplicaciones

Cuando se habilita la capacidad de compartir sesiones de aplicación, todas las aplicaciones se inician en la misma sesión de aplicación. Lo que reduce los costes asociados al inicio de aplicaciones adicionales y permite las funciones de aplicación que hacen uso del Portapapeles, como las operaciones de copiar y pegar contenido. Sin embargo, podría interesarle desactivar el uso compartido de sesiones en algunas situaciones.

Cuando se usan grupos de aplicaciones, se puede configurar el uso compartido de las sesiones de aplicación de las siguientes tres maneras (que amplían el comportamiento estándar del uso compartido de sesiones que solo está disponible cuando se usan grupos de entrega):

- Uso compartido de sesiones habilitado entre grupos de aplicaciones.
- Uso compartido de sesiones habilitado solamente entre las aplicaciones de un mismo grupo de aplicaciones.
- Uso compartido de sesiones inhabilitado.

Compartir sesiones entre grupos de aplicaciones

Puede permitir que las sesiones de aplicaciones se compartan entre los grupos de aplicaciones, o bien, puede inhabilitarlo para limitar la capacidad de compartir sesiones solo a las aplicaciones que se encuentren en el mismo grupo de aplicaciones.

- **Este es un ejemplo de cuándo puede ser útil habilitar el uso compartido de sesiones entre los grupos de aplicaciones:**

  El grupo de aplicaciones 1 contiene aplicaciones de Microsoft Office como Word y Excel. El grupo de aplicaciones 2 contiene otras aplicaciones (como el Bloc de notas y la Calculadora), y ambos grupos de aplicaciones están conectados al mismo grupo de entrega. Un usuario que tiene

© 1999-2019 Citrix Systems, Inc. All rights reserved.

acceso a ambos grupos de aplicaciones inicia una sesión de aplicación abriendo Word y, a continuación, abre 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 de etiqueta excluye la máquina donde se ejecuta la sesión), se crea una nueva sesión en otra máquina, en lugar de compartir sesiones.

- **Este es un ejemplo de cuándo puede ser útil inhabilitar el uso compartido de sesiones entre los grupos de aplicaciones:**

  Tiene un conjunto de aplicaciones que no pueden interactuar correctamente con otras aplicaciones instaladas en las mismas máquinas: por ejemplo, dos versiones diferentes de una misma suite de software o dos versiones diferentes del mismo explorador Web. Usted prefiere no permitir que un usuario inicie ambas versiones en una misma sesión.

  Puede crear un grupo de aplicaciones para cada versión de la suite de software y agregar las aplicaciones para cada versión de la suite al grupo de aplicaciones correspondiente. Si el uso compartido de sesiones entre los grupos se inhabilita para cada uno de esos grupos de aplicaciones, un usuario especificado en esos grupos puede ejecutar las aplicaciones de la misma versión en la misma sesión, y puede ejecutar otras aplicaciones al mismo tiempo, pero no en la misma sesión. Si el usuario inicia una de las aplicaciones de diferente versión (que se encuentra en un grupo de aplicaciones distinto) o inicia cualquier aplicación que no está contenida en un grupo de aplicaciones, esa aplicación se inicia en una nueva sesión.

Compartir sesiones entre los grupos de aplicaciones no es una función de seguridad de sandbox. No es totalmente segura y no puede impedir que los usuarios inicien aplicaciones en sus sesiones por otros medios (por ejemplo, a través del Explorador de Windows).

Si una máquina alcanza su capacidad máxima, no se inician nuevas sesiones en ella. Las nuevas aplicaciones se inician en las sesiones existentes en la máquina compartiendo sesiones si fuera necesario (siempre que eso concuerde con las restricciones respecto a compartir sesiones que se describen aquí).

Solo se pueden ofrecer las sesiones preiniciadas a los grupos de aplicaciones que tienen permitido compartir sesiones. (Las sesiones que usan la funcionalidad Persistencia de sesiones están disponibles a todos los grupos de aplicaciones.) Esas funciones deben habilitarse y configurarse en cada uno de los grupos de entrega asociados al grupo de aplicaciones; no se pueden configurar en los grupos de aplicaciones.

De forma predeterminada, se pueden compartir sesiones entre grupos de aplicaciones cuando se crea un grupo de aplicaciones. No puede cambiar esto cuando crea el grupo. Después de crear un grupo de aplicaciones, puede modificar el grupo para cambiar este parámetro. Consulte Administrar grupos de aplicaciones.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Inhabilitar el uso compartido de sesiones en un grupo de aplicaciones

Puede impedir que las aplicaciones que se encuentran en el mismo grupo compartan sesiones.

- **Este es un ejemplo de cuándo puede ser útil impedir que se compartan sesiones entre los grupos de aplicaciones:**

  Si quiere que los usuarios accedan a varias sesiones simultáneas de pantalla completa de una aplicación en varios monitores.

  Cree un grupo de aplicaciones y agréguele las aplicaciones. Si las aplicaciones de ese grupo no pueden compartir sesiones, cuando un usuario especificado en el grupo inicia una aplicación y después otra, las aplicaciones se inician en sesiones distintas y el usuario puede mover cada una a un monitor aparte.

De forma predeterminada, se pueden compartir sesiones entre grupos de aplicaciones cuando se crea un grupo de aplicaciones. No puede cambiar esto cuando crea el grupo. Después de crear un grupo de aplicaciones, puede modificar el grupo para cambiar este parámetro. Consulte Administrar grupos de aplicaciones.

Crear un grupo de aplicaciones

Para crear un grupo de aplicaciones:

1. Seleccione **Aplicaciones** en el panel de navegación de Studio y, a continuación, seleccione **Crear grupo de aplicaciones** en el panel "Acciones".
2. El asistente Crear grupo de aplicaciones se inicia con la página **Introducción**, que se puede eliminar de futuros inicios de este asistente.
3. El asistente le guiará a través de las páginas que se describen a continuación. Cuando haya terminado con cada página, haga clic en **Siguiente** para ir a la página final.

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 de SO de servidor o de escritorio aleatorias (no asignadas de manera permanente o estática).
- La lista **Grupos de entrega incompatibles** contiene grupos de entrega que no puede seleccionar. Cada entrada explica por qué no es compatible, como, por ejemplo, porque contienen máquinas asignadas estáticas.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Un grupo de aplicaciones se puede asociar con grupos de entrega que contengan máquinas compartidas (no privadas) que puedan entregar aplicaciones.

También puede seleccionar grupos de entrega que contengan máquinas compartidas que solo entregan escritorios, siempre que se cumplan las dos condiciones siguientes:

- El grupo de entrega contiene máquinas compartidas y se creó con una versión de XenDesktop anterior a 7.9.
- Usted tiene el permiso Modificar grupo de entrega.

El tipo de grupo de entrega se convierte automáticamente a “escritorios y aplicaciones” cuando se confirma el asistente Crear grupo de aplicaciones.

Aunque puede crear un grupo de aplicaciones que no tenga grupos de entrega asociados (por ejemplo, para organizar aplicaciones o para servir de almacenamiento para las aplicaciones que no se están utilizando en ese momento), el grupo de aplicaciones no se puede usar para entregar aplicaciones hasta que se especifica al menos un grupo de entrega. Además, no se pueden agregar aplicaciones al grupo de aplicaciones desde la opción de origen **Desde el menú Inicio** si no hay grupos de entrega especificados.

Los grupos de entrega que seleccione especifican las máquinas que se usarán para entregar aplicaciones. Marque las casillas de verificación que aparecen junto a los grupos de entrega que quiere asociar con el 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 quién puede usar las aplicaciones del grupo de aplicaciones. Puede permitir todos los usuarios y los grupos de usuarios de los grupos de entrega seleccionados en la página anterior, o puede seleccionar un grupo específico de usuarios y grupos de usuarios de los grupos de entrega. Si restringe el uso a unos cuantos usuarios especificados, solo los usuarios especificados en el grupo de entrega y el grupo de aplicaciones pueden acceder a las aplicaciones de este grupo de aplicaciones. Básicamente, la lista de usuarios del grupo de aplicaciones proporciona un filtro en las listas de usuarios de los grupos de entrega.

El uso de las aplicaciones por parte de usuarios no autenticados solo puede habilitarse o inhabilitarse en los grupos de entrega, no en los grupos de aplicaciones.

Para obtener información sobre dónde se especifican las listas de usuarios en una implementación, consulte Dónde se especifican las listas de usuarios.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Paso 3: Aplicaciones

Conviene tener en cuenta lo siguiente:

- De forma predeterminada, las aplicaciones nuevas 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 está agregando. Si acepta el nombre único sugerido, la aplicación se agrega con ese nombre. De lo contrario, cambie el nombre antes de agregarla. Para obtener más información, consulte Administrar carpetas de aplicaciones.
- Puede cambiar las propiedades de una aplicación (parámetros) al agregarla, o más tarde. Consulte Cambiar las propiedades de la aplicación. Si publica dos aplicaciones con el mismo nombre para los mismos usuarios, cambie la propiedad **Nombre de la aplicación (para el usuario)** en Studio. De lo contrario, los usuarios verán nombres duplicados en la aplicación Citrix Workspace.
- Al agregar una aplicación a más de un grupo de entrega, puede haber un problema de visibilidad si no dispone de permisos suficientes para ver la aplicación en todos esos grupos de entrega. En tales casos, consulte a un administrador con más permisos o amplíe su ámbito para incluir todos los grupos a los que se haya agregado la aplicación.

Haga clic en la lista desplegable **Agregar** para ver los orígenes de aplicación.

- **Desde el menú Inicio:** Se trata de las aplicaciones que se detectan en una máquina de los grupos de entrega seleccionados. Cuando se selecciona este origen, se abre una nueva página con una lista de aplicaciones detectadas. Marque las casillas de 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 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

origen, se abre una nueva página donde se puede seleccionar el servidor App-V o la biblioteca de aplicaciones. En la vista resultante, marque las casillas de las aplicaciones que quiere agregar y, a continuación, haga clic en **Aceptar**. Para obtener más información, consulte App-V. Este origen no se puede seleccionar (o no aparece) si App-V no está configurado en el sitio.

Como se ha indicado, algunas de las entradas de la lista desplegable **Agregar** no se pueden seleccionar si no existe ningún origen válido de ese tipo. Los orígenes que son incompatibles no aparecen (por ejemplo, no se pueden agregar grupos de aplicaciones a grupos de aplicaciones, por lo que ese origen no aparece en la lista cuando se crea un grupo de aplicaciones).

Paso 4: Ámbitos

Esta página aparecerá solo si se ha creado antes un ámbito personalizado. De forma predeterminada, está seleccionado el ámbito **Todo**. Para obtener más información, consulte Administración delegada.

Paso 5: Resumen

Escriba un nombre para el grupo de aplicaciones. También puede especificar una descripción (optativa).

Revise la información de resumen y, a continuación, haga clic en **Finalizar**.

Administrar grupos de aplicaciones

March 8, 2019

> Nota:
>
> Cuando se utilizan grupos de aplicaciones con Citrix Virtual Apps and Desktops Service, la función de restricción por etiqueta no está disponible por el momento.

Introducción

En este artículo, se describe cómo administrar grupos de aplicaciones después de crearlos.

Consulte el artículo Aplicaciones para obtener información sobre cómo administrar aplicaciones en los grupos de entrega o los grupos de aplicaciones, incluido cómo:

- Agregar o quitar aplicaciones en un grupo de aplicaciones.
- Cambiar asociaciones de grupos de aplicaciones.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

La administración de grupos de aplicaciones requiere los permisos de administración delegada correspondientes al rol integrado de Administrador de grupo de entrega. Para obtener información más detallada, consulte Administración delegada.

Habilitar o inhabilitar un grupo de aplicaciones

Cuando se habilita un grupo de aplicaciones, este grupo puede distribuir las aplicaciones que se hayan agregado a él. Cuando se inhabilita un grupo de aplicaciones, se inhabilitan las aplicaciones incluidas en él. Sin embargo, si esas aplicaciones también están asociadas con otros grupos de aplicaciones que sí están habilitados, esas aplicaciones pueden seguir siendo entregadas desde esos otros grupos. Del mismo modo, si las aplicaciones se agregaron explícitamente a grupos de entrega asociados con el grupo de aplicaciones (además de agregarlas al grupo de aplicaciones), cuando se inhabilita el grupo de aplicaciones esto no afecta a esas aplicaciones agregadas a esos grupos de entrega.

Un grupo de aplicaciones está habilitado cuando se crea. No puede cambiar esto cuando crea el grupo.

1. Seleccione **Aplicaciones** en el panel de navegación de Studio.
2. Seleccione el grupo de aplicaciones en el panel central y, a continuación, seleccione **Modificar grupo de aplicaciones** en el panel "Acciones".
3. En la página **Parámetros**, marque o desmarque la casilla **Habilitar grupo de aplicaciones**.
4. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta, o bien haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

Habilitar o inhabilitar el uso compartido de sesiones de aplicación entre grupos de aplicaciones

Se pueden compartir sesiones entre grupos de aplicaciones cuando se crea un grupo de aplicaciones. No puede cambiar esto cuando crea el grupo. Para obtener más información, consulte Compartir sesiones con grupos de aplicaciones.

1. Seleccione **Aplicaciones** en el panel de navegación de Studio.
2. Seleccione el grupo de aplicaciones en el panel central y, a continuación, seleccione **Modificar grupo de aplicaciones** en el panel "Acciones".
3. En la página **Parámetros**, marque o desmarque la casilla **Habilitar uso compartido de sesiones de aplicaciones entre grupos de aplicaciones**.
4. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta, o bien haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Inhabilitar el uso compartido de sesiones de aplicación en un grupo de aplicaciones

De forma predeterminada, se pueden compartir sesiones de aplicaciones en el mismo grupo de aplicaciones cuando se crea un grupo de aplicaciones. Aunque inhabilite la posibilidad de compartir sesiones de aplicaciones entre grupos de aplicaciones, se podrán compartir sesiones entre aplicaciones del mismo grupo.

Puede usar el SDK de PowerShell para configurar grupos de aplicaciones con el uso compartido de sesiones inhabilitado entre las aplicaciones que contienen. En algunas circunstancias, esto puede ser conveniente. Por ejemplo, si quiere que los usuarios inicien aplicaciones no integradas en ventanas de aplicación de pantalla completa en monitores diferentes.

Cuando se inhabilita el uso compartido de sesiones dentro de un grupo de aplicaciones, cada aplicación de ese grupo se inicia en una nueva sesión de aplicación. Si está disponible una sesión desconectada adecuada (que ejecuta la misma aplicación), se vuelve a conectar a esa sesión. Por ejemplo, si se inicia el Bloc de notas y hay una sesión desconectada que ejecuta el Bloc de notas, se reconecta a esa sesión en lugar de crear una nueva. Si están disponibles varias sesiones desconectadas adecuadas, se elige una de ellas para reconectarse de forma aleatoria pero determinante. En otras palabras, si se vuelve a dar la situación en la mismas circunstancias, se selecciona la misma sesión, pero la elección no es necesariamente predecible en otras circunstancias

Puede usar el SDK de PowerShell para inhabilitar el uso compartido de sesiones de aplicación para todas las aplicaciones de un grupo de existente, o bien, para crear un grupo de aplicaciones con el uso compartido de sesiones inhabilitado.

Ejemplos de cmdlets de PowerShell

Para inhabilitar el uso compartido de sesiones, use los cmdlets Broker de 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
  ```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Consideraciones

- Para habilitar la propiedad `SingleAppPerSession`, debe establecer la propiedad `SessionSharingEnabled` en False. No se deben habilitar las dos propiedades al mismo tiempo. El parámetro `SessionSharingEnabled` hace referencia a compartir sesiones entre grupos de aplicaciones.
- Compartir sesiones solo funciona para aplicaciones que están asociadas a grupos de aplicaciones, pero no están asociadas a grupos de entrega. (Todas las aplicaciones asociadas directamente a un grupo de entrega comparten sesiones de forma predeterminada.)
- Si una aplicación se asigna a varios grupos de aplicaciones, compruebe que los grupos no tienen parámetros en conflicto. Por ejemplo, un grupo tiene la opción establecida en True, mientras que el otro en False, lo que resulta en un comportamiento inesperado.

Cambiar el nombre a un grupo de aplicaciones

1. Seleccione **Aplicaciones** en el panel de navegación de Studio.
2. Seleccione el grupo de aplicaciones en el panel central y, a continuación, seleccione **Cambiar nombre de grupo de aplicaciones** en el panel "Acciones".
3. Especifique un nuevo nombre único y, a continuación, haga clic en **Aceptar**.

Agregar, quitar o cambiar la prioridad de las asociaciones de grupos de entrega con un grupo de aplicaciones

Un grupo de aplicaciones se puede asociar con grupos de entrega que contengan máquinas compartidas (no privadas) que puedan entregar aplicaciones.

También puede seleccionar grupos de entrega que contengan máquinas compartidas que solo entregan escritorios, siempre que se cumplan las dos condiciones siguientes:

- El grupo de entrega contiene máquinas compartidas y se creó con una versión anterior a 7.9.
- Usted tiene el permiso Modificar grupo de entrega.

El tipo de grupo de entrega se convierte automáticamente a "escritorios y aplicaciones" cuando se confirma el cuadro de diálogo Modificar grupo de aplicaciones.

1. Seleccione **Aplicaciones** en el panel de navegación de Studio.
2. Seleccione el grupo de aplicaciones en el panel central y, a continuación, seleccione **Modificar grupo de aplicaciones** en el panel "Acciones".
3. Seleccione la página **Grupos de entrega**.
4. Para agregar grupos de entrega, haga clic en **Agregar**. Marque las casillas de los grupos de entrega disponibles. (Los grupos de entrega incompatibles no se pueden seleccionar.) Cuando termine de seleccionarlos, haga clic en **Aceptar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

5. Para eliminar grupos de entrega, marque las casillas de los grupos que quiere eliminar y luego haga clic en **Eliminar**. Confirme la eliminación cuando se le solicite.
6. Para cambiar la prioridad de un grupo de entrega, seleccione ese grupo y, a continuación, haga clic en **Modificar prioridad**. Especifique una prioridad (0 = máxima prioridad) y, a continuación, haga clic en **Aceptar**.
7. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta, o bien haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

Agregar, modificar o eliminar una restricción de etiqueta en un grupo de aplicaciones

Agregar, modificar o eliminar restricciones de etiqueta puede tener efectos no esperados en las máquinas que se tengan en cuenta para iniciar las aplicaciones. Consulte las precauciones y los aspectos a tener en cuenta en Etiquetas.

1. Seleccione **Aplicaciones** en el panel de navegación de Studio.
2. Seleccione el grupo de aplicaciones en el panel central y, a continuación, seleccione **Modificar grupo de aplicaciones** en el panel "Acciones".
3. Seleccione la página **Grupos de entrega**.
4. Para agregar una restricción 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 de la lista desplegable o quite la restricción de etiqueta por completo desmarcando **Restringir inicios a máquinas con la etiqueta**.
6. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta, o bien haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

Agregar o eliminar usuarios en un grupo de aplicaciones

Para obtener más información acerca de los usuarios, consulte Crear grupos de aplicaciones.

1. Seleccione **Aplicaciones** en el panel de navegación de Studio.
2. Seleccione el grupo de aplicaciones en el panel central y, a continuación, seleccione **Modificar grupo de aplicaciones** en el panel "Acciones".
3. Seleccione la página **Usuarios**. Indique si quiere permitir que todos los usuarios de los grupos de entrega asociados usen las aplicaciones del grupo de aplicaciones, o si solo quiere que la usen grupos y usuarios específicos. Para agregar usuarios, haga clic en **Agregar** y especifique los usuarios que quiere agregar. Para quitar usuarios, seleccione uno o varios usuarios y, a continuación, haga clic en **Quitar**.
4. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta, o bien haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Cambiar ámbitos en un grupo de aplicaciones

Puede cambiar un ámbito solo si usted lo ha creado (no puede modificar el ámbito Todo). Para obtener más información, consulte Administración delegada.

1. Seleccione **Aplicaciones** en el panel de navegación de Studio.
2. Seleccione el grupo de aplicaciones en el panel central y, a continuación, seleccione **Modificar grupo de aplicaciones** en el panel "Acciones".
3. Seleccione la página **Ámbitos**. Marque o deje sin marcar la casilla correspondiente a un ámbito.
4. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta, o bien haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

Eliminar un grupo de aplicaciones

La aplicación debe estar asociada con, al menos, un grupo de entrega o un grupo de aplicaciones. Si eliminar un grupo de aplicaciones provocará que una o varias aplicaciones dejen de pertenecer a un grupo, se le advertirá que, al eliminar el grupo, también se eliminarán esas aplicaciones. Entonces, puede confirmar o cancelar la eliminación.

Eliminar una aplicación aquí no la elimina de su lugar de origen. Sin embargo, si quiere que la aplicación vuelva a estar disponible, tendrá que volver a agregarla.

1. Seleccione **Aplicaciones** en el panel de navegación de Studio.
2. Seleccione el grupo de aplicaciones en el panel central y, a continuación, seleccione **Eliminar grupo** en el panel "Acciones".
3. Confirme la eliminación cuando se le solicite.

Acceso con Remote PC

January 29, 2019

El acceso con Remote PC permite a un usuario final iniciar sesión de forma remota en el equipo físico Windows de la oficina desde prácticamente cualquier lugar.

El Virtual Delivery Agent (VDA) se instala en el equipo de la oficina. Este VDA se registra en Cloud Connector o Delivery Controller, y administra la conexión HDX entre el equipo y los dispositivos cliente del usuario final. El acceso con Remote PC admite un modelo de autoservicio. Después de configurar la lista blanca de máquinas a las que pueden acceder los usuarios, estos podrán iniciar sesión en sus equipos de oficina por cuenta propia, sin la intervención del administrador. La aplicación Citrix Workspace, ejecutada en el dispositivo cliente, permite el acceso a las aplicaciones y los datos almacenados en el equipo de la oficina desde la sesión de escritorio de acceso con Remote PC.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Un usuario puede tener varios escritorios, incluidos varios equipos físicos o una combinación de equipos físicos y escritorios virtuales.

> **Nota:**
>
> Para implementaciones locales: Acceso remoto a PC es válido solo para licencias de Citrix Virtual Desktops. Las sesiones consumen licencias del mismo modo que otras sesiones de Citrix Virtual Desktops.

Consideraciones sobre Active Directory

Antes de configurar el sitio de implementación de acceso con Remote PC, configure las unidades organizativas (OU) y los grupos de seguridad. A continuación, cree las cuentas de usuario.

Si modifica Active Directory después de agregar una máquina a un catálogo de máquinas, la función de acceso con Remote PC no vuelve a evaluar esa asignación. Si fuera necesario, puede volver a asignar manualmente una máquina a otro catálogo.

Si mueve o elimina unidades organizativas, aquellas que se utilizan para el acceso con Remote PC pueden quedarse desactualizadas. Los VDA podrían dejar de estar asociados con el más adecuado (o con algún) catálogo de máquinas o grupo de entrega.

Consideraciones sobre el catálogo de máquinas y el grupo de entrega

- Una máquina solo se puede asignar a un catálogo de máquinas y un grupo de entrega a la vez.
- Puede poner máquinas en uno o varios catálogos de máquinas de acceso con Remote PC.
- Al elegir cuentas de máquinas para un catálogo de máquinas, seleccione la menor unidad organizativa (OU) que se pueda aplicar, con el objetivo de evitar posibles conflictos con las máquinas de otro catálogo. Por ejemplo, en el caso de bancos, funcionarios o cajeros, seleccione “cajeros”.
- Puede asignar todas las máquinas de un catálogo de máquinas de acceso con Remote PC a través de uno o varios grupos de entrega. Por ejemplo, si tiene dos grupos de usuarios que necesitan configuraciones de directiva diferentes, asignar esos usuarios a diferentes grupos de entrega le permitirá filtrar las directivas de HDX según cada grupo de entrega.
- Si su infraestructura de TI asigna la responsabilidad de prestación de servicios a los usuarios en función de su ubicación geográfica, departamento u otra categoría, puede agrupar máquinas y usuarios según corresponda para permitir la administración delegada. Compruebe que cada administrador tenga permisos tanto para los catálogos de máquinas como para los grupos de entrega pertinentes.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Consideraciones sobre la implementación

- Puede crear una implementación de acceso con Remote PC y, más adelante, agregar aplicaciones o escritorios tradicionales de Infraestructura de escritorio virtual (VDI). También puede agregar escritorios de acceso con Remote PC a una implementación existente de VDI.
- Puede habilitar la función Asistencia remota de Windows cuando instale el VDA en el equipo de la oficina. Esta opción permite a los equipos de asistencia que usan Director ver e interactuar con las sesiones de usuario mediante la función Asistencia remota de Windows.
- Plantéese cómo quiere distribuir el VDA en cada PC de oficina. Citrix recomienda usar la distribución electrónica de software (ESD), como los scripts de Active Directory y Microsoft System Center Configuration Manager. Los medios de instalación contienen scripts de ejemplo de Active Directory.
- Revise las consideraciones de seguridad para implementaciones de acceso con Remote PC.
- La funcionalidad Arranque seguro para Acceso con Remote PC recibe respaldo en Windows 10.
- Cada PC de oficina debe estar unido a un dominio con una conexión de red con cable.
- Conecte el teclado y el mouse directamente al equipo de sobremesa o portátil, no al monitor o a otros componentes que se pueden apagar. Si tiene que conectar dispositivos de entrada a componentes como monitores, estos no se deben apagar.
- Si utiliza tarjetas inteligentes, consulte Tarjetas inteligentes.
- La función de acceso con Remote PC se puede utilizar en la mayoría de equipos portátiles. Para mejorar la accesibilidad y ofrecer la mejor experiencia de conexión, configure las opciones de ahorro de energía del equipo portátil como las de un equipo de escritorio. Por ejemplo:
  - Inhabilite la función de hibernación.
  - Inhabilite la función de suspensión.
  - Establezca la opción **No hacer nada** en la acción de cierre de tapa.
  - Establezca la opción **Apagar** en la acción al presionar el botón de encendido.
  - Inhabilite las funciones de ahorro de energía de la tarjeta de vídeo y de la tarjeta de interfaz de red.
  - Inhabilite las tecnologías de ahorro de batería.
- Para dispositivos de acceso con Remote PC, no se admiten:
  - El acoplamiento y el desacoplamiento del equipo portátil.
  - 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.
- Citrix da respaldo al Acceso con Remote PC en dispositivos Surface Pro con Windows 10. Para mejorar la accesibilidad y ofrecer la mejor experiencia de conexión, configure el dispositivo Surface de forma similar a un escritorio o un equipo portátil. Por ejemplo:
  - Inhabilite la función de hibernación o suspensión
  - Use la conectividad de red por cable
  - Tenga siempre el teclado enchufado al conectarse o reconectarse a una sesión

© 1999-2019 Citrix Systems, Inc. All rights reserved.

  - Inhabilite las tecnologías de ahorro de batería
- Instale la aplicación Citrix Workspace en cada dispositivo cliente que acceda de forma remota al PC de la oficina.
- Varios usuarios con acceso remoto al mismo PC de oficina ven el mismo icono de la aplicación Citrix Workspace. Cuando un usuario inicia una sesión en el PC de forma remota, ese recurso aparece como no disponible para otros usuarios.

Funciones administradas a través del Registro

> **Precaución:**
>
> Si modifica el Registro de forma incorrecta, pueden producirse problemas graves, que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

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 el equipo. 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.

RE\Citrix\PortICA\RemotePC “SasNotification”=dword:00000001

Puede personalizar más el comportamiento de esta función en: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA

RpcaMode (con dword):

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Indicar 1 significa que el usuario remoto siempre gana si no responde a los mensajes de la interfaz de usuario en el período de tiempo de espera especificado.
- Indicar 2 significa que siempre gana el usuario local. Si este parámetro no se especifica, el usuario remoto ganará siempre de forma predeterminada.

RpcaTimeout (con dword):

- La cantidad de segundos que tiene el usuario antes de que se determine el tipo de modo a efectuarse. Si este parámetro no se especifica, el valor predeterminado es de 30 segundos. El valor mínimo debe ser de 30 segundos. Reinicie la máquina para aplicar estos cambios.

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 donde se le pregunta si quiere permitir o denegar la conexión del usuario local. Si permite la conexión, la sesión del usuario remoto se desconecta.

Wake on LAN

En Citrix Cloud, Wake on LAN no es compatible con el acceso con Remote PC.

La función de acceso con Remote PC admite Wake on LAN, el cual ofrece a los usuarios la capacidad de encender equipos físicos de forma remota. Esta función permite a los usuarios mantener apagados sus equipos de oficina cuando no estén en uso, lo que disminuye costes de energía. También permite el acceso remoto aunque el equipo se haya apagado accidentalmente, como, por ejemplo, durante fenómenos meteorológicos extremos.

La función Wake on LAN del acceso con Remote PC se admite en:

- Equipos que tienen la opción Wake on LAN habilitada en la BIOS. Este respaldo incluye proxy de activación y paquetes Magic sin procesar, y está disponible cuando se utiliza Microsoft System Center Configuration Manager (ConfigMgr) 2012, Configuration Manager 2012 R2 y Configuration Manager 2016.
- Equipos que admiten la Tecnología de administración activa Intel (AMT). En máquinas que admitan AMT, la función Wake on LAN también admite las acciones de forzar el cierre y el reinicio en Studio y Director. Además, en StoreFront y la aplicación Citrix Workspace está disponible la acción de reinicio. El respaldo a AMT solo está disponible si se utiliza Configuration Manager 2012 o 2012 R2, no 2016.

Configure Configuration Manager para que utilice la función Wake on LAN. A continuación, cuando use Studio para crear una implementación de acceso con Remote PC (o al agregar otra conexión de administración de energía que se usará para el acceso con Remote PC), habilite la función Administración de energía y especifique la información de acceso de Configuration Manager.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configuration Manager y Wake on LAN para el acceso con Remote PC

Para configurar la función Wake on LAN de acceso con Remote PC, complete los siguientes pasos antes de instalar un VDA en los equipos de oficina.

- Configure Configuration Manager 2012, 2012 R2 o 2016 dentro de la organización. A continuación, implemente el cliente de Configuration Manager en todas las máquinas de acceso con Remote PC. Debe dejar tiempo suficiente para que se ejecute el ciclo de inventario de SCCM programado (o fuerce uno manualmente, si fuera necesario). Las credenciales de acceso que especifique en Studio para configurar la conexión a ConfigMgr deben incluir las colecciones en el ámbito y el rol de Operador de herramientas remotas.
- Para el respaldo con Tecnología de administración activa Intel (AMT):
  - La versión mínima respaldada de AMT en el equipo debe ser 3.2.1.
  - Aprovisione el equipo en el que vaya a usar AMT con certificados y procesos asociados de aprovisionamiento.
  - Recuerde: Solo puede utilizarse Configuration Manager 2012 y 2012 R2 (no Configuration Manager 2016).
- Para el respaldo de Magic Packet o proxy de reactivación de ConfigMgr:
  - Configure la función Wake on LAN en los ajustes de BIOS de cada equipo.
  - Para el respaldo al proxy de reactivación, habilite la opción en Configuration Manager. Asegúrese de que haya tres o más máquinas que puedan utilizarse como centinelas para cada subred de la organización que contiene los equipos que usarán la función Wake on LAN del acceso con Remote PC.
  - Para el respaldo de Magic Packet, configure los firewalls y los enrutadores de red para que permitan el envío de ese tipo de paquetes mediante una difusión o unidifusión dirigidas a las subredes.

Después de instalar el VDA en los equipos de oficina, habilite o inhabilite la administración de energía cuando cree la conexión y el catálogo de máquinas.

- Si habilita la administración de energía en el catálogo, especifique los datos de conexión: el nombre, la dirección y las credenciales de acceso de ConfigMgr.
- Si no habilita la administración de energía, puede agregar más tarde una conexión de administración de energía (Configuration Manager) y luego modificar un catálogo de máquinas de acceso con Remote PC para habilitar la administración de energía y especificar la nueva conexión de administración de energía.

Puede modificar una conexión de administración de energía para configurar opciones de configuración avanzadas. Puede habilitar:

- Proxy de reactivación entregado por ConfigMgr.
- Paquetes Wake on LAN (Magic Packets). Si habilita paquetes Wake on LAN, puede seleccionar un método de transmisión Wake on LAN: unidifusión o difusiones dirigidas a subredes.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

El equipo usa los comandos de encendido AMT (si se admiten), además de cualquier configuración avanzada que esté habilitada. Si el equipo no utiliza comandos de encendido AMT, recurre a la configuración avanzada.

Implementaciones Citrix Cloud: Aspectos a tener en cuenta y secuencia de configuración

Consulte CTX220737: How to Enable XenDesktop Remote PC Access in Citrix Cloud.

Implementaciones locales: Aspectos a tener en cuenta y secuencia de configuración

1. Antes de crear el sitio de acceso con Remote PC:

   Para usar la función de administración de energía del acceso con Remote PC (también conocida como Wake on LAN de acceso con Remote PC), complete las tareas de configuración en los equipos y en Microsoft System Center Configuration Manager (ConfigMgr) antes de crear la implementación de acceso con Remote PC en Studio.

2. En el Asistente para la creación de sitios de Studio:

   - Seleccione el tipo de sitio de **acceso con Remote PC**.
   - En la página **Administración de energía**, puede habilitar o inhabilitar la administración de energía de las máquinas que se encuentren en el catálogo predeterminado de acceso con Remote PC. Si habilita la administración de energía, especifique la información de conexión de ConfigMgr.
   - Complete la información en las páginas **Usuarios** y **Cuentas de máquina**.

   Cuando se crea un sitio de acceso con Remote PC, se crea también un catálogo de máquinas predeterminado llamado “Máquinas de acceso con Remote PC” y un grupo de entrega predeterminado llamado “Escritorios de acceso con Remote PC”.

3. Si crea otro catálogo de máquinas para el acceso con Remote PC:

   - En la página **Sistema operativo**, seleccione **Acceso con Remote PC** y elija una conexión de administración de energía. También puede optar por no usar ninguna administración de energía. Si no se ha definido ninguna conexión de administración de energía, puede agregarla después de finalizar el Asistente para la creación de catálogos de máquinas (tipo de conexión = Microsoft Configuration Manager Wake on LAN). A continuación, modifique el catálogo de máquinas al especificar esa nueva conexión.
   - En la página **Cuentas de máquina**, puede seleccionarlas de las cuentas de máquina o las unidades organizativas (OU) que aparecen, o bien, puede agregar cuentas de máquina y unidades organizativas.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

4. Instale el VDA en los PC de oficina utilizados para el acceso local y remoto. Por lo general, el VDA se puede distribuir automáticamente usando un software de administración de paquetes; sin embargo, en caso de implementaciones pequeñas o pruebas de concepto, puede instalar el VDA manualmente en cada PC de oficina. Hay varias formas de instalar un VDA de escritorio para una implementación de acceso con Remote PC.

   Si utiliza el instalador de producto completo o VDAWorkstationSetup.exe:

   - Interfaz gráfica: Seleccione **Acceso con Remote PC** en la página **Entorno** del asistente. Los componentes de la página **Componentes adicionales** no se marcan de forma predeterminada. No son necesarios para el funcionamiento de acceso con Remote PC.
   - Interfaz de línea de comandos: especifique la opción /remotepc. Esta opción impide la instalación de componentes adicionales. Como alternativa, puede usar la opción /exclude para excluir cada uno de estos componentes. Para obtener información más detallada, consulte las descripciones de las opciones de la línea de comandos.

   Si usa el instalador VDAWorkstationCoreSetup.exe, no se pueden instalar ni la aplicación Citrix Workspace ni los componentes adicionales.

   Después de haber instalado el VDA, el escritorio de acceso con Remote PC se asignará automáticamente al primer usuario de dominio que inicie una sesión de consola en el equipo de oficina (ya sea de manera local o por RDP). Si otros usuarios de dominio inician una sesión de consola, también se agregan a la lista de usuarios de ese escritorio, sujetos a las restricciones que se hayan configurado.

   Para usar conexiones RDP fuera del entorno de Citrix Virtual Apps and Desktops, debe agregar usuarios o grupos al grupo de usuarios de acceso directo.

5. Indique a los usuarios que descarguen e instalen la aplicación Citrix Workspace en cada dispositivo cliente que usarán para acceder al equipo de oficina de forma remota. La aplicación Citrix Workspace está disponible en https://www.citrix.com o en los sistemas de distribución de aplicaciones para los dispositivos móviles respaldados.

Solucionar problemas

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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Cuando se habilita la administración de energía para 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 no se admite AMT, pruebe el método de unidifusión o de proxy de reactivación (compruebe que estos parámetros están habilitados en las propiedades avanzadas de administración de energía de la conexión).

App-V

March 14, 2019

Usar App-V con Citrix Virtual Apps and Desktops

Microsoft Application Virtualization (App-V) permite implementar, actualizar y admitir aplicaciones como si fueran servicios. Los usuarios acceden a las aplicaciones sin instalarlas en sus dispositivos. App-V y Microsoft User State Virtualization (USV) ofrecen acceso a aplicaciones y datos, independientemente de la ubicación y de la conexión a Internet.
La tabla siguiente muestra las versiones admitidas.

App-V	Delivery Controller de Citrix Virtual Apps and Desktops	VDA de Citrix Virtual Apps and Desktops
5.0 y 5.0 SP1	Desde XenDesktop 7 hasta la versión actual, desde XenApp 7.5 hasta la versión actual	Desde 7.0 hasta la versión actual
5.0 SP2	Desde XenDesktop 7 hasta la versión actual, desde XenApp 7.5 hasta la versión actual	Desde 7.1 hasta la versión actual
5.0 SP3 y 5.1	Desde XenDesktop 7.6 hasta la versión actual, desde XenApp 7.6 hasta la versión actual	Desde 7.6.300 hasta la versión actual
App-V en Windows Server 2016	Desde XenDesktop 7.12 hasta la versión actual, desde XenApp 7.12 hasta la versión actual	Desde 7.12 hasta la versión actual

El cliente de App-V no admite el acceso sin conexión a las aplicaciones. En la compatibilidad con la

© 1999-2019 Citrix Systems, Inc. All rights reserved.

integración de App-V se incluye el uso de recursos compartidos SMB para aplicaciones. El protocolo HTTP no se admite.
Si no está familiarizado con App-V, consulte la documentación de Microsoft. A continuación, se ofrece una recapitulación de los componentes de App-V mencionados en este artículo:

- **Servidor de administración**. Ofrece una consola centralizada para administrar la infraestructura de App-V y entrega aplicaciones virtuales tanto a un cliente App-V de escritorio como a un cliente de Servicios de escritorio remoto. El servidor de administración de App-V autentica, solicita y proporciona la seguridad, las métricas, la supervisión y la recopilación de datos que necesita el administrador. El servidor utiliza Active Directory y herramientas adicionales para administrar a usuarios y aplicaciones.
- **Servidor de publicación**. Proporciona clientes de App-V con aplicaciones para usuarios específicos y aloja el paquete de aplicaciones virtuales para distribuirlo por streaming. Obtiene los paquetes del servidor de administración.
- **Cliente**. Recupera aplicaciones virtuales, publica aplicaciones en el cliente, y automáticamente establece y administra entornos virtuales en el momento de la ejecución en dispositivos Windows. El cliente de App-V se instala en el VDA, donde almacena parámetros de aplicaciones virtuales específicos de los usuarios, tales como los cambios en el Registro y en los archivos de cada perfil de usuario.

Las aplicaciones están siempre disponibles sin tener que definir o cambiar previamente la configuración del sistema operativo. Puede iniciar aplicaciones App-V desde grupos de entrega con SO de servidor y con SO de escritorio:

- A través de la aplicación Citrix Workspace
- A través del cliente de App-V y la aplicación Citrix Workspace
- Varios usuarios simultáneos en varios dispositivos
- A través de Citrix StoreFront

Las propiedades modificadas de las aplicaciones App-V se implementan al iniciar las aplicaciones. Por ejemplo, para las aplicaciones con un nombre simplificado modificado o un icono personalizado, la modificación aparece cuando los usuarios inician la aplicación. Las personalizaciones de aplicaciones que se guardan en los archivos de configuración dinámica también se aplican cuando se inicia la aplicación.

Métodos de administración

Puede usar los paquetes de App-V y los archivos de configuración dinámica que se crearon con el secuenciador de App-V y se encuentran en servidores App-V o recursos compartidos de red.

- **Servidores App-V:** Para poder usar las aplicaciones de los paquetes en servidores App-V, se requiere una comunicación continua entre Studio y los servidores App-V para la detección, la

© 1999-2019 Citrix Systems, Inc. All rights reserved.

configuración y la descarga a los VDA. Lo que resulta en una sobrecarga de hardware, infraestructura y administración. Studio y los servidores App-V deben estar sincronizados, especialmente para los permisos de usuario.

Esto se conoce como el método de *administración dual* porque el paquete App-V y el acceso a la aplicación requieren tanto la consola de Studio como la consola del servidor App-V. Este método funciona mejor en implementaciones de App-V y Citrix estrechamente ligadas. En este método, el servidor de administración gestiona los archivos de configuración dinámica. Cuando se utiliza el método de administración dual, los componentes de Citrix App-V administran el registro del servidor de publicación apropiado que se necesita para el lanzamiento de aplicaciones. Así, se garantiza que, en un momento dado, el servidor de publicación esté sincronizado para el usuario. El servidor de publicación conserva otros aspectos del ciclo de vida del paquete (como la actualización en los inicios de sesión y los grupos de conexión) mediante su configuración.

- **Recurso compartido de red:** Los paquetes y los archivos XML de configuración para implementación colocados en un recurso compartido de red eliminan la dependencia que tiene Studio del servidor App-V y de la infraestructura de la base de datos, por lo que se reduce la sobrecarga (necesita instalar el cliente de App-V de Microsoft en cada VDA).

  Esto se conoce como el método de *administración única* porque el paquete App-V y la aplicación solo necesitan la consola de Studio. Puede ir al recurso compartido de red y agregar uno o varios paquetes de App-V desde esa ubicación a la biblioteca de aplicaciones que se encuentre al nivel del sitio [1]. En este método, los componentes App-V de Citrix procesan los archivos de configuración de la implementación cuando se inicia la aplicación (no se admiten los archivos de configuración de usuario). Cuando se utiliza el método de administración única, los componentes de Citrix App-V administran todos los aspectos del ciclo de vida del paquete en la máquina host. Los paquetes se agregan a la máquina al iniciar el broker o cuando se detecta un cambio de configuración (que también puede ser al iniciar una sesión). Los paquetes se publican por primera vez para los usuarios “a petición” cuando se recibe una solicitud de lanzamiento de la aplicación Citrix Workspace.

  La administración única también administra el ciclo de vida de los grupos de conexión necesarios para cumplir con las definiciones de configuración del grupo de aislamiento realizadas en Studio.

  La [1] *biblioteca de aplicaciones* es un término de Citrix para el repositorio de almacenamiento en caché que guarda información sobre los paquetes de App-V. La biblioteca de aplicaciones también almacena información acerca de otras tecnologías de Citrix para la entrega de aplicaciones.

En los dos métodos de administración, si el VDA está configurado para descartar datos de usuario, la publicación (o sincronización) debe volver a realizarse en el inicio de la siguiente sesión.

Puede usar uno o ambos métodos de administración de forma simultánea. En otras palabras, al agre-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

gar aplicaciones a grupos de entrega, esas aplicaciones pueden proceder de paquetes de App-V ubicados en servidores App-V o en un recurso compartido de red.

> **Nota:**
>
> Si utiliza simultáneamente ambos métodos de administración, y el paquete de App-V tiene un archivo de configuración dinámica en ambas ubicaciones, se utiliza el archivo que se encuentra en el servidor App-V (administración dual).

Cuando se seleccione **Configuración > Publicación App-V** en el panel de navegación de Studio, aparecerán los orígenes y los nombres de los paquetes de App-V. La columna de origen indica si los paquetes se encuentran en el servidor App-V o en la memoria caché de la biblioteca de aplicaciones. Al seleccionar un paquete, el panel de detalles muestra las aplicaciones y los accesos directos que contiene ese paquete.

Archivos de configuración dinámica

Información general

Los paquetes de App-V se pueden personalizar utilizando archivos de configuración dinámica. Cuando esos archivos se aplican al paquete, se pueden cambiar las características de este. Por ejemplo, puede usarlos para definir comportamientos y accesos directos adicionales de la aplicación. Citrix App-V admite ambos tipos de archivo de configuración dinámica. Los parámetros que contiene el archivo se aplican cuando se inicia la aplicación:

- Los archivos de configuración de la implementación proporcionan una configuración de toda la máquina para todos los usuarios. Estos archivos se suelen denominar *<NombreDeArchivoDePaquete>*_Deplo y suelen estar en la misma carpeta que el paquete App-V al que se aplican. Se admiten en la administración única y dual.
- Los archivos de configuración de usuario proporcionan una configuración específica del usuario que admite personalizaciones por usuario para el paquete. La administración única admite archivos de configuración de usuario nombrados en el siguiente formato: *<NombreDeArchivoDePaquete>[SIDdelUsuario* | *NombreDeUsuario* | *SIDdelGrupo* |*NombreDelGrupo*]UserConfig.xml, ubicados en la misma carpeta que el paquete App-V al que se aplican.

Cuando existen varios archivos de configuración de usuario para un paquete en particular, se aplican con la siguiente prioridad:

1. SID del usuario
2. Nombre
3. SID del grupo de AD (el primero encontrado prevalece)
4. Nombre del grupo de AD (el primero encontrado prevalece)
5. Predeterminado

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Por ejemplo

```
MyAppVPackage_S-1-5-21-000000001-0000000001-000000001-001_UserConfig.
    xml
MyAppVPackage_joeblogs_UserConfig.xml
MyAppVPackage_S-1-5-32-547_UserConfig.xml
MyAppVPackage_Power Users_UserConfig.xml
MyAppVPackage_UserConfig.xml
```

> **Nota:**
>
> La parte específica del usuario en el nombre del archivo también puede aparecer opcionalmente al final (por ejemplo, MiPaqueteAppV_UserConfig_ **pedroblogs**.xml).

Ubicación de los archivos de configuración dinámica

En la administración única, los componentes de Citrix App-V solo procesan los archivos de configuración dinámica que se encuentran en la misma carpeta que su paquete App-V. Cuando se inician las aplicaciones que contiene el paquete, se vuelven a aplicar los cambios a los archivos de configuración dinámica correspondientes. Si sus archivos de configuración dinámica no comparten ubicación con sus paquetes, use un archivo de asignación para vincular los paquetes a sus archivos de configuración de la implementación.

Para crear un archivo de asignación

1. Abra un nuevo archivo de texto.
2. Para cada archivo de configuración dinámica, agregue una línea que especifique la ruta al paquete siguiendo el formato <GUIDPaquete> : ruta.

   Por ejemplo:

   F1f4fd78ef044176aad9082073a0c780 : c:\windows\file\packagedeploy.xml
3. Guarde el archivo como ctxAppVDynamicConfigurations.cfg en la misma carpeta que el paquete. Toda la jerarquía de directorios que haya en el mismo recurso compartido UNC que el paquete App-V se examina de forma recurrente hacia arriba para buscar este archivo cada vez que se inicia una aplicación del paquete.

> **Nota**
>
> No puede aplicar cambios a la configuración de una implementación dinámica cuando hay sesiones de usuario que tienen abierta una aplicación del paquete. Puede aplicar cambios a los archivos de configuración dinámica del usuario si otros usuarios, *pero no el usuario actual*, tienen abierta una aplicación del paquete.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Grupos de aislamiento

Cuando se usa el método de administración única de App-V, crear grupos de aislamiento permite especificar grupos interdependientes de aplicaciones que deben ejecutarse en el sandbox. Esta funcionalidad es similar (pero no idéntica) a los grupos de conexión de App-V. En lugar de la terminología "paquetes obligatorios" y "paquetes optativos" que utiliza el servidor de administración de App-V, Citrix utiliza los términos "automática" y "explícita" cuando se refiere a las opciones de implementación de paquetes.

- Así, cuando un usuario inicia una aplicación App-V (la aplicación principal), se buscan en los grupos de aislamiento otros paquetes de aplicación que estén marcados para la inclusión automática. Esos paquetes se descargan y se incluyen automáticamente en el grupo de aislamiento. No es necesario que los agregue al grupo de entrega que contiene la aplicación principal.
- En cambio, un paquete de aplicación que esté marcado para la inclusión explícita en el grupo de aislamiento se descarga solo si agrega explícitamente esa aplicación al mismo grupo de entrega que contiene la aplicación principal.

Esto permite crear grupos de aislamiento que contengan una mezcla de aplicaciones incluidas automáticamente que están disponibles globalmente para todos los usuarios. Además, el grupo puede contener un conjunto de plug-ins y otras aplicaciones (que pueden tener restricciones concretas de licencias), que puede limitar a un determinado grupo de usuarios (identificado a través de grupos de entrega) sin necesidad de crear más grupos de aislamiento.

Por ejemplo, la aplicación A requiere JRE 1.7 para ejecutarse. Puede crear un grupo de aislamiento que contenga la aplicación A (con un tipo de implementación explícito) y JRE 1.7 (con un tipo de implementación automático). A continuación, agregue esos paquetes de App-V a uno o varios grupos de entrega. Cuando un usuario inicie la aplicación A, JRE 1.7 se implementará automáticamente con ella.

Puede agregar una aplicación a más de un grupo de aislamiento de App-V. No obstante, cuando un usuario inicia una aplicación, siempre se utiliza el primer grupo de aislamiento al que se agregó la aplicación. No se puede ordenar ni priorizar a los demás grupos de aislamiento que contengan dicha aplicación.

Servidores de equilibrio de carga de App-V

Los servidores de administración y publicación de equilibrio de carga que utilizan el sistema de nombres de dominio round robin son compatibles si está utilizando el método de administración "Administración dual". El equilibrio de carga del servidor de administración detrás de Netscaler, IP virtual F5 (o similar) no se admite debido a la forma en que Studio necesita comunicarse con el servidor de

© 1999-2019 Citrix Systems, Inc. All rights reserved.

administración a través de PowerShell remoto. Para obtener más información, consulte este artículo del blog de Citrix.

Configurar

En la siguiente tabla, se resume la secuencia de las tareas de configuración a realizar para utilizar App-V en Citrix Virtual Apps and Desktops cuando se utilizan los métodos de administración única y dual.

Administración única	Administración dual	Tarea
X	X	Implementar App-V
X	X	Empaquetar y seleccionar ubicación
	X	Configurar direcciones de servidor App-V en Studio
X	X	Instalar software en máquinas VDA
X		Agregar paquetes de App-V a la biblioteca de aplicaciones
X		Agregar grupos de aislamiento de App-V (opcional)
X	X	Agregar aplicaciones App-V a grupos de entrega

Implementar Microsoft App-V

Para obtener las instrucciones de implementación de App-V, consulte https://technet.microsoft.com/en-us/windows/hh826068.

Si lo prefiere, puede cambiar la configuración del servidor de publicación de App-V. Citrix recomienda usar los cmdlets del SDK presente en el Controller. Consulte la documentación del SDK para obtener más información.

- Para ver la configuración del servidor de publicación, escriba **Get-CtxAppvServerSetting -AppVPublishingServer <*pubServer*>**.
- Para asegurarse de que las aplicaciones App-V se inicien correctamente, escriba **Set-CtxAppvServerSetting –UserRefreshonLogon 0**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Si ya ha utilizado parámetros de objeto de directiva de grupo para administrar la configuración del servidor de publicación, estos parámetros anulan cualquier configuración de integración de App-V, incluida la configuración de cmdlets. Esto puede dar lugar a fallos de inicio de la aplicación App-V. Citrix recomienda quitar todos los parámetros de directiva de grupo (GPO) y utilizar el SDK para definir esa configuración.

Empaquetar y seleccionar ubicación

Puede crear paquetes de aplicación mediante el secuenciador de App-V para ambos métodos de administración. Consulte la documentación de Microsoft para obtener más detalles.

- Para la administración única, ponga los paquetes (y sus archivos de configuración dinámica correspondientes) a disposición en una ubicación de red compartida UNC o SMB. Compruebe que el administrador de Studio que agregue las aplicaciones a los grupos de entrega tenga al menos el acceso de lectura a esa ubicación.
- Para la administración dual, publique los paquetes en el servidor de administración de App-V desde una ruta UNC. (No se admite la publicación desde direcciones URL de HTTP.)

Independientemente de si los paquetes están en el servidor App-V o en un recurso compartido de red, compruebe que tienen los permisos de seguridad adecuados para que el administrador de Studio acceda a ellos. Los recursos compartidos de red deben compartirse con "Usuarios autenticados" para garantizar que el VDA y Studio tienen el acceso de lectura de forma predeterminada.

Configurar direcciones de servidor App-V en Studio

> **Importante:**
>
> Citrix recomienda usar los cmdlets de PowerShell en el Controller para especificar las direcciones de servidores App-V si esos servidores utilizan valores de propiedad no predeterminados. Consulte la documentación del SDK para obtener más información. Si cambia las direcciones de servidor App-V en Studio, algunas propiedades de conexiones de servidor que especifique pueden restablecerse a los valores predeterminados. Estas propiedades se utilizan en los VDA para conectarse a los servidores de publicación de App-V. Si eso ocurriera, vuelva a configurar en los servidores los valores no predeterminados de las propiedades restablecidas.

Este procedimiento solo es válido para la administración dual.

Puede especificar las direcciones de los servidores de administración y publicación de App-V para la administración dual durante o después de la creación de sitios. Puede hacerlo durante o después de crear el sitio.

Durante la creación de sitio:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- En la página **App-V** del asistente, escriba la URL del servidor de administración de App-V, así como la URL y el número de puerto del servidor de publicación de App-V.
- Pruebe la conexión antes de continuar con el asistente. Si se produce un error en la prueba, consulte la sección "Solucionar problemas" que se presenta más adelante en este artículo.

Después de la creación de sitio:

1. Seleccione **Configuración > Publicación App-V** en el panel de navegación de Studio.
2. Si no ha especificado previamente direcciones de servidor de App-V, seleccione **Agregar servidor de Microsoft** en el panel "Acciones".
3. Para cambiar las direcciones del servidor de App-V, seleccione **Modificar servidor de Microsoft** en el panel "Acciones".
4. Escriba la URL del servidor de administración de App-V, así como la URL y el número de puerto del servidor de publicación de App-V.
5. Pruebe la conexión a esos servidores antes de cerrar el cuadro de diálogo. Si se produce un error en la prueba, consulte la sección "Solucionar problemas" que se presenta más adelante en este artículo.

Más adelante, si quiere eliminar todos los enlaces a los servidores de administración y publicación de App-V y evitar que Studio detecte los paquetes App-V de esos servidores, seleccione **Quitar servidor de Microsoft** en el panel "Acciones". Esta acción solo se permite si ninguna de las aplicaciones que se encuentran en los paquetes de esos servidores está publicada en los grupos de entrega. Si lo están, debe quitar esas aplicaciones de los grupos de entrega antes de poder quitar los servidores App-V.

Instalar software en máquinas VDA

Las máquinas que contienen los VDA deben tener dos conjuntos de software instalados para admitir App-V: uno de Microsoft y otro de Citrix.

Cliente de Microsoft App-V

Este software recupera aplicaciones virtuales, publica aplicaciones en el cliente, y automáticamente establece y administra entornos virtuales en el momento de la ejecución en dispositivos Windows. El cliente de App-V almacena parámetros de aplicaciones virtuales específicos de los usuarios, tales como los cambios en el Registro y en los archivos de cada perfil de usuario.

El cliente de App-V está disponible en Microsoft. Instale un cliente en todas las máquinas que contienen agentes VDA o en la imagen maestra que se usa en el catálogo de máquinas para crear las máquinas virtuales. **Nota:** Windows 10 (1607 o posterior) y Windows Server 2016 ya incluyen el cliente de App-V. Solo en esos sistemas operativos, habilite el cliente de App-V. Para ello, ejecute el cmdlet **Enable-AppV** (sin parámetros) de PowerShell. El cmdlet **Get-AppVStatus** obtiene el estado actual (habilitado o no habilitado).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> **Sugerencia:**
>
> Después de instalar el cliente de App-V, con permisos de administrador, ejecute el cmdlet **Get-AppvClientConfiguration** de PowerShell y verifique que EnablePackageScripts esté establecido en 1. Si no está establecido en 1, ejecute **Set-AppvClientConfiguration -EnablePackageScripts $true**.

Componentes de Citrix App-V

El software del componente Citrix App-V se excluye de manera predeterminada cuando se instala un VDA.

Se puede controlar este comportamiento predeterminado durante la instalación del VDA. En la interfaz gráfica, marque la casilla **Citrix Personalization para App-V - VDA** en la página **Componentes adicionales**. En la interfaz de línea de comandos, use la opción **/IncludeAdditional "CitrixPersonalization for App-V VDA"**.

Si no incluye los componentes de App-V desarrollados por Citrix durante la instalación de VDA, pero más tarde quiere usar aplicaciones App-V: En la lista "Programas y características" de la máquina Windows, haga clic con el botón secundario en la entrada **Citrix Virtual Delivery Agent** y, a continuación, seleccione **Cambiar**. Se iniciará un asistente. En el asistente, habilite la opción que instala y habilita los componentes de publicación de App-V.

Agregar o eliminar paquetes de App-V de la biblioteca de aplicaciones

Estos procedimientos solo son válidos para el método de administración única.

Debe tener al menos el acceso de lectura al recurso compartido de red que contiene los paquetes de App-V.

Agregar un paquete de App-V a la biblioteca de aplicaciones

1. Seleccione **Configuración > Publicación App-V** en el panel de navegación de Studio.
2. Seleccione **Agregar paquetes** en el panel "Acciones".
3. Vaya al recurso compartido que contiene los paquetes de App-V y seleccione uno o varios paquetes.
4. Haga clic en **Agregar**.

Eliminar un paquete de App-V de la biblioteca de aplicaciones

Si quita un paquete de App-V de la biblioteca de aplicaciones, este se quita del nodo Publicación de App-V en Studio. Sin embargo, esta acción no elimina, de los grupos de entrega, las aplicaciones

© 1999-2019 Citrix Systems, Inc. All rights reserved.

que contenía el paquete, por lo que esas aplicaciones aún se pueden iniciar. El paquete sigue en su ubicación de red física. (Este efecto difiere de la eliminación de una aplicación App-V de un grupo de entrega.)

1. Seleccione **Configuración > Publicación App-V** en el panel de navegación de Studio.
2. Seleccione uno o varios paquetes que se van a quitar.
3. Seleccione **Quitar paquete** en el panel "Acciones".

Agregar, modificar o eliminar grupos de aislamiento de App-V

Agregar un grupo de aislamiento de App-V

1. Seleccione **Publicación App-V** en el panel de navegación de Studio.
2. Seleccione **Agregar grupo de aislamiento** en el panel "Acciones".
3. En el cuadro de diálogo **Agregar parámetros del grupo de aislamiento**, escriba un nombre y una descripción para el grupo de aislamiento.
4. En la lista Paquetes disponibles, seleccione las aplicaciones a agregar al grupo de aislamiento y, a continuación, haga clic en la flecha derecha. Las aplicaciones seleccionadas deberían aparecer en la lista Paquetes en grupo de aislamiento. En la lista desplegable **Implementación** situada junto a cada aplicación, seleccione **Explícita** o **Automática**. También puede usar las flechas arriba y abajo para cambiar el orden de las aplicaciones en la lista.
5. Cuando haya terminado, haga clic en **Aceptar**.

Modificar un grupo de aislamiento de App-V

1. Seleccione **Publicación App-V** en el panel de navegación de Studio.
2. Seleccione la ficha **Grupos de aislamiento** en el panel central y, a continuación, seleccione el grupo de aislamiento a modificar.
3. Seleccione **Modificar grupo de aislamiento** en el panel "Acciones".
4. En el cuadro de diálogo **Edit Isolation Group Settings**, cambie el nombre o la descripción del grupo de aislamiento, agregue o elimine aplicaciones, cambie el tipo de implementación o cambie el orden de aplicaciones.
5. Cuando haya terminado, haga clic en **Aceptar**.

Eliminar un grupo de aislamiento de App-V

Quitar un grupo de aislamiento no quita los paquetes de aplicaciones. Solo elimina la agrupación.

1. Seleccione **Publicación App-V** en el panel de navegación de Studio.
2. Seleccione la ficha **Grupos de aislamiento** en el panel central y, a continuación, seleccione el grupo de aislamiento a eliminar.
3. Seleccione **Quitar grupo de aislamiento** en el panel "Acciones".

© 1999-2019 Citrix Systems, Inc. All rights reserved.

4. Confirme la eliminación.

Agregar aplicaciones App-V a grupos de entrega

El siguiente procedimiento se centra en cómo agregar aplicaciones App-V a grupos de entrega. Para obtener información completa sobre cómo crear un grupo de entrega, consulte Crear grupos de entrega.

Paso 1: Elija si quiere crear un grupo de entrega o agregar aplicaciones App-V a un grupo de entrega existente:

Para crear un grupo de entrega que contenga las aplicaciones App-V:

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione **Crear grupo de entrega** en el panel "Acciones".
3. En las siguientes páginas del asistente, especifique un catálogo de máquinas y unos usuarios.

Para agregar aplicaciones App-V a grupos de entrega existentes:

1. Seleccione **Aplicaciones** en el panel de navegación de Studio.
2. Seleccione **Agregar aplicaciones** en el panel "Acciones".
3. Seleccione uno o varios grupos de entrega a los que se agregarán las aplicaciones App-V.

Paso 2: En la página **Aplicaciones** del asistente, haga clic en la lista desplegable **Agregar** para ver los orígenes de las aplicaciones. Seleccione **App-V**.

Paso 3: En la página **Agregar aplicaciones App-V**, elija el origen de App-V: el servidor App-V o la biblioteca de aplicaciones. La pantalla resultante contiene los nombres de las aplicaciones y sus nombres y versiones de paquete. Marque las casillas situadas junto a las aplicaciones o los accesos directos a ellas que quiera agregar. Luego haga clic en **Aceptar**.

Paso 4: Complete el asistente.

Conviene tener en cuenta lo siguiente:

- Si cambia las propiedades de una aplicación App-V cuando la agregue a un grupo de entrega, esos cambios se realizan cuando se inicia la aplicación. Por ejemplo, si modifica el icono o el nombre simplificado de una aplicación cuando la agregue al grupo, el cambio aparece cuando un usuario inicia la aplicación.
- Si usa archivos de configuración dinámica para personalizar las propiedades de una aplicación App-V, esas propiedades anulan los cambios que haya hecho cuando las agregó a un grupo de entrega.
- Si, más adelante, quiere modificar un grupo de entrega que contenga aplicaciones App-V, no habrá ningún cambio en el rendimiento de esas aplicaciones si se cambia el tipo de entrega del grupo de "escritorios y aplicaciones" a "solo aplicaciones".

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Solucionar problemas

Los problemas que solo pueden ocurrir cuando se utiliza el método de administración dual están marcados con "(DUAL)".

(DUAL) Se produce un error de conexión de PowerShell cuando selecciona **Configuración > Publicación App-V** en el panel de navegación de Studio.

- ¿El administrador de Studio es también un administrador del servidor App-V? El administrador de Studio debe pertenecer al grupo "administradores" en el servidor de administración de App-V para que los administradores se puedan comunicar con él.

(DUAL) La operación "Probar conexión" devuelve un error cuando se especifican las direcciones de servidores App-V en Studio.

- ¿Está encendido el servidor App-V? Envíe un comando Ping o compruebe el Administrador de IIS; todos los servidores App-V deben tener el estado Iniciado y En ejecución.
- ¿Está habilitada la comunicación remota de PowerShell en el servidor App-V? Si no, consulte http://technet.microsoft.com/en-us/magazine/ff700227.aspx.
- ¿El administrador de Studio es también un administrador del servidor App-V? El administrador de Studio debe pertenecer al grupo *administradores* en el servidor de administración de App-V para que los administradores se puedan comunicar con él.
- ¿Está habilitado el uso compartido de archivos en el servidor App-V? Escriba `\\<App-V server FQDN>` en el Explorador de Windows o con el comando Ejecutar.
- ¿El servidor App-V tiene los mismos permisos de uso compartido de archivos que el administrador de App-V? En el servidor App-V, agregue una entrada para `\\<App-V server FQDN>` en "Nombres de usuarios y contraseñas almacenados", especificando las credenciales del usuario que tiene privilegios de administrador en el servidor App-V. Para obtener instrucciones, consulte http://support.microsoft.com/kb/306541.
- ¿Se encuentra el servidor App-V en Active Directory?

  Si la máquina de Studio y el servidor App-V se encuentran en dominios de Active Directory distintos que no tienen una relación de confianza, desde la consola de PowerShell en la máquina de Studio, ejecute **winrm s winrm/Config/client '@(TrustedHosts="*<FQDN del servidor App-V>*")'**.

  Si TrustedHosts está administrado por un objeto de directiva de grupo (GPO), aparece un mensaje de error como el siguiente: "*El parámetro de configuración TrustedHosts no se puede cambiar porque el uso se controla mediante directivas. La directiva debe establecerse como 'No configurada' para poder cambiar el parámetro de configuración*". En este caso, agregue una entrada para el nombre del servidor App-V a la directiva de hosts de confianza en GPO (Plantillas admin-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

istrativas > Componentes de Windows > Administración remota de Windows (WinRM) > Cliente WinRM).

(DUAL) Falla la detección cuando se agrega una aplicación App-V a un grupo de entrega.

- ¿El administrador de Studio es también un administrador del servidor de administración de App-V? El administrador de Studio debe pertenecer al grupo *administradores* en el servidor de administración de App-V para que los administradores se puedan comunicar con él.
- ¿Se está ejecutando el servidor de administración de App-V? Envíe un comando Ping o compruebe el Administrador de IIS; todos los servidores App-V deben tener el estado Iniciado y En ejecución.
- ¿Está habilitada la comunicación remota de PowerShell en ambos servidores App-V? Si no, consulte http://technet.microsoft.com/en-us/magazine/ff700227.aspx.
- ¿Los paquetes tienen los permisos de seguridad adecuados para que el administrador de Studio tenga acceso a ellos?

Las aplicaciones App-V solo se inician en una versión del explorador Web.

- Si publica varias versiones en secuencia de la misma aplicación de explorador Web, solo podrá iniciarse una versión de la aplicación a la vez por usuario en el VDA. Se da el mismo comportamiento incluso cuando los componentes de Citrix no intervienen y el usuario inicia las aplicaciones secuenciadas desde accesos directos de escritorio que apuntan a rutas diferentes.

  La primera versión de explorador que inicie el usuario determina la versión que se ejecutará posteriormente para él. Cuando Firefox detecta un segundo inicio de sí mismo, prefiere crear una instancia del proceso ya en ejecución, en lugar de crear un nuevo proceso. Otros exploradores Web pueden comportarse de la misma manera.

  Puede hacer que la aplicación se inicie en la versión del explorador Firefox deseada. Para ello, agregue el parámetro de línea de comandos **-no-remote** al comando de inicio del acceso directo. Otros navegadores ofrecen el mismo recurso o uno similar.

  > **Nota:**
  >
  > Debe usar XenApp 7.17 o posterior para poder usar la función de enumeración de acceso directo. También debe cambiar el paquete en ambas versiones de la aplicación para obtener este comportamiento bidireccional.

Las aplicaciones App-V no se inician.

- (DUAL) ¿Se está ejecutando el servidor de publicación?
- (DUAL) ¿Los paquetes de App-V tienen los permisos de seguridad adecuados para que los usuarios puedan acceder a ellos?
- (DUAL) En el agente VDA, compruebe que Temp hace referencia a la ubicación correcta y que hay espacio suficiente disponible en el directorio Temp.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- (DUAL) En el servidor de publicación de App-V, ejecute **Get-AppvPublishingServer *** para que se muestre la lista de servidores de publicación.
- (DUAL) En el servidor de publicación de App-V, compruebe si UserRefreshonLogon está establecido en False.
- (DUAL) En el servidor de publicación de App-V, con privilegios de administrador, ejecute **Set-AppvPublishingServer** y establezca UserRefreshonLogon en "False".
- ¿El VDA tiene instalada una versión admitida del cliente de App-V? ¿El VDA tiene habilitada la opción de **habilitar scripts de paquetes**?
- En la máquina que contiene el VDA y el cliente de App-V, desde el editor del Registro (regedit), vaya a HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\AppV. Compruebe que la clave AppVServers tiene un valor en el siguiente formato: AppVManagementServer+metadata;PublishingServer (por ejemplo: `http://xmas-demo-appv.blrstrm.com+0+0+0+1+1+1+0+1;http://xmas-demo-appv.blrstrm.com:8082`).
- En la máquina o imagen maestra que contiene el VDA y el cliente de App-V, compruebe que el parámetro ExecutionPolicy de PowerShell está establecido en RemoteSigned. El cliente de App-V suministrado por Microsoft no está firmado, y esta directiva ExecutionPolicy permite que PowerShell ejecute cmdlets y scripts locales sin firma. Utilice uno de los siguientes dos métodos para configurar ExecutionPolicy: 1) Como administrador, escriba el cmdlet **Set-ExecutionPolicy RemoteSigned** o (2) En "Configuración de directiva de grupo", vaya a Configuración del equipo > Directivas > Plantillas administrativas > Componentes de Windows > Windows PowerShell > Activar la ejecución de scripts.

Si estos pasos no resuelven el problema, habilite y examine los registros.

Registros

Los registros relacionados con la configuración de App-V están ubicados en C:\CtxAppvLogs. Los registros de inicio de aplicaciones se encuentran en: %LOCALAPPDATA%\Citrix\CtxAppvLogs. LOCALAPPDATA es la carpeta local del usuario que ha iniciado sesión. Consulte la carpeta local del usuario para el que falló el inicio de la aplicación.

Para habilitar los registros de Studio y VDA que se utilizan para App-V, debe tener privilegios de administrador. También necesitará un editor de texto, como el Bloc de notas.

Para habilitar los registros de Studio:

1. Cree la carpeta C:\CtxAppvLogs.
2. Vaya a C:\Archivos de programa\Citrix\StudioAppVIntegration\SnapIn\Citrix.Appv.Admin.V1. Abra CtxAppvCommon.dll.config en un editor de texto y quite la marca de comentario de la línea siguiente: <add key ="LogFileName" value="C:\CtxAppvLogs\log.txt"/>
3. Reinicie el servicio de Broker para comenzar la captura de registros.

Para habilitar los registros del VDA:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

1. Cree la carpeta C:\CtxAppvLogs.
2. Vaya a C:\Archivos de programa\Citrix\Virtual Desktop Agent. Abra CtxAppvCommon.dll.config en un editor de texto y quite la marca de comentario de la línea siguiente: <add key =”LogFileName” value=”C:\CtxAppvLogs\log.txt”/>
3. Quite la marca de comentario de la línea y establezca el valor en 1: <add key =”EnableLauncherLogs” value=”1”/>
4. Reinicie la máquina para comenzar a capturar registros.

AppDisks

March 8, 2019

Información general

Administrar las aplicaciones y, a su vez, las imágenes en que esas aplicaciones están instaladas puede ser complejo. En estos casos, la función Citrix AppDisks puede solucionar el problema. AppDisks separa, por un lado, el sistema operativo y, por el otro, las aplicaciones y los grupos de aplicaciones, lo que permite administrarlos de forma independiente.

Puede crear varios AppDisks que contengan aplicaciones diseñadas para los distintos grupos de usuarios y, a continuación, puede combinar esos AppDisks en la imagen maestra que decida. Agrupar y administrar las aplicaciones de esta forma permite controlar de manera más precisa las aplicaciones que utilice. Además, permite reducir la cantidad de imágenes maestras que mantener. Esto simplifica la administración de TI y permite responder mejor a las necesidades del usuario. Las aplicaciones contenidas en AppDisks se entregan por medio de grupos de entrega.

Si su implementación incluye la función Citrix AppDNA, puede integrar AppDisks en ella, ya que AppDNA permite que Citrix Virtual Apps and Desktops analicen automáticamente las aplicaciones presentes en cada AppDisk. Usar AppDNA ayuda a sacar el máximo provecho de la función AppDisks. Sin ella, la compatibilidad de las aplicaciones no se prueba ni se notifica.

Dos características distinguen AppDisks de otras tecnologías de aprovisionamiento de aplicaciones: la administración de cambios y la administración de aislamientos.

- Microsoft App-V permite que existan aplicaciones no compatibles aislándolas. La función AppDisks no aísla las aplicaciones. Las separa (a ellas y a sus archivos auxiliares y claves del Registro) del sistema operativo. Para el sistema operativo y el usuario, los AppDisks aparecen y se comportan como si estuvieran instalados directamente en la imagen maestra.
- La administración de cambios (actualizar las imágenes maestras y probar la compatibilidad de las actualizaciones con las aplicaciones instaladas) puede redundar en un gasto considerable.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Con los informes de AppDNA, puede identificar problemas y sugerir correcciones. Por ejemplo, AppDNA puede identificar las aplicaciones que tienen dependencias comunes (como .NET) para, así, instalarlas en una sola imagen base común. Asimismo, AppDNA puede identificar las aplicaciones que se cargan pronto en la secuencia de inicio del SO, por lo que puede comprobar si se comportan de la manera esperada.

Conviene tener en cuenta lo siguiente:

- Después de actualizar una imagen, algunas aplicaciones no funcionan correctamente porque no se pueden verificar las licencias previamente instaladas. Por ejemplo, después de una actualización de imagen, iniciar Microsoft Office puede provocar que aparezca un mensaje de error similar al siguiente:

  "Microsoft Office Professional Plus 2010 no puede verificar la licencia de esta aplicación. Se produjo un error en el intento de reparación o lo canceló el usuario. La aplicación se cerrará ahora".

  Para resolver este problema, desinstale Microsoft Office e instale la nueva versión en la imagen base.
- En algunos casos, falla la descarga de aplicaciones de Metro desde la Tienda Windows en una máquina virtual publicada después de una cantidad considerable de tiempo.
- Citrix recomienda que siempre coloque todos los componentes de Microsoft Office en el mismo AppDisk. Por ejemplo, un AppDisk con Microsoft Office y Project; otro AppDisk con Microsoft Office con Project y Visio.
- En algunos sistemas, SCCM deja de responder cuando se actualiza una imagen. Esta situación ocurre cuando se realizan y se aplican actualizaciones en la imagen base, lo que provoca fallos del cliente SCCM. Para resolver este problema, primero instale la instancia de cliente SCCM en la imagen base.
- En algunos casos, es posible que una aplicación instalada en el AppDisk no aparezca en el menú Inicio de Windows tras haber sido asignada a un grupo de entrega y a la máquina virtual de un usuario. Consulte Cómo aparecen las aplicaciones en el menú Inicio para obtener más información.
- Los usuarios no detectan la separación de aplicaciones y sistema operativo; tampoco son conscientes de ningún otro aspecto de la función AppDisks. Las aplicaciones se comportan como si estuvieran instaladas en la imagen. Los AppDisks que contienen aplicaciones complejas pueden provocar un pequeño retraso en el inicio del escritorio.
- Puede usar AppDisks solamente con escritorios alojados agrupados y compartidos.
- Asimismo, puede usar AppDisks con escritorios compartidos alojados.
- Puede compartir AppDisks entre las imágenes maestras y las plataformas de SO (por cada aplicación); sin embargo, esto no funcionará para todas las aplicaciones. Si dispone de aplicaciones

© 1999-2019 Citrix Systems, Inc. All rights reserved.

con scripts de instalación para SO de escritorio que les impiden funcionar en un SO de servidor, Citrix recomienda empaquetar las aplicaciones por separado para cada sistema operativo.

- En muchos casos, AppDisks funciona en diferentes sistemas operativos. Por ejemplo, puede agregar un AppDisk, creado en una VM de Windows 7, a un grupo de entrega que contenga máquinas con Windows 2008 R2, siempre que ambos sistemas operativos tengan el mismo valor de bits (32 bits o 64 bits) y admitan la aplicación. Sin embargo, Citrix recomienda no agregar AppDisks creados en una versión posterior de sistema operativo (como Windows 10) a grupos de entrega que contengan máquinas con una versión anterior de sistema operativo (por ejemplo, Windows 7), porque es posible que no funcionen correctamente.
- Aun así, si debe conceder acceso a las aplicaciones de un AppDisk a solo un subconjunto de usuarios pertenecientes a un grupo de entrega, Citrix recomienda utilizar una directiva de grupo para ocultar a algunos usuarios las aplicaciones que corresponda de un AppDisk. El archivo ejecutable de la aplicación en cuestión sigue estando disponible, pero no se ejecutará para esos usuarios.
- En entornos en ruso y chino que ejecutan el sistema operativo Windows 7, el diálogo de reinicio no desaparece automáticamente. En estos casos, después de iniciar sesión en un escritorio entregado, el diálogo de reinicio aparece y debería desaparecer rápidamente.
- Cuando se utiliza la herramienta de script `Upload-PvDDiags`, falta información de registro relacionada con la capa de usuario PVD cuando la designación de la unidad del usuario no está establecida en “P”.
- En entornos configurados en vasco, un sistema operativo Windows 7 puede no mostrar correctamente el idioma apropiado en la pantalla de solicitud de reinicio. Antes de establecer el idioma a vasco, instale el francés o el español como idioma primario. A continuación, instale el vasco y establézcalo como idioma del sistema operativo.
- Al apagar un equipo, aparece un aviso de actualización PVD incluso aunque el disco PVD esté establecido en modo de solo lectura.
- Durante una actualización en contexto, podría suprimirse un archivo de registro (DaFsFilter), lo que provoca error en la actualización.

> **Sugerencia:**
>
> Al crear un disco AppDisk, utilice una VM que solo tenga instalado el sistema operativo (es decir, que no incluya otras aplicaciones); el sistema operativo debe contener todas las actualizaciones correspondientes antes de crear el AppDisk.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Introducción a la implementación

En la siguiente lista, se ofrece un resumen de los pasos a seguir para implementar AppDisks. Los detalles se proporcionan más adelante en este artículo.

1. Desde la consola de administración del hipervisor, instale un Virtual Delivery Agent (VDA) en una máquina virtual.
2. Cree un AppDisk, lo que implica completar los pasos de Studio y de la consola de administración del hipervisor.
3. Desde la consola de administración del hipervisor, instale aplicaciones en el AppDisk.
4. Selle el AppDisk (desde Studio o la consola de administración del hipervisor). El sellado permite que Citrix Virtual Apps and Desktops registren las aplicaciones y los archivos auxiliares del AppDisk en una biblioteca de aplicaciones (AppLibrary).
5. En Studio, cree o modifique un grupo de entrega y seleccione los AppDisks a incluir; esto se denomina *asignación de AppDisks* (aunque use la acción **Administrar AppDisks** en Studio). Cuando se inicien las máquinas virtuales del grupo de entrega, Citrix Virtual Apps and Desktops se coordinarán con la librería AppLibrary, interactuarán con Machine Creation Services (MCS) o Citrix Provisioning (antes Provisioning Services) y el Delivery Controller para distribuir por streaming los dispositivos de arranque después de que los AppDisks hayan sido configurados en ellos.

Requisitos

Los requisitos de AppDisks se suman a los que se muestran en Requisitos del sistema.

La función AppDisks solo se admite en implementaciones que contienen (como mínimo) las versiones de Delivery Controller y Studio suministradas en XenApp y XenDesktop 7.8, incluidos los requisitos previos que el instalador instala automáticamente (como .NET).

Los AppDisks se pueden crear en las mismas versiones de sistema operativo Windows que se admiten para los VDA. Las máquinas de los grupos de entrega que utilizarán AppDisks deben tener instalada al menos la versión 7.8 de VDA.

Citrix recomienda instalar o actualizar todas las máquinas a la versión más reciente de VDA y, a continuación, actualizar los catálogos de máquinas y los grupos de entrega si es necesario. Al crear un grupo de entrega, si selecciona máquinas que tienen instaladas versiones diferentes de VDA, el grupo de entrega será compatible con la versión más antigua de VDA. Este es el *nivel funcional* del grupo. Para obtener más información sobre el nivel funcional, consulte Crear grupos de entrega.

Si quiere aprovisionar las máquinas virtuales que se usarán para crear AppDisks, puede usar:

- MCS proporcionado con Delivery Controller.
- La versión de Citrix Provisioning que se ofrece en la página de descargas junto con la versión de Citrix Virtual Apps and Desktops.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Hipervisores compatibles:
  - XenServer
  - VMware (versión mínima 5.1)
  - Microsoft System Center Virtual Machine Manager

AppDisks no se puede utilizar con otros hipervisores de host y tipos de servicios de nube que se admiten para Citrix Virtual Apps and Desktops.

La creación de AppDisks no está disponible en las máquinas de catálogos de MCS que usan caché de datos temporales.

> **Nota:**
>
> Se pueden conectar discos AppDisk a máquinas aprovisionadas con MCS usando caché de escritura, pero no se pueden usar para crear los discos AppDisk.

Los catálogos de Acceso con Remote PC no admiten el uso de AppDisks.

El Servicio de instantáneas de volumen de Windows debe estar habilitado en la máquina virtual donde se cree el AppDisk. Este servicio está habilitado de forma predeterminada.

Los grupos de entrega que se utilicen con AppDisks pueden contener máquinas provenientes de catálogos de máquinas agrupadas aleatorias con SO de servidor o de escritorio. No se puede usar AppDisks con máquinas provenientes de otros tipos de catálogos, como escritorios agrupados estáticos o dedicados (asignados).

Las máquinas en que esté instalado Studio deben tener instalado .NET Framework 3.5 (además de otras versiones instaladas de .NET).

AppDisks puede afectar al almacenamiento. Para obtener más información, consulte Consideraciones sobre rendimiento y almacenamiento.

Si utiliza AppDNA:

- Consulte la documentación de AppDNA y las preguntas frecuentes de AppDisk.
- El software de AppDNA y Controller no deben estar instalados en el mismo servidor. Utilice la versión de AppDNA proporcionada con esta versión de Citrix Virtual Apps and Desktops. Para conocer otros requisitos de AppDNA, consulte la documentación referente a esa función.
- En el servidor AppDNA, compruebe que haya una excepción de firewall para el puerto predeterminado 8199.
- No inhabilite la conexión de AppDNA cuando cree AppDisks.
- Al crear el sitio de Citrix Virtual Apps and Desktops, puede habilitar el análisis de compatibilidad con AppDNA en la página **Características adicionales** del asistente para la creación de sitios. También puede habilitarlo o inhabilitarlo más adelante. Para ello, deberá seleccionar **Configuración > AppDNA** en el panel de navegación de Studio.
- En Studio, al hacer clic en el enlace “Ver informe de problemas”, aparece el informe de AppDNA. Sin embargo, las combinaciones de sistema operativo que utiliza AppDNA de forma predeter-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

minada son Windows 7 de 64 bits para grupos de entrega de escritorios y Windows Server 2012 R2 para grupos de entrega de servidores. Si los grupos de entrega cuentan con versiones diferentes de Windows, las combinaciones predeterminadas de imagen en los informes que muestra Studio serán incorrectas. Para solucionar este problema, edite manualmente el informe en AppDNA después de que Studio lo haya creado.

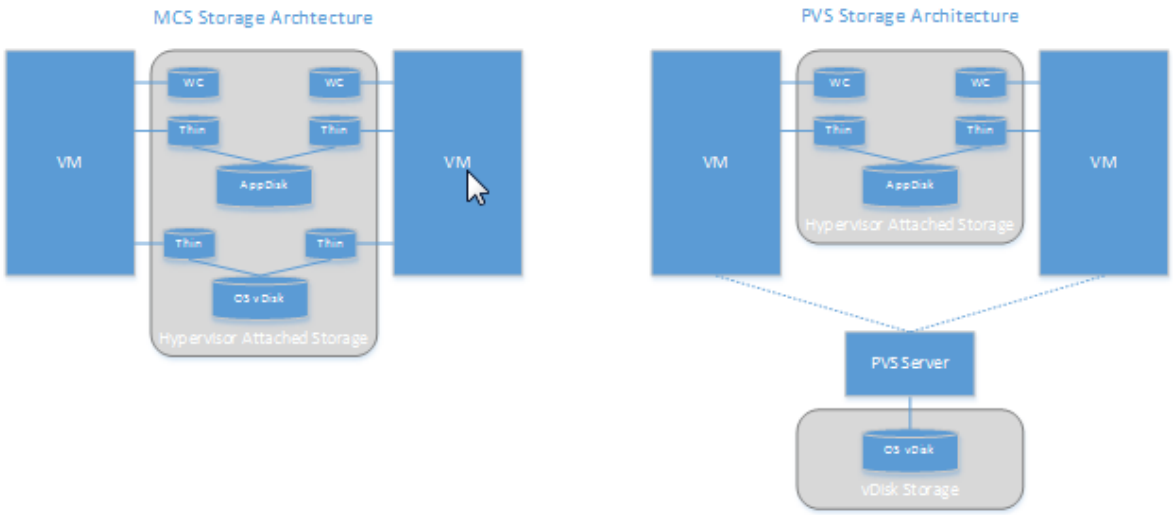
- Hay una dependencia entre las distintas versiones de servidor AppDNA y Studio.
  - Desde la versión 7.12, Studio debe ser tener la misma versión (o una posterior) que el servidor AppDNA.
  - Para las versiones 7.9 y 7.11, las versiones del servidor Studio y AppDNA deben coincidir.
  - En la siguiente tabla se resumen las versiones que pueden combinarse (Sí = versiones a combinar; - = no funcionan combinadas):

Versión del producto	Studio 7.9	Studio 7.11	Studio 7.12	Studio 7.13	Studio 7.14	Studio 7.15
AppDNA 7.9	Sí	-	-	-	-	-
AppDNA 7.11	-	Sí	-	-	-	-
AppDNA 7.12	-	-	Sí	Sí	Sí	Sí
AppDNA 7.13	-	-	Sí	Sí	Sí	Sí
AppDNA 7.14	-	-	-	-	Sí	Sí
AppDNA 7.15	-	-	-	-	-	Sí

Consideraciones sobre rendimiento y almacenamiento

Separar aplicaciones y sistema operativo mediante dos discos y almacenar esos discos en áreas diferentes puede afectar a su planificación de almacenamiento. En el gráfico siguiente, se muestran las arquitecturas de almacenamiento de Machine Creation Services y Citrix Provisioning. “WC” indica la memoria caché de escritura, mientras que “Thin” indica el disco ligero usado para almacenar las diferencias entre los discos virtuales de sistema operativo y el AppDisk de una máquina virtual.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



En entornos de MCS:

- Puede seguir equilibrando el tamaño de los discos virtuales (vDisk) del sistema operativo y de los AppDisks con las directrices de tamaño de datos existentes en la empresa. Si los AppDisks se comparten entre varios grupos de entrega, se puede reducir la capacidad total de almacenamiento.
- Los AppDisks y los discos virtuales de SO se encuentran en las mismas áreas de almacenamiento, por lo que debe planificar con cuidado sus requisitos de capacidad de almacenamiento con el fin de evitar cualquier efecto negativo en la capacidad resultante cuando implemente los AppDisks. Los AppDisks pueden sobrecargarse, por lo que su almacenamiento debe poder adaptarse a esa sobrecarga y a las aplicaciones.
- No hay ningún efecto relevante sobre IOPS porque los discos virtuales del SO y los AppDisks se encuentran en el mismo área de almacenamiento. No hay aspectos a tener en cuenta sobre la memoria caché de escritura cuando se utilice Machine Creation Services.

En entornos de Citrix Provisioning:

- Debe permitir IOPS y la capacidad aumentada porque las aplicaciones se moverán desde el almacenamiento de AppDisk al almacenamiento correspondiente al hipervisor.
- Con Citrix Provisioning, los AppDisks y los discos virtuales (vDisk) del SO no comparten las áreas de almacenamiento. La capacidad de almacenamiento del disco virtual (vDisk) del sistema operativo se reduce, mientras que el almacenamiento correspondiente al hipervisor aumenta. Por lo tanto, debe dar a los entornos de Citrix Provisioning el tamaño adecuado para dar cabida a esos cambios.
- Los AppDisks del almacenamiento correspondiente al hipervisor requieren más IOPS, mientras que los discos virtuales del sistema operativo requieren menos.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Memoria caché de escritura: Citrix Provisioning utiliza un archivo VHDX dinámico en una unidad con formato NTFS; cuando se escriben bloques en la memoria caché de escritura, el archivo VHDX se extiende dinámicamente. Cuando los AppDisks se conectan a su máquina virtual asociada, se combinan con los discos virtuales (vDisk) del sistema operativo para ofrecer una vista unificada del sistema de archivos. Por lo general, esta combinación tiene como resultado que se escriban datos adicionales en la caché de escritura, lo que aumenta el tamaño del archivo de caché de escritura. Debe tener esto en cuenta cuando planifique la capacidad necesaria.

En ambos entornos, MCS o Citrix Provisioning, no olvide reducir el tamaño del disco virtual (vDisk) del SO para aprovechar los AppDisks que cree. Si no, deberá planificar más almacenamiento.

Cuando varios usuarios de un sitio enciendan sus equipos simultáneamente (por ejemplo, al inicio de la jornada laboral), las múltiples solicitudes de inicio ejercen presión sobre el hipervisor, lo que puede afectar al rendimiento. En caso de Citrix Provisioning, las aplicaciones no se encuentran en el disco virtual (vDisk) del SO, por lo que se realizan menos solicitudes al servidor Citrix Provisioning. Con la menor carga resultante en cada dispositivo de destino, el servidor Citrix Provisioning puede transmitir a más destinos. Sin embargo, tenga en cuenta que una mayor densidad entre destino y servidor podría afectar negativamente al rendimiento cuando haya una gran cantidad de arranques de máquinas.

Consideraciones sobre la creación de AppDisks

Hay dos formas de crear un AppDisk, instalar aplicaciones en él y sellarlo. Ambos métodos incluyen pasos a completar desde Studio y la consola de administración del hipervisor. Los métodos se diferencian en dónde se completa la mayoría de los pasos.

Independientemente del método que utilice:

- Reserve 30 minutos para la creación del AppDisk.
- No inhabilite la conexión de AppDNA cuando cree AppDisks.
- Cuando agregue aplicaciones a un AppDisk, instale aplicaciones para todos los usuarios. Rearme aquellas aplicaciones que usen la activación de Key Management Server (KMS). Para obtener más información, consulte la documentación de la aplicación.
- No se conservan los archivos, las carpetas ni las entradas de Registro que se hayan creado en ubicaciones específicas del usuario durante la creación de AppDisk. Además, algunas aplicaciones ejecutan un asistente de primer uso para crear datos de usuario durante la instalación. Use una solución de administración de perfiles para conservar esos datos y evitar que el asistente aparezca cada vez que se inicie el AppDisk.
- Si usa AppDNA, el análisis comienza automáticamente después de que se complete el proceso de creación. Durante este intervalo, el estado del AppDisk en Studio es “analizando”.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Consideraciones sobre Citrix Provisioning

En máquinas procedentes de catálogos creados con Provisioning Services, AppDisks requiere una configuración adicional durante la creación de AppDisk. Desde la consola de Provisioning Services:

1. Cree una nueva versión del disco virtual (vDisk) asociado a la colección de dispositivos que contiene la máquina virtual.
2. Coloque la máquina virtual en el modo de mantenimiento.
3. Durante la creación de AppDisk, seleccione la versión de mantenimiento en la pantalla de inicio cada vez que se reinicie la máquina virtual.
4. Después de sellar el AppDisk, coloque la máquina virtual de nuevo en producción y elimine la versión de disco virtual (vDisk) creada.

Crear un AppDisk principalmente en Studio

Este procedimiento incluye tres tareas: crear el AppDisk, crear las aplicaciones en el AppDisk y, a continuación, sellar el AppDisk.

Crear un AppDisk:

1. Seleccione **AppDisks** en el panel de navegación de Studio y, a continuación, seleccione **Crear AppDisk** en el panel "Acciones".
2. Revise la información en la página **Introducción** del asistente y haga clic en **Siguiente**.
3. En la página **Crear AppDisk**, seleccione el botón de opción **Crear nuevo AppDisk**. Seleccione un tamaño de disco predefinido (pequeño, mediano o grande), o bien especifique un tamaño de disco en GB; el tamaño mínimo es de 3 GB. El tamaño del disco debe ser lo suficientemente grande para alojar las aplicaciones que se vayan a agregar. Haga clic en **Siguiente**.
4. En la página **Máquina de preparación**, seleccione un catálogo de máquinas agrupadas aleatorias para que se utilicen como la imagen maestra en la que se generará el AppDisk. Nota: La pantalla muestra todos los catálogos de máquinas presentes en el sitio separados por tipo; solo se pueden seleccionar aquellos catálogos que contengan al menos una máquina disponible. Si elige un catálogo que no contiene máquinas virtuales agrupadas aleatorias, fallará la creación del AppDisk. Después de seleccionar una VM de un catálogo de máquinas virtuales agrupadas aleatorias, haga clic en **Siguiente**.
5. En la página **Resumen**, escriba un nombre y una descripción para el AppDisk. Revise la información especificada en las páginas anteriores del asistente. Haga clic en **Finish**.

Recuerde: Si utiliza Citrix Provisioning, siga las instrucciones de Consideraciones sobre Citrix Provisioning.

Una vez cerrado el asistente, la pantalla de Studio referente al nuevo AppDisk indicará "Creando". Después de crear el AppDisk, la pantalla cambia a "Listo para instalar aplicaciones".

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Instalar aplicaciones en el AppDisk:

Desde la consola de administración del hipervisor, instale aplicaciones en el AppDisk. (**Sugerencia:** Si olvida el nombre de la VM, seleccione **AppDisks** en el panel de navegación de Studio y, a continuación, seleccione **Instalar aplicaciones** en el panel "Acciones" para ver el nombre.) Consulte la documentación del hipervisor para obtener información sobre cómo instalar las aplicaciones. (Recuerde: Debe instalar aplicaciones en el AppDisk desde la consola de administración del hipervisor. No use la tarea **Instalar aplicaciones** en el panel "Acciones" de Studio.)

Sellar el AppDisk:

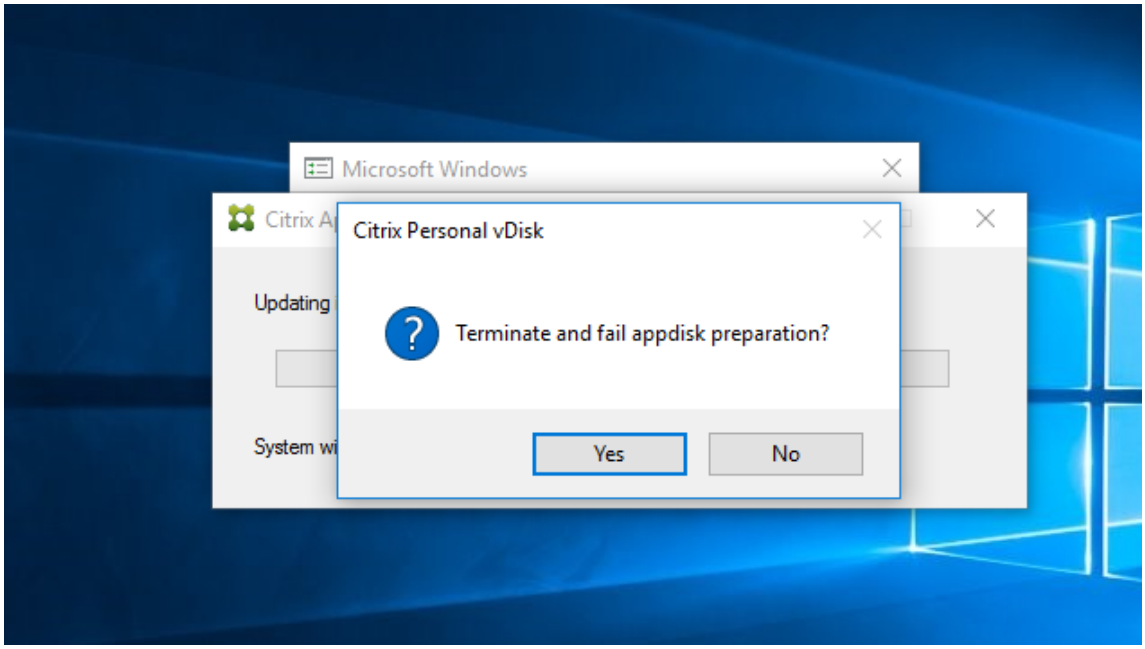
1. Seleccione **AppDisks** en el panel de navegación de Studio.
2. Seleccione el AppDisk que ha creado y seleccione **Sellar AppDisk** en el panel "Acciones".

Después de crear el AppDisk, instale aplicaciones en él, séllelo y asígnelo a un grupo de entrega.

Cancelar la preparación y el sellado de AppDisk

En algunos casos, puede que un administrador necesite cancelar la creación o el sellado de AppDisk:

1. Acceda a la máquina virtual.
2. Cierre el cuadro de diálogo:
3. Después de cerrar el cuadro de diálogo, aparece un mensaje emergente que solicita confirmación para cancelar la operación seleccionada. Haga clic en **Sí**.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

> **Nota**
>
> Si cancela la preparación de AppDisk, reiniciar la máquina la devuelve a su estado inicial; de lo contrario, debe crear una VM limpia.

Crear un AppDisk en el hipervisor e importarlo en Studio

En este procedimiento, se completan las tareas de creación y preparación del AppDisk desde la consola de administración del hipervisor y, a continuación, el AppDisk se importa en Studio.

Preparar, instalar aplicaciones y sellar un AppDisk en el hipervisor:

1. Desde la consola de administración del hipervisor, cree una máquina virtual e instale un VDA en ella.
2. Apague la máquina y tome una instantánea de ella.
3. Cree una nueva máquina a partir de la instantánea y, a continuación, agréguele un disco nuevo. Ese disco (que se convertirá en el AppDisk) debe ser lo suficientemente grande como para alojar todas las aplicaciones que se instalarán en él.
4. Inicie la máquina y seleccione **Inicio > Preparar AppDisk**. Si este acceso directo al menú Inicio no está disponible en el hipervisor, abra un símbolo del sistema en C:\Archivos de programa\Citrix\personal vDisk\bin y escriba: **CtxPvD.Exe –s LayerCreationBegin**. La máquina se reiniciará y preparará el disco. Se produce un segundo reinicio después de unos minutos, cuando se complete la preparación.
5. Instale las aplicaciones que quiere poner a disposición de los usuarios.
6. Haga doble clic en el acceso directo **Paquete AppDisk** en el escritorio de la máquina. La máquina se reinicia y comienza el proceso de sellado. Cuando se cierre el cuadro de diálogo “En proceso”, apague la máquina virtual.

Use Studio para importar el AppDisk creado en el hipervisor:

1. Seleccione **AppDisks** en el panel de navegación de Studio y, a continuación, seleccione **Crear AppDisk** en el panel “Acciones”.
2. Revise la información en la página **Introducción** y haga clic en **Siguiente**.
3. En la página **Crear AppDisk**, seleccione el botón de opción **Importar AppDisk existente**. Seleccione el recurso (red y almacenamiento) donde reside el AppDisk que ha creado en el hipervisor. Haga clic en **Siguiente**.
4. En la página **Máquina de preparación**, vaya a la máquina, seleccione el disco y haga clic en **Siguiente**.
5. En la página **Resumen**, escriba un nombre y una descripción para el AppDisk. Revise la información especificada en las páginas anteriores del asistente. Haga clic en **Finish**. Studio importa el AppDisk.

Después de importar el AppDisk en Studio, asígnelo a un grupo de entrega.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Asignar un AppDisk a un grupo de entrega

Puede asignar uno o varios AppDisks a un grupo de entrega a la hora de crear el grupo de entrega o más adelante. La información que proporcione sobre los AppDisks es esencialmente la misma.

Si está agregando AppDisks a un grupo de entrega que está creando, use la siguiente guía para la página **AppDisks** en el asistente para crear el grupo de entrega. (Para obtener información sobre otras páginas de ese asistente, consulte Crear grupos de entrega.)

Para agregar (o quitar) AppDisks de un grupo de entrega existente:

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo de entrega y seleccione **Administrar AppDisks** en el panel "Acciones". Consulte las siguientes instrucciones para la página **AppDisks**.
3. Al cambiar la configuración de AppDisk en un grupo de entrega, es obligatorio reiniciar las máquinas del grupo.

Página de AppDisks:

La página **AppDisks** (en el asistente para crear grupos de entrega o en el flujo "Administrar AppDisks") ofrece una lista de los AppDisks ya implementados para el grupo de entrega, junto con la prioridad que tienen. (Si está creando el grupo de entrega, la lista estará vacía.) Para obtener más información, consulte la sección "Prioridad de AppDisk".

1. Haga clic en **Agregar**. En el cuadro de diálogo Seleccionar AppDisks, se ofrece una lista de todos los AppDisks de la columna izquierda. Los AppDisks que ya están asignados a ese grupo de entrega tienen las casillas marcadas y no se pueden seleccionar.
2. Marque una o varias casillas de los AppDisks disponibles en la columna izquierda. En la columna derecha, se ofrece una lista de las aplicaciones presentes en el AppDisk. (Al seleccionar la ficha **Aplicaciones** situada encima de la columna derecha, se muestran aplicaciones en un formato similar al del menú Inicio. Al seleccionar la ficha **Paquetes instalados**, se ofrece una lista de las aplicaciones en un formato similar al de la lista Programas y características.)
3. Después de seleccionar uno o varios AppDisks disponibles, haga clic en **Aceptar**.
4. Haga clic en **Siguiente** en la página de AppDisks.

Prioridad de AppDisk en un grupo de entrega

Cuando un grupo de entrega tiene asignado más de un AppDisk, la página **AppDisks** (en las pantallas "Crear grupo de entrega", "Modificar grupo de entrega" y "Administrar AppDisks") muestra los AppDisks por prioridad descendente. Las entradas situadas en la parte superior de la lista tienen la prioridad más alta. La prioridad indica el orden en que se procesan los AppDisks.

Puede usar las flechas de dirección arriba y abajo ubicadas junto a la lista para cambiar la prioridad de cada AppDisk. Si está AppDNA integrado en la implementación de AppDisk, entonces analiza au-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

tomáticamente las aplicaciones y establece la prioridad cuando los AppDisks se asignan al grupo de entrega. Posteriormente, si agrega o quita AppDisks del grupo, hacer clic en **Orden automático** indica al AppDNA que debe volver a analizar la lista actual de AppDisks y volver a determinar las prioridades. El análisis (y la reordenación de prioridades, si fuera necesario) puede tardar varios minutos en completarse.

Administrar AppDisks

Después de crear y asignar AppDisks a los grupos de entrega, puede cambiar las propiedades de un AppDisk con la ayuda del nodo AppDisks en el panel de navegación de Studio. Los cambios a las aplicaciones de un AppDisk deben realizarse desde la consola de administración del hipervisor.

Consideraciones importantes sobre Windows Update:

Puede usar el servicio Windows Update para actualizar aplicaciones (por ejemplo, el conjunto de aplicaciones Office) en un AppDisk. Sin embargo, no use el servicio Windows Update para aplicar las actualizaciones del sistema operativo a un AppDisk. Aplique las actualizaciones de sistema operativo a la imagen maestra, no al AppDisk; de lo contrario, el AppDisk no se inicializará correctamente.

- Al aplicar correcciones y otras actualizaciones a las aplicaciones de un AppDisk, aplique solo aquellas que requiera cada aplicación. No aplique actualizaciones para otras aplicaciones.
- Cuando se instalen actualizaciones de Windows, primero deseleccione todas las entradas y, a continuación, seleccione el subconjunto que necesiten las aplicaciones en los AppDisks que esté actualizando.

Consideraciones sobre antivirus para la creación de AppDisk

En algunos casos, puede toparse con problemas si intenta crear un AppDisk cuando la VM base tiene un agente antivirus instalado. En esos casos, la creación de AppDisk puede fallar porque el antivirus marca ciertos procesos como peligrosos. Estos procesos, **CtxPvD.exe** y **CtxPvDSrv.exe**, se deben agregar a la lista de excepciones del antivirus que se utilice en la VM base.

En esta sección, se ofrece información sobre cómo agregar excepciones en las siguientes aplicaciones de antivirus:

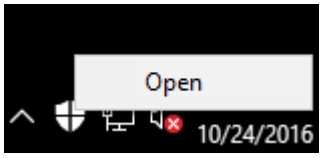
- Windows Defender (para Windows 10)
- OfficeScan (versión 11.0)
- Symantec (versión 12.1.16)
- McAfee (versión 4.8)

Windows Defender

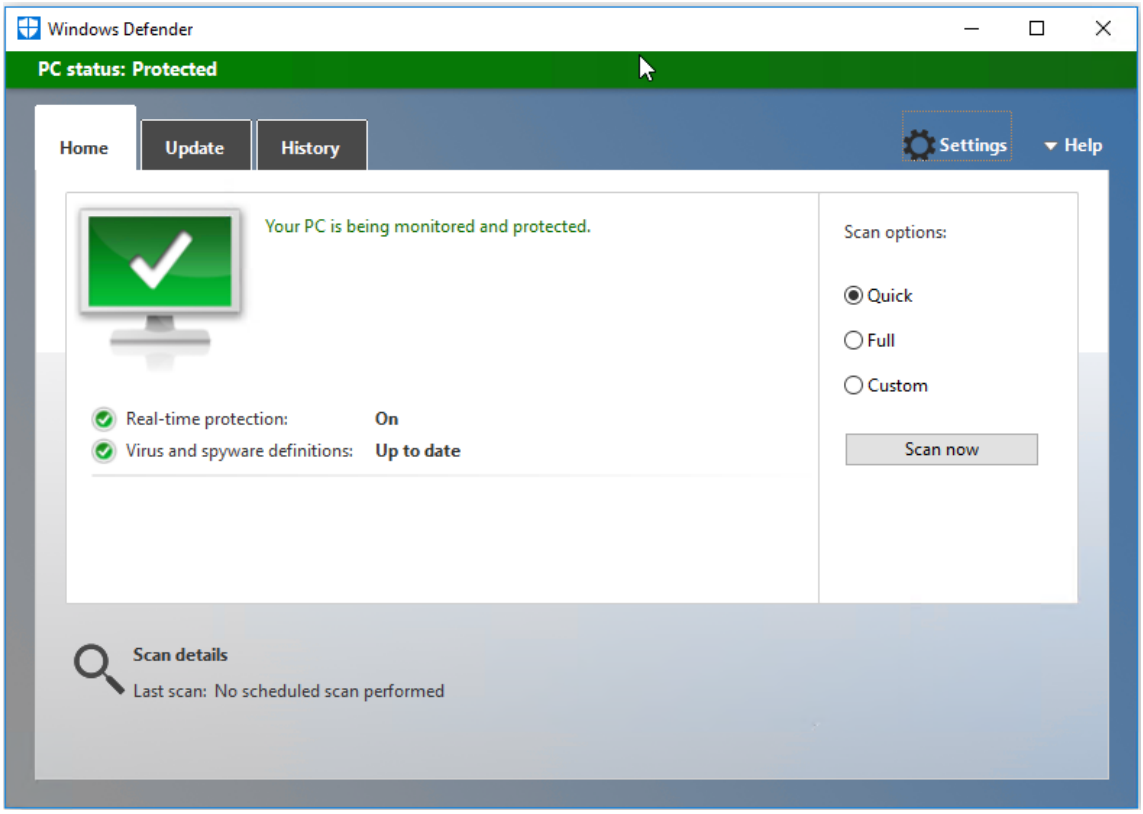
Si la VM base usa Windows Defender (versión 10):

© 1999-2019 Citrix Systems, Inc. All rights reserved.

1. Inicie sesión en el equipo con privilegios de administrador local.
2. Seleccione el icono de Windows Defender y haga clic con el botón secundario para ver el botón **Abrir**:

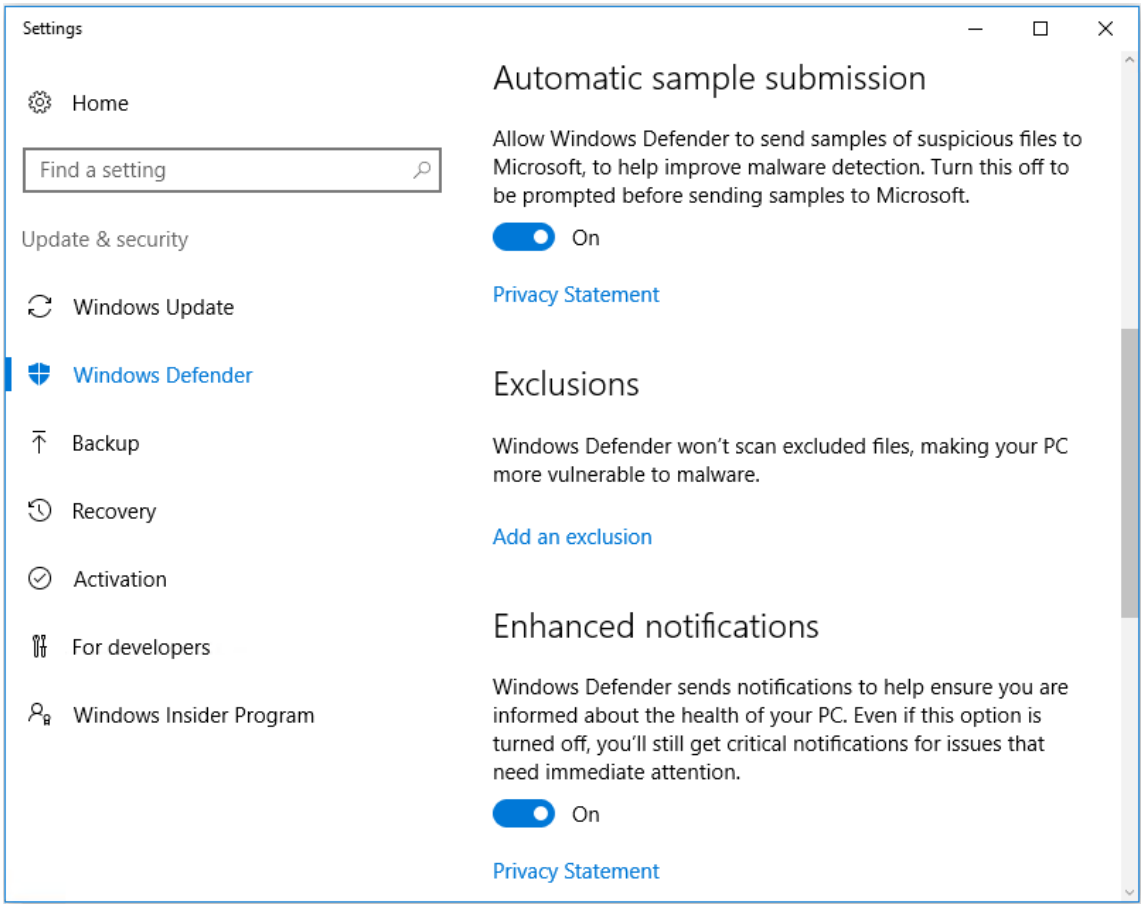


3. En la consola de Windows Defender, seleccione **Configuración** en la parte superior derecha de la interfaz:



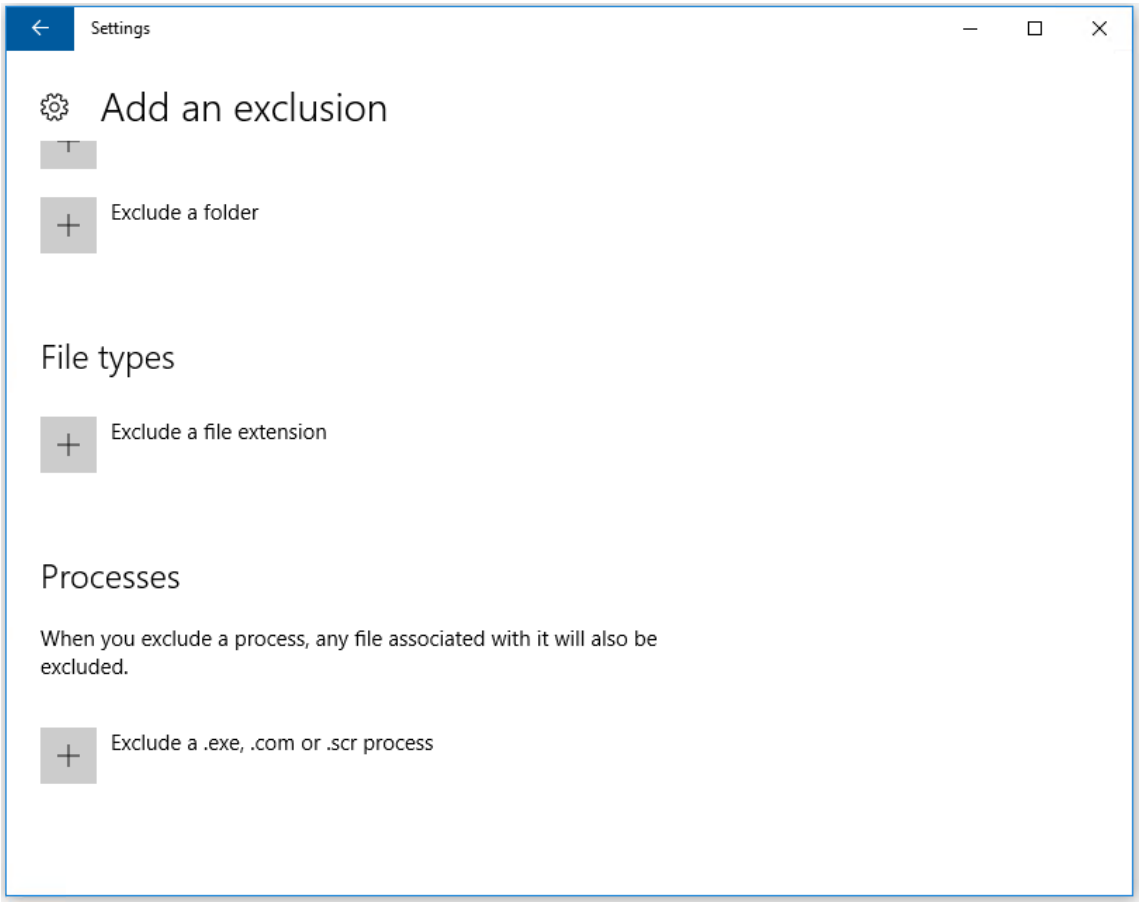
4. En la sección **Exclusiones** de la pantalla “Configuración”, haga clic en **Agregar exclusión**:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

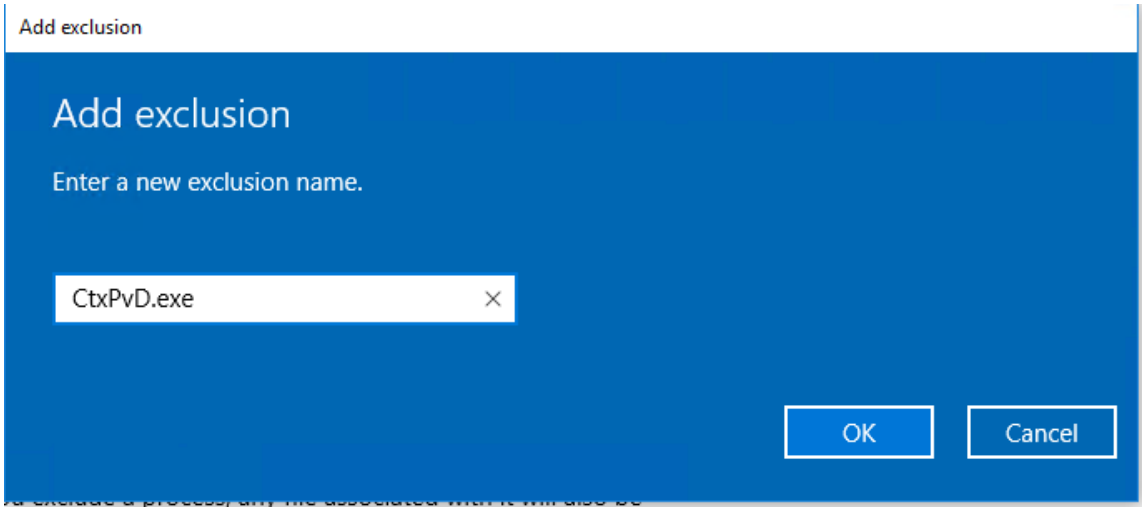


5. En la pantalla **Agregar exclusión**, seleccione **Excluir un proceso .exe, .com o .scr**:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

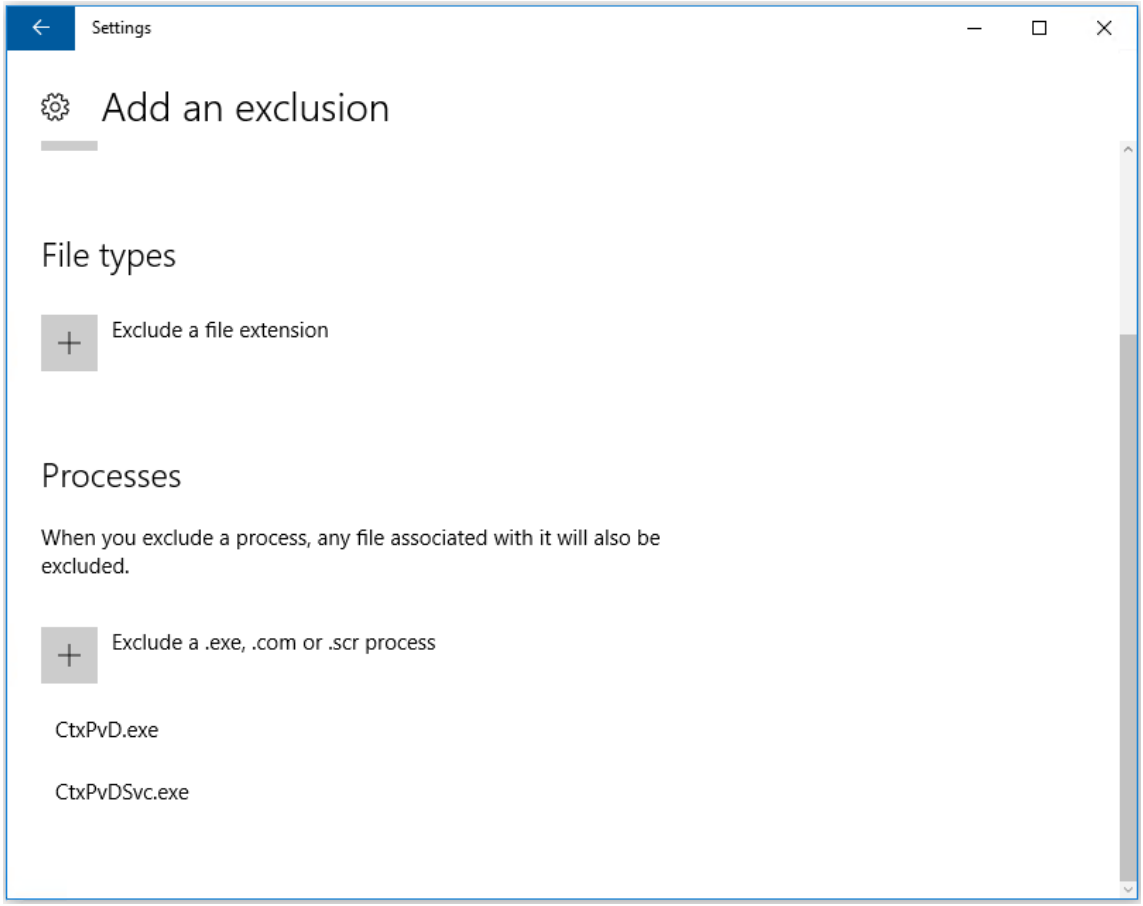


6. En la pantalla **Agregar exclusión**, escriba el nombre de la exclusión; deben agregarse **CtxPvD.exe** y **CtxPvDSvc.exe** a fin de evitar conflictos en el momento de crear un AppDisk. Después de escribir el nombre de la exclusión, haga clic en **Aceptar**:



Después de agregar las exclusiones, aparecen en la lista de procesos excluidos en la pantalla **Configuración**:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

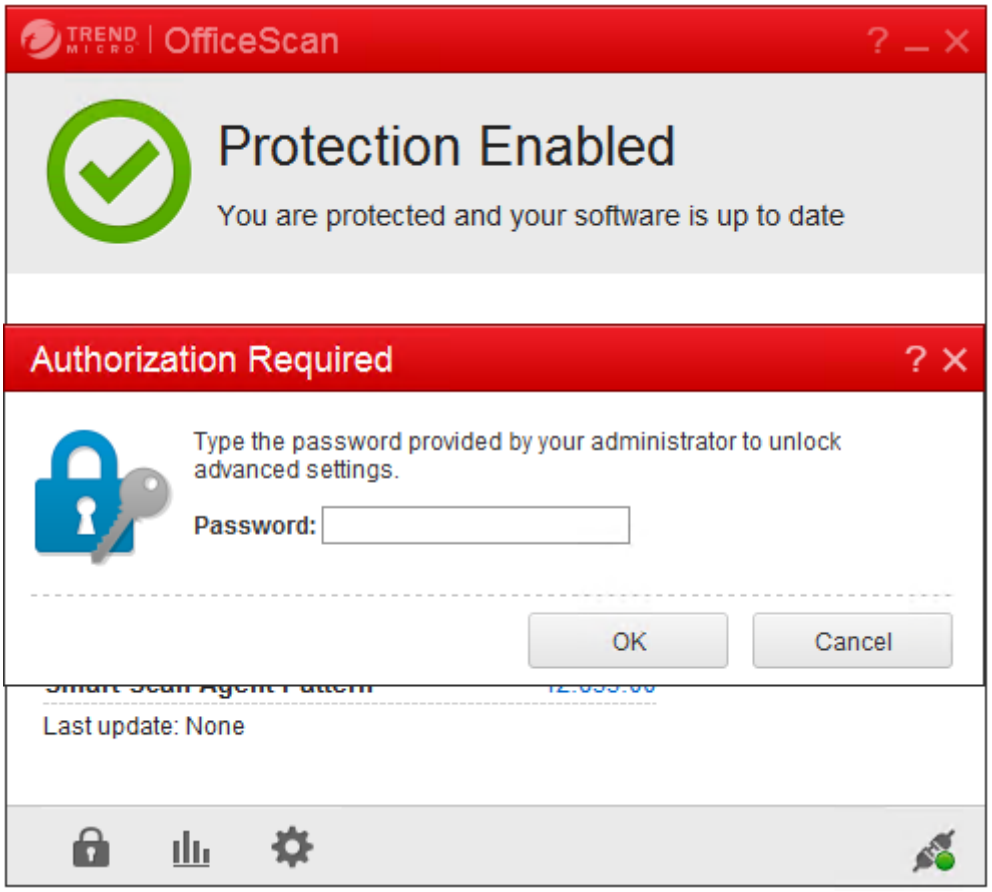


OfficeScan

Si la VM base usa OfficeScan (versión 11):

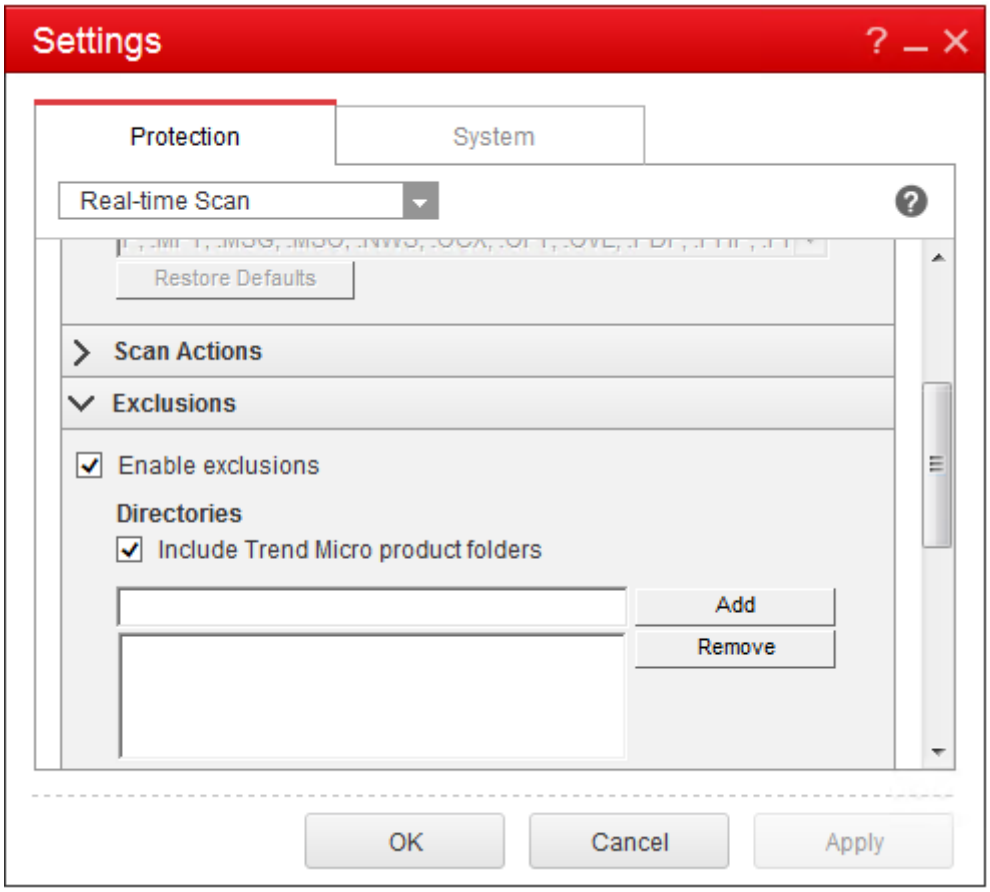
1. Inicie la consola de OfficeScan.
2. Haga clic en el icono de bloqueo en la parte inferior izquierda de la interfaz y escriba la contraseña:

© 1999-2019 Citrix Systems, Inc. All rights reserved.



3. Haga clic en el icono **Settings** para ver las opciones de configuración.
4. En la pantalla “Settings”, seleccione la ficha **Protection**.
5. En la ficha de protección, desplácese hasta encontrar la sección **Exclusions**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

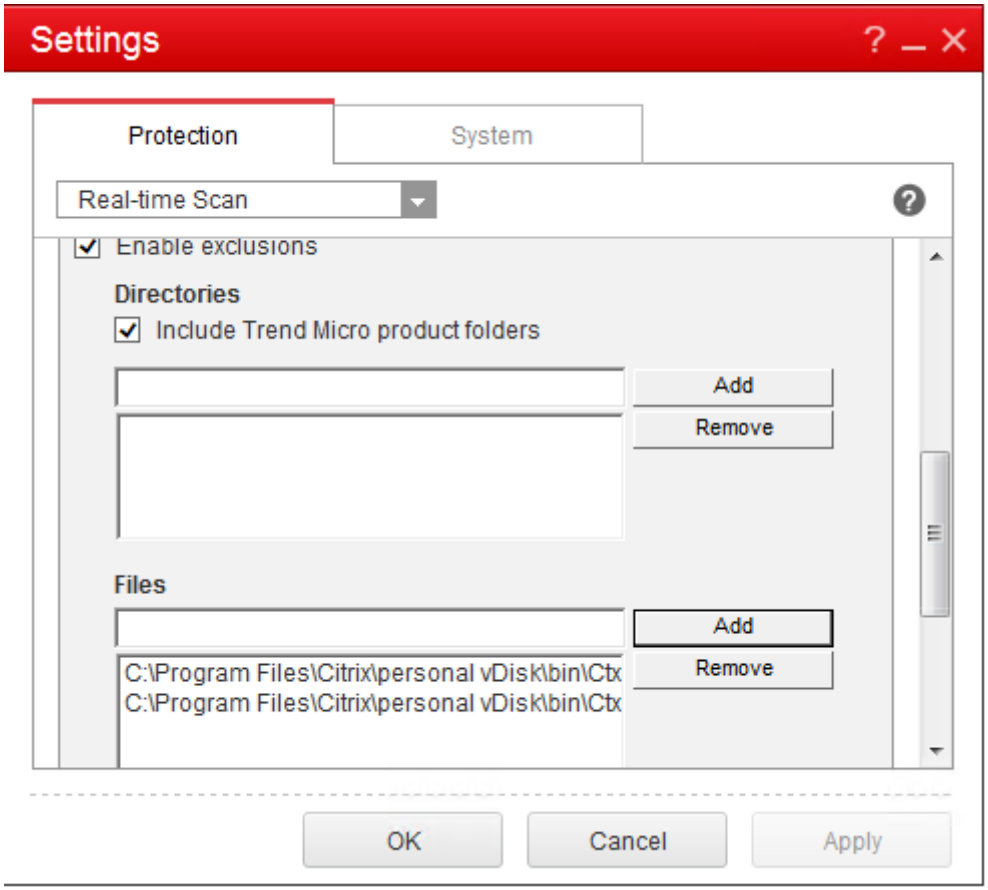


6. En la sección **Files**, haga clic en **Add** y, a continuación, introduzca los siguientes procesos de AppDisk a la lista de excepciones:

   ```
   C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe
   ```

   ```
   C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe
   ```

© 1999-2019 Citrix Systems, Inc. All rights reserved.



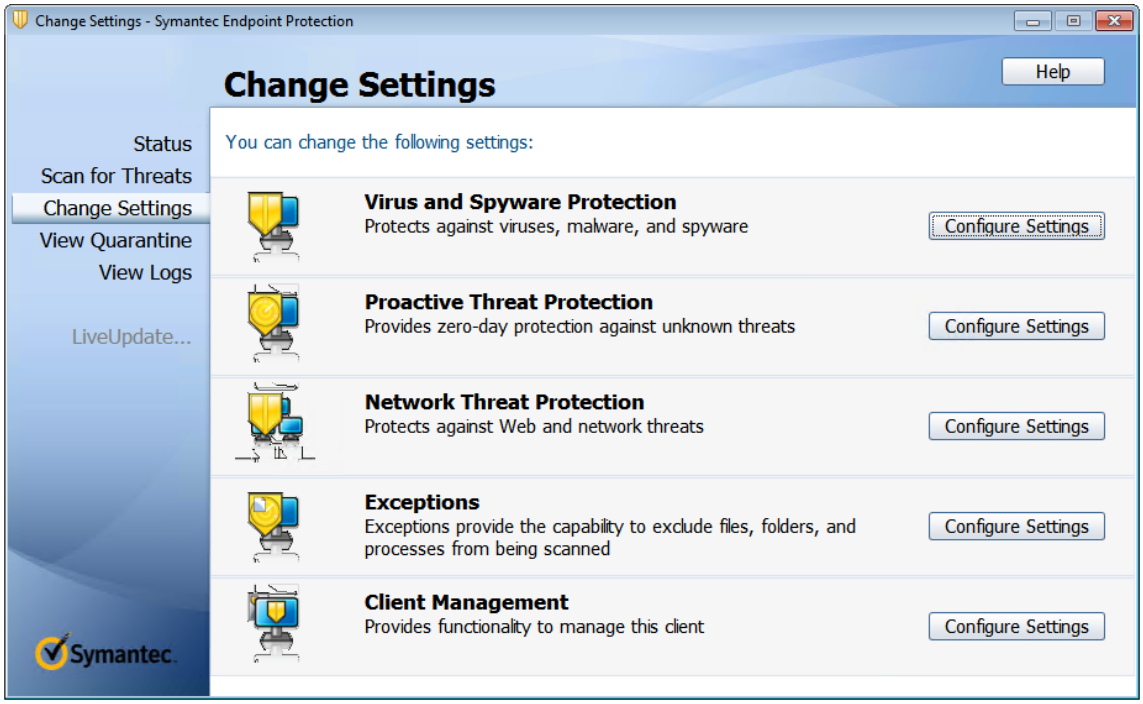
7. Haga clic en **Apply** y, a continuación, en **OK** para agregar las exclusiones.

Symantec

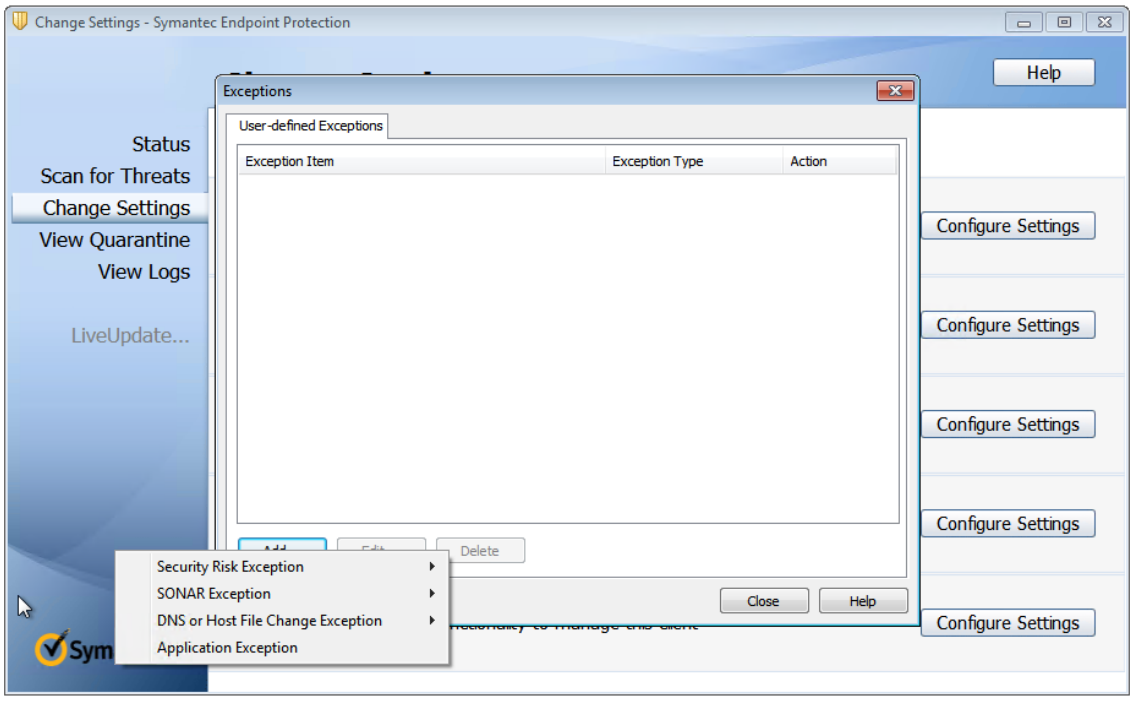
Si la VM base usa Symantec (versión 12.1.16):

1. Inicie la consola de Symantec.
2. Haga clic en **Change Settings**.
3. En la sección **Exceptions**, haga clic en **Configure Settings**:

© 1999-2019 Citrix Systems, Inc. All rights reserved.



4. En la pantalla de configuración, haga clic en **Add**.
5. Después de hacer clic en la opción de agregar, aparecerá el menú contextual, que permite especificar el tipo de aplicación. Seleccione **Application Exception**:

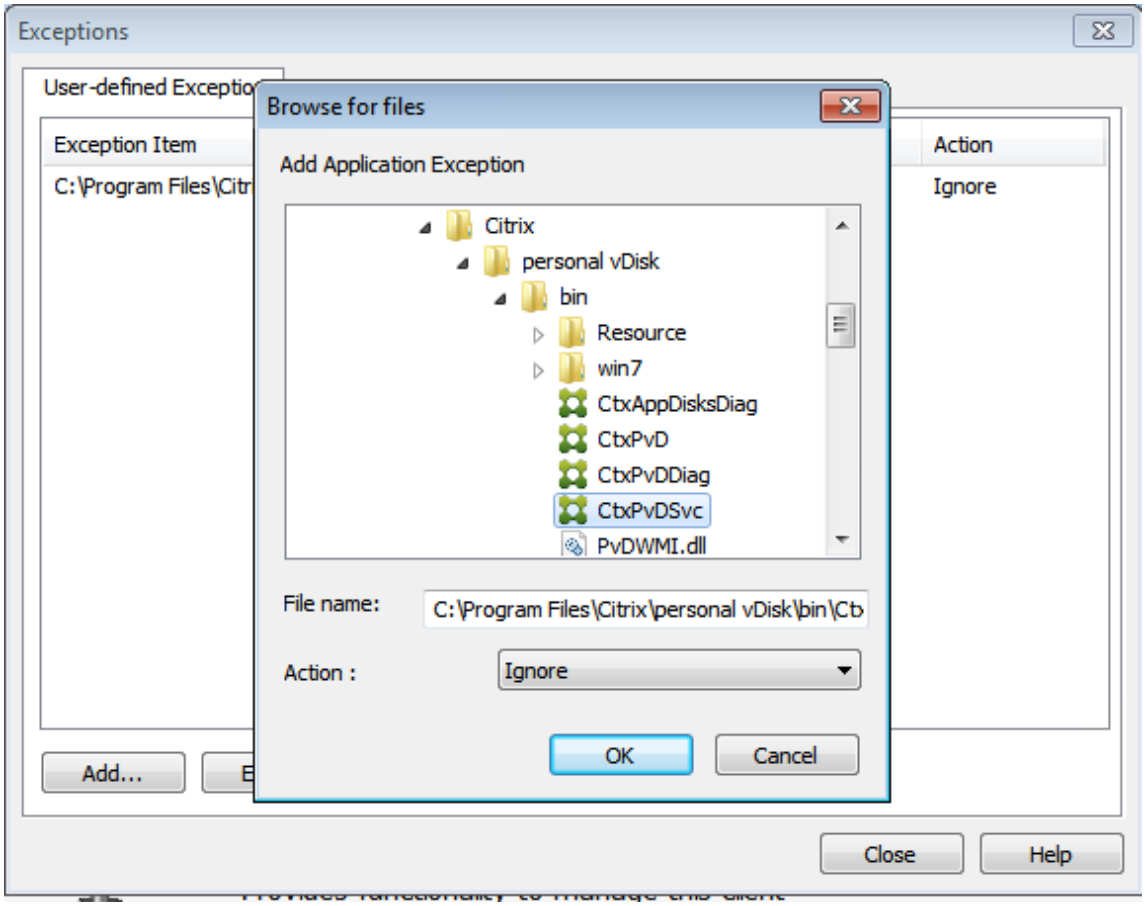


6. En la pantalla de excepciones, introduzca las siguientes rutas de archivo de AppDisk y establezca la acción en **Ignore**:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

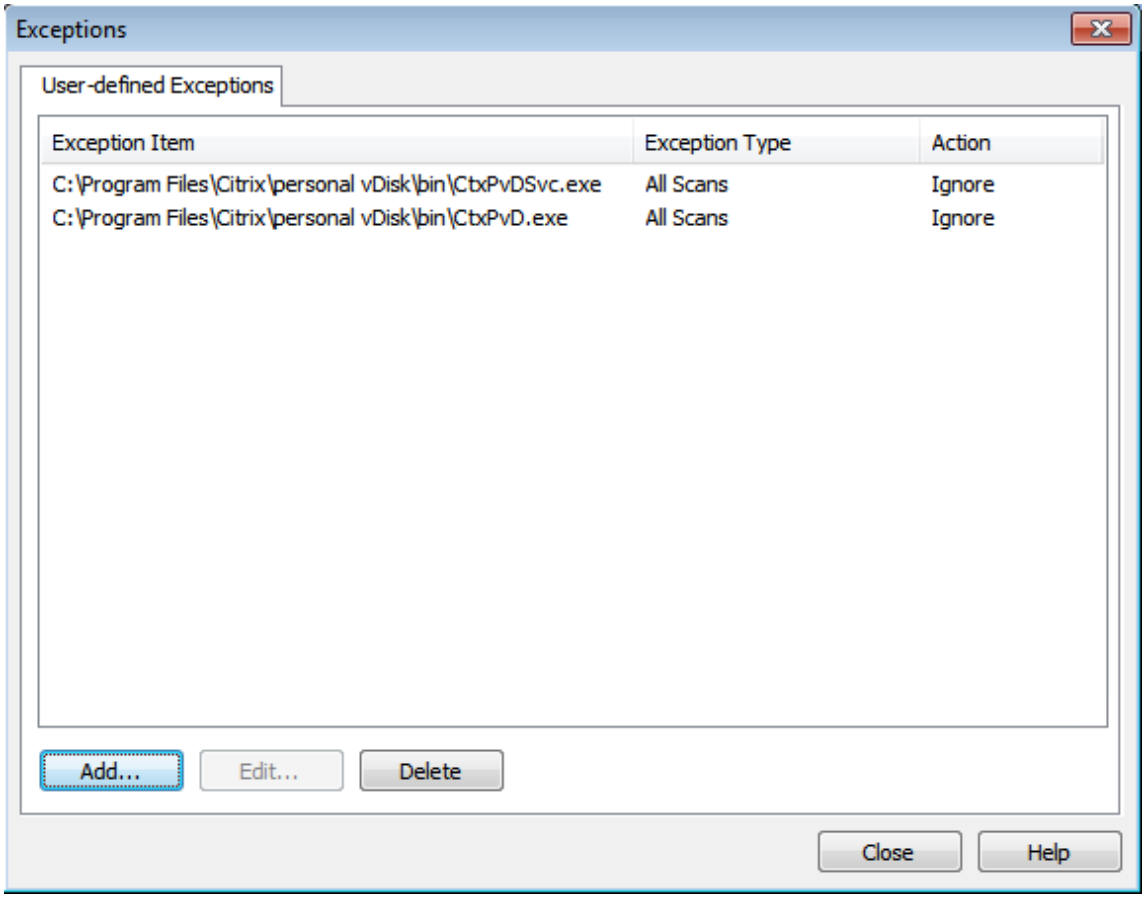
```
C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe
```

```
C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe
```



Las excepciones indicadas se agregan a la lista. Cierre la ventana para aplicar los cambios.

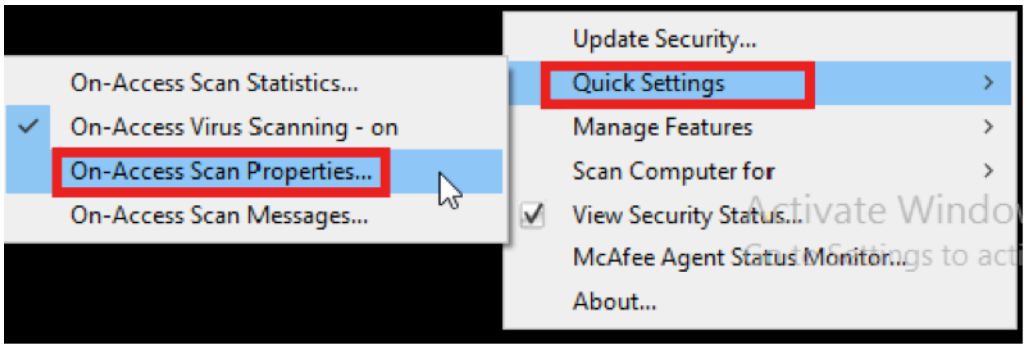
© 1999-2019 Citrix Systems, Inc. All rights reserved.



McAfee

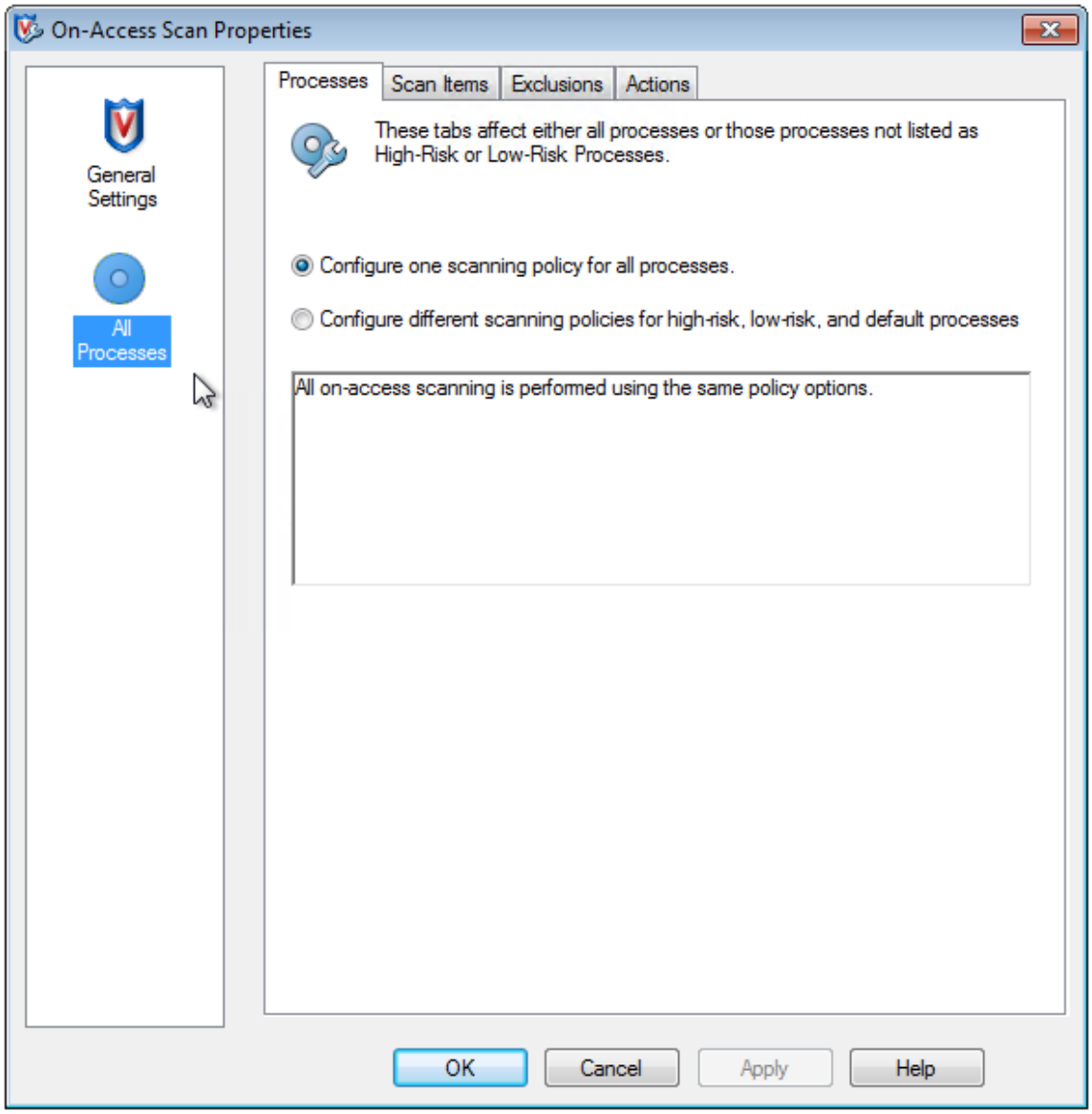
Si la VM base usa McAfee (versión 4.8):

1. Haga clic con el botón secundario en el icono de McAfee y expanda la opción **Quick Settings**.
2. En el menú expandido, seleccione **On-Access Scan Properties**:



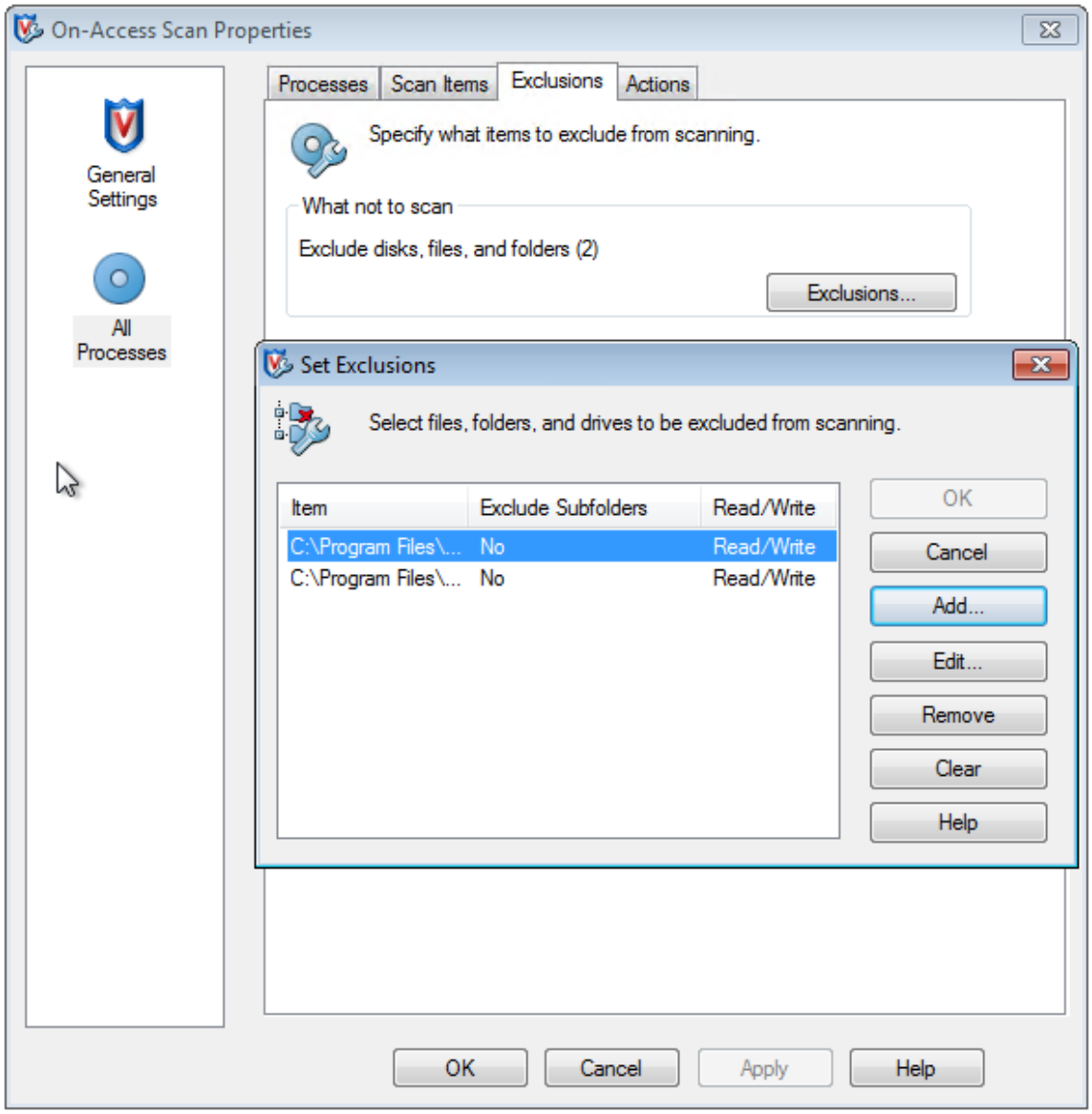
3. En la pantalla **On-Access Scan Properties**, haga clic en **All Processes**:

© 1999-2019 Citrix Systems, Inc. All rights reserved.



4. Seleccione la ficha **Exclusions**.
5. Haga clic en el botón **Exclusions**.
6. En la pantalla **Set exclusions**, haga clic en **Add**:

© 1999-2019 Citrix Systems, Inc. All rights reserved.



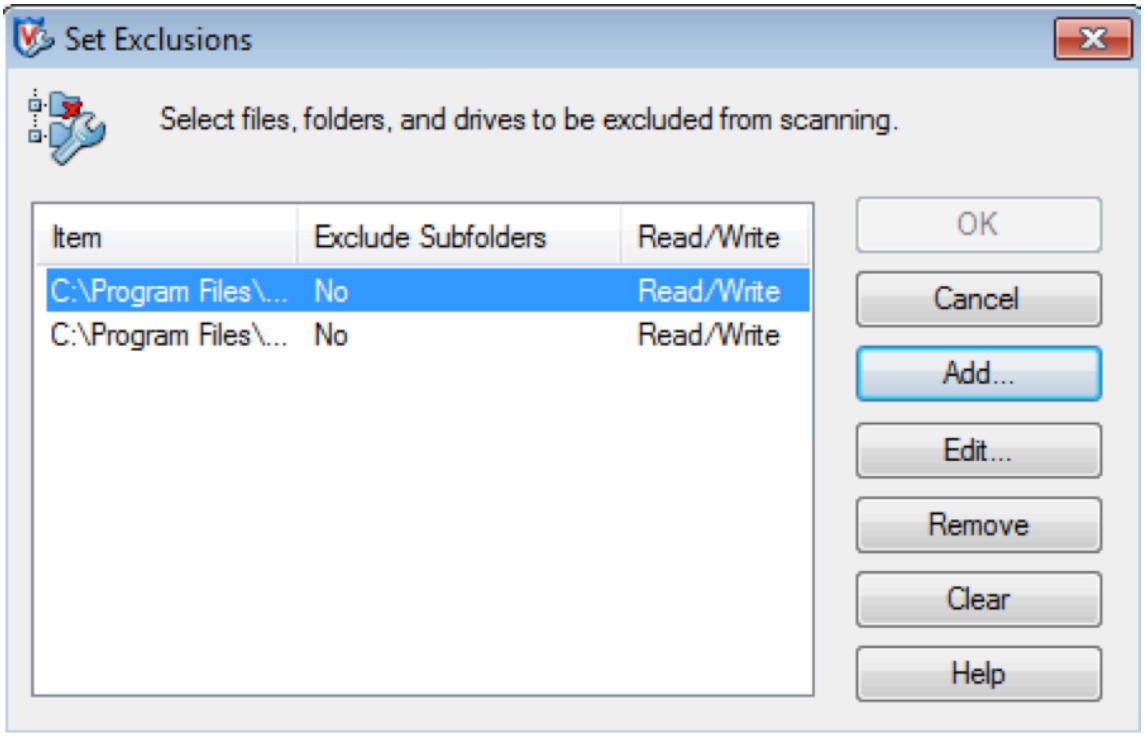
7. En la pantalla **Add Exclusion Item**, seleccione **By name/location (can include wildcards * or ?)**. Haga clic en **Browse** para buscar los archivos ejecutables de exclusión:

   ```
   C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe
   ```

   ```
   C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe
   ```

8. Haga clic en **Aceptar**.
9. Ahora, la pantalla **Set Exclusions** muestra las exclusiones agregadas. Haga clic en **OK** para aplicar los cambios:

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Después de la configuración de estas exclusiones, cree el AppDisk.

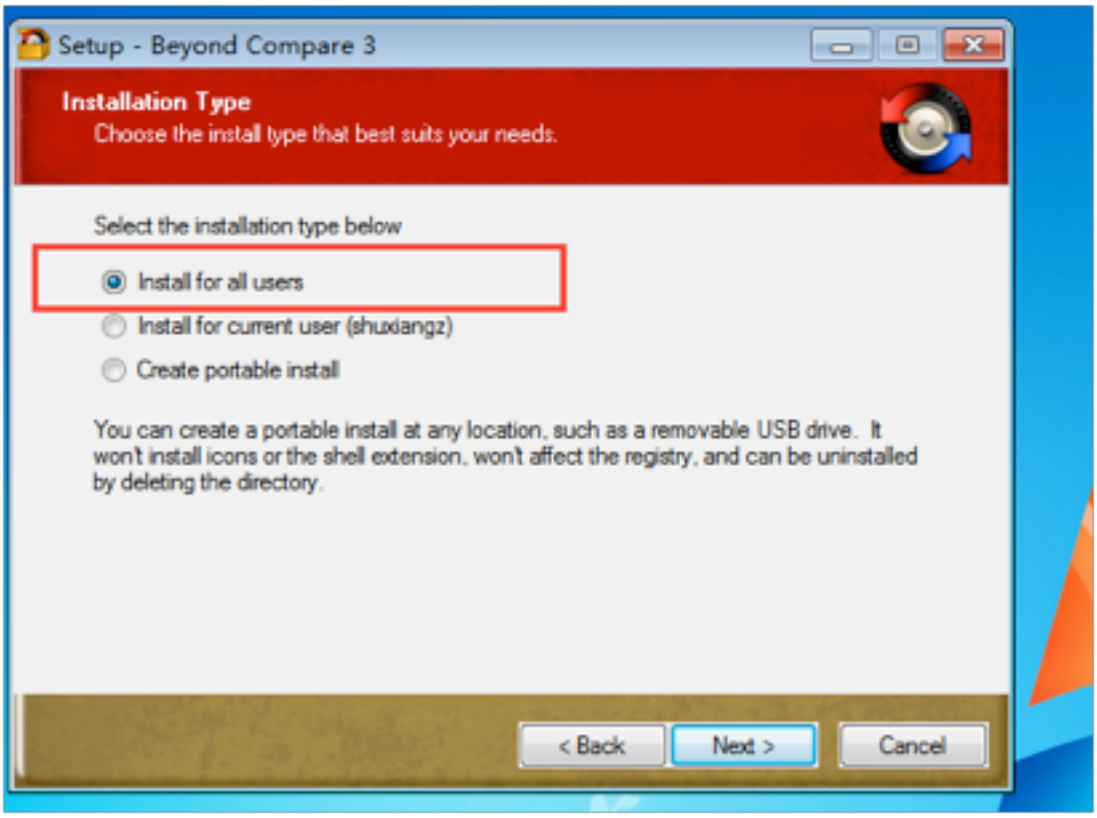
Cómo aparecen las aplicaciones en el menú Inicio

Si se crea un nuevo AppDisk y una aplicación se pone a disposición de todos los usuarios a los que está conectado el disco del escritorio, aparece un acceso directo de la aplicación en el menú Inicio. Si se crea un AppDisk y se instala solo para el usuario actual, y el disco está conectado al escritorio, el acceso directo de la aplicación no aparece en el menú Inicio.

Por ejemplo, cree una nueva aplicación y póngala a disposición de todos los usuarios:

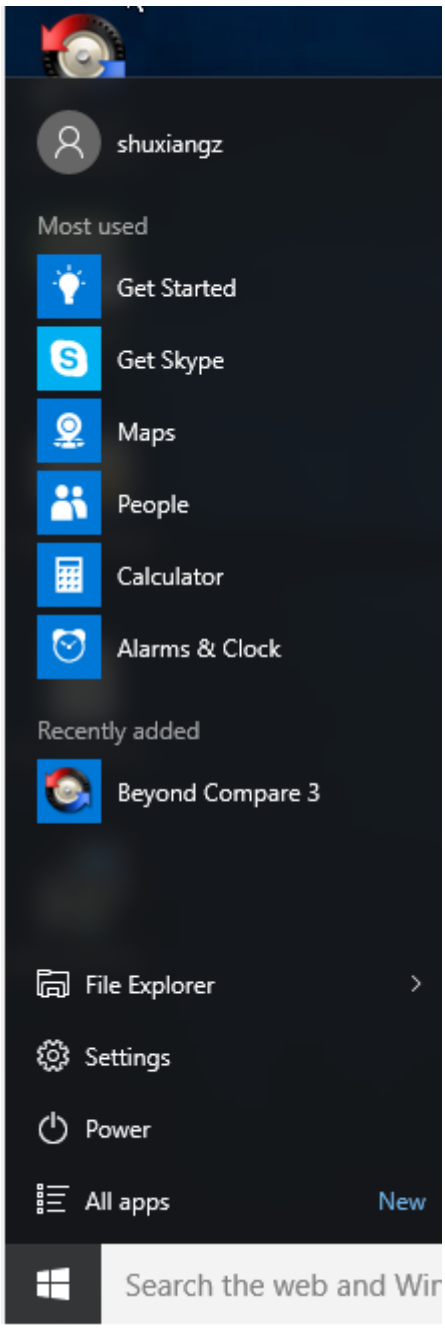
1. Instale una aplicación en el AppDisk (por ejemplo, *Beyond Compare*):

© 1999-2019 Citrix Systems, Inc. All rights reserved.



2. Conecte el disco al escritorio y el acceso directo de la aplicación recién instalada (*Beyond Compare*) aparecerá en el menú Inicio:

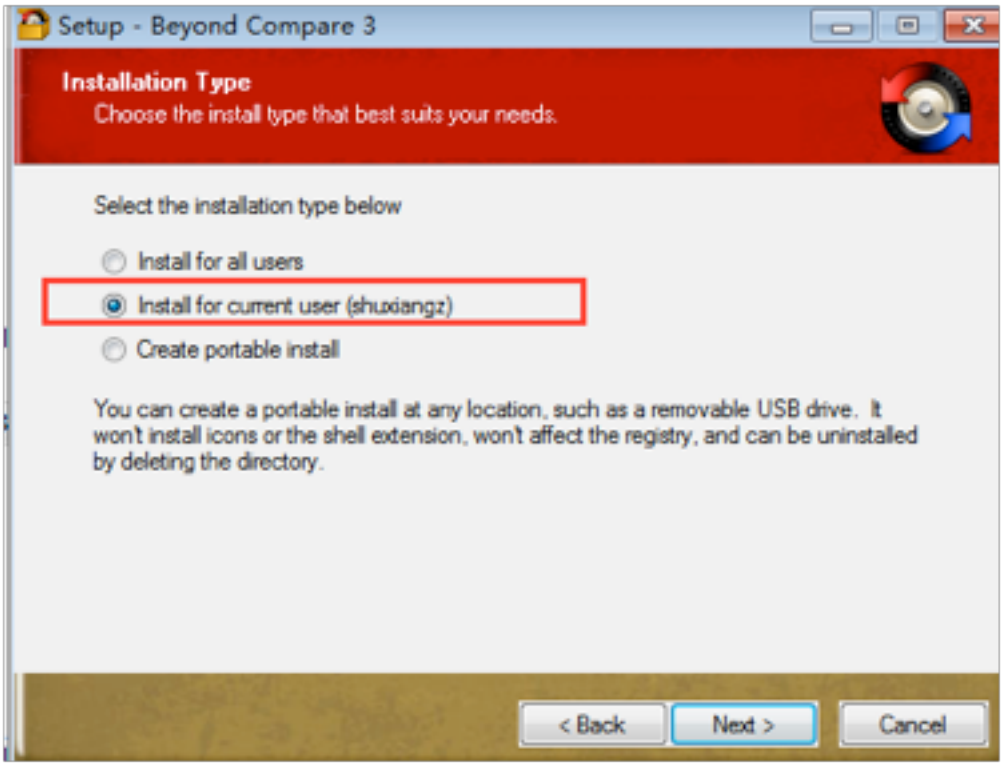
© 1999-2019 Citrix Systems, Inc. All rights reserved.



Para instalar una aplicación solo para el usuario actual:

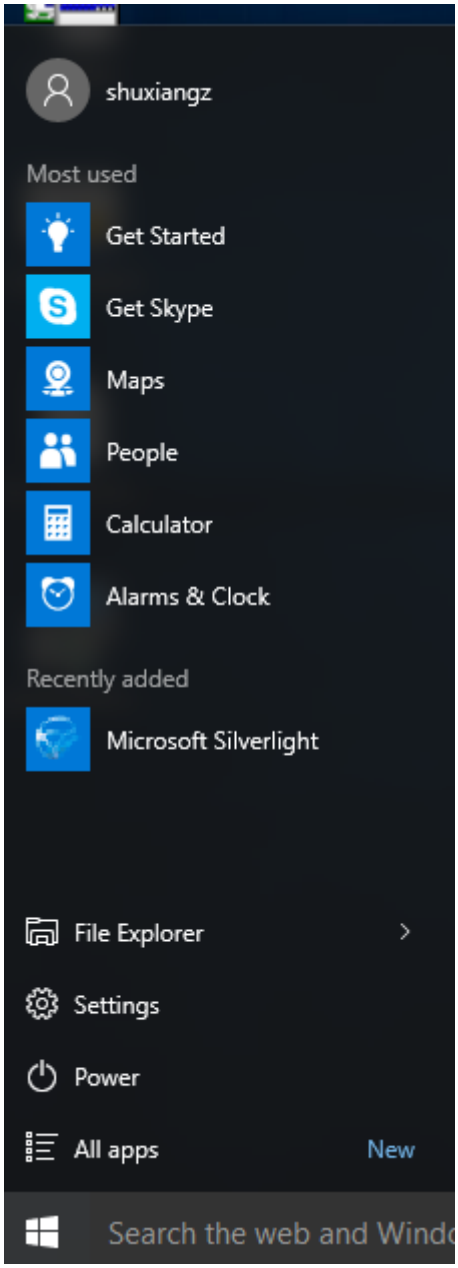
1. Instale una aplicación en el AppDisk y póngala a disposición del usuario actual:

© 1999-2019 Citrix Systems, Inc. All rights reserved.



2. Conecte el disco al escritorio; tenga en cuenta que el acceso directo no aparecerá en el menú Inicio:

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Registros de AppDisk

Los usuarios de AppDisk pueden obtener información de diagnóstico y cargarla en el sitio Web de Citrix Insight Services (CIS).

Cómo funciona

En esta funcionalidad, se utiliza una herramienta de scripts de PowerShell que identifica todos los archivos de registro creados por AppDisk o PVD, recopila los resultados de los comandos de Power-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Shell que contienen información sobre el sistema (y los procesos), lo comprime todo en un archivo único y organizado y, finalmente, ofrece la opción de guardar la carpeta comprimida localmente o cargarla en CIS (Citrix Insight Services).

> **Nota:**
>
> CIS recopila información anónima de diagnóstico que usa para mejorar la funcionalidad de AppDisk o PVD. Debe acceder al sitio Web de Citrix CIS para cargar manualmente el paquete de diagnóstico. Necesita sus credenciales de Citrix para iniciar sesión en este sitio.

Usar scripts de PowerShell para recopilar archivos de registro de AppDisk o PVD

El instalador de AppDisk o PVD agrega dos scripts para la recopilación de datos de diagnóstico:

- `Upload-AppDDiags.ps1`: Lleva a cabo la recopilación de datos de diagnóstico de AppDisk.
- `Upload-PvDDiags.ps1`: Lleva a cabo la recopilación de datos de diagnóstico de PvD.

Estos archivos se agregan a C:\Archivos de programa\Citrix\personal vDisk\bin\scripts. Estos scripts de PowerShell se deben ejecutar como administrador.

Upload-AppDDiags.ps1

Use este script para iniciar la recopilación de datos de diagnóstico de AppDisk y cargar manualmente los datos en el sitio Web de CIS.

```
Upload-AppDDiags [[-OutputFile] <string>] [-help] [<CommonParameters>]
```

`-OutputFile`: Ruta local al archivo ZIP en lugar de cargarlo en CIS. Cuando se omite `-OutputFile`, se realiza la carga. En cambio, cuando se especifica `-OutputFile`, el script crea un archivo ZIP que usted puede cargar manualmente más tarde.

Ejemplos:

- `Upload-AppDDiags`: Carga datos de diagnóstico en el sitio Web de Citrix CIS utilizando las credenciales que haya escrito el usuario interactivo.
- `Upload-AppDDiags -OutputFile C:\MyDiags.zip`: Guarda los datos de diagnóstico de AppDisk en el archivo ZIP especificado. Puede acceder a https://cis.citrix.com/ para cargarlo más tarde.

Upload-PvDDiags.ps1

Use este script para iniciar la recopilación de datos de diagnóstico de PvD y cargar manualmente los datos en el sitio Web de CIS.

```
Upload-PvDDiags [[-OutputFile] <string>] [-help] [<CommonParameters>]
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

`-OutputFile`: Ruta local al archivo ZIP en lugar de cargarlo en CIS. Cuando se omite `-OutputFile`, se realiza la carga. En cambio, cuando se especifica `-OutputFile`, el script crea un archivo ZIP que usted puede cargar manualmente más tarde.

Ejemplos:

- `Upload-PvDDiags`: Carga datos de diagnóstico de PvD en el sitio Web de Citrix CIS utilizando las credenciales que haya escrito el usuario interactivo.
- `Upload-PvDDiags -OutputFile C:\MyDiags.zip`: Guarda los datos de diagnóstico de PvD en el archivo ZIP especificado. Puede acceder a https://cis.citrix.com/ para cargarlo más tarde.

Secure Browser de Virtual Apps

October 3, 2018

Cuando las aplicaciones se llevan a la Web, los usuarios se ven obligados a utilizar varios proveedores y múltiples versiones de exploradores para obtener compatibilidad con aplicaciones Web. Si la aplicación en cuestión está alojada internamente, a menudo las empresas se ven obligadas a instalar y configurar soluciones complejas de VPN para ofrecer acceso a usuarios remotos. Además, las soluciones habituales de VPN requieren de un agente en el lado del cliente que también se debe mantener en varios sistemas operativos.

Con Secure Browser, los usuarios pueden disfrutar de una experiencia fluida en que una aplicación Web alojada aparece simplemente dentro del explorador local favorito de cada usuario. Por ejemplo, un usuario tiene como preferido el explorador Mozilla Firefox, pero la aplicación solo es compatible con Microsoft Internet Explorer. Secure Browser muestra la aplicación compatible con Internet Explorer como una pestaña en el explorador Firefox.

Implementar Virtual Apps Secure Browser Edition

1. Descargue la imagen ISO de Citrix Virtual Apps Secure Browser Edition desde el sitio de descargas de Citrix.
2. Siga las instrucciones para instalar los diferentes componentes de Citrix Virtual Apps.
3. Configure la edición y el modo de licencia de Secure Browser después de la instalación. Para ello, realice estos pasos adicionales:
    a) En el Delivery Controller, inicie una sesión de PowerShell. Para ello, puede hacer clic en el icono azul de la barra de tareas o ir a Inicio > Todos los programas > Accesorios > Windows PowerShell > Windows PowerShell.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

En sistemas de 64 bits, se iniciará la versión de 64 bits. Se admite tanto la versión de 32 bits como la de 64 bits.

b) Escriba `asnp Citrix*` y presione **Entrar** para cargar los módulos de PowerShell específicos de Citrix. (`asnp` representa `Add-PSSnapin`.)

c) Verifique la configuración actual del sitio y el modo de licencia: ejecute `Get-ConfigSite`.

d) Establezca el modo de licencia en Virtual Apps Secure Browser Edition: ejecute `Set-ConfigSite -ProductCode XDT -ProductEdition BAS`.

e) Confirme que el modo de licencia y Virtual Apps Secure Browser Edition están configurados correctamente: ejecute `Get-BrokerSite`.

Después de completar la instalación, puede optimizar más el entorno para la entrega de aplicaciones Web siguiendo los pasos de configuración especificados en la Guía de implementación de XenApp Secure Browser.

Publicar contenido

October 3, 2018

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 característica se conoce como Contenido publicado. La capacidad para publicar contenido flexibiliza la entrega de contenido a los usuarios. Le permite aprovechar las aplicaciones existentes de administración y control del acceso. Además, puede especificar qué se debe utilizar para abrir el contenido: aplicaciones locales o publicadas.

El contenido publicado aparece como las demás aplicaciones en StoreFront y la aplicación Citrix Workspace. Los usuarios acceden a él de la misma forma que acceden a las aplicaciones. En el cliente, el recurso se abre como es habitual.

- Si existe una aplicación instalada localmente que sea adecuada, ésta se inicia para abrir el recurso.
- Si se ha definido una asociación de tipos de archivo, se inicia una aplicación publicada para abrir el recurso.

Puede publicar contenido con el SDK de PowerShell. (No se puede utilizar Studio para publicar contenido. No obstante, puede usar Studio para editar 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 de servicios de Citrix Virtual Apps and Desktops, descargue e instale Citrix Virtual Apps and Desktops Remote PowerShell SDK.
- Para implementaciones locales de Citrix Virtual Apps and Desktops, use el SDK de PowerShell que se instala con el Delivery Controller. Agregar una aplicación de contenido publicado requiere como mínimo la versión 7.11 de Delivery Controller.

Se usan ejemplos en los siguientes procedimientos. En los ejemplos:

- Se ha creado un catálogo de máquinas.
- Se ha creado un grupo de entrega llamado PublishedContentApps. El grupo utiliza una máquina de SO de servidor proveniente del catálogo. Se ha agregado la aplicación WordPad al grupo.
- Se han hecho asignaciones para el nombre del grupo de entrega, la ubicación CommandLineExecutable y el nombre de la aplicación.

Introducción

En la máquina que contiene el SDK de PowerShell, abra PowerShell.

El cmdlet siguiente agrega el complemento adecuado del SDK de PowerShell y asigna el registro devuelto del grupo de entrega.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

```
Add-PsSnapin Citrix\* $dg = Get-BrokerDesktopGroup -Name PublishedContentApps
```

Si utiliza el servicio Citrix Virtual Apps and Desktops, debe autenticarse con sus credenciales de Citrix Cloud. Si hay más de un cliente, elija uno.

Publicar una URL

Después de asignar el nombre y la ubicación de la aplicación, el cmdlet siguiente publica la página de inicio de Citrix como una aplicación.

```
$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"
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

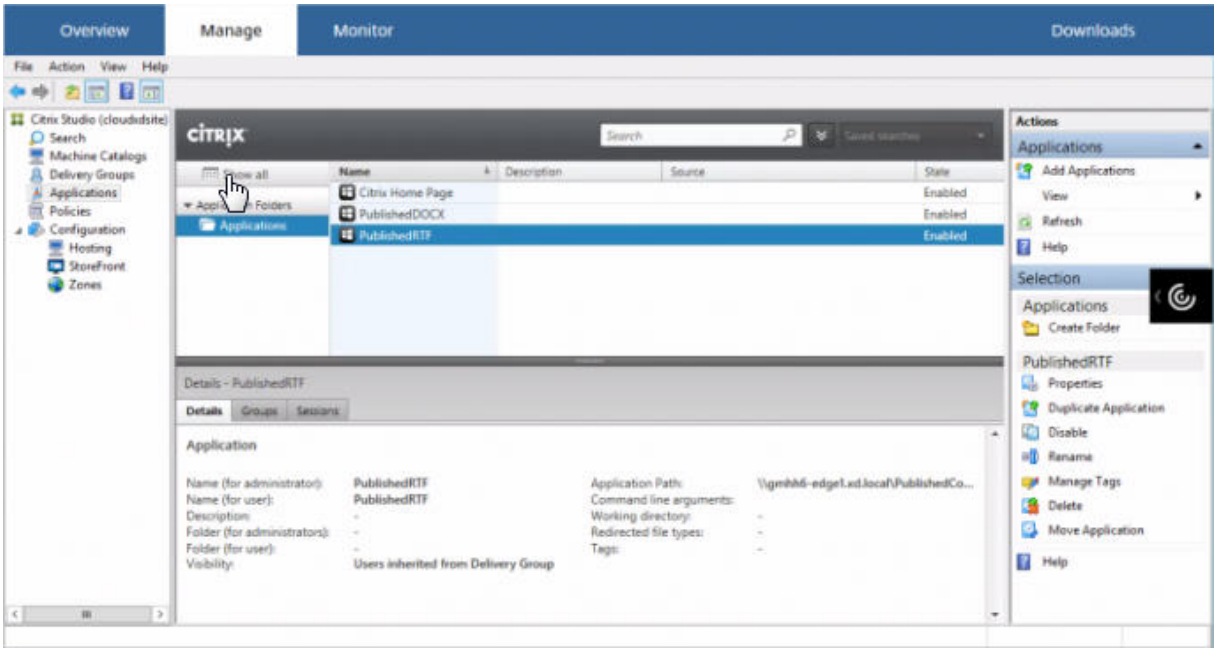
```
10
11 New-BrokerApplication  -ApplicationType PublishedContent
12  -CommandLineExecutable $docxUNC -Name $docxAppName
13 -DesktopGroup $dg.Uid
```

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.

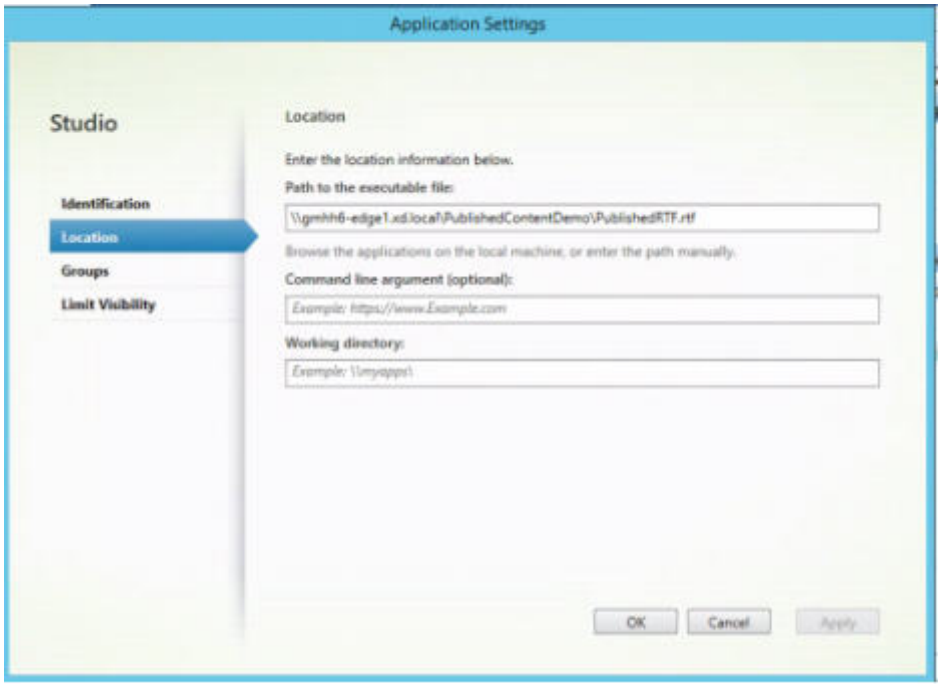
Ver y modificar aplicaciones PublishedContent

Puede administrar el contenido publicado con los mismos métodos que se utilizan para otros tipos de aplicación. Los elementos publicados aparecerán en la lista Aplicaciones en Studio y pueden modificarse en Studio.



Las propiedades de aplicación (por ejemplo, la visibilidad a los usuarios, la asociación de grupo y el acceso directo) se aplican al contenido publicado. Sin embargo, no puede cambiar el argumento de la línea de comandos ni las propiedades del directorio de trabajo que se ven en la página **Ubicación**. Para cambiar el recurso, modifique el campo **Ruta del archivo ejecutable** en dicha página.

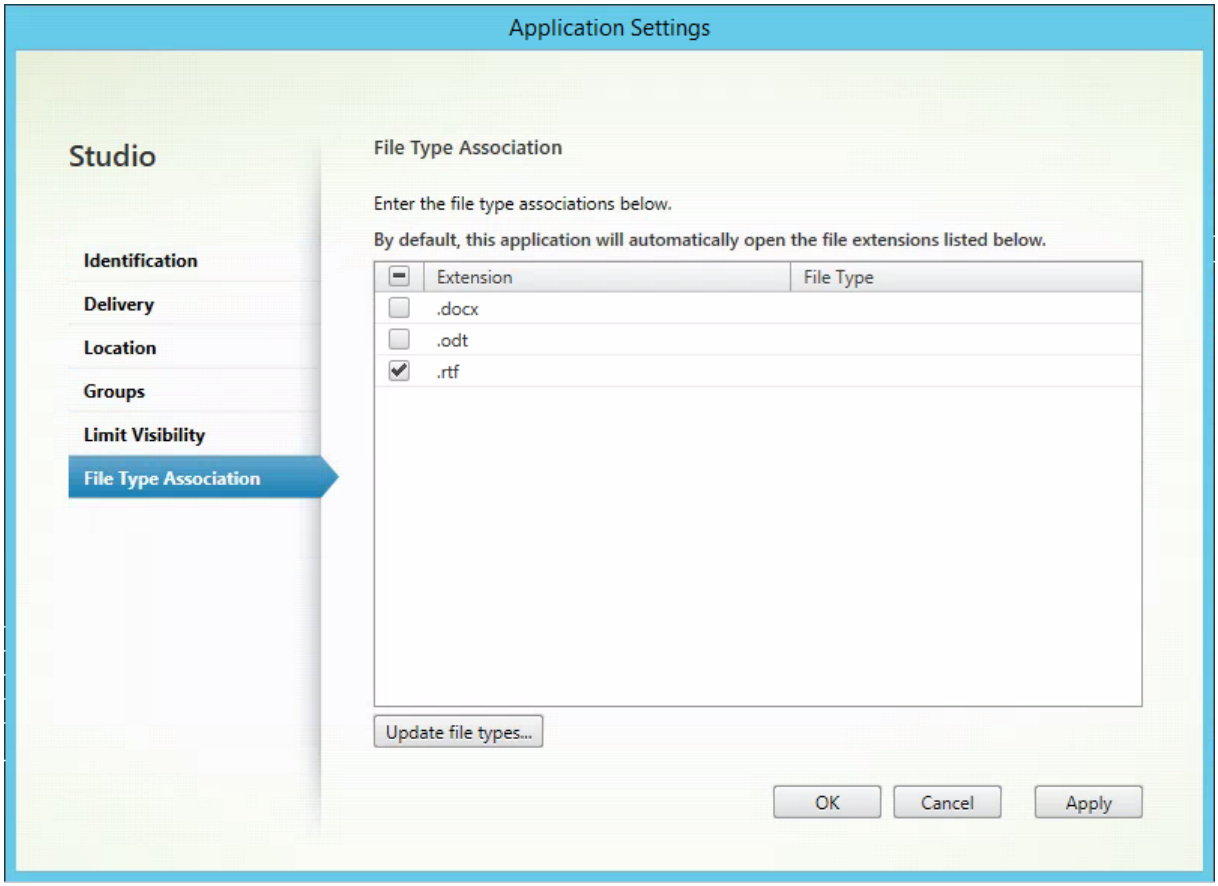
© 1999-2019 Citrix Systems, Inc. All rights reserved.



Si quiere usar una aplicación publicada para abrir una aplicación PublishedContent (en lugar de una aplicación local), modifique la propiedad **Asociación de tipos de archivo** de la aplicación publicada. En este ejemplo, la aplicación publicada de WordPad se modificó para crear una asociación de tipos de archivo para archivos RTF.

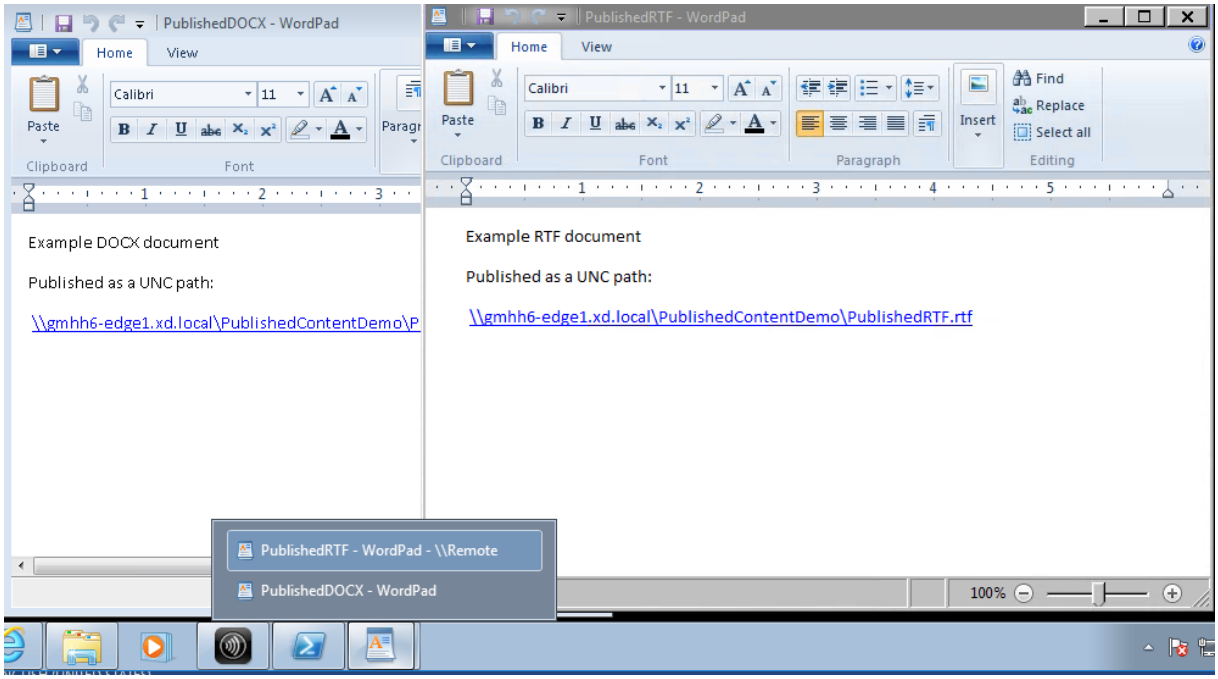
Active el modo de mantenimiento para el grupo de entrega antes de modificar la asociación de tipos de archivo. Recuerde que debe desactivar el modo de mantenimiento cuando haya terminado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



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 WordPad local. No obstante, ahora PublishedRTF se abre en WordPad publicado debido a la nueva asociación de tipos de archivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Para obtener más información

- Crear catálogos de máquinas
- Crear grupos de entrega
- Cambiar las propiedades de la aplicación

VDI de servidor

December 4, 2018

Use la función VDI (infraestructura de escritorios virtuales) de servidor para entregar escritorios desde un sistema operativo de servidor a un solo usuario.

- Los administradores de empresa pueden entregar sistemas operativos de servidor como escritorios VDI, lo cual puede ser útil para usuarios como ingenieros y diseñadores.
- Los proveedores de servicios pueden ofrecer escritorios desde la nube; esos escritorios cumplen con el Contrato de licencia de proveedor de servicios (SPLA) de Microsoft.

Puede usar la configuración de directiva “Enhanced Desktop Experience” de Citrix para que el sistema operativo del servidor parezca un sistema operativo de escritorio.

Las siguientes funciones no se pueden usar con VDI de servidor:

- Discos Personal vDisk
- Aplicaciones alojadas

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Acceso a aplicaciones locales
- Conexiones de escritorio directas (sin broker)
- Acceso con Remote PC

Actualmente se admite VDI de servidor en máquinas Windows Server 2019 y Windows Server 2016.

Para que los servidores VDI funcionen con los dispositivos TWAIN (por ejemplo, escáneres), debe instalarse la característica Experiencia de escritorio de servidor Windows.

Instalar y configurar VDI de servidor

1. Prepare el servidor Windows para la instalación.
    - Use el Administrador del servidor de Windows para asegurarse de que los servicios de rol de los Servicios de Escritorio remoto no están instalados. Si se instalaron anteriormente, elimínelos. La instalación de VDA falla si se instalan esos servicios de rol.
    - Compruebe que la propiedad “Restringir cada usuario a una sola sesión” está habilitada. En el servidor Windows, modifique el Registro y establezca el parámetro de Terminal Server:
        - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer
        - DWORD fSingleSessionPerUser = 1
2. Use la interfaz de la línea de comandos que tiene el instalador de Citrix Virtual Apps and Desktops para instalar un VDA en un servidor respaldado o en la imagen maestra de un servidor respaldado. Debe especificar las opciones “quiet” y “servervdi”. (De forma predeterminada, la interfaz gráfica del instalador impide que aparezca la opción del VDA de SO de escritorio Windows en un sistema operativo de servidor. Con la línea de comandos, se anula 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 servicios de Citrix Virtual Apps and Desktops:
        - `VDAWorkstationSetup.exe /quiet /servervdi`

    Para otras opciones:

    - Puede especificar el Delivery Controller o Cloud Connector con la opción “controllers”.
    - Use la opción `enable_hdx_ports` para abrir puertos en el firewall, a menos que el firewall deba configurarse manualmente.
    - Agregue la opción `mastermcsimage` (o `masterimage`) si está instalando el VDA en una imagen y va a usar MCS para crear máquinas virtuales de servidor a partir de esa imagen.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- No incluya opciones para funciones que no se respaldan con VDI de servidor, por ejemplo, “baseimage”.
- Para obtener más información sobre todas las opciones, consulte Instalar usando 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 escritorio**.
   - En la página **Resumen**, especifique un nombre del catálogo de máquinas y una descripción para los administradores que claramente lo identifique como VDI de servidor. Será lo único que indique en Studio que el catálogo admite VDI de servidor.

   Al usar “Buscar” en Studio, el catálogo de VDI de servidor aparece en la ficha **Máquinas de SO de escritorio**, aunque el VDA se instalara en un servidor.
4. Cree un grupo de entrega y seleccione el catálogo de VDI de servidor que ha creado.

Si no especificó Delivery Controllers ni Cloud Connector mientras instalaba el VDA, recuerde especificarlos posteriormente. Para obtener información detallada, consulte Registro de VDA.

Personal vDisk

October 3, 2018

La función Personal vDisk conserva la administración de imágenes únicas para escritorios agrupados y distribuidos por streaming, al tiempo que permite a los usuarios instalar aplicaciones y cambiar la configuración de sus escritorios. A diferencia de las implementaciones de VDI (Virtual Desktop Infrastructure) tradicionales con escritorios agrupados, donde los usuarios pierden sus personalizaciones y sus aplicaciones personales cuando el administrador modifica la imagen maestra, las implementaciones con discos Personal vDisk conservan dichos cambios. Esto significa que los administradores pueden administrar de manera centralizada y sencilla las imágenes maestras, al mismo tiempo que proporcionan a los usuarios una experiencia de escritorio personalizada.

Los discos Personal vDisk permiten esta separación al redirigir todos los cambios que efectúa el usuario en la máquina virtual a un disco aparte (el disco Personal vDisk) asociado a la máquina virtual del usuario. El contenido del disco Personal vDisk se fusiona en tiempo de ejecución con el contenido de la imagen publicada para proporcionar una experiencia unificada. De este modo, los usuarios pueden seguir accediendo a las aplicaciones aprovisionadas por el administrador en la imagen maestra.

Los discos virtuales personales constan de dos partes, que utilizan letras de unidad distintas y tienen el mismo tamaño de manera predeterminada:

- Perfil de usuario: contiene los datos, los documentos y el perfil del usuario. De manera predeterminada, esta parte usa la unidad P: pero se puede seleccionar otra letra de unidad cuando

© 1999-2019 Citrix Systems, Inc. All rights reserved.

se crea un catálogo de máquinas con discos Personal vDisk. La unidad usada también depende del parámetro EnableUserProfileRedirection.

- Disco duro virtual (.vhd): contiene todos los demás elementos, como, por ejemplo, las aplicaciones instaladas en C:\Archivos de programa. Esta parte no se muestra en el Explorador de Windows y, a partir de la versión 5.6.7, ya no necesita una letra de unidad.

Los discos Personal vDisk respaldan el aprovisionamiento de aplicaciones específicas de cada departamento, así como el de aplicaciones descargadas e instaladas por los propios usuarios, incluidas las que necesitan controladores (excepto los controladores de fase 1), bases de datos y software de administración de máquinas. Si un cambio efectuado por un usuario entra en conflicto con otro cambio realizado por un administrador, el disco Personal vDisk ofrece un método sencillo y automático para resolver dichos cambios.

Además, también pueden aprovisionarse en el entorno del usuario aplicaciones administradas localmente (como pueden ser las aprovisionadas y administradas por departamentos de TI locales). El usuario no nota diferencia alguna en cuanto a la usabilidad; los discos virtuales personales garantizan que todos los cambios hechos y todas las aplicaciones instaladas se guardan en el disco virtual. Cuando una aplicación de un disco virtual personal coincide exactamente con una aplicación existente en la imagen maestra, la copia del disco virtual personal se descarta para ahorrar espacio, sin que el usuario pierda acceso a ella.

Físicamente, los discos virtuales personales (Personal vDisk) se almacenan en el hipervisor, pero no es necesario que residan en la misma ubicación que los otros discos conectados al escritorio virtual. Esto puede reducir los costes de almacenamiento de Personal vDisk.

Durante la creación de sitios, cuando crea una conexión, debe definir las ubicaciones de almacenamiento para los discos utilizados por las máquinas virtuales. Puede separar los discos Personal vDisk de los discos que utilice el sistema operativo. Cada máquina virtual debe tener acceso a una ubicación de almacenamiento para ambos discos. Si usa almacenamiento local para ambos, deben estar accesibles desde el mismo hipervisor. Para garantizar que se cumple este requisito, Studio ofrece únicamente ubicaciones de almacenamiento compatibles. Más adelante, también puede agregar discos Personal vDisk y almacenarlos en hosts existentes (pero no en catálogos de máquinas) desde Configuración > Alojamiento en Studio.

Haga copias de seguridad de los discos Personal vDisk con regularidad con el método que prefiera. Los discos virtuales son volúmenes estándar en el nivel de almacenamiento de un hipervisor, de modo que puede realizar copias de seguridad de ellos como de cualquier otro volumen.

Novedades en Personal vDisk 7.6.1

En esta versión se incluyen las siguientes mejoras:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Esta versión de Personal vDisk contiene mejoras de rendimiento que reducen el tiempo que lleva aplicar una actualización de imagen a un catálogo de Personal vDisk.

Se han solucionado los problemas siguientes en esta versión:

- Al intentar una actualización en contexto de una máquina virtual base desde Microsoft Office 2010 a Microsoft Office 2013, el usuario veía una ventana de reconfiguración, seguida de un mensaje de error similar al siguiente: "Error 25004. La clave de producto que escribió no se puede usar en este equipo". En el pasado, se recomendaba desinstalar Office 2010 de la máquina virtual base antes de instalar Office 2013. Ahora ya no es necesario desinstalar Office 2010 al llevar a cabo una actualización en contexto en la máquina virtual base (#391225).
- Durante el proceso de actualización de imagen, si existía una versión más reciente de Microsoft .NET en el disco Personal vDisk del usuario, esta versión se sobrescribía con la versión anterior existente en la imagen base. Esto provocaba problemas para los usuarios que ejecutaban ciertas aplicaciones instaladas en su disco Personal vDisk que requerían la versión posterior, tales como Visual Studio (#439009).
- Un disco creado con una imagen de Provisioning Services que tiene Personal vDisk instalado y habilitado no se puede usar para crear un catálogo de máquinas sin Personal vDisk. Esta limitación se ha eliminado (#485189).

Acerca de Personal vDisk 7.6

Novedades en la versión 7.6:

- Gestión y notificación de errores de Personal vDisk mejoradas. En Studio, al mostrar máquinas con Personal vDisk (PvD) habilitado de un catálogo de máquinas, la ficha "PvD" muestra el estado de la supervisión y el progreso y la hora de finalización estimados de las actualizaciones de imagen. También se ha mejorado la información relacionada con los estados.
- Se ofrece una herramienta de supervisión de actualizaciones de imágenes de Personal vDisk, Personal vDisk Image Update Monitoring Tool, en los medios de soporte ISO (ISO\Support\Tools\Scripts\PvdTool). Las capacidades de supervisión reciben respaldo para versiones anteriores, pero las capacidades de creación de informes no serán tan sólidas comparadas con las de la versión actual.
- El modo de prueba de Provisioning Services permite iniciar máquinas con una imagen actualizada de un catálogo de pruebas. Después de comprobar la estabilidad, puede transferir la versión de prueba de Personal vDisk a producción.
- Una nueva función permite calcular el diferencial entre dos inventarios durante un proceso de inventariado, en lugar de calcularlo para cada escritorio de PvD. Se ofrecen nuevos comandos para exportar e importar un inventario anterior para los catálogos de MCS. (Los discos maestros de vDisk de Provisioning Services ya disponen del inventario anterior.)

Problemas conocidos de 7.1.3 resueltos en la versión 7.6:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Si se interrumpe una actualización de instalación de Personal vDisk, se puede dañar una instalación actual de Personal vDisk. [#424878]
- Un escritorio virtual puede dejar de responder si Personal vDisk se ejecuta durante un periodo de tiempo largo y se produce una pérdida de memoria no paginada. [#473170]

Nuevos problemas conocidos en la versión 7.6:

- La presencia de productos antivirus puede afectar el tiempo necesario para ejecutar el inventario o realizar una actualización. El rendimiento se puede mejorar si agrega CtxPvD.exe y CtxPvDSvc.exe a la lista de exclusión PROCESS del producto antivirus. Estos archivos se encuentran en C:\Archivos de programa\Citrix\Personal vDisk\bin. [#326735]
- Los vínculos físicos que hay entre los archivos heredados de la imagen maestra no se conservan en los catálogos de Personal vDisk. [#368678]
- Después de actualizar de Office 2010 a 2013 en la imagen maestra del disco Personal vDisk, es posible que Office no se inicie en máquinas virtuales porque la clave de producto de la licencia de KMS de Office se quitara durante el proceso de actualización. Como solución temporal, desinstale Office 2010 y vuelva a instalar Office 2013 en la imagen maestra. [#391225]
- Los catálogos de Personal vDisk no admiten Controllers (PVSCSI) SCSI Paravirtual de VMware. Para evitar este problema, use el controlador predeterminado. [#394039]
- Si se trata de escritorios virtuales creados con la versión 5.6.0 de Personal vDisk y se actualizan a 7, es posible que los usuarios que iniciaron sesión en la máquina virtual (VM) maestra no encuentren todos sus archivos en su VM agrupada. Este problema se produce porque se crea un nuevo perfil de usuario cuando los usuarios inician sesión en sus VM agrupadas. No existe ninguna solución para este problema. [#392459]
- La función Copia de seguridad y restauración no se puede usar en los discos Personal vDisk que ejecutan Windows 7 cuando la función Protección del sistema de Windows está habilitada. Si la protección del sistema está inhabilitada, se hacen copias de seguridad del perfil de usuario, pero no del archivo userdata.v2.vhd. Citrix recomienda inhabilitar la protección del sistema y utilizar la función Copia de seguridad y restauración para hacer copias de seguridad del perfil de usuario. [#360582]
- Cuando se crea un archivo VHD en la VM base mediante la herramienta de administración de disco, es posible que no pueda montar el disco VHD. Como solución temporal, copie el archivo VHD al volumen de PvD. [#355576]
- Los accesos directos de Office 2010 permanecen en los escritorios virtuales después de eliminar este software. Como solución temporal, elimine los accesos directos. [#402889]
- Cuando se usa Microsoft Hyper-V, no se puede crear un catálogo de máquinas con discos Personal vDisk cuando las máquinas están almacenadas localmente y los discos virtuales están almacenados en volúmenes compartidos en clúster (CSV); la creación de catálogos falla y genera un error. Como solución temporal, use un almacenamiento alternativo para los discos vDisk. [#423969]
- Al iniciar sesión por primera vez en un escritorio virtual creado a partir de un catálogo de Pro-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

visioning Services, el escritorio solicita un reinicio si el disco Personal vDisk ha sido restablecido (mediante el comando ctxpvd.exe -s reset). Como solución temporal, reinicie el escritorio cuando se le solicite. Solo hay que hacer esto una vez, no es necesario hacerlo cuando se vuelve a iniciar la sesión. [#340186]

- Si se instala .NET 4.5 en un disco Personal vDisk y una actualización de imagen posterior instala o modifica .NET 4.0, las aplicaciones que dependen de .NET 4.5 fallarán. Como solución alternativa, distribuya .NET 4.5 a partir de la imagen base como una actualización de imagen.
- Consulte también la documentación de problemas conocidos referentes a la versión 7.6 de XenApp y XenDesktop.

Acerca de Personal vDisk 7.1.3

Problemas conocidos de 7.1 resueltos en la versión 7.1.3:

- Las actualizaciones directas desde Personal vDisk 5.6.0 a Personal vDisk 7.x pueden hacer que falle el disco Personal vDisk. [#432992]
- Es posible que los usuarios solo puedan conectarse de forma intermitente a escritorios virtuales que tienen discos Personal vDisk.[#437203]
- Si una operación de actualización de imagen de Personal vDisk se interrumpe mientras Personal vDisk 5.6.5 o una versión posterior se actualiza a Personal vDisk 7.0 o una versión posterior, las operaciones de actualización posteriores pueden fallar. [#436145]

Acerca de Personal vDisk 7.1.1

Problemas conocidos de 7.1 resueltos en la versión 7.1.1:

- Cuando se actualiza a Symantec Endpoint Protection 12.1.3 a través de una actualización de imagen, symhelp.exe notifica definiciones de antivirus dañadas. [#423429]
- Personal vDisk puede causar que los escritorios agrupados se reinicien si falla Service Control Manager (services.exe). [#0365351]

Nuevos problemas conocidos en la versión 7.1.1: ninguno

Acerca de Personal vDisk 7.1

Novedades en la versión 7.1:

- Ahora se puede usar Personal vDisk con escritorios que ejecutan Windows 8.1 y se ha mejorado el registro de eventos.
- Ya no se admite Copy-on-Write (CoW). Cuando se actualiza desde la versión 7.0 a la versión 7.1 de Personal vDisk, todos los cambios hechos en los datos administrados por CoW se pierden.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Se trataba de una funcionalidad que se probó en XenDesktop 7 y estaba inhabilitada de manera predeterminada, de modo que, si no la habilitó, este problema no le afectará.

Problemas conocidos de 7.0.1 resueltos en la versión 7.1:

- Si el valor de la clave del registro de Personal vDisk EnableProfileRedirection está establecido en 1 o en ON y, después, al actualizar la imagen, este valor se cambia a 0 o a OFF, es posible que todo el espacio de Personal vDisk se asigne a aplicaciones instaladas por el usuario, sin dejar espacio para los perfiles de usuario, que permanecen en el disco vDisk. Si esta redirección de perfiles está inhabilitada en un catálogo y se la habilita durante una actualización de imagen, es posible que los usuarios no puedan iniciar sesiones en su escritorio virtual. [#381921]
- El servicio Desktop Service no registra el error correcto en el visor de sucesos cuando falla la actualización de inventario de Personal vDisk. [#383331]
- Cuando se actualiza a Personal vDisk 7.x, las reglas modificadas no se conservan. Este problema se ha resuelto para las actualizaciones desde la versión 7.0 a la versión 7.1. Cuando se actualiza desde la versión 5.6.5 a la versión 7.1, primero debe guardar el archivo de reglas y luego aplicarlas de nuevo después de realizar la actualización. [#388664]
- Los discos Personal vDisk que ejecutan Windows 8 no pueden instalar aplicaciones desde la Tienda Windows. Aparece un error con el siguiente mensaje: “Su compra no se pudo completar”. Este problema no se soluciona habilitando el servicio Windows Update, pero ya se ha resuelto. No obstante, las aplicaciones instaladas por el usuario deben reinstalarse después de reiniciarse el sistema. [#361513]
- Faltan algunos vínculos simbólicos en escritorios agrupados de Windows 7 con discos Personal vDisk. Como resultado de ello, las aplicaciones que guardan iconos en C:\Usuarios\Todos los usuarios no muestran estos iconos en el menú Inicio. [#418710]
- Un disco Personal vDisk no se inicia si se produce un desbordamiento del diario de USN (números de secuencia de actualización) debido a una gran cantidad de cambios hechos en el sistema después de una actualización de inventario. [#369846]
- Un disco Personal vDisk no se inicia, con el código de estado 0x20 y el código de error 0x20000028. [#393627]
- Symantec Endpoint Protection 12.1.3 muestra el mensaje “Proactive Threat Protection is malfunctioning” y el estado LUA (Live Update Status) de este componente no está disponible. [#390204]

Nuevos problemas conocidos en la versión 7.1: Consulte la documentación “Problemas conocidos” para XenDesktop 7.1.

Acerca de Personal vDisk 7.0.1

Novedades en la versión 7.0.1: Ahora, Personal vDisk es más resistente a los cambios del entorno. Los escritorios virtuales con discos Personal vDisk ahora se registran con Delivery Controller incluso

© 1999-2019 Citrix Systems, Inc. All rights reserved.

aunque fallen las actualizaciones de la imagen, y los apagados no seguros del sistema ya no dejan los discos virtuales en un estado inhabilitado permanente. Además, mediante el uso de reglas se pueden excluir archivos y carpetas de los discos virtuales durante una implementación.

Problemas conocidos de 5.6.13 resueltos en la versión 7.0.1:

- Los cambios hechos por los usuarios en la pertenencia a un grupo en un escritorio virtual agrupado se pueden perder cuando se actualiza la imagen. [#286227]
- Las actualizaciones de la imagen pueden fallar con un error de poco espacio en disco, incluso aunque el disco Personal vDisk tenga espacio suficiente. [#325125]
- La instalación de algunas aplicaciones en escritorios virtuales con disco Personal vDisk falla, y aparece un mensaje indicando que hay que reiniciar. Esto se debe a una operación pendiente de cambio de nombre. [#351520]
- Los vínculos simbólicos creados dentro de una imagen maestra no funcionan en escritorios virtuales con discos Personal vDisk. [#352585]
- En entornos que usan Citrix Profile Management y Personal vDisk, las aplicaciones que exploran perfiles de usuario en un volumen de sistema pueden no funcionar correctamente si está habilitada la redirección de perfiles. [#353661]
- El proceso de actualización del inventario falla en las imágenes maestras si el tamaño del inventario es superior a 2 GB. [#359768]
- Las actualizaciones de imagen fallan con un código de error 112 y los discos Personal vDisk quedan dañados, incluso aunque estos discos tengan espacio suficiente para la actualización. [#363003]
- El script de cambio de tamaño falla para los catálogos que contienen más de 250 escritorios. [#363365]
- Los cambios hechos por los usuarios en una variable de entorno se pierden cuando se realiza una actualización de la imagen. [#372295]
- Los usuarios locales creados en un escritorio virtual con un disco Personal vDisk se pierden cuando se realiza una actualización de la imagen. [#377964]
- Es posible que un disco Personal vDisk no pueda iniciarse si se produjo un desbordamiento del diario de USN (números de secuencia de actualización) debido a una gran cantidad de cambios hechos en el sistema después de una actualización de inventario. Para evitar este problema, aumente el tamaño del diario USN a un mínimo de 32 MB en la imagen maestra y actualice la imagen. [#369846]
- Se ha identificado un problema en Personal vDisk que evita el funcionamiento correcto del Registro de AppSense Environment Manager y oculta acciones cuando AppSense se usa en modo de reemplazo. Citrix y AppSense están trabajando en forma conjunta para resolver el problema, que está relacionado con el comportamiento de la API RegRestoreKey cuando Personal vDisk está instalado.[#0353936]

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Problemas conocidos no relacionados con la versión

- Si Windows Store y las aplicaciones Metro se actualizan en la imagen maestra, pueden surgir conflictos para los dispositivos de destino habilitados con PvD después de que el disco vDisk se actualice al entorno de prueba o producción. Además, es posible que las aplicaciones Metro no se inicien mientras se desencadenan errores de registro de eventos de la aplicación. Citrix recomienda que desactive Windows Store y las aplicaciones Metro para dispositivos de destino habilitados con PvD.
- Cuando una aplicación instalada en un disco Personal vDisk (PvD) está relacionada con otra aplicación de la misma versión que está instalada en la imagen maestra, la aplicación del disco PvD puede dejar de funcionar después de una actualización de imagen. Esto ocurre si se desinstala la aplicación de la imagen maestra o si la aplicación se actualiza a una versión posterior, ya que esa acción quita de la imagen maestra los archivos que necesita la aplicación ubicada en el disco PvD. Para evitar esto, mantenga en la imagen maestra la aplicación que contiene los archivos necesarios para la aplicación del disco PvD.

  Por ejemplo, la imagen maestra contiene Office 2007, y un usuario instala Visio 2007 en el disco PvD; las aplicaciones de Office y Visio funcionan correctamente. Posteriormente, el administrador reemplaza Office 2007 por Office 2010 en la imagen maestra y, a continuación, actualiza todas las máquinas pertinentes con la imagen actualizada. En consecuencia, Visio 2007 deja de funcionar. Para evitarlo, conserve Office 2007 en la imagen maestra. [#0353936]
- Al implementar McAfee Virus Scan Enterprise (VSE), use el parche 4 de la versión 8.8 o posterior en una imagen maestra si utiliza Personal vDisk. [#303472]
- Si un acceso directo creado para un archivo ubicado en la imagen maestra deja de funcionar (porque el destino de ese acceso ha cambiado de nombre en el disco PvD), vuelva a crear ese acceso directo. [#367602]
- No use enlaces absolutos o físicos en una imagen maestra. [#368678]
- Personal vDisk no admite la función Copias de seguridad y restauración de Windows 7. [#360582]
- Después de la aplicación de una imagen maestra actualizada, la consola del usuario local y del grupo deja de ser accesible y muestra datos incoherentes. Para resolver este problema, restablezca las cuentas de usuario en la VM, lo que requiere restablecer también el subárbol de Registro de seguridad. Este problema se ha resuelto en la versión 7.1.2 (y funciona en las máquinas virtuales creadas con versiones posteriores), pero la corrección no funciona en el caso de máquinas virtuales que se crearon con una versión anterior y se actualizaron posteriormente. [#488044]
- Cuando se usa una VM agrupada en un entorno de hipervisor ESX, los usuarios ven una solicitud de reinicio si el tipo de controlador SCSI seleccionado es “VMware Paravirtual”. Para solucionar

© 1999-2019 Citrix Systems, Inc. All rights reserved.

el problema, use un tipo de controlador SCSI LSI. [#394039]

- Después de restablecer un disco PvD en un escritorio creado mediante Provisioning Services, es posible que se solicite a los usuarios que reinicien después de iniciar sesión en la máquina virtual. Para solucionarlo, reinicie el escritorio. [#340186]
- Es posible que los usuarios del escritorio Windows 8.1 no puedan iniciar sesión en su PvD. Es posible que el administrador vea un mensaje similar a "PvD se ha inhabilitado debido a un apagado no seguro". También es posible que el registro PvDActivation contenga un mensaje similar a "No se ha podido cargar el subárbol del Registro [\Device\IvmVhdDisk00000001\CitrixPvD\Settings\RingCube.dat]". Esto ocurre cuando la máquina virtual de un usuario se apaga de forma no segura. Como solución temporal, restablezca Personal vDisk. [#474071]

Instalar y actualizar

March 8, 2019

Personal vDisk 7.x se respalda en la versión actual de Citrix Virtual Apps and Desktops (y versiones anteriores, a partir de XenDesktop 5.6). La documentación referente a los requisitos del sistema para cada versión ofrece una lista de los sistemas operativos respaldados en los agentes Virtual Delivery Agent (VDA), las versiones compatibles de hosts (recursos de virtualización) y Citrix Provisioning (antes Provisioning Services). Para obtener información más detallada sobre las tareas de Citrix Provisioning, consulte la documentación de Citrix Provisioning.

Instalar y habilitar Personal vDisk

Puede instalar y habilitar los componentes de PvD al instalar o actualizar un VDA para SO de escritorio en una máquina. Estas acciones se seleccionan en las páginas **Componentes adicionales** y **Características** del Asistente de instalación, respectivamente. Para obtener más información, consulte Instalar agentes VDA.

Si actualiza el software de Personal vDisk después de instalar el VDA, utilice el archivo MSI de PvD proporcionado en los medios de instalación de Citrix Virtual Apps and Desktops.

Habilitar Personal vDisk:

- Si utiliza Machine Creation Services (MCS), Personal vDisk se habilita automáticamente cuando se crea un catálogo de máquinas con SO de escritorio que usarán un disco Personal vDisk.
- Si utiliza Citrix Provisioning, Personal vDisk se habilita automáticamente, ya sea cuando ejecuta el inventario durante el proceso de creación de imagen maestra (base) o cuando la actualización automática ejecuta el inventario por usted.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Por lo tanto, si instala los componentes de PvD, pero no los habilita durante la instalación del VDA, puede utilizar la misma imagen para crear escritorios con o sin PvD, debido a que PvD se habilita durante el proceso de creación del catálogo.

Agregar discos Personal vDisk

Los discos Personal vDisk se agregan a hosts cuando configura un sitio. Puede utilizar el mismo almacenamiento en el host tanto para las VM como para los discos Personal vDisk, o bien puede usar otro almacenamiento para los discos Personal vDisk.

Más adelante, también podrá agregar discos Personal vDisk y su almacenamiento a los hosts existentes (conexiones), pero no a catálogos de máquinas.

1. Seleccione Configuración > Alojamiento en el panel de navegación de Studio.
2. Seleccione Agregar almacenamiento de Personal vDisk en el panel Acciones y especifique la ubicación de la unidad de almacenamiento.

Actualizar PvD

La forma más sencilla de actualizar Personal vDisk desde una versión anterior 7.x consiste simplemente en actualizar los agentes VDA de los SO de escritorio a la versión proporcionada con la versión más reciente de Citrix Virtual Desktops. A continuación, se puede ejecutar el inventario de PvD.

Desinstalar PvD

Dispone de las siguientes dos maneras para quitar el software de Personal vDisk:

- Desinstalar el agente VDA. Esta acción quita también el software de Personal vDisk.
- Si ha actualizado Personal vDisk mediante el archivo MSI de PvD, puede desinstalarlo desde la lista de programas.

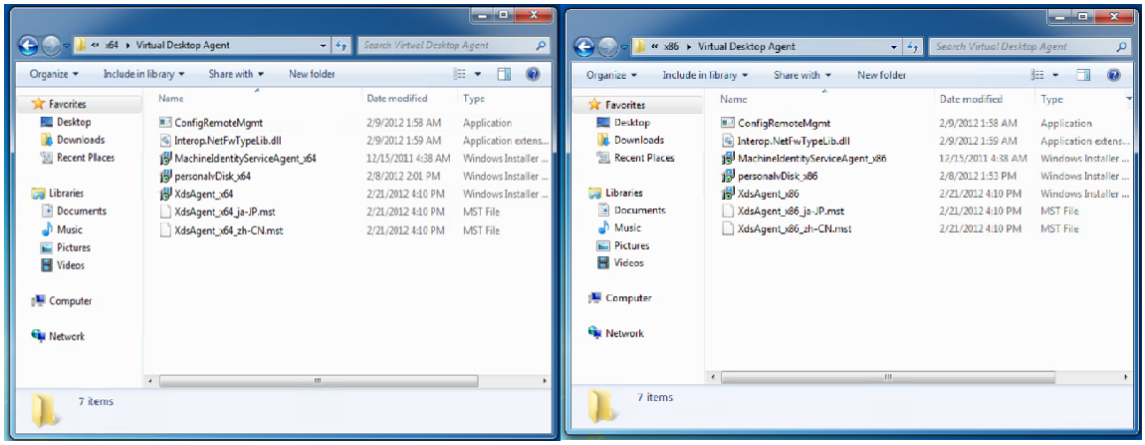
Si desinstala PvD y quiere volver a instalar la misma versión o una versión más reciente, primero haga una copia de seguridad de la clave de Registro HKLM\Software\Citrix\personal vDisk\config, que contiene los parámetros de configuración del entorno que pueden haber cambiado. Después de instalar PvD, restablezca los valores del Registro que puedan haber cambiado. Para ello, compárelos con la versión de la copia de seguridad.

La desinstalación puede fallar si se ha instalado un disco Personal vDisk con Windows 7 (64 bits) en la imagen base. Para evitar este problema, Citrix recomienda que quite el disco Personal vDisk antes de actualizar.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

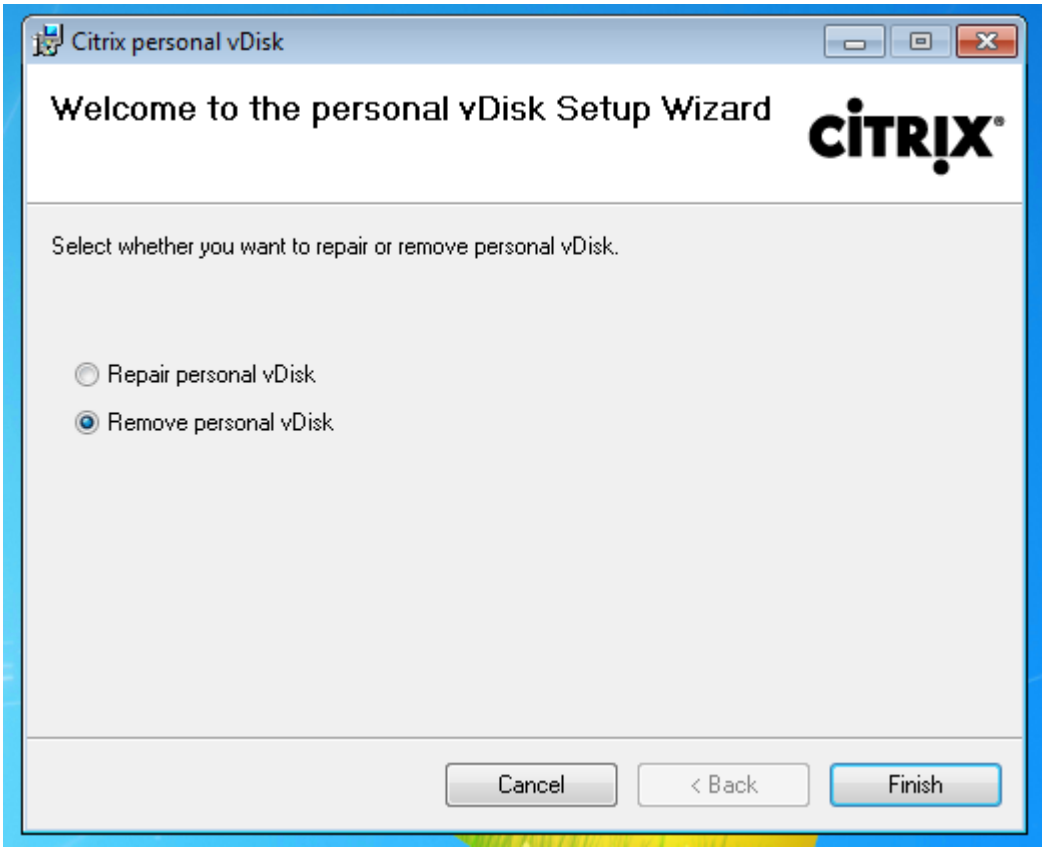
1. Seleccione la copia correspondiente del instalador vDisk en los medios de Citrix Virtual Apps and Desktops. Busque el instalador MSI más reciente de Personal vDisk en uno de los siguientes directorios (según si la máquina virtual actualizada es de 32 o 64 bits):

   - 32 bits: XA and XD\x86\Virtual Desktop Components\personalvDisk_x86.msi
   - 64 bits: XA and XD\x64\Virtual Desktop Components\personalvDisk_x64.msi



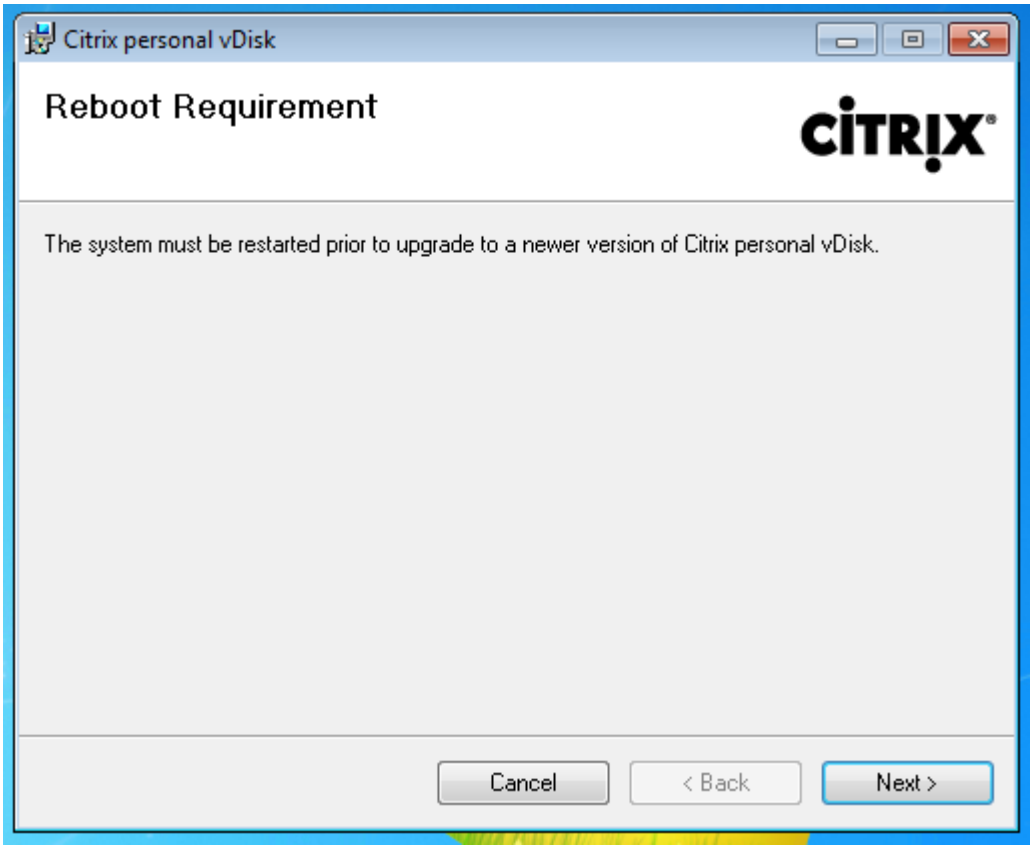
2. Quite la instalación de Personal vDisk. Seleccione el paquete de instalador MSI de Personal vDisk que ha localizado en el paso 1. Aparecerá la pantalla de configuración de Personal vDisk.
3. Seleccione **Quitar Personal vDisk**.
4. Haga clic en **Finish**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

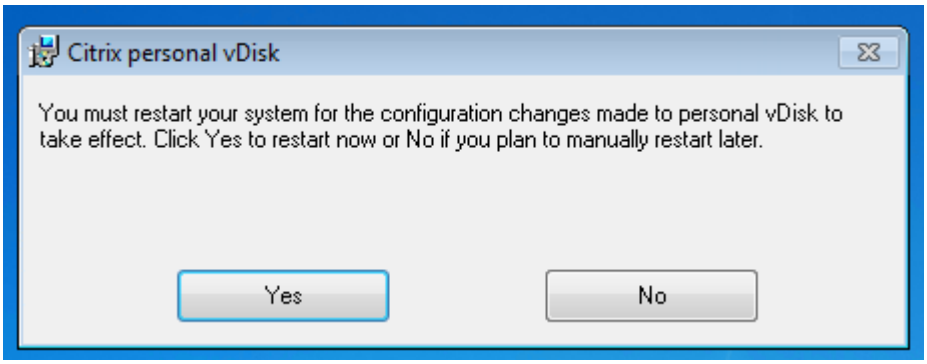


5. Aparecerá una página con el requisito de reiniciar la máquina. Haga clic en **Siguiente**:

© 1999-2019 Citrix Systems, Inc. All rights reserved.



6. Haga clic en **Sí** para reiniciar el sistema y aplicar los cambios de configuración:



Configurar y administrar

March 8, 2019

En este apartado se describen los elementos que se deben tener en cuenta a la hora de configurar y administrar un entorno de Personal vDisk (PvD). También se incluyen las prácticas recomendadas y las descripciones de las tareas pertinentes.

En el caso de tareas que implican trabajar con el Registro de Windows:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Precaución: Si modifica el Registro de forma incorrecta, podrían generarse problemas graves que pueden provocar la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Consideraciones: tamaño del disco Personal vDisk

Los siguientes factores repercuten en el tamaño del volumen principal del disco Personal vDisk:

- **El tamaño de las aplicaciones que los usuarios instalarán en sus discos PvD**

  Durante los reinicios, PvD determina el espacio libre restante en el área de aplicaciones (UserData.v2.vhd). Si el espacio cae por debajo del 10%, el área de aplicaciones se expande hacia el espacio no utilizado del área de perfiles (de manera predeterminada, el espacio disponible en la unidad P:). El espacio que se agrega al área de aplicaciones es aproximadamente el 50% del espacio libre combinado que queda en el área de aplicaciones y el área de perfiles.

  Por ejemplo, si el área de aplicaciones de un disco PvD de 10 GB (que de manera predeterminada tiene un tamaño de 5 GB) alcanza los 4,7 GB y el área de perfiles tiene 3 GB libres, el espacio que se agrega al área de aplicaciones se calcula de la siguiente manera:

  Espacio agregado = (5,0-4,7)/2 + 3,0/2 = 1,65 GB

  El espacio agregado al área de aplicaciones es solo aproximado porque se reserva un pequeño espacio para guardar registros y otros usos auxiliares. El cálculo y posible cambio de tamaño tienen lugar en cada reinicio.

- **El tamaño de los perfiles de los usuarios (si no se va a usar una solución de administración de perfiles aparte)**

  Además del espacio requerido para las aplicaciones, también debe comprobar que haya suficiente espacio disponible en los discos PvD para almacenar los perfiles de los usuarios. Incluya las carpetas especiales no redirigidas (por ejemplo, Mis documentos y Mi música) al calcular los requisitos de espacio. Los tamaños de los perfiles existentes se pueden consultar en el Panel de control (sysdm.cpl).

  Algunas soluciones de redirección de perfiles almacenan archivos stub (archivos de centinela) en lugar de los datos de perfil reales. Inicialmente, puede parecer que estas soluciones de perfiles no almacenan ningún dato, pero, en realidad, consumen una entrada de directorio de archivos en el sistema por cada archivo stub (generalmente, son 4 KB por archivo). Si usa una solución de este tipo, debe calcular el tamaño según los datos de perfil reales y no según los archivos stub.

  Las aplicaciones empresariales de uso compartido de archivos (como ShareFile y Dropbox) pueden sincronizar o descargar datos en las áreas de perfiles de los usuarios de los discos

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Personal vDisk. Para utilizar esas aplicaciones, incluya suficiente espacio en los cálculos de tamaño para esos datos.

- **Los recursos consumidos por el disco VHD de plantilla que contiene el inventario de PvD**

  El disco VHD de plantilla contiene datos de inventario de PvD (archivos de centinela correspondientes al contenido de la imagen maestra). El área de aplicaciones del PvD se crea a partir de este VHD. Cada carpeta o archivo de centinela comprende una entrada de directorio de archivos en el sistema de archivos, por lo que el contenido de VHD de plantilla consume espacio de aplicaciones del PvD incluso aunque el usuario final todavía no haya instalado ninguna aplicación. Puede determinar el tamaño del disco VHD de plantilla si examina la imagen maestra después seleccionar un inventario. También puede usar la siguiente ecuación para un cálculo aproximado:

  tamaño del disco VHD de plantilla = (número de archivos en la imagen base) x 4 KB

  Puede determinar la cantidad de archivos y carpetas si hace clic con el botón secundario en la unidad C: (ubicada en la imagen de la máquina virtual base) y selecciona Propiedades. Por ejemplo, una imagen con 250 000 archivos da como resultado un disco VHD de plantilla de 1 024 000 000 bytes aproximadamente (casi 1 GB). Este espacio no estará disponible para la instalación de aplicaciones en el área de aplicaciones de PvD.

- **Recursos consumidos por operaciones de actualización de imágenes de PvD**

  Durante las operaciones de actualización de imagen de PvD, debe haber suficiente espacio disponible en la raíz del disco PvD (de manera predeterminada, P:) para fusionar los cambios de las dos versiones de la imagen y los cambios que el usuario efectuó en su disco PvD. Por lo general, PvD reserva unas centenas de megabytes con este fin, pero los datos adicionales que se escribieron en la unidad P: pueden llegar a consumir este espacio reservado, lo que no deja espacio suficiente para completar correctamente la actualización de la imagen. El script de estadísticas de agrupación de PvD (ubicado en la carpeta Support/Tools/Scripts de los medios de instalación de Citrix Virtual Apps and Desktops) o la herramienta Personal vDisk Image Update Monitoring Tool (en la carpeta Support/Tools/Scripts\PvdTool) pueden identificar los discos PvD de un catálogo que se estén actualizando y que están casi llenos.

  La presencia de productos antivirus puede afectar el tiempo necesario para ejecutar el inventario o realizar una actualización. El rendimiento se puede mejorar si agrega CtxPvD.exe y CtxPvDSvc.exe a la lista de exclusión del producto antivirus. Estos archivos se encuentran en C:\Archivos de programa\Citrix\Personal vDisk\bin. La exclusión de esos ejecutables para que no sean analizados por el antivirus puede mejorar el rendimiento del inventario y de las actualizaciones de imagen y mejorar su velocidad hasta diez veces.

- **Los recursos por crecimiento inesperado (instalación inesperada de aplicaciones, entre otros)**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Tenga en cuenta la conveniencia de agregar una cantidad de espacio extra (ya sea una cantidad fija o un porcentaje del total del disco PvD) al tamaño total para que, de ese modo, quepan instalaciones no previstas de aplicaciones que el usuario realice durante la implementación.

Cómo configurar el tamaño y la asignación del disco Personal vDisk

Es posible ajustar de forma manual el algoritmo de cambio automático de tamaño que determina el tamaño del disco VHD en relación a la unidad P:. Para ello, establezca el tamaño inicial del disco VHD. Esto puede resultar útil si, por ejemplo, se sabe que los usuarios instalarán varias aplicaciones que son demasiado grandes para la capacidad del VHD, aún después de cambiar el tamaño mediante el algoritmo. En este caso, puede aumentar el tamaño inicial del espacio destinado a las aplicaciones para que quepan las aplicaciones instaladas por los usuarios.

Es preferible que ajuste el tamaño inicial del disco VHD en una imagen maestra. También puede ajustar el tamaño del disco VHD de un escritorio virtual cuando un usuario no tiene espacio suficiente para instalar una aplicación. Sin embargo, debe repetir esta operación en cada escritorio virtual afectado; no es posible ajustar el tamaño inicial del disco VHD en un catálogo ya creado.

Asegúrese de que el VHD tenga un tamaño lo suficientemente grande como para almacenar archivos de definiciones de antivirus, que suelen ser grandes.

Busque y configure las siguientes claves de Registro en HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\personal vDisk\Config. (No modifique ningún otro parámetro de esta clave del Registro.) Todos los parámetros deben especificarse en la imagen maestra (excepto MinimumVHDSizeInMB, que se puede cambiar en una máquina individual); los parámetros especificados en la imagen maestra se aplicarán durante la próxima actualización de imagen.

- **MinimumVHDSizeMB**

  Especifica el tamaño mínimo (en megabytes) de la parte de las aplicaciones (C:) del disco Personal vDisk. El nuevo tamaño debe ser mayor que el tamaño existente, pero menor que el tamaño del disco menos PvDReservedSpaceMB.

  Cuando se aumenta este valor se asigna espacio libre desde el área del disco virtual a la unidad C:. Este parámetro se ignora si se usa un valor más bajo que el tamaño actual de la unidad C:, o si EnableDynamicResizeOfAppContainer tiene el valor 0.

  Valor predeterminado = 2048

- **EnableDynamicResizeOfAppContainer**

  Habilita o inhabilita el algoritmo de cambio dinámico de tamaño.

  – Cuando el valor se establece en 1, cambia el tamaño del área de las aplicaciones (C:) automáticamente cuando el espacio disponible en C: baja del 10%. Los valores permitidos son 1 y 0. Para que el cambio de tamaño tenga efecto, es necesario un reinicio.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Cuando se establece en 0, el tamaño del disco VHD se determina según el método usado en las versiones anteriores a XenDesktop 7.x.

Valor predeterminado = 1

- **EnableUserProfileRedirection**

  Habilita o inhabilita la redirección del perfil del usuario al disco Personal vDisk.

  - Cuando se establece en 1, PvD redirige los perfiles de los usuarios a la unidad del disco Personal vDisk (de manera predeterminada, P:). Los perfiles se redirigen normalmente a P:\Users, lo que corresponde a un perfil de Windows estándar. Esta redirección permite conservar los perfiles en caso de que el escritorio de PvD deba restablecerse.
  - Cuando se le da el valor 0, todo el espacio del disco virtual (vDisk) menos PvDReservedSpaceMB se asigna a C:, la parte de aplicaciones del disco virtual, y la unidad P: del disco virtual se oculta en el Explorador de Windows. Citrix recomienda inhabilitar la redirección (para ello, establezca el valor en 0) al usar Citrix Profile Management o alguna otra solución de administración de perfiles móviles.

    Este parámetro conserva los perfiles en C:\Usuarios en lugar de redirigirlos al disco Personal vDisk, y deja que la solución de administración de perfiles móviles se ocupe de gestionarlos.

    Este valor garantiza que todo el espacio en P: esté asignado a las aplicaciones.

    Se asume que si este valor está establecido en 0, hay una solución de administración de perfiles implementada. No se recomienda inhabilitar la redirección de perfiles sin tener una solución de administración de perfiles implementada, porque los restablecimientos de PvD subsiguientes provocan la eliminación de perfiles.

  Este parámetro no debe cambiarse cuando la imagen se actualiza porque no cambia la ubicación de los perfiles existentes, pero asigna todo el espacio en el disco PvD a C: y oculta el disco.

  Configure este valor antes de implementar un catálogo. No se puede cambiar después de que el catálogo se haya implementado.

  Importante: A partir de XenDesktop 7.1, no se respetan los cambios efectuados en este valor al actualizar una imagen. Establezca el valor de la clave la primera vez que cree los catálogos a partir de los que se originarán los perfiles. Más adelante, no podrá modificar el comportamiento de redirección.

  Valor predeterminado = 1

- **PercentOfPvDForApps**

  Define la división entre la parte de las aplicaciones (C:) y la parte de los perfiles del disco Personal vDisk. Este valor se usa al crear nuevas máquinas virtuales y durante las actualizaciones

© 1999-2019 Citrix Systems, Inc. All rights reserved.

de imagen cuando EnableDynamicResizeOfAppContainer tiene el valor 0.

Cambiar PercentOfPvDForApps solo es efectivo cuando EnableDynamicResizeOfAppContainer tiene el valor 0. De forma predeterminada, EnableDynamicResizeOfAppContainer está establecido en 1 (habilitado), lo que significa que AppContainer (que aparece como la unidad C:) es dinámico, por lo que solo se expande cuando queda menos del 10% del espacio disponible.

Cuando se aumenta PercentOfPvDForApps solo se aumenta el espacio máximo para el que se permite expandir la parte de Aplicaciones. El espacio no se aprovisiona inmediatamente. También debe configurar la división de espacio en la imagen maestra donde se aplicará durante la próxima actualización de imagen.

Si ya ha generado un catálogo de máquinas con el parámetro EnableDynamicResizeOfAppContainer establecido en 1, cambie ese parámetro a 0 en la imagen maestra para la siguiente actualización y configure una división de espacio apropiada. El tamaño de división solicitado se aplicará siempre que sea mayor que el tamaño actualmente asignado para la unidad C:.

Si quiere conservar el control total sobre la división de espacio, este valor debe establecerse en 0. Esto permite el control total sobre el tamaño de la unidad C:, en lugar de depender de que un usuario consuma espacio por debajo del umbral para expandir la unidad.

Valor predeterminado = 50 % (se asigna un espacio de igual tamaño a ambas partes)

- **PvDReservedSpaceMB**

  Define el tamaño del espacio reservado (en MB) en el disco Personal vDisk para almacenar los registros y otros datos de Personal vDisk.

  Si la implementación incluye XenApp 6.5 (o una versión anterior) y usa la distribución de aplicaciones por streaming, aumente este valor según el tamaño utilizado para Rade Cache.

  Valor predeterminado = 512

- **PvDResetUserGroup**

  Válido solamente para XenDesktop 5.6: Permite que un grupo especificado de usuarios restablezca un disco Personal vDisk. En las versiones posteriores se usa la Administración delegada para ello.

Otros parámetros:

- **Windows Update Service:** Defina las actualizaciones de Windows con el valor “No buscar actualizaciones” y Windows Update Service con el valor “Inhabilitado” en la imagen maestra. Además, Citrix recomienda que inhabilite las funciones y actualizaciones de Windows Store y las aplicaciones Metro.
- **Actualizaciones de Windows:** Incluidas las actualizaciones de Internet Explorer, que se deben aplicar a la imagen maestra.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Actualizaciones que requieren reinicios:** Las actualizaciones de Windows aplicadas a la imagen maestra pueden requerir varios reinicios para instalarse completamente, según el tipo de revisión que se entregue con ellas. Compruebe que reinicia la imagen maestra correctamente para completar totalmente la instalación de las actualizaciones de Windows aplicadas a ella, antes de seleccionar el inventario de PvD.
- **Actualizaciones de aplicaciones:** Actualice las aplicaciones instaladas en la imagen maestra para conservar espacio en los discos Personal vDisk de los usuarios. Esto también evita que se dupliquen esfuerzos actualizando las aplicaciones en todos y cada uno de los discos virtuales de los usuarios.

Consideraciones: aplicaciones en la imagen maestra

Algunos programas de software pueden entrar en conflicto con el modo en que Personal vDisk crea el entorno del usuario, por lo que hay que instalarlos en la imagen maestra (y no en la máquina en sí) para evitar dichos conflictos. Además, aunque otro software no entre en conflicto con el funcionamiento de Personal vDisk, Citrix recomienda instalarlo en la imagen maestra.

Aplicaciones que deben instalarse en la imagen maestra:

- Agentes y clientes (por ejemplo, el agente de System Center Configuration Manager, el cliente de App-V, la aplicación Citrix Workspace)
- Aplicaciones que instalan o modifican controladores de la primera fase de arranque
- Aplicaciones que instalan controladores o software de impresoras o escáneres
- Aplicaciones que modifican la pila de red de Windows
- Herramientas de la VM como VMware Tools y XenServer Tools

Aplicaciones que se recomienda instalar en la imagen maestra:

- Aplicaciones que se distribuyen a un gran número de usuarios. En cada caso, desactive las actualizaciones de la aplicación antes de implementarla:
  - Aplicaciones de empresa que usan licencias de volumen como, por ejemplo, Microsoft Office y Microsoft SQL Server
  - Aplicaciones de uso frecuente, como Adobe Reader, Firefox y Chrome
- Aplicaciones de gran tamaño como, por ejemplo, SQL Server, Visual Studio y marcos de trabajo de aplicaciones como .NET Framework.

Las siguientes recomendaciones y restricciones se aplican a las aplicaciones instaladas por los usuarios en las máquinas que tienen discos Personal vDisk. Algunas de ellas no pueden imponerse si los usuarios tienen privilegios de administrador:

- Los usuarios no deben desinstalar ninguna aplicación que esté presente en la imagen maestra para volver a instalar esa misma aplicación en su disco Personal vDisk.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Ponga cuidado a la hora de actualizar o desinstalar aplicaciones en la imagen maestra. Después de instalar una versión de una aplicación en la imagen, un usuario podría instalar una aplicación complementaria (por ejemplo, un plug-in) que requiriera esa versión. Si existe tal dependencia, la actualización o desinstalación de la aplicación en la imagen puede hacer que el complemento no funcione correctamente. Por ejemplo, con Microsoft Office 2010 instalado en la imagen maestra, un usuario instala Visio 2010 en su disco Personal vDisk. Una posterior actualización de Office en la imagen maestra podría hacer que la versión local instalada de Visio pasara a ser inutilizable.
- El software que usa licencias dependientes del hardware (ya sea mediante llaves o hardware basado en firma) no recibe respaldo.

Consideraciones: Citrix Provisioning

Al usar Citrix Provisioning con Personal vDisk:

- La cuenta de Soap Service debe agregarse al nodo Administradores de Studio, y debe tener un rol de Administrador de máquinas o superior. Eso garantiza que los escritorios PvD se colocan en el estado de preparación (Preparing) cuando el vDisk de Citrix Provisioning pasa a la fase de producción.
- Debe usarse la función de control de versiones de Citrix Provisioning para actualizar el disco Personal vDisk. Cuando la versión se eleva a la fase de producción, Soap Service pone los escritorios con PvD en el estado de preparación (Preparing).
- El tamaño del disco Personal vDisk siempre debe ser mayor que el disco de memoria caché de escritura de Citrix Provisioning (de lo contrario, Citrix Provisioning podría elegir erróneamente el disco Personal vDisk para usarlo como memoria caché de escritura).
- Después de crear un grupo de entrega, puede supervisar el disco Personal vDisk mediante la herramienta PvD Image Update Monitoring Tool o los scripts Resize y Poolstats (personal-vdisk-poolstats.ps1).

Asigne el tamaño adecuado al disco de memoria caché de escritura. Durante una operación normal, PvD captura la mayoría de las escrituras de usuario (cambios) y las redirige al disco PvD. Eso implica que se puede reducir el tamaño del disco de memoria caché de escritura de Citrix Provisioning. No obstante, cuando PvD no está activo (por ejemplo, durante las operaciones de actualización de la imagen), un disco pequeño de caché de escritura de Citrix Provisioning podría llegar a llenarse, lo que provocaría un bloqueo de la máquina.

Citrix recomienda asignar a los discos de caché de escritura de Citrix Provisioning el tamaño adecuado siguiendo las prácticas recomendadas de Citrix Provisioning. Asimismo, se recomienda agregar un espacio que doble el tamaño del disco VHD de plantilla en la imagen maestra (para que se cumplan los requisitos de fusión). Es muy poco probable que una operación de fusión requiera todo este espacio, pero podría darse el caso.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Al usar Citrix Provisioning para implementar un catálogo de máquinas con Personal vDisk habilitado:

- Siga las instrucciones indicadas en la documentación de Citrix Provisioning.
- Puede cambiar los parámetros de limitación de acciones de energía si modifica la conexión en Studio. Para obtener más información, consulte los apartados siguientes.
- Si actualiza el disco Personal vDisk de Citrix Provisioning después de instalar o actualizar aplicaciones y otro software y de reiniciar el disco, ejecute el inventario de PvD y apague la VM. A continuación, transfiera la nueva versión al modo de producción. Los escritorios con PvD del catálogo deben entrar automáticamente en el estado de preparación (Preparing). Si no lo hacen, compruebe que la cuenta de Soap Service tiene privilegios de administrador de máquinas o superior en el Controller.

La función del modo de prueba de Citrix Provisioning permite crear un catálogo de prueba que contenga máquinas que utilicen una imagen maestra actualizada. Si las pruebas confirman la viabilidad del catálogo de prueba, el catálogo se puede transferir al modo de producción.

Consideraciones: Machine Creation Services

Al usar Machine Creation Services (MCS) para implementar un catálogo de máquinas con Personal vDisk habilitado:

- Siga las instrucciones indicadas en la documentación del producto.
- Ejecute un inventario de PvD después de crear la imagen maestra y, luego, apague la VM (PvD no funcionará correctamente si no se apaga la VM). A continuación, tome una instantánea de la imagen maestra.
- En el asistente Crear catálogo de máquinas, especifique el tamaño del disco Personal vDisk y su letra de unidad.
- Después de crear un grupo de entrega, puede supervisar el disco Personal vDisk mediante la herramienta PvD Image Update Monitoring Tool o los scripts Resize y Poolstats (personal-vdisk-poolstats.ps1).
- Puede cambiar los parámetros de limitación de acciones de energía si modifica la conexión en Studio. Para obtener más información, consulte los apartados siguientes.
- Si actualiza la imagen maestra, ejecute el inventario de PvD después de actualizar las aplicaciones y otros programas de software en la imagen y, a continuación, apague la VM. A continuación, tome una instantánea de la imagen maestra.
- Use el script personal-vdisk-poolstats.ps1 o la herramienta Personal vDisk Image Update Monitoring Tool para comprobar que haya suficiente espacio en cada máquina virtual con PvD habilitado que usará la imagen maestra actualizada.
- Después de actualizar el catálogo de máquinas, los escritorios con PvD entran en el estado de preparación (Preparing) a medida que procesan individualmente los cambios hechos a la nueva imagen maestra. Los escritorios se actualizan de acuerdo con la estrategia de distribución es-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

pecificada durante la actualización de la máquina.
- Use la herramienta Personal vDisk Image Update Monitoring Tool o el script personal-vdisk-poolstats.ps1 para supervisar el disco Personal vDisk en el estado de preparación (Preparing).
- La selección del almacenamiento en caché de E/S de PVD y MCS se excluyen mutuamente. Si instala PVD, no podrá crear un catálogo con el almacenamiento en caché de E/S de MCS habilitado.

Cómo excluir archivos y carpetas de los discos Personal vDisk

Use los archivos de reglas para excluir archivos y carpetas de los discos virtuales. Puede hacer esto cuando los discos Personal vDisk están en fase de implementación. Los archivos de reglas tienen el nombre custom_*_rules.template.txt y se encuentran en la carpeta \config. Los comentarios de cada archivo ofrecen documentación adicional.

Cómo ejecutar el inventario al actualizar una imagen maestra

Con Personal vDisk habilitado, después de realizar actualizaciones en la imagen maestra posteriores a la instalación, es importante actualizar el inventario del disco ("ejecutar el inventario") y tomar una nueva instantánea.

Puesto que son los administradores y no los usuarios quienes administran las imágenes maestras, si instala una aplicación que coloca archivos binarios en el perfil de usuario del administrador, dicha aplicación no está disponible para los usuarios de los escritorios virtuales compartidos (incluidos aquellos basados en catálogos agrupados de máquinas y catálogos agrupados de máquinas con Personal vDisk). Son los propios usuarios quienes tienen que instalar las aplicaciones.

Se recomienda tomar una instantánea de la imagen después de realizar cada paso de este procedimiento.

1. Actualice la imagen maestra instalando aplicaciones y actualizaciones del sistema operativo y configurando el sistema en la máquina como desee.

   Para las imágenes maestras basadas en Windows XP que desee implementar con discos Personal vDisk, compruebe que no haya ningún cuadro de diálogo abierto (por ejemplo, mensajes que confirman la instalación de un programa o mensajes que piden autorización para usar controladores sin firma). Cuando quedan cuadros de diálogo abiertos en imágenes maestras en este entorno, se impide que VDA pueda registrarse con el Delivery Controller. Para impedir la aparición de mensajes que piden autorización para usar controladores sin firma, use el Panel de control. Por ejemplo, vaya a Sistema > Hardware > Firma de controladores, y seleccione la opción pertinente para omitir advertencias.

2. Apague la máquina. Para máquinas con Windows 7, haga clic en Cancelar cuando el disco Personal vDisk de Citrix bloquee el apagado de la máquina.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

3. En el cuadro de diálogo del disco Citrix Personal vDisk, haga clic en Actualizar inventario. Este paso puede tardar varios minutos en completarse.

   Importante: Si interrumpe el siguiente apagado (aunque sea para realizar una pequeña actualización en la imagen), el inventario del disco Personal vDisk ya no coincidirá con la imagen maestra. Esto hace que la función Personal vDisk deje de funcionar. Si interrumpe el apagado del sistema, debe reiniciar la máquina, apagarla y, cuando lo pida el sistema, hacer clic de nuevo en Actualizar inventario.

4. Cuando la operación de inventario haya apagado la máquina, tome una instantánea de la imagen maestra.

Puede exportar un inventario a un punto compartido de red y, a continuación, importar ese inventario en una imagen maestra. Para obtener más información, consulte Exportar e importar un inventario de PvD.

Cómo configurar los parámetros de la limitación de conexiones

Citrix Broker Service controla el estado de energía de las máquinas que proporcionan los escritorios y las aplicaciones. El servicio Broker Service puede controlar varios hipervisores a través de un Delivery Controller. Mediante las acciones de energía del servicio Broker Service, se controla la interacción entre un Controller y el hipervisor. Para evitar sobrecargar el hipervisor, las acciones que cambian el estado de energía de una máquina reciben una prioridad y se envían al hipervisor mediante un mecanismo de limitación de peticiones. Los siguientes parámetros afectan a la limitación de peticiones. Para especificar esos valores, modifique la conexión (página Avanzada) en Studio.

Para configurar los valores de limitación de conexiones:

1. Seleccione Configuración > Alojamiento en el panel de navegación de Studio.
2. Seleccione la conexión y, a continuación, seleccione Modificar conexión en el panel Acciones.
3. Puede cambiar los siguientes valores:
   - **Acciones simultáneas (de cualquier tipo):** La cantidad máxima de acciones de energía en curso y simultáneas permitidas. Este parámetro se especifica tanto como valor absoluto como un porcentaje de la conexión al hipervisor. Se utiliza el menor de los dos valores.
     Valor predeterminado = 100 absoluto, 20%
   - **Actualizaciones de inventario de Personal vDisk simultáneas:** La cantidad máxima de acciones de energía simultáneas permitidas de Personal vDisk. Este parámetro se especifica tanto como valor absoluto como un porcentaje de la conexión. Se utiliza el menor de los dos valores.
     Valor predeterminado = 50 absoluto, 25 %
     Para calcular el valor absoluto: determine el total de IOPS (TIOPS) que admite el almacenamiento del usuario final (se debe calcular o debe ser especificado por el fabricante). Con 350 IOPS por VM (IOPS/VM), determine el número de máquinas virtuales que deben

© 1999-2019 Citrix Systems, Inc. All rights reserved.

estar activas en un momento dado en el almacenamiento. Calcule este valor dividiendo el total de IOPS entre IOPS/VM.

Por ejemplo, si el almacenamiento del usuario final es de 14000 IPS, el número de máquinas virtuales es: 14000 IOPS / 350 IOPS/VM = 40.

- **Máximo de acciones nuevas por minuto:** La cantidad máxima de acciones de energía nuevas que se pueden enviar al hipervisor por minuto. Especificadas con valor absoluto. Valor predeterminado= 10

Para identificar más fácilmente el valor óptimo de estos parámetros en la implementación:

1. Con la ayuda de los valores predeterminados, mida el tiempo total de respuesta de la actualización de una imagen de un catálogo de prueba. Esta es la diferencia entre el inicio de una actualización de imagen (T1) y el momento en que el agente VDA de la última máquina del catálogo se registra con el Controller (T2). Tiempo total de respuesta = T2 - T1.
2. Mida las operaciones de entrada y salida por segundo (IOPS) del almacenamiento del hipervisor durante la actualización de la imagen. Esta información puede servir como referencia para la optimización. (Los valores predeterminados pueden ser la mejor opción; de lo contrario, es posible que el sistema alcance la cantidad máxima de IOPS, lo que requerirá reducir los valores del parámetro.)
3. Cambie el valor “Actualizaciones de inventario simultáneas de Personal vDisk” tal y como se describe a continuación (sin cambiar ninguno de los demás parámetros).
    a) Aumente el valor en 10 y mida el tiempo total de respuesta después de cada cambio. Siga aumentando el valor de 10 en 10 y realice pruebas con el resultado hasta el deterioro o hasta que el tiempo total de respuesta no cambie en absoluto.
    b) Si el paso anterior, consistente en aumentar el valor, no produjo ninguna mejora, disminuya el valor de 10 en 10 y mida el tiempo total de respuesta después de cada disminución. Repita este proceso hasta que el tiempo total de respuesta no cambie o hasta que no mejore más. Seguramente, este será el valor óptimo para las acciones de energía de Personal vDisk.
4. Después de obtener el valor del parámetro de acciones de energía de Personal vDisk, modifique uno a uno los valores de las acciones simultáneas (todos los tipos) y la cantidad máxima de acciones nuevas por minuto. Siga el procedimiento descrito anteriormente (aumentar o disminuir) para probar distintos valores.

Cómo configurar Personal vDisk con Microsoft System Center Configuration Manager 2007

System Center Configuration Manager (Configuration Manager) 2012 no requiere ninguna configuración especial y se puede instalar igual que otra aplicación de imagen maestra. La siguiente información se aplica solo a System Center Configuration Manager 2007. No se respaldan las versiones de Configuration Manager anteriores a Configuration Manager 2007.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Complete los siguientes pasos para utilizar el software de agente Configuration Manager 2007 en un entorno de Personal vDisk.

1. Instale el agente cliente en la imagen maestra.
    a) Instale el cliente de Configuration Manager en la imagen maestra.
    b) Detenga el servicio ccmexec (SMS Agent) e inhabilítelo.
    c) Elimine certificados del cliente o SMS del almacén de certificados del equipo local de este modo:
        - Modo mixto: Certificados (equipo local)\SMS\Certificados
        - Modo nativo
            - Certificados (equipo local)\Personal\Certificados
            - Elimine el certificado del cliente emitido por su entidad de certificación (por regla general, una infraestructura de clave pública PKI interna)
    d) Elimine o cambie de nombre el archivo C:\Windows\smscfg.ini.
2. Quite la información que identifique de manera exclusiva al cliente.
    a) (Optativo) Elimine o mueva archivos de registros de C:\Windows\System32\CCM\Logs.
    b) Instale Virtual Delivery Agent (si no estaba ya instalado) y seleccione el inventario de PvD.
    c) Apague la imagen maestra, tome una instantánea y cree un catálogo de máquinas a partir de esa instantánea.
3. Valide Personal vDisk e inicie los servicios. Lleve a cabo estos pasos una vez en cada escritorio con PvD después de iniciarlos por primera vez. Esto puede hacerse usando un objeto de directiva de grupo (GPO) de dominio, por ejemplo.
    - Confirme que PvD está activo comprobando la presencia de la clave de Registro HKLM\Software\Citrix\personal vDisk\config\virtual.
    - Configure el servicio ccmexec (agente SMS) en Automático e inicie el servicio. El cliente de Configuration Manager contacta con el servidor de Configuration Manager y obtiene certificados y GUID nuevos y exclusivos.

Herramientas

October 3, 2018

Puede utilizar las siguientes herramientas y utilidades para adaptar, acelerar y supervisar operaciones de PvD.

Archivos de reglas personalizadas

Los archivos de reglas personalizadas que se proporcionan con PvD permiten modificar el comportamiento predeterminado de las actualizaciones de imagen de PvD de las siguientes maneras:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- La visibilidad de los archivos en el disco PvD
- Cómo se fusionan los cambios hechos en los archivos
- Si los archivos permiten escritura

Para obtener instrucciones detalladas sobre los archivos de reglas personalizadas y la función CoW, consulte los comentarios en los propios archivos, que se encuentran en C:\ProgramData\Citrix\personal vDisk\Config, en la VM donde está instalado PvD. Los archivos llamados "custom_*" describen las reglas y cómo habilitarlas.

Scripts de cambio de tamaño y poolstats

Se ofrecen dos scripts para supervisar y administrar el tamaño de los discos PvD; se encuentran en la carpeta Support\Tools\Scripts, en los medios de instalación de Citrix Virtual Apps and Desktops. También puede utilizar la herramienta Personal vDisk Image Update Monitoring Tool (herramienta de supervisión de actualizaciones de imagen de Personal vDisk), que se encuentra en la carpeta Support\Tools\Scripts\PvdTool. Para obtener más información, consulte http://blogs.citrix.com/2014/06/02/introducing-the-pvd-image-update-monitoring-tool/.

Use resize-personalvdisk-pool.ps1 para aumentar el tamaño de los discos PvD en todos los escritorios de un catálogo. Los siguientes complementos y módulos del hipervisor deben estar instalados en la máquina donde se ejecuta Studio:

- XenServer requiere XenServerPSSnapin
- vCenter requiere vSphere PowerCli
- System Center Virtual Machine Manager requiere la consola VMM

Use personal-vdisk-poolstats.ps1 para verificar el estado de las actualizaciones de imágenes y comprobar el espacio dedicado a aplicaciones y perfiles de usuarios en un grupo de escritorios con PvD. Ejecute este script antes de actualizar una imagen para comprobar si hay algún escritorio que esté quedándose sin espacio. Esto ayuda a prevenir errores durante el proceso de actualización. El script requiere que el firewall de Windows Management Instrumentation (WMI-In) esté habilitado en los escritorios con PvD. Puede habilitarlo en la imagen maestra o a través de un objeto de directiva de grupo (GPO).

Si una actualización de imagen falla, la entrada en la columna Update da información sobre el motivo del fallo.

Restablecer el área de aplicaciones

Si un escritorio queda dañado (después de instalar una aplicación defectuosa o por algún otro motivo), puede revertir el área de aplicaciones del disco PvD a su estado predeterminado de fábrica (vacío). La operación de restablecimiento deja intacta el área de datos de perfil de usuario.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para restablecer el área de aplicaciones del disco PvD, use alguno de estos métodos:

- Inicie una sesión como Administrador en el escritorio del usuario. Inicie un símbolo del sistema y ejecute el comando C:\Archivos de programa\Citrix\Personal vDisk\bin\CtxPvD.exe -s Reset.
- Busque el escritorio del usuario en Citrix Director. Haga clic en **Restablecer Personal vDisk** y, a continuación, en **Aceptar**.

Exportar e importar un inventario de PvD

El proceso de actualización de imagen forma parte de la implementación de imágenes nuevas en escritorios con PvD; este proceso incluye ajustar el disco Personal vDisk existente para que funcione con la nueva imagen base. En caso de implementaciones que usan Machine Creation Services (MCS), puede exportar el inventario de una VM activa a un punto compartido de red y, a continuación, importarlo en una imagen maestra. Se calcula un diferencial con este inventario en la imagen maestra. Aunque no sea obligatorio usar la función de exportación o importación de inventario, puede mejorar el rendimiento de todo el proceso de actualización de imágenes.

Para usar la función de importación o exportación de inventario, debe ser un administrador. Si es necesario, autentíquese con “net use” en el recurso compartido de archivos que se va a utilizar para la exportación o importación. El contexto de usuario debe ser capaz de acceder a los recursos compartidos de archivos utilizados para la importación o exportación.

- Para exportar un inventario, ejecute el comando de exportación como administrador en una máquina que contenga un VDA con PvD habilitado (versión mínima 7.6):

  Ctxpvdsvc.exe exportinventory “”

  El software detecta la ubicación del inventario actual y lo exporta a una carpeta denominada “ExportedPvdInventory” en la ubicación especificada. A continuación dispone de un fragmento del resultado del comando:

```
C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe
   exportinventory
\share location\ExportedInventory
Current inventory source location C:\CitrixPvD\Settings\Inventory
   \VER-LAS
...
Exporting current inventory to location \ ….
...
Deleting any pre-existing inventory folder at \ ….
.Successfully exported current inventory to location \ …. Error
   code = OPS
```

- Para importar un inventario ya exportado, ejecute el comando de importación como administrador en la imagen maestra:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para importar:

Ejecute el comando de importación como administrador en la imagen maestra.

```
Ctxpvdsvc.exe importinventory “<path-to-exported-inventory>”
```

La <path to exported inventory> debe ser la ruta completa a los archivos del inventario; suele ser <ubicación de red\ExportedPvdInventory>.

El inventario se obtiene a partir de la ubicación de importación (donde se exportó previamente mediante la opción exportinventory) y se importa al almacén de inventario de la imagen maestra. A continuación dispone de un fragmento del resultado del comando:

```
1 C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe
     importinventory
2 \share location\ExportedInventory\ExportedPvdInventory
3 Importing inventory \share location\ExportedInventory\
     ExportedPvdInventory
4 …
5 Successfully added inventory \share location\ExportedInventory\
     ExportedPvdInventory to the
6 store at c:\ProgramData\Citrix\personal vDisk\InventoryStore
```

Después de la exportación, el punto compartido de red debería contener los siguientes nombres de archivo. Después de la importación, el almacén de inventario ubicado en la imagen maestra debe contener los mismos nombres de archivo.

- Components.DAT
- files_rules
- folders_rules
- regkey_rules
- RINGTHREE.DAT
- S-1-5-18.DAT
- SAM.DAT
- SECURITY.DAT
- SNAPSHOT.DAT
- SOFTWARE.DAT
- SYSTEM.CurrentControlSet.DAT
- VDCATALOG.DAT
- vDiskJournalData

Pantallas, mensajes y solución de problemas

March 8, 2019

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Supervisar PvD a través de informes

Puede usar una herramienta de diagnóstico para supervisar los cambios hechos por los usuarios en ambas partes de los discos Personal vDisk (la parte dedicada a los datos de usuario y la parte dedicada a aplicaciones). Estos cambios incluyen las aplicaciones que los usuarios han instalado y los archivos que han modificado. Los cambios se almacenan en un conjunto de informes.

1. En la máquina que quiere supervisar, ejecute `C:\\Program Files\\Citrix\\personal vDisk\\bin\\CtxPvdDiag.exe`.
2. Vaya a la ubicación donde almacenar los registros e informes, seleccione los informes a generar y haga clic en **Aceptar**. A continuación, se ofrece una lista de los informes disponibles.

Informe del subárbol Software: Este informe genera dos archivos: `Software.Dat.Report.txt` y `Software.Dat.delta.txt`.

El archivo `Software.Dat.Report.txt` registra los cambios que haya realizado el usuario en el subárbol HKEY_LOCAL_MACHINE\Software. Contiene las siguientes secciones:

- Lista de aplicaciones instaladas en la base: Aplicaciones instaladas en la capa 0.
- Lista de software instalado por el usuario: Aplicaciones que el usuario ha instalado en la parte de aplicaciones del disco Personal vDisk.
- Lista de software desinstalado por el usuario: Aplicaciones originalmente presentes en la capa 0 que el usuario ha quitado.

Consulte el informe delta de subárbol para obtener información acerca de Software.Dat.delta.txt.

Informe del subárbol System: El archivo generado SYSTEM.CurrentControlSet.DAT.Report.txt registra los cambios que haya realizado el usuario en el subárbol HKEY_LOCAL_MACHINE\System. Contiene las siguientes secciones:

- Lista de servicios instalados por el usuario: Servicios y controladores que haya instalado el usuario.
- Se han cambiado los inicios de los siguientes servicios: Servicios y controladores cuyo tipo de inicio haya modificado el usuario.

Informe del subárbol Security: El archivo generado SECURITY.DAT.Report.txt supervisa todos los cambios que el usuario realiza en el subárbol HKEY_LOCAL_MACHINE\Security.

Informe del subárbol Security Account Manager (SAM): El archivo generado SAM.DAT.Report.txt supervisa todos los cambios que el usuario realiza en el subárbol HKEY_LOCAL_MACHINE\SAM.

Informe delta de subárbol: El archivo generado Software.Dat.delta.txt registra todos los valores y claves de Registro que se hayan agregado o quitado, así como todos los valores que haya modificado el usuario en el subárbol HKEY_LOCAL_MACHINE\Software.

Registros de Personal vDisk: De forma predeterminada, los archivos de registro Pud-IvmSupervisor.log, PvDActivation.log, PvDSvc.log, PvDWMI.log, SysVol-IvmSupervisor.log y vDeskService-<#>.log se

© 1999-2019 Citrix Systems, Inc. All rights reserved.

generan en P:\Usuarios\<cuenta de usuario>\AppData\Local\Temp\PVDLOGS, aunque se transfieren a la ubicación seleccionada.

Registros del sistema operativo Windows:

- EvtLog_App.xml y EvtLog_System.xml son los registros de eventos del sistema y de la aplicación en formato XML del volumen del disco Personal vDisk.
- Setupapi.app.log y setuperr.log contienen mensajes registrados en la ejecución de msiexec.exe durante la instalación del disco Personal vDisk.
- Setupapi.dev.log contiene los mensajes del registro de la instalación de dispositivo.
- Msinfo.txt contiene la salida de msinfo32.exe. Para obtener información, consulte la documentación de Microsoft.

Informe del sistema de archivos: El archivo generado FileSystemReport.txt registra los cambios que haya realizado el usuario en el sistema de archivos. Se divide en las siguientes secciones:

- Archivos reubicados: Archivos de la capa 0 que el usuario ha transferido al disco Personal vDisk. Los archivos de la capa 0 son aquellos que la máquina a la que está vinculado el disco Personal vDisk hereda de la imagen maestra.
- Archivos eliminados: Archivos de la capa 0 que se han ocultado por una acción del usuario (por ejemplo, al eliminar una aplicación).
- Archivos agregados (MOF, INF, SYS): Archivos con las extensiones .mof, .inf o .sys que el usuario ha agregado al disco Personal vDisk (por ejemplo, al instalar una aplicación, como Visual Studio 2010, que registra un archivo .mof para la autorrecuperación).
- Otros archivos agregados: Otros archivos que el usuario ha agregado al disco Personal vDisk (por ejemplo, al instalar una aplicación).
- Archivos base modificados pero no reubicados: Archivos de la capa 0 que el usuario ha modificado, pero que los controladores modo kernel del disco Personal vDisk no han capturado en el disco Personal vDisk.

Actualizaciones de imagen

En Studio, al elegir una máquina con Personal vDisk (PvD) habilitado de un catálogo de máquinas, la ficha “PvD” muestra el estado de la supervisión y el progreso y la hora de finalización estimados de las actualizaciones de imagen. Los estados que pueden aparecer durante una actualización de imagen son: Ready, Preparing, Waiting, Failed y Requested.

El proceso de actualización de una imagen puede fallar por diversos motivos, incluidos la falta de espacio o que el escritorio no encuentre el disco PvD a tiempo. Cuando Studio indica que un proceso de actualización de imagen no se ha podido realizar, aparece un código de error con texto descriptivo para ayudar a solucionar el problema. Use la herramienta Personal vDisk Image Update Monitoring Tool (herramienta de supervisión de actualizaciones de imagen de Personal vDisk) o el script personal-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

vdisk-poolstats.ps1 para supervisar el progreso de actualización de imagen y obtener los códigos de error asociados al fallo pertinente.

Si una actualización de imagen no llega a completarse, los siguientes archivos de registro pueden proporcionar más información para la solución de problemas:

- Registro del servicio de PvD: C:\ProgramData\Citrix\personal vDisk\Logs\PvDSvc.log.txt
- Registro de activación de PvD: P:\PVDLOGS\PvDActivation.log.txt

El contenido más reciente se encuentra al final del archivo de registro.

Mensajes de error: 7.6 y versiones posteriores

Los siguientes errores son válidos para PvD 7.6 y versiones posteriores:

- **Error interno. Revise los registros de Personal vDisk para obtener más información. Código de error %d (%s)**

  Este es un comodín para todos los errores sin clasificar, por lo que no tiene ningún valor numérico. Todo error inesperado que haya ocurrido durante la creación de inventario o una actualización de Personal vDisk se indica con este código de error.

  - Recopile los registros y póngase en contacto con la asistencia técnica de Citrix.
  - Si este error se produce durante una actualización de catálogo, revierta el catálogo a la versión anterior de la imagen maestra.

- **Los archivos de reglas contienen errores de sintaxis. Revise los registros para obtener más información.**

  Código de error 2. El archivo de reglas contiene errores de sintaxis. El archivo de registro de Personal vDisk contiene el nombre del archivo de reglas y el número de línea referentes al error de sintaxis encontrado. Corrija el error de sintaxis en el archivo de reglas y vuelva a intentar la operación.

- **El inventario almacenado en el disco Personal vDisk correspondiente a la versión anterior de la imagen maestra está dañado o no se puede leer.**

  Código de error 3. El inventario más reciente se guarda en "UserData.V2.vhd" en "\ProgramData\CitrixPvD\Se
  LAST". Restaure el inventario que corresponde a la última versión de la imagen maestra. Puede hacerlo si importa la carpeta 'VER-LAST' desde una máquina con PvD conocida que funcione y que esté asociada a la versión anterior de la imagen maestra.

- **El inventario almacenado en el disco Personal vDisk correspondiente a la versión anterior de la imagen maestra es de una versión posterior.**

  Código de error 4. Este conflicto se debe a incompatibilidades de versión de Personal vDisk entre la última imagen maestra y la imagen maestra actual. Intente actualizar el catálogo después de instalar la última versión de Personal vDisk en la imagen maestra.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Se ha detectado un desbordamiento del diario de cambios.**

  Código de error 5. Se ha producido un desbordamiento del diario USN porque se ha efectuado un gran número de cambios a la imagen maestra cuando se creaba el inventario. Si este problema sigue produciéndose después de varios intentos, use procmon para determinar si el software de terceros está creando o eliminando un gran número de archivos durante la creación del inventario.

- **Personal vDisk no ha podido encontrar ningún disco conectado al sistema para el almacenamiento de los datos de usuario.**

  Código de error 6. En primer lugar, compruebe que el disco PvD está conectado a la máquina virtual a través de la consola del hipervisor. Este error suele ocurrir debido al software de "prevención de pérdida de datos", el cual impide el acceso al disco PvD. Si el disco PvD está conectado a la VM, intente agregar una excepción para el "disco conectado" a la configuración del software de "prevención de pérdida de datos".

- **El sistema no se ha reiniciado después de la instalación. Reinicie para implementar los cambios.**

  Código de error 7. Reinicie el escritorio y vuelva a intentar la operación.

- **Instalación dañada. Intente volver a instalar Personal vDisk.**

  Código de error 8. Instale Personal vDisk e inténtelo de nuevo.

- **El inventario de Personal vDisk no está actualizado. Actualice el inventario en la imagen maestra y, a continuación, inténtelo de nuevo.**

  Código de error 9. El inventario de Personal vDisk no se ha actualizado en la imagen maestra antes de apagar el escritorio. Reinicie la imagen maestra y apague el escritorio por medio de la opción "Actualizar Personal vDisk" y, a continuación, cree una nueva instantánea; utilice esa instantánea para actualizar el catálogo.

- **Se ha producido un error interno durante el inicio de Personal vDisk. Revise los registros de Personal vDisk para obtener más información.**

  Código de error 10. Esto puede deberse a que el controlador de PvD no haya podido iniciar una sesión de virtualización a raíz de un error interno o a que Personal vDisk está dañado. Intente reiniciar el escritorio a través del Controller. Si el problema persiste, recopile los registros y póngase en contacto con la asistencia técnica de Citrix.

- **Se ha agotado el tiempo de espera de Personal vDisk cuando intentaba encontrar un disco para almacenar los parámetros de personalización de los usuarios.**

  Código de error 11. Este error se produce cuando el controlador de PvD no puede encontrar el disco PvD en 30 segundos después del reinicio. Esto suele deberse a un tipo de controlador

© 1999-2019 Citrix Systems, Inc. All rights reserved.

SCSI incompatible o a una latencia de almacenamiento. Si esto ocurre con todos los escritorios del catálogo, cambie el tipo de controlador SCSI asociado a la "VM de plantilla" o a la "VM maestra" por un tipo compatible con la tecnología de Personal vDisk. Si esto ocurre con solo algunos escritorios del catálogo, es posible que se deba a picos de latencia de almacenamiento causados por una gran cantidad de escritorios que se inician al mismo tiempo. Intente limitar el parámetro de número máximo de acciones de energía activo asociado a la conexión de host.

- **Personal vDisk se ha desactivado porque se ha detectado un apagado no seguro del sistema. Reinicie la máquina.**

  Código de error 12. Esto puede deberse a un escritorio que no haya podido completar el proceso de arranque con PvD habilitado. Intente reiniciar el escritorio. Si el problema persiste, vea el inicio del escritorio por medio de la consola del hipervisor y, allí, compruebe si el escritorio se bloquea. Si el escritorio se bloquea durante el inicio, restaure PvD a partir de la copia de seguridad (si dispone de una copia) o bien restablezca PvD.

- **La letra de unidad especificada para montar Personal vDisk no está disponible.**

  Código de error 13. Esto puede deberse a que Personal vDisk no puede montar el disco PvD en el punto de montaje especificado por el administrador. El disco PvD no se podrá montar si otro hardware ya utiliza la letra de unidad. Seleccione otra letra como punto de montaje para Personal vDisk.

- **Los controladores de modo kernel de Personal vDisk no se han podido instalar.**

  Código de error 14. Personal vDisk instala controladores durante la primera actualización de inventario que se realiza después de la instalación. Algunos productos antivirus impiden la instalación del controlador cuando esta instalación tiene lugar fuera del contexto de un instalador. Inhabilite temporalmente el análisis en tiempo real del antivirus o bien agregue excepciones al antivirus para los controladores de PvD durante la creación del primer inventario.

- **No se puede crear una instantánea del volumen del sistema. Compruebe que el Servicio de instantáneas de volumen esté habilitado.**

  Código de error 15. Esto puede suceder porque el Servicio de instantáneas de volumen está inhabilitado. Habilite el Servicio de instantáneas de volumen e intente seleccionar un inventario de nuevo.

- **El diario de cambios no se ha podido activar. Inténtelo de nuevo después de esperar unos minutos.**

  Código de error 16. Personal vDisk utiliza el diario de cambios para realizar un seguimiento de los cambios efectuados en la imagen maestra. Durante una actualización de inventario, si PvD detecta que el diario de cambios está inhabilitado, intenta habilitarlo; este error se produce cuando ese intento falla. Espere unos minutos y vuelva a intentarlo.

- **No hay suficiente espacio disponible en el volumen del sistema.**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Código de error 17. No hay suficiente espacio disponible en la unidad C: del escritorio para la actualización de imagen. Amplíe el volumen del sistema o quite archivos no utilizados para liberar espacio en él. La actualización de la imagen deberá volver a comenzar tras el próximo reinicio.

- **No hay suficiente espacio disponible en el almacenamiento de Personal vDisk. Expanda el almacenamiento de Personal vDisk para proporcionar más espacio.**

  Código de error 18. No hay suficiente espacio disponible en la unidad de Personal vDisk cuando se realiza una actualización de imagen. Expanda el almacenamiento de Personal vDisk o elimine archivos no utilizados para liberar espacio en el disco de almacenamiento de Personal vDisk. La actualización de imagen debería volver a iniciarse tras el próximo reinicio.

- **La unidad de almacenamiento de Personal vDisk tiene demasiadas confirmaciones. Expanda el almacenamiento de Personal vDisk para proporcionar más espacio.**

  Código de error 19. No hay suficiente espacio disponible en la unidad de Personal vDisk para que quepa el disco de aprovisionamiento pesado "UserData.V2.vhd". Expanda el almacenamiento de Personal vDisk o elimine archivos no utilizados para liberar espacio en el disco de almacenamiento de Personal vDisk.

- **Registro del sistema dañado.**

  Código de error 20. El Registro del sistema está dañado, es ilegible o no se puede encontrar. Restablezca Personal vDisk o restáurelo a partir de una copia de seguridad anterior.

- **Se ha producido un error interno durante el restablecimiento de Personal vDisk. Revise los registros de Personal vDisk para obtener más información.**

  Código de error 21. Este es un comodín para todos los errores detectados durante un restablecimiento de Personal vDisk. Recopile los registros y póngase en contacto con la asistencia técnica de Citrix.

- **No se ha podido restablecer Personal vDisk porque no hay suficiente espacio libre en el disco de almacenamiento de Personal vDisk.**

  Código de error 22. No hay suficiente espacio disponible en la unidad de Personal vDisk al realizar una operación de restablecimiento. Expanda el almacenamiento de Personal vDisk o elimine archivos no utilizados para liberar espacio en el disco de almacenamiento de Personal vDisk.

Mensajes de error: versiones anteriores a 7.6

Los siguientes errores son válidos para versiones de PvD 7.x anteriores a 7.6:

- **No se pudo iniciar. Personal vDisk no ha podido encontrar el disco para almacenar los parámetros de personalización de usuario.**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

El software de PvD no pudo encontrar el disco Personal vDisk (de manera predeterminada, la unidad P:) o no pudo montarlo como el punto de montaje seleccionado por el administrador cuando se creó el catálogo.

- Compruebe los registros del servicio de PvD para ver si contienen la entrada: “PvD 1 status –> 18:183”.
- Si está usando una versión de PvD anterior a la versión 5.6.12, resolverá el problema actualizando a la versión más reciente.
- Si está usando la versión 5.6.12 o posterior, use la herramienta de administración de discos (diskmgmt.msc) para determinar si la unidad P: está presente como volumen sin montar. Si está presente, ejecute chkdsk en el volumen para determinar si está dañado e intente recuperarlo usando chkdsk.

- **No se pudo iniciar. Citrix Personal vDisk no se ha podido iniciar. Para obtener ayuda... Código de estado: 7, código de error: 0x70.**

  El código de estado 7 implica que se encontró un error al intentar actualizar el disco PvD. El error puede ser uno de los siguientes:

Código de error	Description
0x20000001	No se pudo guardar el paquete de diferenciación (diff), seguramente debido a que no hay suficiente espacio en disco libre en el VHD.
0x20000004	No se pudo obtener los privilegios requeridos para actualizar el PvD.
0x20000006	No se pudo cargar una sección de la imagen del PvD o del inventario de PvD, seguramente debido a que la imagen o el inventario están dañados.
0x20000007	No se pudo cargar el inventario de sistema de archivos, seguramente debido a que la imagen o el inventario de PvD están dañados.
0x20000009	No se pudo abrir el archivo que contiene el inventario de sistema de archivos, seguramente debido a que la imagen o el inventario de PvD están dañados.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Código de error	Description
0x2000000B	No se pudo guardar el paquete de diferenciación (diff), seguramente debido a que no hay suficiente espacio en disco libre en el VHD.
0x20000010	No se pudo cargar el paquete de diferenciación.
0x20000011	Faltan archivos de reglas.
0x20000021	Inventario de PvD dañado.
0x20000027	El catálogo “MojoControl.dat” está dañado.
0x2000002B	Falta el inventario de PvD, o está dañado.
0x2000002F	No se pudo registrar un archivo MOF instalado por el usuario en la actualización de la imagen. Actualice el software a la versión 5.6.12 para solucionar el problema.
0x20000032	Consulte PvDactivation.log.txt para ver la entrada de registro más reciente que contenga un código de error Win32.
0x20	No se pudo montar el contenedor de aplicaciones para la actualización de la imagen. Actualice el software a la versión 5.6.12 para solucionar el problema.
0x70	No hay espacio suficiente en el disco.

- **No se pudo iniciar. Citrix Personal vDisk no se ha podido iniciar [o se ha producido un error interno en Personal vDisk]. Para obtener ayuda... Código de estado: 20, código de error: 0x20000028.**

  Se ha encontrado Personal vDisk, pero no se ha podido crear una sesión de PvD.

  Recopile los registros y compruebe SysVol-IvmSupervisor.log para ver la creación de sesiones no realizadas:

  1. Compruebe si existe la entrada “ IvmpNativeSessionCreate: failed to create native session, status XXXXX”.
  2. Si el estado es 0xc00002cf, solucione el problema agregando una nueva versión de la imagen maestra al catálogo. Este código de estado implica que el diario USN se saturó debido a una gran cantidad de cambios realizados después de una actualización de inventario.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

3. Reinicie el escritorio virtual afectado. Si el problema continúa, póngase en contacto con la asistencia técnica de Citrix.

- **No se pudo iniciar. Citrix Personal vDisk se ha desactivado porque se ha detectado un apagado no seguro del sistema. Para volver a intentarlo, seleccione Reintentar. Si el problema continúa, póngase en contacto con el administrador del sistema.**

  La VM agrupada no puede iniciarse completamente con PvD habilitado. Primero determine por qué no se puede completar el proceso de inicio. Los motivos posibles por los que aparece una pantalla azul son los siguientes:

  - La imagen maestra contiene un producto antivirus incompatible. Por ejemplo: versiones antiguas de Trend Micro.
  - El usuario ha instalado software que es incompatible con PvD. Es poco probable, pero puede comprobarlo si agrega una nueva máquina al catálogo y verifica si la VM se reinicia correctamente.
  - La imagen de PvD está dañada. Esto se ha observado en la versión 5.6.5.

  Para comprobar si la VM agrupada está mostrando una pantalla azul o se está reiniciando prematuramente:

  - Inicie sesión en la máquina por medio de la consola del hipervisor.
  - Haga clic en Reintentar y espere a que la máquina se apague.
  - Inicie la máquina mediante Studio.
  - Use la consola del hipervisor para observar el inicio de la consola de la máquina.

  Otras soluciones:

  - Obtenga un volcado de memoria de la máquina que muestra una pantalla azul y envíelo al servicio de asistencia técnica Citrix Technical Support para su análisis.
  - Compruebe si hay errores en los registros de eventos asociados a PvD:
    1. Monte UserData.V2.vhd desde el directorio raíz de la unidad P:, haciendo clic en Acción > Exponer VHD en DiskMgmt.msc.
    2. Inicie Eventvwr.msc.
    3. Abra el registro de eventos de sistema (Windows\System32\winevt\logs\system.evtx) desde UserData.V2.vhd haciendo clic en Acción > Abrir registro guardado.
    4. Abra el registro de eventos de aplicación (Windows\System32\winevt\logs\application.evtx) desde UserData.V2.vhd haciendo clic en Acción > Abrir registro guardado.

- **Personal vDisk no se puede iniciar. Personal vDisk no se ha podido iniciar porque el inventario no se ha actualizado. Actualice el inventario en la imagen maestra e inténtelo de nuevo. Código de estado: 15, código de error: 0x0.**

  El administrador seleccionó una instantánea incorrecta al crear o al actualizar el catálogo de PvD (es decir, la imagen maestra no se apagó usando Actualizar Personal vDisk cuando se creó la instantánea).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Eventos registrados por Personal vDisk

Si Personal vDisk no está habilitado, puede ver los siguientes eventos en el Visor de eventos de Windows. Seleccione el nodo Aplicaciones en el panel de la izquierda; el Origen de los sucesos en el panel derecho es Citrix Personal vDisk. Si Personal vDisk está habilitado, no se muestra ninguno de estos eventos.

El ID de evento 1 indica un mensaje informativo, un ID de evento 2 indica un error. Es posible que no se usen todos los eventos en cada versión de Personal vDisk.

ID de suceso	Description
1	Estado de Personal vDisk: Se ha iniciado la actualización del inventario.
1	Estado de Personal vDisk: Se ha completado la actualización del inventario. GUID: %s.
1	Estado de Personal vDisk: Se ha iniciado la actualización de la imagen.
1	Estado de Personal vDisk: Se ha completado la actualización de la imagen.
1	Restablecimiento en curso.
1	Aceptar.
2	Estado de Personal vDisk: Ha fallado la actualización del inventario con el error: %s.
2	Estado de Personal vDisk: Ha fallado la actualización de la imagen con el error: %s.
2	Estado de Personal vDisk: Ha fallado la actualización de la imagen con un error interno.
2	Estado de Personal vDisk: Ha fallado la actualización del inventario con un error interno.
2	Personal vDisk se ha inhabilitado debido a un apagado inapropiado.
2	La actualización de la imagen falló. Código de error %d.
2	Personal vDisk encontró un error interno. Código de estado[%d], código de error[0x%X].

© 1999-2019 Citrix Systems, Inc. All rights reserved.

ID de suceso	Description
2	El restablecimiento de Personal vDisk falló.
2	No se encuentra el disco para almacenar los parámetros de personalización de usuario.
2	No hay suficiente espacio disponible en el disco de almacenamiento para crear un contenedor de Personal vDisk.

Migrar Personal vDisk a App Layering

March 13, 2019

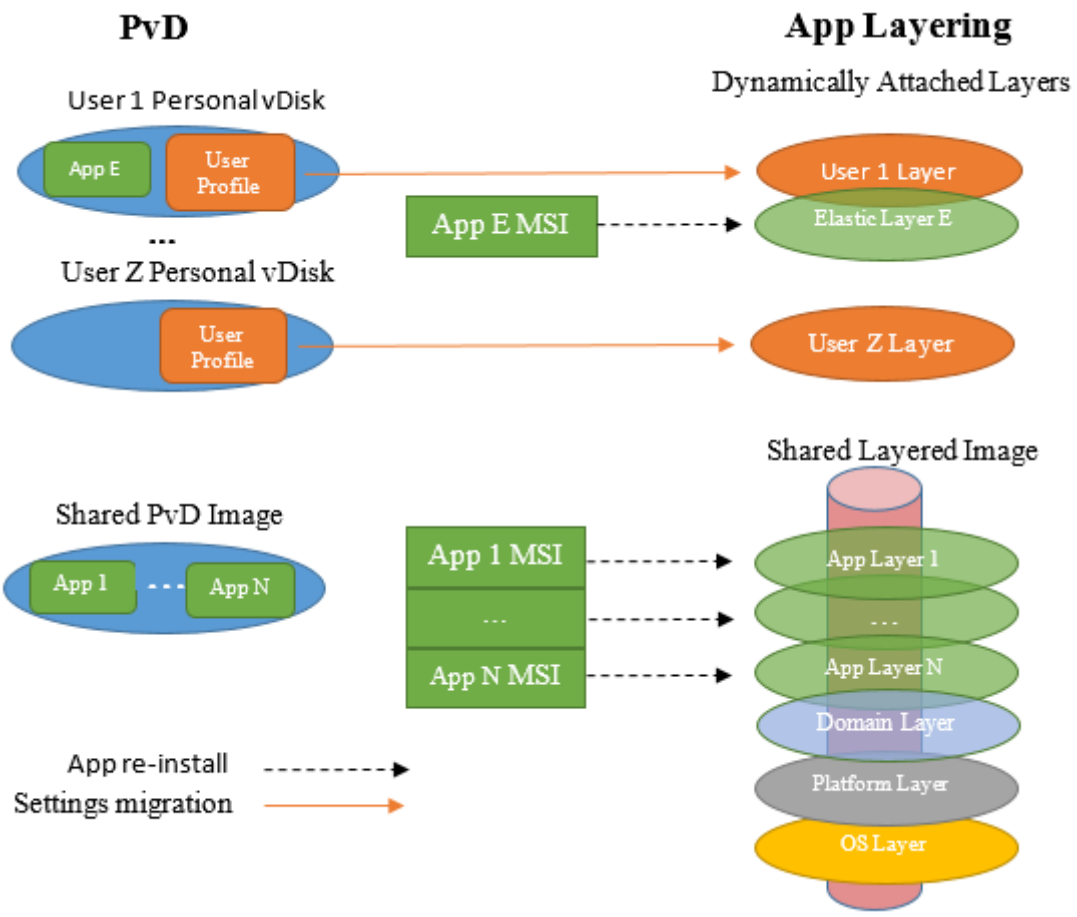
Citrix está reemplazando la funcionalidad Personal vDisk (PvD) por la tecnología Citrix App Layering. Utilice la información de este artículo para crear una máquina virtual (VM) de App Layering que sea equivalente en funciones a una VM basada en PvD.

Para obtener información acerca de las capas y el proceso de creación y publicación de plantillas de imagen, consulte la documentación de Citrix App Layering.

Las máquinas virtuales típicas de PvD constan de una imagen compartida y un disco virtual personal. La imagen compartida se distribuye a varios usuarios, cada uno de ellos con su propio disco Personal vDisk. Una máquina virtual típica de App Layering consta de varias capas: una capa de sistema operativo, una capa de plataforma y, por lo general, una o varias capas de aplicaciones. Esta VM se comparte entre varios usuarios, cada uno con su propia capa de usuario (User Layer).

Al migrar un conjunto de usuarios que comparten una VM con imagen PvD, se crea una VM de imagen compartida de App Layering con funciones equivalentes. Cada usuario dispone de su perfil y sus parámetros personales migrados desde su disco Personal vDisk a su nueva capa de usuario en App Layering, como se ilustra en la siguiente imagen:

© 1999-2019 Citrix Systems, Inc. All rights reserved.



En este artículo se adopta un enfoque para migrar los datos personales de un usuario y otro enfoque para migrar las aplicaciones. Para los datos personales, en este artículo se recomienda utilizar herramientas para copiarlos desde un disco Personal vDisk a una capa de usuario. En cambio, para las aplicaciones, no se recomienda copiarlas. En vez de ello, se recomienda que las aplicaciones se reinstalen en una capa de aplicaciones (App Layer). Además, en este artículo se asume:

- que la VM de PvD ejecuta Windows 7. La migración desde otras versiones de sistema operativo debería ser similar si App Layering las admite. Por ejemplo, App Layering no admite Windows XP.
- XenServer se utiliza como hipervisor, por lo que se asume que está familiarizado con la administración de éste mediante XenCenter.
- Se utiliza Machine Creation Services (MCS) o Citrix Provisioning (antes Provisioning Services) para el aprovisionamiento. Para MCS o Citrix Provisioning, necesitará la imagen ISO de Citrix Virtual Apps and Desktops. Para Citrix Provisioning, necesitará “ProvisioningServicesxxx.iso”.
- Se usa Citrix Virtual Desktops para administrar las máquinas virtuales generadas de App Layering.

Si utiliza otro hipervisor o servicio de aprovisionamiento, los procedimientos de migración indicados

© 1999-2019 Citrix Systems, Inc. All rights reserved.

en este artículo son similares.

En los ejemplos de este artículo se presupone que el usuario es miembro de un dominio de Active Directory (AD).

Personal vDisk y App Layering

App Layering facilita una separación clara entre las aplicaciones y la información específica del usuario. Las aplicaciones se encuentran en las capas de aplicaciones (App Layer), a menudo con una aplicación por capa, mientras que la información específica del usuario se encuentra en una capa de usuario (User Layer). Se recomienda que un usuario no instale una aplicación en su capa de usuario si cree que la aplicación puede ser de utilidad general. En vez de ello, el usuario puede instalarla en una capa elástica de aplicaciones (Elastic App Layer), que se uniría dinámicamente a sus máquinas virtuales (y a otras) cuando ese usuario iniciara sesión.

PvD no admite esta separación clara porque solo tiene dos capas: la imagen compartida (compartida entre varios usuarios) y un disco virtual específico del usuario. Los usuarios a menudo instalan una aplicación en su disco Personal vDisk si no está disponible en la imagen compartida.

Al migrar una imagen PvD compartida a App Layering, debe determinar todas las aplicaciones que contiene. Para cada aplicación (o un conjunto relacionado de aplicaciones) debe crear una capa de aplicaciones. Se deben tener en cuenta las siguientes cuestiones:

- Si la aplicación es de utilidad general, debe adjuntar la capa de aplicaciones a una plantilla de imagen desde la que esa aplicación se publicará en una imagen en capas (Layered Image).
- Si la aplicación es útil solo para un grupo de usuarios, debe asignarla a ese grupo. Así, cuando los miembros de ese grupo inicien sesión en la máquina virtual, esa aplicación se adjuntará dinámicamente en una capa elástica de aplicaciones.
- Si la aplicación resulta útil solamente para un usuario, debe instalarla en la capa de ese usuario.

Otros elementos de App Layering

En el proceso de creación de una VM de App Layering, se crean algunos elementos (máquinas virtuales de empaquetado, conectores, agentes y plantillas de máquinas virtuales). Estos elementos son exclusivos de App Layering y se describen brevemente en las siguientes secciones. Para obtener una descripción completa, consulte la documentación de App Layering.

Máquinas virtuales de empaquetado

El método de App Layering para personalizar el contenido de las capas de plataformas y las capas de aplicaciones consiste en crear una *VM de empaquetado* (Packaging VM), a veces denominada *máquina de instalación* (Install Machine). Crear una capa es un proceso de seis pasos:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

1. Desde Enterprise Layer Manager (ELM), cree la capa, y especifique su nombre, entre otros datos.
2. ELM genera una máquina virtual de empaquetado y la copia (normalmente) al hipervisor.
3. Desde el hipervisor, inicie la VM de empaquetado y personalícela.
4. Cuando haya terminado la personalización, haga clic en el icono **Shutdown to Finalize** (Cerrar para finalizar), que está en el escritorio de la VM de empaquetado. Esta acción realiza una comprobación de integridad de la capa, lo que garantiza que no haya reinicios pendientes y que ngen no se está ejecutando. No termina hasta que todas estas tareas estén completas.
5. Desde ELM, haga clic en la acción **Finalize**.
6. ELM termina la generación de la capa en función de la VM de empaquetado personalizada y elimina esa VM de empaquetado.

App Layering no usa una VM de empaquetado para crear la capa de sistema operativo. En vez de ello, usted crea una VM, la personaliza según sea necesario y ELM la importa.

Conectores y agentes

El ELM se comunica con varias entidades, como hipervisores, recursos compartidos de archivos y herramientas de aprovisionamiento. Realiza diversas tareas en esas entidades, como la creación de máquinas virtuales, lo que implica copiar diversos tipos de datos, como VHD y archivos, hacia o desde esas entidades.

Un conector es un objeto que ELM utiliza cuando se comunica con otra entidad para realizar un conjunto de tareas. Está configurado con el nombre o la dirección IP de la otra entidad, las credenciales necesarias para acceder a esa entidad y cualquier otra información requerida para realizar las tareas. Por ejemplo, una ruta de archivo en la entidad donde se leen o escriben los datos.

Los siguientes elementos son conectores:

- Conector de XenServer: ELM utiliza este conector para crear o eliminar máquinas virtuales, como las máquinas virtuales de empaquetado, que haya en XenServer.
- Conector de archivos compartidos de red (Network File Share Connector): Este conector se configura desde la ficha “System”, la subficha “Settings and Configurations”, en la sección “Network File Share”. ELM y las VM utilizan este proceso para crear archivos en un recurso compartido de archivos de red.
- Citrix MCS para el conector de XenServer: Si utiliza MCS como servicio de aprovisionamiento, se crea este conector. ELM lo usa para copiar las imágenes en capas a XenServer después de eliminar los controladores que MCS no necesita.
- Citrix Provisioning Connector: Si utiliza Citrix Provisioning como servicio de aprovisionamiento, se crea este conector. ELM lo usa para copiar el VHD de imagen en capas al servidor de Citrix Provisioning. Crea un disco virtual allí después de eliminar los controladores no requeridos por Citrix Provisioning.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Plantilla de VM

Si utiliza XenServer como hipervisor, se crea una plantilla de VM basada en la capa de SO que tenga la VM. Esta plantilla contiene información sobre el sistema operativo, como las interfaces de red y la cantidad de procesadores. La plantilla es creada después de que su capa de sistema operativo se haya creado. Se utiliza cuando se crea un conector XenServer.

Instalar Unidesk Agent en el servidor Citrix Provisioning

Si implementa con Citrix Provisioning, debe instalar Unidesk Agent en el servidor Citrix Provisioning. Eso permite que ELM ejecute comandos en el servidor Citrix Provisioning.

Consulte “Install the App Layering Agent (required for Citrix Provisioning and Connector Scripts)” (Instalar el agente de App Layering, requerido para Citrix Provisioning y Connector Scripts) en la documentación de App Layering.

Migrar imágenes compartidas

Para migrar una imagen PvD compartida a App Layering, debe crear una imagen compartida en capas (Shared Layered Image) que tenga funciones equivalentes a la imagen PvD compartida. La imagen compartida en capas se construye publicando una plantilla de imagen. La plantilla de imagen combina una capa de sistema operativo, una capa de plataforma y una o varias capas de aplicaciones. Deberá crear cada una de esas capas. Estos procedimientos se describen en las siguientes secciones.

Capa de SO

Lleve a cabo estos pasos para crear una capa de sistema operativo.

Desde XenCenter:

Cree una VM en XenServer. Esta es la base para su capa de SO y su plantilla de VM.

La versión de SO de la máquina virtual debe coincidir con la de la imagen PvD compartida que está migrando. En estas instrucciones, se presupone que ejecuta Windows 7.

Desde la VM de la capa de SO:

Inicie sesión con la cuenta de administrador local.

Instale todas las actualizaciones importantes de Windows.

Realice las tareas de preparación descritas en “Preparar una imagen de Windows 7”, en la documentación de App Layering.

Desde XenCenter:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Haga una copia de la VM de la capa de SO. Elimine todo el almacenamiento local. Convierta la VM a una plantilla. Debe utilizar esta plantilla de VM cuando cree un conector de XenServer.

Desde ELM:

En la ficha **Layers**, haga clic en **Create OS Layer**.

Si utiliza XenServer y aún no ha creado ningún conector de XenServer, deberá hacerlo ahora. Cuando se le solicite la plantilla de máquina virtual (Virtual Machine Template), especifique la plantilla de VM que creó en la sección anterior.

Cuando se le solicite seleccionar la máquina virtual (Select Virtual Machine), elija su VM de capa de sistema operativo.

Después de asignar un icono y especificar cualquier otra información detallada, haga clic en "Create Layer". Esto copia su VM de capa de sistema operativo a la tienda de ELM y generará su capa de sistema operativo.

Con ello, se completa la creación de la capa de SO y esa capa se puede implementar.

Capa de plataforma

Una vez generada la capa de SO, puede continuar con la creación de una capa de plataforma para la imagen compartida.

Un paso en el proceso de personalización de la capa de plataforma es unirse al dominio de Active Directory de los usuarios. Si los usuarios son miembros de varios dominios, debe crear una capa de plataforma por separado para cada dominio. En este artículo se asume que todos los usuarios pertenecen a un solo dominio.

Desde ELM:

1. En la ficha **Layers**, haga clic en **Create Platform Layer**.
2. En el panel "OS Layers", seleccione la capa de SO que creó en la sección anterior.
3. En el panel "Connector", seleccione el conector de XenServer que creó en la sección anterior. ELM utiliza esta información cuando escribe la VM de empaquetado de la capa de plataforma en XenServer.
4. En el panel "Platform Types", marque "This platform will be used for publishing Layered Images" (Esta plataforma se utilizará para publicar imágenes en capas).
5. Elija el hipervisor apropiado. En este artículo, se presupone que utiliza "Citrix XenServer".
6. Elija el servicio de aprovisionamiento apropiado. Se asume que utiliza "Citrix MCS" o "Citrix PVS" (si usa Citrix Provisioning).
7. Para el broker de conexión, seleccione "Citrix XenDesktop".

Después de asignar un icono y especificar cualquier otra información detallada, haga clic en **Create Layer**. Esta acción genera una VM de empaquetado de capa de plataforma. Una vez completado, el

© 1999-2019 Citrix Systems, Inc. All rights reserved.

estado de la tarea de creación indica “Action Required” (Acción requerida).

Desde XenCenter:

Una vez generada su VM de empaquetado de capa de plataforma, aparece en XenCenter. Lleve a cabo lo siguiente:

1. Arránquela.
2. Desde su VM de empaquetado de capa de plataforma, inicie sesión con la cuenta de administrador local.
3. Si se le solicita, reinicie e inicie sesión de nuevo.
4. Únase al dominio de Active Directory de los usuarios de la forma habitual. Es decir, **Panel** de **control > sistema > cambiar parámetros \ > cambiar**. Reinicie y vuelva a iniciar sesión con la cuenta de administrador local.

Instale el agente Citrix Virtual Delivery Agent (VDA):

1. Monte la ISO de Citrix Virtual Apps and Desktops.
2. Ejecute “AutoSelect.exe” si no se inicia automáticamente.
3. Haga clic en **Iniciar** junto a Citrix Virtual Desktops.
4. Haga clic en **Virtual Delivery Agent para SO de escritorio Windows**.

   En general, elija los valores predeterminados en los siguientes paneles de opciones. Sin embargo:

   - Puede especificar su Delivery Controller cuando se le solicite, o indique “Do It Later (Advanced)”.
   - Compruebe que “Personal vDisk” no esté seleccionado.

   Después de instalarse el VDA, se reinicia la VM de empaquetado de capa de plataforma.

Vuelva a iniciar sesión.

Si utiliza Citrix Provisioning como servicio de aprovisionamiento, también debe instalar el software del dispositivo de destino. Para hacerlo:

1. Monte “ProvisionServicesxxx.iso”.
2. Ejecute “AutoSelect.exe” si no se inicia automáticamente.
3. Haga clic en “Target Device Installation”.
4. Haga clic nuevamente en “Target Device Installation” para iniciar el asistente de instalación. El instalador instala Citrix Diagnostics Facility (CDF) y el código del dispositivo de destino de Citrix Provisioning Service.
5. En general, elija los valores predeterminados en los siguientes paneles de opciones.
6. Cuando el asistente de instalación finalice, desmarque “Launch Imaging Wizard” y haga clic en “Finish”.
7. Permita que la máquina virtual se reinicie e inicie sesión.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

8. Ejecute la utilidad Citrix Provisioning Optimizer.

Después de instalar todo el software relacionado con la plataforma y realizar todas las personalizaciones, haga clic en el icono del escritorio “Shutdown to Finalize”.

Desde ELM:

Seleccione el icono de su capa de plataforma, cuyo estado debería ser “Editing”, y haga clic en **Finalize**.

Capas de aplicaciones

Una vez generada la capa de plataforma, puede continuar con la creación de capas de aplicaciones para la imagen PvD compartida. Determine las aplicaciones instaladas en la imagen PvD compartida. Hay varias formas de hacerlo, por ejemplo:

- Si tiene una versión de arranque de la imagen PvD compartida, arránquela y, desde el Panel de control, seleccione “Programas y características”.
- De lo contrario, desde Citrix Virtual Desktops, use la imagen PvD compartida para crear una VM de PvD para un usuario ficticio. Como el disco Personal vDisk del usuario ficticio está vacío, todas las aplicaciones que se muestran en “Programas y características” se han instalado en la imagen PvD compartida.

Use el panel **Programas y características** para verificar todas las aplicaciones necesarias.

Como alternativa, puede utilizar el programa PCmover, que se describe en la sección “Herramientas de migración”. Identifica muy bien las aplicaciones presentes en un equipo. Detecta programas que se hayan instalado de una forma inhabitual (por lo que no aparecen en “Programas y características”). Si se usa para este propósito, permita que realice su análisis sin realizar ninguna migración en sí. Una vez que la herramienta haya realizado su análisis y usted haya anotado todas las aplicaciones de la imagen compartida, cancele PCmover. Para obtener información más detallada, consulte la sección **Usar PCmover para determinar las aplicaciones necesarias** más adelante en este artículo.

> **Sugerencia:**
>
> Si está migrando varias máquinas virtuales PvD, esta sería una buena oportunidad para arrancar cada una de ellas y compilar una lista de las aplicaciones instaladas por el usuario. Todas las aplicaciones que vea situadas encima de las que encontró en la imagen compartida son aplicaciones instaladas por el usuario.

Una vez disponga de la lista completa de las aplicaciones necesarias, cree una o varias capas de aplicaciones. A continuación, instale una o varias aplicaciones necesarias en cada capa de aplicaciones. Por ejemplo, todas las aplicaciones relacionadas pueden instalarse en una sola capa de aplicaciones. Las aplicaciones que utilicen varios usuarios pueden instalarse en una capa elástica de aplicaciones. Una aplicación que utilice un solo usuario se puede instalar en la capa propia de ese usuario. Aunque

© 1999-2019 Citrix Systems, Inc. All rights reserved.

para muchas aplicaciones es sencillo crear una capa de aplicaciones, otras requieren una preparación especial.

Para muchas aplicaciones, es sencillo crear una capa, mientras que otras requieren una preparación especial. Consulte las diferentes recetas de configuración desarrolladas por Citrix Solution Architects y por la comunidad de App Layering. Verá, por ejemplo, que hay algunas aplicaciones que solo se pueden instalar en una capa de usuario, no en una capa de aplicaciones.

Para cada capa de aplicaciones, desde ELM:

1. En la ficha **Layers**, haga clic en **Create App Layer**.
2. En la sección **Layer Details**, especifique el nombre de la capa y su versión.
3. En la capa de sistema operativo, seleccione la capa de SO que creó en la sección anterior.
4. Si esta aplicación depende de aplicaciones que se encuentran en otra capa de aplicaciones, especifíquelas en las capas de requisitos previos. Esto determina el orden en que se crean las capas de aplicaciones.
5. En el panel "Connector", seleccione el conector de XenServer que creó en la sección anterior. ELM utiliza este conector para escribir la VM de empaquetado de la capa de aplicaciones en XenServer, donde, utilizando XenCenter, puede arrancarla y personalizarla.
6. Cuando haya especificado todas las opciones, haga clic en **Create Layer**. Esta acción genera una VM de empaquetado de capa de aplicaciones. Una vez completado, el estado de la tarea de creación indica "Action Required" (Acción requerida). En este ejemplo, no se necesita ninguna capa de plataforma porque se presupone que esta capa de aplicaciones se implementa en el mismo hipervisor que se eligió cuando creó la capa de sistema operativo.

Desde XenCenter:

Una vez generada su VM de empaquetado de capa de aplicaciones, aparece en XenCenter. Realice las siguientes tareas:

1. Arránquela.
2. Desde su VM de empaquetado de capa de aplicaciones, inicie sesión con la cuenta de administrador local.
3. Si se requiere un reinicio de inmediato, reinicie y vuelva a iniciar sesión.
4. Instale la aplicación o las aplicaciones que quiere que haya en la capa de aplicaciones y realice las personalizaciones necesarias. Debido a que esta capa es compartida por varios usuarios, no deben realizarse personalizaciones ni configuraciones específicas del usuario. Se realizan cuando se migra el disco personal vDisk de un usuario, como se describe más adelante en este artículo.
5. Después de instalar las aplicaciones en esta capa y realizar todas las personalizaciones, haga clic en el icono de escritorio **Shutdown to Finalize**.

Desde ELM:

1. Seleccione el icono de la capa de aplicaciones, cuyo estado debería ser *Editing*.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

2. Haga clic en **Finalize**. Con ello, se completa la creación de la capa de aplicaciones y esa capa se puede implementar.
3. Repita este procedimiento para cada capa de aplicaciones requerida.

Plantilla de imagen

Después de haber generado la capa de SO, la capa de plataforma y una o varias capas de aplicaciones, ahora puede continuar con el proceso y crear una plantilla de imagen. Decida cuáles serán las capas de aplicaciones que se vincularán a la imagen en capas y cuáles se deben asignar dinámicamente a los usuarios en capas elásticas de aplicaciones. Tenga en cuenta lo siguiente:

- Todas las capas de aplicaciones que incluya en la plantilla de imagen están disponibles para todos los usuarios de la imagen compartida en capas.
- Las capas de aplicaciones que asigne a usuarios específicos (o grupos de AD) están disponibles solo para esos usuarios (o grupos de AD). Puede cambiar dichas asignaciones más adelante, para que las capas de aplicaciones estén disponibles para otros usuarios o grupos.

> **Importante:**
>
> Estas dos alternativas son mutuamente excluyentes; es decir, no debe incluir nunca una capa de aplicaciones en una plantilla de imagen y, además, asignarla a un usuario. Hacerlo es innecesario y no se admite.

Como regla general, las aplicaciones que se instalaron en la imagen PvD compartida deben incluirse en la plantilla de imagen. Las aplicaciones que se instalaron en la imagen PvD compartida deberían incluirse en la plantilla de imagen; las aplicaciones que se instalaron en el disco Personal vDisk del usuario deberían asignarse como capas elásticas de aplicaciones; las aplicaciones que utilice un solo usuario y es poco probable que se compartan se instalan en la capa propia de ese usuario.

Desde ELM:

1. En la ficha **Imágenes**, haga clic en **Crear Plantilla**.
2. Proporcione un nombre y una versión.
3. Seleccione la capa de SO que creó en la sección anterior.
4. Seleccione las capas de aplicaciones que quiera incluir en la plantilla de imagen. No seleccione las capas de aplicaciones que tiene la intención de asignar a usuarios y grupos de AD como capas elásticas de aplicaciones.
5. Seleccione una configuración de conector. Esto determina dónde se implementa la imagen compartida cuando se publica. Cree una configuración de conector la primera vez que use un nuevo destino de implementación.

Suponiendo que utiliza XenServer, dispone de tres tipos de implementación:

- XenServer: Al utilizar el conector de XenServer, ELM implementa la imagen compartida publicada como una VM en XenServer, donde, desde XenCenter, puede arrancarla. Lo habitual, sin

© 1999-2019 Citrix Systems, Inc. All rights reserved.

embargo, es elegir una de las siguientes dos opciones: Citrix Provisioning o Machine Creation Services.

- Citrix Provisioning: La imagen compartida publicada se implementa como un disco vDisk en un servidor Citrix Provisioning. Al crear una configuración de conector de este tipo, debe especificar el nombre del servidor Citrix Provisioning. Credenciales de inicio de sesión para un usuario con permiso para administrar Citrix Provisioning. Para obtener información más detallada, consulte "Connector Configuration & Optional Script (Citrix Provisioning)" (Configurar conector y script opcional (Citrix Provisioning)) en la documentación en línea de App Layering.
- Citrix MCS para XenServer: La imagen compartida publicada se implementa como una máquina virtual en XenServer donde, utilizando Citrix Virtual Desktops, puede usarla para crear un catálogo de máquinas.

Al crear este tipo de configuración de conector, debe especificar la dirección y las credenciales de XenServer (para que ELM pueda escribir en él) y el repositorio de almacenamiento de destino. Asimismo, especifique la plantilla de máquina virtual que creó en la sección anterior.

Además:

- Seleccione una capa de plataforma: la capa de plataforma MCS o Citrix Provisioning que creó en la sección anterior o, si está implementando en XenServer, omita esta opción.
- En el panel **Layered Image Disk**: si aparece la opción "SysPrep", seleccione "Not Generalized".
- Para "Elastic Layering" (capa elástica), seleccione "Application and User Layers". Esta configuración tiene dos efectos.
  - Permite asignar capas adicionales de aplicaciones adicionales a usuarios y grupos de AD, capas que se conectan dinámicamente cuando un usuario inicia sesión.
  - Provoca la creación de una nueva capa del usuario la primera vez que inicia sesión. (En App Layering 4.1, esta opción solo está disponible si está habilitada explícitamente. Para habilitarla, vaya a ELM. A continuación, en System > Settings and Configuration > Labs, marque la casilla "User Layers".)

Una capa de usuario captura el perfil del usuario, sus configuraciones, sus documentos, etc. Como se describe en la siguiente sección, este es el destino donde las herramientas de migración transfieren toda la información específica del usuario proveniente del disco Personal vDisk.

En el panel **Confirm and Complete**, haga clic en **Create Template**. Esto debería completarse casi de inmediato.

Publicar imagen compartida en capas

El último paso para generar la imagen compartida en capas es seleccionar la **plantilla de imagen creada anteriormente** y hacer clic en **Publish Layered Image**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Cuando esto finalice, la imagen en capas resultante se implementa como 1) para MCS, una VM en XenServer o 2) para Citrix Provisioning, un disco vDisk en el servidor Citrix Provisioning.

Ahora puede usar las herramientas de administración habituales de MCS o Citrix Provisioning para crear un grupo de entrega y un catálogo de máquinas de Citrix Virtual Desktops:

- Para MCS, utilice Studio para crear un catálogo de máquinas e importe la VM de la imagen compartida en capas.
- Para Citrix Provisioning, use el asistente Citrix Virtual Desktops Setup Wizard para crear un catálogo de máquinas en Studio.

En la siguiente sección, se describe el último paso para migrar la VM de Personal vDisk de un usuario a App Layering. Como vista previa del proceso: se ejecuta al mismo tiempo la máquina virtual original de PvD y la nueva máquina virtual de App Layering, se inicia sesión como usuario en la máquina virtual de App Layering y se ejecuta una herramienta de migración para transferir el perfil y la configuración del usuario desde PvD a la capa de usuario de App Layering.

Herramientas de migración

Citrix recomienda que use una de las dos herramientas, PCmover o USMT, para migrar la información personal desde el disco personal de un usuario a la capa de usuario de App Layering.

- PCmover es un programa que ofrece LapLink.com a la venta. Puede ejecutar la VM de PvD y la VM de App Layering de un usuario, y usar PCmover para transferir la configuración del usuario de la primera VM a la segunda. Ambas máquinas virtuales pueden ejecutarse al mismo tiempo que la información que se transfiera a través de una red, o pueden ejecutarse consecutivamente, con la información transferida por archivo.

  PCmover presenta una interfaz gráfica de usuario fácil de usar, con la que puede adaptar con precisión la información que se transfiere. Si tiene varias máquinas virtuales de PvD a migrar, puede usar PCmover Policy Manager para crear un Policy File (archivo de directiva). Al usar un archivo de directiva, puede realizar migraciones con interacciones mínimas.

  Para obtener más información, consulte la guía de usuario de PCmover.

- USMT es un conjunto de programas disponibles de Microsoft como parte del kit de instalación de automatización de Windows (AIK). Se ejecuta un programa Scanstate en la VM del disco Personal vDisk para escribir un archivo de transferencia. Se ejecuta LoadState en la VM de App Layering para leer y aplicar el archivo de transferencia. Varios archivos XML determinan los datos que se transfieren. Esos archivos se pueden modificar si los valores predeterminados no se ajustan a sus necesidades.

En este artículo, se presupone que ejecutará PCmover.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Migrar la información del usuario

En este punto, ya debe haber utilizado su imagen PvD compartida original para crear una imagen compartida en capas de App Layering funcionalmente equivalente. Tiene una o varias máquinas virtuales PvD de usuarios, cada una con un disco Personal vDisk que contiene el perfil de usuario y otra información que quiere migrar a una capa de usuario de App Layering.

Debe iniciar la máquina virtual PvD de cada usuario, iniciar la imagen compartida en capas y, en ambas máquinas virtuales, iniciar sesión con las credenciales de dominio de cada usuario y ejecutar PCmover.

Para migrar la información del usuario:

1. Instale PCmover en un recurso compartido al que se pueda acceder desde la VM de PvD y la imagen compartida en capas.
2. Desde Studio, inicie la máquina virtual PvD del usuario. Inicie sesión como el usuario. Inhabilite los firewalls.
3. Desde ELM, asigne al usuario las capas elásticas de aplicaciones que requiera.
4. Compruebe que el usuario tiene acceso de escritura en el directorio donde se encuentra su capa de usuario. Consulte “Configure Security on User Layer Folders” (Configurar la seguridad de las carpetas en la capa de usuario) en la documentación en línea.
5. Desde Studio, inicie la VM de la imagen compartida en capas. Inicie sesión como el usuario. La primera vez que el usuario inicia sesión, la VM crea una capa de usuario en el recurso compartido de archivos de red. Inhabilite los firewalls, los antivirus y el antispyware.
6. Ejecute PCmover en la VM de PvD.
    a) Seleccione “PC to PC Transfer” y “Next”.
    b) Seleccione “Old” y “Next”.
    c) Seleccione “Wifi or Wired Network” y “Next”.
    d) PCmover tarda unos minutos en examinar la máquina virtual de PvD. Después de eso, seleccione “Next”.
    e) Suponiendo que no quiere recibir ninguna notificación por correo electrónico cuando se complete la transferencia, simplemente seleccione “Next”.
    f) Puede introducir una contraseña o no hacerlo. Una contraseña garantiza que la información del usuario se enviará desde la máquina virtual de PvD a la máquina virtual de la imagen compartida en capas, a ninguna otra máquina virtual. Luego, seleccione “Next”.
7. Ejecute PCmover en la VM de App Layering.
    a) Seleccione “PC to PC Transfer” y “Next”.
    b) Seleccione “New” y “Next”.
    c) Introduzca los valores requeridos de validación del número de serie.
    d) En “Network Name”, especifique el nombre de la VM de PvD y haga clic en “Next”.
    e) Consulte el panel “Application Selections”. Se recomienda desmarcar todas las aplicaciones. Deben haberse creado capas de aplicaciones para todas las aplicaciones nece-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

sarias.

f) Consulte el panel “User Account Selections”. Se recomienda marcar con “Do not transfer this user” a todos los usuarios que no sean el propietario del disco Personal vDisk.
g) Consulte el panel “Custom Settings”. Se recomienda seleccionar “Files and Settings Only”.
h) Consulte el panel “Drive Selections”. Se recomienda marcar con “Do not transfer this drive” a todas las unidades que no sean “C:”.
i) Después de consultar todos los paneles, haga clic en “Next”.
j) Suponiendo que no quiere recibir ninguna notificación por correo electrónico cuando se complete la transferencia, simplemente seleccione “Next”.

En este punto, PCmover comienza a transferir archivos y configuraciones desde la máquina virtual de PvD a la capa del usuario de App Layering.

Usar PCmover para determinar las aplicaciones necesarias

Puede usar PCmover para analizar una VM de PvD y determinar las aplicaciones instaladas. Esto proporciona una alternativa a “Programas y características” del Panel de **control**.

1. Ejecute PCmover en la VM de PvD.
2. Seleccione “PC to PC Transfer” y “Next”.
3. Seleccione “Old” y “Next”.
4. Seleccione “File Storage Device” y “Next”.
5. Consulte el panel “Application Selections” y tome nota de las aplicaciones instaladas.
6. Cancele PCmover.

Eliminar componentes

December 4, 2018

Para quitar componentes, Citrix recomienda usar la función de Windows para quitar o cambiar programas. También puede quitar componentes usando 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Preparar

Antes de eliminar un Controller, quítelo del sitio. Para obtener más detalles, consulte Quitar un Controller.

Cierre Studio y Director antes de eliminarlo.

Eliminar componentes con la función de Windows para quitar o cambiar programas

Con la función de Windows para quitar o cambiar programas:

- Para quitar un Controller, Studio, Director, un servidor de licencias o StoreFront, haga clic con el botón secundario en **Citrix Virtual Apps *versión*** o **Citrix Virtual Desktops *versión***. A continuación, seleccione **Desinstalar**. Se inicia el instalador. Seleccione los componentes que se eliminarán.

  También puede quitar StoreFront si hace clic con el botón secundario en **Citrix StoreFront** y selecciona **Desinstalar**.

- Para quitar un VDA, haga clic con el botón secundario en **Citrix Virtual Delivery Agent *versión*** y seleccione **Desinstalar**. Se inicia el instalador y puede seleccionar los componentes que quiere quitar. De forma predeterminada, la máquina se reinicia automáticamente después de la eliminación.

- Para quitar Universal Print Server, haga clic con el botón secundario en **Citrix Universal Print Server** y seleccione **Desinstalar**.

Eliminar componentes principales mediante la línea de comandos

Desde el directorio \x64\XenDesktop Setup en los medios de instalación, ejecute el comando `XenDesktopServerSetup.exe`.

- Para quitar uno o varios componentes, use las opciones `/remove` y `/components`.
- Para quitar todos los componentes, use la opción `/removeall`.

Para obtener información detallada acerca de parámetros y comandos, consulte Instalar usando la línea de comandos.

Por ejemplo, el siguiente comando elimina Studio.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components
studio
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Eliminar VDA usando la línea de comandos

Desde el directorio \x64\XenDesktop Setup en los medios de instalación, ejecute el comando `XenDesktopVdaSetup.exe`.

- Para quitar uno o más componentes, use las opciones /remove y /components.
- Para quitar todos los componentes, use la opción /removeall.

Para obtener información detallada acerca de parámetros y comandos, consulte Instalar usando la línea de comandos.

De forma predeterminada, la máquina se reinicia automáticamente después de la eliminación.

Por ejemplo, el siguiente comando elimina el VDA y la aplicación Citrix Workspace.

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /removeall
```

Para quitar agentes VDA mediante un script en Active Directory, consulte Instalar o eliminar VDA usando scripts.

Actualizar y migrar

March 14, 2019

> **Nota:**
>
> Puede obtener información sobre los cambios en los nombres de producto aquí.

Acerca de las actualizaciones

Las actualizaciones cambian la implementación de la Versión actual (Current Release) Citrix Virtual Apps and Desktops, 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. Además, las actualizaciones pueden contener correcciones, aclaraciones y mejoras de versiones anteriores.

¿Qué versiones puede actualizar?

Puede actualizar a la versión actual (CR) desde:

- XenDesktop 5.6 (Para actualizar desde XenDesktop 5.6 a esta versión actual, actualice a la versión 7.6 LTSR con la actualización acumulativa más reciente y, a continuación, actualice a esta versión actual).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- XenDesktop 7.0
- XenDesktop 7.1
- XenApp y XenDesktop 7.5
- XenApp y XenDesktop 7.6
- XenApp y XenDesktop 7.6 LTSR
- XenApp y XenDesktop 7.7
- XenApp y XenDesktop 7.8
- XenApp y XenDesktop 7.9
- XenApp y XenDesktop 7.11
- XenApp y XenDesktop 7.12
- XenApp y XenDesktop 7.13
- XenApp y XenDesktop 7.14
- XenApp y XenDesktop 7.15 LTSR
- XenApp y XenDesktop 7.16
- XenApp y XenDesktop 7.17
- XenApp y XenDesktop 7.18
- Citrix Virtual Apps and Desktops 7 1808

Cómo actualizar

> Importante:
>
> Revise la documentación antes de comenzar la actualización.

Para actualizar los componentes principales y los agentes VDA:

1. Ejecute el instalador en las máquinas donde están instalados los componentes. El software determina si hay una actualización disponible e instala la versión más reciente.
2. Use el recién actualizado Studio para actualizar la base de datos y el sitio.

Preparación y orientación para actualizaciones: el artículo Actualizar una implementación es la fuente de información principal para los componentes principales y los agentes VDA. En ese artículo se describe la secuencia y el orden de actualización, las limitaciones, los pasos de preparación y otras consideraciones. También proporciona el procedimiento de actualización paso a paso e instrucciones para actualizar las bases de datos y el sitio después de actualizar los componentes principales.

Detalles de la instalación: Después de completar cualquier trabajo de preparación y estar listo para iniciar el instalador, el artículo de instalación muestra lo que verá (si está utilizando la interfaz gráfica) o lo que tendrá que escribir (si está utilizando la interfaz de línea de comandos) para actualizar los componentes. Cuando finalice el programa de instalación, vuelva a la guía de Actualizar una implementaciónpara actualizaciones de bases de datos y sitios.

- Instalar/actualizar componentes principales utilizando la interfaz gráfica
- Instalar/actualizar componentes principales mediante la línea de comandos

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Instalar/actualizar los agentes VDA mediante la interfaz gráfica
- Instalar/actualizar los agentes VDA mediante la línea de comandos

Para obtener información acerca de la instalación de revisiones hotfix de Controller, consulte CTX201988.

Actualizar licencias

Para obtener una visión completa de la administración de Citrix Licensing, consulte Activar, actualizar y administrar licencias de Citrix.

Para una implementación de la versión actual local, puede usar el instalador de producto completo para actualizar el servidor de licencias. O bien, puede descargar y actualizar los componentes de la licencia por separado. Consulte Actualizar.

Actualizar otros componentes

Además de los componentes principales y los agentes VDA, las implementaciones locales de la versión actual de Citrix Virtual Apps and Desktops incluyen los siguientes componentes que puede actualizar cuando se publican nuevas versiones.

- StoreFront
- AppDNA
- Citrix App Layering
- HDX RealTime Optimization Pack
- Profile Management
- Citrix Provisioning
- Grabación de sesiones
- Workspace Environment Management

Migrar

La migración mueve los datos de una implementación a la versión más reciente. Puede migrar una implementación de XenApp 6. La migración incluye la instalación de los componentes actuales y la creación de un sitio nuevo, la exportación de datos desde la comunidad de servidores original y la importación de esos datos en el sitio nuevo.

- Para obtener información sobre los cambios de arquitectura, componentes y características que se han introducido en las versiones 7.x, consulte Cambios en 7.x.
- Para migrar desde XenApp 6, consulte Migrar XenApp 6.x.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Más información

Las actualizaciones de implementación deLong Term Service Release (LTSR) utilizan actualizaciones acumulativas (CUs). Una CU actualiza los componentes de línea base de la LTSR, y cada CU incluye su propio metainstalador.

Cada actualización acumulativa (CU) tiene su propia documentación dedicada. Por ejemplo, para la versión 7.15 LTSR, consulte el enlace en la página [Novedades]/es-es/xenapp-and-xendesktop/7-15-ltsr/whats-new.html()de esa LTSR para la última CU. Cada página de CU incluye información de versión admitida, instrucciones y un enlace al paquete de descarga de CU.

Cambios en 7.x

December 11, 2018

La arquitectura, la terminología y las características de Citrix Virtual Apps and Desktops han cambiado a partir de las versiones de XenApp y XenDesktop 7.x. Si solo conoce las versiones anteriores (a 7.x), en este artículo se le explicarán los cambios.

Una vez haya cambiado a la versión 7.x, los cambios en las versiones posteriores se indican en Novedades.

A menos que se indique específicamente, *7.x* y "versiones posteriores" hacen referencia a XenApp 7.5 o posterior y XenDesktop 7 o posterior, incluidas todas las versiones de Citrix Virtual Apps and Desktops.

En este artículo, se ofrece una descripción general. Para obtener información detallada sobre cómo cambiar desde versiones anteriores a 7.x a la versión más reciente, consulte Actualizar a XenApp 7.

Diferencias de elementos entre XenApp 6 y versiones posteriores

Aunque no son equivalentes exactos, la siguiente tabla ayuda a establecer una correspondencia entre los elementos funcionales de XenApp 6.5 y sus versiones anteriores con versiones posteriores. A continuación, dispone de descripciones de las diferencias que existen entre cada arquitectura.

En lugar de esto en XenApp 6.x y versiones anteriores	Piense en esto en versiones más recientes
Arquitectura IMA (Independent Management Architecture)	Arquitectura FMA (FlexCast Management Architecture)
Comunidad	Sitio
Grupo de trabajo	Catálogo de máquinas, grupo de entrega

© 1999-2019 Citrix Systems, Inc. All rights reserved.

En lugar de esto en XenApp 6.x y versiones anteriores	Piense en esto en versiones más recientes
Trabajador	Virtual Delivery Agent (VDA), máquina de SO de servidor, VDA de SO de servidor, máquina de SO de escritorio, VDA de SO de escritorio
Máquina de Servicios de Escritorio remoto (RDS) o Terminal Services	Máquina de SO de servidor, VDA de SO de servidor
Recopilador de datos y zonas	Delivery Controller
Delivery Services Console	Citrix Studio y Citrix Director
Publicación de aplicaciones	Entrega de aplicaciones
Almacén de datos	Base de datos
Patrón de carga	Directiva de administración de carga
Administrador	Administrador delegado, rol, ámbito

Diferencias de arquitecturas

A partir de las versiones 7.x, Citrix Virtual Apps and Desktops (antes XenApp y XenDesktop) se basan en la arquitectura FMA (FlexCast Management Architecture). FMA es una arquitectura orientada a servicios que permite la interoperabilidad y administración modular de las diversas tecnologías de Citrix. FMA ofrece una plataforma para la entrega de aplicaciones, movilidad, servicios, aprovisionamiento flexible y administración en la nube.

FMA sustituye a la arquitectura IMA (Independent Management Architecture) de XenApp 6.5 y versiones anteriores.

Estos son los elementos clave de FMA en términos de cómo se relacionan con los elementos de XenApp 6.5 y versiones anteriores:

- **Sitios de entrega:** Las comunidades eran los objetos de nivel superior en XenApp 6.5 y versiones anteriores. En versiones posteriores, el sitio es el elemento de nivel más alto. Los sitios ofrecen aplicaciones y escritorios a grupos de usuarios. FMA requiere que usted se encuentre en un dominio para implementar un sitio. Por ejemplo, para instalar los servidores, su cuenta debe tener privilegios de administrador local y ser un usuario de dominio de Active Directory.
- **Catálogos de máquinas y grupos de entrega:** Las máquinas que alojaban aplicaciones en XenApp 6.5 y versiones anteriores pertenecían a grupos de trabajo para una administración eficaz de las aplicaciones y del software de servidor. Los administradores podían administrar todas las máquinas de un grupo de trabajo como una sola unidad con el objetivo de mejorar la administración de la aplicación y el equilibrio de carga. Las carpetas se utilizaban para organizar

© 1999-2019 Citrix Systems, Inc. All rights reserved.

aplicaciones y máquinas. En las versiones posteriores, se utiliza una combinación de catálogos de máquinas, grupos de entrega y grupos de aplicaciones para administrar las máquinas, el equilibrio de carga, así como las aplicaciones y los escritorios alojados. También se pueden usar carpetas de aplicaciones.

- **VDA:** En XenApp 6.5 y versiones anteriores, las máquinas de trabajo (trabajadores) de los grupos de trabajo ejecutaban aplicaciones para el usuario y se comunicaban con los recopiladores de datos. En las versiones posteriores, el VDA se comunica con los Delivery Controllers que administran las conexiones de usuario.
- **Delivery Controllers**. En XenApp 6.5 y versiones anteriores, había un maestro de zona que se encargaba de las solicitudes de conexión de los usuarios y de la comunicación con los hipervisores. En las versiones posteriores, los Controllers del sitio se encargan de distribuir y gestionar las solicitudes de conexión. En XenApp 6.5 y las versiones anteriores, las zonas ofrecían una manera de agregar servidores y replicar datos a través de conexiones WAN. Aunque las zonas no tienen equivalente exacto en las versiones posteriores, la función de zonas y preferencia de zonas permiten a los usuarios de regiones remotas a conectarse a recursos sin que las conexiones recorran necesariamente grandes segmentos de red WAN.
- **Studio y Director**. Use la consola de Studio para configurar los entornos y ofrecer a los usuarios acceso a aplicaciones y escritorios. Studio reemplaza Delivery Services Console en XenApp 6.5 y versiones anteriores. Los administradores usan Director para supervisar el entorno, remedar dispositivos de usuario y solucionar problemas de TI. Para remedar usuarios, la Asistencia remota de Windows debe estar habilitada; se habilita de forma predeterminada cuando se instala el VDA.
- **Entrega de aplicaciones**. En XenApp 6.5 y versiones anteriores, se utilizaba el asistente Publicar aplicación para preparar aplicaciones y entregarlas a los usuarios. En las versiones posteriores, se utiliza Studio para crear aplicaciones, agregarlas y ponerlas a disposición de los usuarios que formen parte de grupos de entrega y, opcionalmente, de grupos de aplicaciones. Mediante Studio, primero debe configurar un sitio, crear y especificar los catálogos de máquinas y, a continuación, crear grupos de entrega en dichos catálogos. Los grupos de entrega determinan qué usuarios tienen acceso a las aplicaciones que usted entrega. Si quiere, puede optar por crear grupos de aplicaciones como alternativa a varios grupos de entrega.
- **Base de datos:** En las versiones posteriores no se usa el almacén de datos IMA para la información de configuración. En su lugar, utilizan una base de datos de Microsoft SQL Server para almacenar información de configuración y de sesión.
- **Directiva de administración de carga:** En XenApp 6.5 y versiones anteriores, los patrones de carga utilizaban métricas predeterminadas para determinar la carga de una máquina. Las conexiones de usuarios se podían asociar a máquinas con menos carga. En las versiones posteriores, se utilizan directivas de administración de carga para equilibrar la carga entre las máquinas.
- **Administración delegada**. En XenApp 6.5 y versiones anteriores, se creaban administradores

© 1999-2019 Citrix Systems, Inc. All rights reserved.

personalizados y se les asignaban permisos basados en carpetas y objetos. En las versiones posteriores, los administradores personalizados se crean en función de pares de ámbito y rol. Un rol representa una función de trabajo y tiene asociados permisos definidos para él con el objetivo de permitir la delegación. Un ámbito representa un conjunto de objetos. Los roles predefinidos de administrador disponen de conjuntos específicos de permisos, como el servicio de asistencia técnica, las aplicaciones, el alojamiento y el catálogo. Por ejemplo, los administradores del servicio de asistencia pueden trabajar únicamente con usuarios individuales en sitios especificados, mientras que los administradores totales pueden supervisar toda la implementación y resolver problemas de TI de todo el sistema.

Comparación de características

La transición a FMA también implica que algunas características que estaban disponibles en XenApp 6.5 y versiones anteriores ahora se implementan de otra forma, o que haya que usar funciones, componentes o herramientas distintas para conseguir los mismos objetivos.

En lugar de esto en XenApp 6.5 y versiones anteriores:	Use esto en versiones posteriores:
Preinicio de sesiones y persistencia de sesiones configurados por directivas	Preinicio de sesiones y persistencia de sesiones configurados mediante los parámetros del grupo de entrega. Al igual que en XenApp 6.5, estas características ayudan a que los usuarios se conecten rápidamente con las aplicaciones, iniciando sesiones antes de que se soliciten (preinicio de sesiones) y manteniendo las sesiones activas después de que el usuario cierra todas las aplicaciones (persistencia de sesiones). En las versiones posteriores, estas funciones se habilitan para usuarios especificados configurando estos parámetros en los grupos de entrega existentes. Consulte Configurar el preinicio y la persistencia de sesiones.
Respaldo para usuarios no autenticados (anónimos) mediante la concesión de derechos a usuarios anónimos al configurar las propiedades de las aplicaciones publicadas	El respaldo para usuarios no autenticados (anónimos) se ofrece configurando esta opción cuando establezca las propiedades de los usuarios de un grupo de entrega. Consulte Usuarios.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

En lugar de esto en XenApp 6.5 y versiones anteriores:	Use esto en versiones posteriores:
El caché de host local permite que los servidores de trabajo funcionen incluso aunque pierdan la conexión con el almacén de datos	La Caché de host local permite que la intermediación de operaciones continúe cuando se interrumpa la conexión entre un Controller y la base de datos del sitio. Esta implementación es más sólida y requiere menos mantenimiento. Consulte Caché de host local.
Distribución de aplicaciones por streaming	App-V de Citrix ofrece aplicaciones distribuidas por streaming que se administran mediante Studio. Consulte App-V.
Interfaz Web	Citrix recomienda realizar la transición a StoreFront.
SmartAuditor para grabar la actividad en pantalla de la sesión de un usuario	A partir de 7.6 Feature Pack 1, esta función se ofrece con la grabación de sesiones. También puede usar el Registro de configuración para registrar todas las actividades de sesión desde una perspectiva administrativa.
La característica “Administración de energía y capacidad” ayuda a reducir el consumo de energía y administrar la capacidad del servidor	Use el Administrador de configuración de Microsoft.

Cambios y funciones admitidas

Las siguientes características no se ofrecen, ya no se respaldan o han cambiado significativamente en Citrix Virtual Apps and Desktops, a partir de XenApp o XenDesktop 7.x.

Cifrado Secure ICA por debajo de 128 bits: En versiones anteriores a 7.x, Secure ICA podía cifrar conexiones de cliente para el cifrado básico de 40, 56 y 128 bits. Con las versiones 7.x, el cifrado Secure ICA solo está disponible para el cifrado de 128 bits.

Impresión antigua: Las funciones de impresión siguientes ya no se admiten en las versiones 7.x:

- Compatibilidad con versiones anteriores de los clientes de DOS e impresoras de 16 bits.
- Compatibilidad para impresoras conectadas a los sistemas operativos de Windows 95 y Windows NT, incluidas las propiedades de impresora extendidas y mejoradas y Win32FavorRetainedSetting.
- Capacidad para habilitar o inhabilitar impresoras conservadas y restauradas automáticamente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- DefaultPrnFlag, un parámetro de Registro para servidores que se utiliza para habilitar o inhabilitar impresoras conservadas y restauradas automáticamente, almacenadas en perfiles de usuario del servidor.

Se admiten los nombres de las impresoras del cliente heredadas.

Secure Gateway: En versiones anteriores a 7.x, Secure Gateway era una opción para ofrecer conexiones seguras entre el servidor y los dispositivos de usuario. Citrix Gateway es la nueva opción para proteger las conexiones externas.

Remedo de usuarios: En versiones anteriores a 7.x, los administradores establecían directivas para controlar el remedo de usuario a usuario. En las versiones 7.x, el remedo de usuarios finales es una función integrada en el componente Director, que utiliza la Asistencia remota de Microsoft para permitir a los administradores remedar y solucionar problemas en la entrega de aplicaciones y escritorios virtuales.

Redirección de Flash 1: Los clientes que no admiten la redirección de Flash de segunda generación (incluido Citrix Receiver para Windows anterior a la versión 3.0, Citrix Receiver para Linux anterior a la versión 11.100 y Citrix Online Plug-in 12.1) utilizarán la generación en el lado del servidor para las funciones de redirección de Flash antiguas. Los VDA que se incluyen en las versiones 7.x respaldan las funciones de redirección de Flash de segunda generación.

Repetición local del texto. Esta funcionalidad se usaba con tecnologías de aplicaciones Windows anteriores para acelerar la presentación del texto introducido en los dispositivos de usuario en conexiones de alta latencia. Ya no se incluye en las versiones 7.x porque se han hecho mejoras en el subsistema de gráficos y el HDX SuperCodec.

Single Sign-On. Esta funcionalidad, que ofrece la seguridad de contraseñas, no se admiten en Windows 8, Windows Server 2012 ni en las nuevas versiones de los sistemas operativos Windows compatibles. Sigue recibiendo respaldo para entornos de Windows 2008 R2 y Windows 7, pero no está incluida en las versiones 7.x. Se encuentra en el sitio Web de descargas de Citrix: https://citrix.com/downloads.

Respaldo para bases de datos de Oracle. Las versiones 7.x requieren bases de datos SQL Server.

Supervisión del estado y recuperación (HMR). En versiones anteriores a 7.x, la supervisión del estado y la recuperación podía ejecutar pruebas en los servidores de una comunidad de servidores para supervisar su estado y detectar cualquier riesgo de funcionamiento. En las versiones 7.x, Director ofrece una vista centralizada del estado del sistema al presentar la supervisión y las alertas para toda la infraestructura en la misma consola de Director.

Archivos ICA personalizados: Los archivos ICA personalizados se utilizaban para permitir la conexión directa desde dispositivos de usuario (con el archivo ICA) a una máquina concreta. En las versiones 7.x, esta función está inhabilitada de forma predeterminada, pero puede habilitarse para su uso normal mediante un grupo local, o se puede usar en el modo de alta disponibilidad si el Controller deja de estar disponible.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Módulo de administración para System Center Operations Manager (SCOM) 2007. El módulo de administración, que supervisaba la actividad de comunidades de XenApp mediante SCOM, no se admite en versiones 7.x. Consulte el artículo actualizado Módulo de administración SCOM de Citrix para XenApp y XenDesktop.

Función CNAME. La función CNAME estaba habilitada de forma predeterminada en las versiones anteriores a 7.x. Las implementaciones en función de los registros CNAME para el reenrutamiento de FQDN y el uso de nombres NETBIOS podrían fallar. En las versiones 7.x, la actualización automática del Delivery Controller actualiza dinámicamente la lista de Controllers y notifica a los VDA automáticamente cuando se agregan y se quitan Controllers en el sitio. La funcionalidad de actualización automática de Controllers está habilitada de forma predeterminada en las directivas de Citrix, pero puede inhabilitarse. De forma alternativa, puede volver a habilitar la función CNAME en el Registro para continuar con la implementación existente y permitir el reenrutamiento de FQDN y el uso de nombres NETBIOS. Para obtener más información, consulte CTX137960.

Asistente de Implementación rápida. En versiones de XenDesktop anteriores a 7.x, esta opción permitía una instalación rápida de una implementación completa de XenDesktop. La nueva y simplificada secuencia de instalación y configuración de las versiones posteriores elimina la necesidad de utilizar el asistente de Implementación rápida.

Archivo de configuración de servicio de Remote PC y script de PowerShell para la administración automática: Ahora, el acceso con Remote PC está integrado en Studio y en el Controller.

Workflow Studio: En versiones anteriores a 7.x, Workflow Studio era la interfaz gráfica de la composición de flujos de trabajo para XenDesktop. Esta característica no recibe respaldo en las versiones posteriores.

Inicio de programas no publicados durante la conexión del cliente: En versiones anteriores a 7.x, esta configuración de directiva de Citrix especificaba si ejecutar aplicaciones de inicio o aplicaciones publicadas mediante ICA o RDP en el servidor. En versiones 7.x, esta configuración solo especifica si ejecutar las aplicaciones de inicio o las aplicaciones publicadas mediante RDP en el servidor.

Inicios de escritorio: En versiones anteriores a 7.x, esta configuración de directiva de Citrix especificaba si los usuarios no administrativos podían conectarse a sesiones de escritorio. En las versiones 7.x, los usuarios no administrativos deben formar parte del grupo de usuarios con acceso directo en una máquina de VDA para poder conectarse a las sesiones en ese VDA. La configuración Inicios de escritorio permite a usuarios no administrativos que formen parte del grupo de usuarios con acceso directo en un VDA conectarse al VDA mediante una conexión ICA. La configuración “Inicios de escritorio” no afecta a las conexiones RDP, por lo que los usuarios que estén en el grupo de usuarios con acceso directo en un VDA se pueden conectar al VDA mediante una conexión RDP tanto si esta configuración está habilitada como si no.

Profundidad de color: En versiones de Studio anteriores a 7.6, se especificaba la profundidad de color en la configuración de usuarios de un grupo de entrega. A partir de la versión 7.6, la profun-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

didad de color para el grupo de entrega se puede configurar mediante los cmdlets de PowerShell Set-BrokerDesktopGroup o New-BrokerDesktopGroup.

Iniciar escritorio con optimización táctil: Este parámetro se ha inhabilitado y no está disponible para máquinas Windows 10 y Windows Server 2016. Para obtener más información, consulte Configuración de directiva de Experiencia móvil.

Funciones no incluidas en la aplicación Citrix Workspace o que tienen diferentes valores predeterminados

Se han dado los siguientes cambios en la aplicación Citrix Workspace (anteriormente Citrix Receiver):

- **Asignación de puertos COM:** La asignación de puertos COM permitía o impedía el acceso a los puertos COM en el dispositivo del usuario. La asignación de puertos COM estaba habilitada de forma predeterminada. En las versiones 7.x, la asignación de puertos COM está inhabilitada de forma predeterminada. Para obtener más información, consulte Configuración de la redirección de puertos COM y puertos LPT mediante el Registro.
- **Asignación de puertos LPT:** La asignación de puertos LPT controla el acceso de aplicaciones antiguas a los puertos LPT. La asignación de puertos LPT estaba habilitada de forma predeterminada. En las versiones 7.x, la asignación de puertos LPT está inhabilitada de forma predeterminada.
- **Códec de audio PCM:** En las versiones 7.x, solo los clientes HTML5 respaldan el códec de audio PCM.
- **Respaldo para Microsoft ActiveSync**.
- **Respaldo de proxy para versiones anteriores:** Incluye:
  - Microsoft Internet Security and Acceleration (ISA) 2006 (Windows Server 2003)
  - Servidor proxy Oracle iPlanet 4.0.14 (Windows Server 2003)
  - Servidor proxy Squid 3.1.14 (Ubuntu Linux Server 11.10)

Para obtener más información, consulte la documentación de la aplicación Citrix Workspace correspondiente a su versión.

Actualizar una implementación

March 14, 2019

> **Nota:**
>
> Puede obtener información sobre los cambios de nombres de producto aquí y los cambios de números de versión aquí.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Introducción

Puede actualizar algunas implementaciones a versiones más recientes sin tener que configurar antes nuevas máquinas o sitios. Este proceso se llama “actualización en contexto”. Consulte Actualizar para ver una lista de las versiones que se pueden actualizar.

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.

Si intenta actualizar un componente en un sistema operativo que no es compatible con esta versión del producto, un mensaje lo guiará a un artículo. La información de ese artículo también está disponible en este artículo. Consulte Sistemas operativos anteriores.

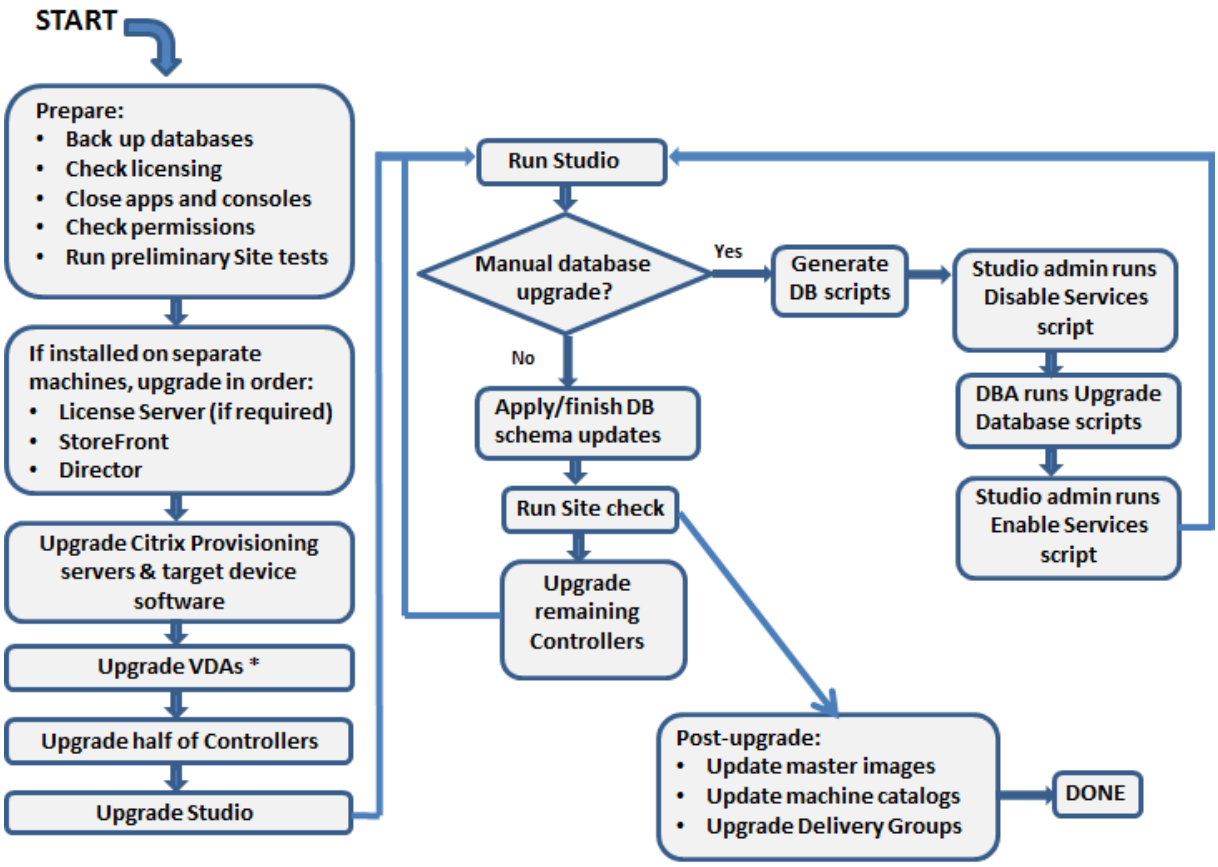
Con el instalador de producto completo, puede actualizar cualquier componente que se pueda instalar, si hay disponible una versión más reciente de este. Para conocer los componentes que no se instalan con el instalador de producto completo (como Citrix Provisioning y Profile Management), consulte la 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 la actualización.

Secuencia de actualización

El diagrama siguiente resume la secuencia de actualización. Se ofrece información detallada en Procedimiento de actualización. Por ejemplo, si tiene más de un componente principal instalado en un servidor, ejecutar el instalador en esa máquina actualiza todos los componentes que tengan versiones nuevas. Puede que le interese actualizar el VDA utilizado en una imagen maestra y, luego, actualizar la imagen. A continuación, actualizar el catálogo que usa esa imagen y el grupo de entrega que utiliza ese catálogo. En la información detallada que se ofrece, también se explica cómo actualizar las bases de datos del sitio y el sitio automática o manualmente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Pruebas preliminares en el sitio

Cuando actualiza los Delivery Controllers y un sitio, se ejecutan pruebas preliminares en el sitio antes de que comience la actualización en sí. En estas pruebas se comprueba si:

- Se puede establecer conexión con la base de datos del sitio y esta tiene copia de seguridad
- Las conexiones a los servicios esenciales de Citrix funcionan correctamente
- La dirección del servidor de licencias de Citrix está disponible
- Se puede establecer conexión con la base de datos de registros de configuración

Tras ejecutarse las pruebas, podrá ver un informe de los resultados. A continuación, podrá solucionar los problemas que se detectaran y ejecutar las pruebas nuevamente. El funcionamiento del sitio puede verse afectado negativamente si no ejecuta las pruebas preliminares del sitio y no resuelve los problemas que surjan.

El informe que contiene los resultados de las pruebas es un archivo HTML (PreliminarySiteTestResult.html) ubicado en el mismo directorio que los registros de instalación. Si aún no existe, el archivo se creará. Si el archivo ya existe, su contenido se sobrescribirá.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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. Si incluye la opción /ignore_site_test_failure, se ignorarán todos los errores de las pruebas y la actualización continuará.

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 recordará. 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 utilizando 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 de XenApp anteriores a 7.5:** No se puede actualizar desde una versión de XenApp anterior a 7.5. Puede migrar desde XenApp 6.x; consulte Migrar XenApp 6.x.

- **Versiones de XenDesktop anteriores a 7.x:** No puede actualizar desde una versión de XenDesktop anterior a 5.6. Para actualizar desde XenDesktop 5.6 a esta versión, actualice a la versión 7.6 LTSR (con la Cumulative Update más reciente) y, a continuación, actualice a esta versión de Citrix Virtual Desktops.

- **XenDesktop Express Edition:** No se puede actualizar XenDesktop Express Edition. Obtenga e instale una licencia para una edición respaldada actualmente y, a continuación, realice la actualización.

- **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 respaldar. Para obtener más información, consulte Sistemas operativos anteriores.

- **Selección de producto:** Cuando actualice desde una versión anterior, no seleccione ni especifique el producto (Citrix Virtual Apps o Citrix Virtual Desktops), porque ya lo ha establecido durante la instalación inicial.

- **Entornos o sitios mixtos:** Si debe seguir ejecutando sitios con una versión anterior y sitios con la versión actual, consulte Consideraciones sobre entornos mixtos.

- **Delivery Controllers anteriores a 7.13:** Cuando actualiza un Delivery Controller desde una versión anterior a 7.13, puede producirse un error (excepción) si la configuración “Tiempo de espera de la reconexión automática de clientes” está definida en las directivas. Este error ocurre si el valor de la configuración “Tiempo de espera de la reconexión automática de clientes” se establece fuera del rango permitido de entre 0 y 300, que se introdujo por primera vez en la

© 1999-2019 Citrix Systems, Inc. All rights reserved.

versión 7.13. Para evitar este error, use Citrix Group Policy PowerShell Provider y anule la configuración definida o establézcala en un valor que se encuentre dentro del intervalo especificado. Para ver un ejemplo, consulte CTX229477.

Preparar

Antes de comenzar una actualización, revise la siguiente información y complete las tareas necesarias.

Elegir un instalador y una interfaz

Puede usar el instalador de producto completo que se proporciona en el archivo ISO del producto para actualizar los componentes.

Puede actualizar los VDA con la ayuda del instalador de producto completo o con uno de los instaladores independientes de VDA.

Todos los instaladores ofrecen interfaces gráficas y de línea de comandos. Para obtener más información, consulte Instaladores.

No puede actualizar importando ni migrando datos desde una versión que se puede actualizar. Algunas versiones muy anteriores se deben migrar en lugar de actualizarse; consulte Actualizar y migrar para ver qué versiones se pueden actualizar.

Si instaló en un principio un VDA de escritorio con el instalador VDAWorkstationCoreSetup.exe, Citrix recomienda usar el mismo instalador para actualizarlo. 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.

Por ejemplo, supongamos que instaló originalmente una versión 7.14 de VDA utilizando VDAWorkstationCoreSetup.exe. Más tarde, utiliza el instalador de producto completo para actualizar ese VDA. Si acepta la configuración predeterminada en el instalador de producto completo, los componentes que se excluyeron en su momento de la instalación original (como Profile Management) se instalan durante 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).

Comprobar el estado del sitio

Si un sitio presenta problemas, la actualización no los solucionará. De hecho, puede dejar el sitio en un estado muy complejo del que puede ser difícil recuperarlo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Cuando inicia el instalador de producto completo para actualizar un Controller, se ejecutan pruebas preliminares en el sitio antes de que comience la actualización en sí. Tras ejecutarse las pruebas, podrá ver un informe de los resultados. Si se encontraron problemas, puede detener la actualización y solucionar los problemas. Luego, después de resolver los problemas, puede comenzar la actualización nuevamente.

Para ver información más detallada, consulte Pruebas preliminares en el sitio.

Copia de seguridad de la 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.

Otras tareas de preparación

- **Compruebe que las licencias de Citrix están actualizadas:** Antes de actualizar, compruebe que la fecha de Customer Success Services, Software Maintenance o Subscription Advantage es válida para la nueva versión del producto. Si va a actualizar desde una versión de producto anterior a 7.x, la fecha debe ser al menos 2018.1114.
- **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 en la máquina que contiene el servidor de licencias. Si se necesita una actualización, el instalador la inicia.
  - Desde el directorio de instalación de XenDesktop en los medios de instalación, ejecute el comando `.\LicServ\Verify.exe -h <delivery-controller-fqdn> -p 27000 -v`. La pantalla resultante indica si el servidor de licencias es compatible. Si el servidor de licencias no es compatible, ejecute el instalador en esa máquina para actualizarlo.
- **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 otros servicios de agentes de supervisión de terceros.
- **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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

La base de datos del sitio y el sitio pueden actualizarse automática o manualmente. 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.

- También puede hacer una copia de seguridad de las plantillas y actualizar los hipervisores, si fuera necesario.
- Complete las demás tareas de preparación estipuladas en el plan de continuidad empresarial.

Consideraciones sobre entornos mixtos

Si el entorno contiene sitios o comunidades con diferentes versiones de producto (por ejemplo, un sitio de XenDesktop 7.14 y un sitio de Citrix Virtual Desktops 1808), Citrix recomienda usar StoreFront para agregar escritorios y aplicaciones desde diferentes versiones de producto. Para obtener más información, consulte la documentación de StoreFront.

- En un entorno mixto, puede continuar usando versiones de Studio y Director para cada versión, pero compruebe que las distintas versiones están instaladas en máquinas independientes.
- Si va a ejecutar sitios de XenDesktop 5.6 y 7.x simultáneamente y va a usar Citrix Provisioning (antes Provisioning Services) para ambos, implemente un nuevo Citrix Provisioning para usarlo con el sitio 7.x, o actualice al Citrix Provisioning actual, aunque entonces ya no podrá aprovisionar nuevas cargas de trabajo en el sitio de XenDesktop 5.6.

Citrix recomienda actualizar todos los componentes en todos los sitios. Aunque se pueden usar las versiones anteriores de algunos componentes, es posible que no estén disponibles todas las funcionalidades de la versión más reciente. Por ejemplo, aunque puede usar agentes VDA actuales en implementaciones que contienen versiones anteriores de Controller, las nuevas funcionalidades de la versión actual pueden no estar disponibles. También se pueden dar problemas de registro de VDA cuando se usan versiones no actuales.

- Si tiene un sitio con Controllers 5.x y agentes VDA de una versión más reciente, complete la actualización de todos los componentes lo antes posible.
- No actualice una versión autónoma de Studio hasta que esté listo para usar la nueva versión.

Sistemas operativos anteriores

Supongamos que ha instalado una versión anterior de un componente en una máquina que ejecutaba una versión respaldada de sistema operativo (SO). Ahora, quiere utilizar una versión más reciente del

© 1999-2019 Citrix Systems, Inc. All rights reserved.

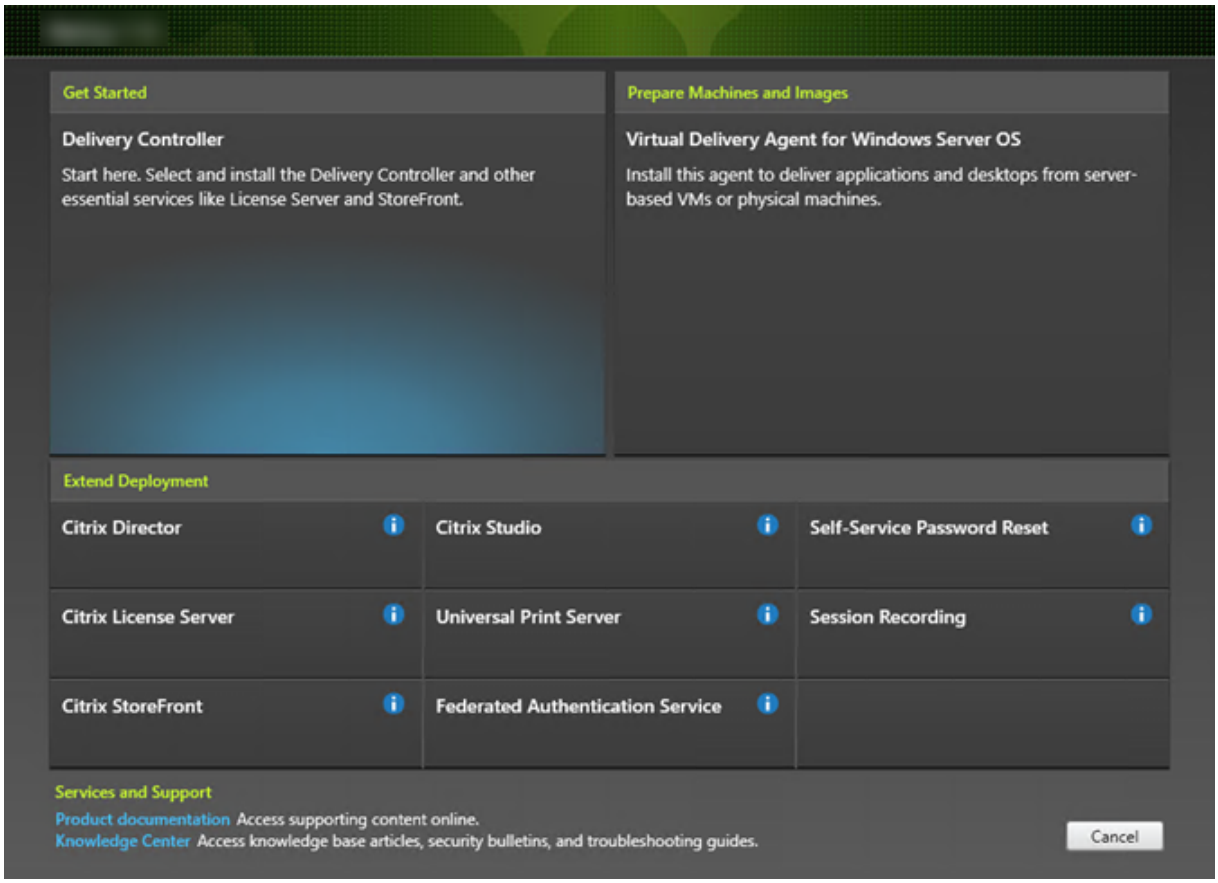
componente, pero ese SO ya no es válido para la versión actual del componente.

Por ejemplo, supongamos que instaló un VDA 7.14 para SO de escritorio en una máquina con Windows 7 SP1. Ahora quiere actualizar ese VDA a la versión actual (digamos, Citrix Virtual Apps and Desktops 7 1808), pero Windows 7 ya no es un SO válido para agentes VDA de escritorio.

Un SO no válido va más allá de "no admitido". Los elementos no admitidos pueden desaconsejarse, pero están permitidos. No válido significa que el instalador de Citrix Virtual Apps and Desktops no le permite instalar o actualizar el componente en la máquina que ejecuta esa versión del sistema operativo.

Cuando 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").

En el siguiente gráfico se muestran los componentes del instalador afectados. (Aunque la imagen muestra la interfaz gráfica del instalador de producto completo, se detectan sistemas operativos no válidos cuando se utilizan ambos, la interfaz gráfica o la línea de comandos del instalador, además de los instaladores de VDA independiente.)



© 1999-2019 Citrix Systems, Inc. All rights reserved.

Sistemas operativos válidos

Siga los enlaces para saber qué sistemas operativos se admiten en una versión.

- 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. Por ejemplo, Windows 7 incluye Windows 7 SP1 y Windows 8 incluye Windows 8.1. Se asume que, si actualiza, es desde una versión 7.x a una versión más reciente.

Sistema operativo	Componente o característica	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
Windows Server 2008 R2	VDA	7.15 LTSR	7.16
Windows Server 2008 R2	Otros componentes del instalador	7.17	7.18
Windows Server 2012	VDA	7.15 LTSR	7.16

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Sistema operativo	Componente o característica	Última versión válida	Instalar o actualizar no es posible a partir de la versión
Windows Server 2012	Otros componentes del instalador	7.17	7.18
Windows Server 2012 R2	VDI de servidor	7.15 LTSR	7.16

Windows XP y Windows Vista no son válidos para ningún componente o tecnología de 7.x.

Lo que puede hacer

Tienes opciones. Revise las siguientes opciones.

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, supongamos que 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 utilizando 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 actualiza la máquina:

Estos métodos son factibles para VDA y otras máquinas que no tienen componentes principales (como Delivery Controllers) instalados. Elija una de las siguientes opciones:

- Tras colocar la máquina en el modo de mantenimiento y permitir que se cierren todas las sesiones, puede restablecer su imagen a una versión compatible de SO Windows, y luego instalar la versión más reciente del componente.
- Para actualizar el sistema operativo sin restablecer imágenes, desinstale el software de Citrix antes de actualizar el sistema operativo. De lo contrario, el software Citrix entrará en un estado no admitido. Luego, instale el nuevo componente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Agregue máquinas nuevas con sistemas operativos admitidos y luego elimine las máquinas antiguas:

Este método es factible si debe actualizar el sistema operativo en máquinas que contienen un Delivery Controller u otro componente principal.

Citrix recomienda que todos los Controllers de un sitio tengan el mismo sistema operativo. En la siguiente secuencia de actualización se minimiza el intervalo en que los Controllers tienen diferentes sistemas operativos.

1. Tome una instantánea de todos los Delivery Controllers en el sitio y haga una copia de seguridad de la base de datos del sitio.
2. Instale los nuevos Delivery Controllers en servidores limpios con sistemas operativos admitidos. Por ejemplo, instale un Controller en dos máquinas Windows Server 2016.
3. Agregue los nuevos Controllers al sitio.
4. Elimine los Controllers que se ejecutan en sistemas operativos no válidos para la versión actual. Por ejemplo, elimine dos Controllers en dos máquinas Windows Server 2008 R2. Siga las recomendaciones para eliminar Controllers en Delivery Controllers.

Opciones de servicio:

La mayoría de los ejemplos de este artículo se aplican a las implementaciones que utilizan la opción de servicio Current Release (CR). Los conceptos también se aplican a las implementaciones que utilizan la opción de servicio Long Term Service Release (LTSR).

- Entre las versiones de XenApp y XenDesktop 7.6 LTSR y 7.15 LTSR, ningún SO admitido dejó de ser válido. Por lo tanto, no se produjeron problemas de actualización al pasar de la versión anterior de LTSR a la siguiente.
- En el futuro (por ejemplo, al pasar de 7.15 LTSR a la próxima versión de LTSR), podrían surgir problemas debido a sistemas operativos identificados como no válidos durante el intervalo.

Asistencia para los VDA mixtos

Cuando actualice el producto a una versión más reciente, Citrix recomienda actualizar todos los componentes principales y los VDA para aprovechar todas las funciones nuevas y mejoradas de la nueva edición.

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. De forma predeterminada, este parámetro especifica la versión de VDA más reciente recomendada. Cambie este parámetro solamente si el catálogo de máquinas contiene máquinas con versiones anteriores de VDA. 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 recomendada, y alguna de las máquinas del catálogo tiene una versión anterior de VDA, esas máquinas no

© 1999-2019 Citrix Systems, Inc. All rights reserved.

podrán registrarse en el Controller y no funcionarán.

Para obtener más información, consulte Niveles funcionales y versiones de VDA.

Procedimiento de actualización

Para ejecutar la interfaz gráfica del instalador de producto, 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 Instalar desde la línea de comandos.

1. Si hay más de un componente principal instalado en el mismo servidor (por ejemplo, el Controller, Studio y Citrix License Server) y varios de esos componentes tienen nuevas versiones disponibles, se actualizarán todos al ejecutar el instalador.

   Si alguno de los componentes principales está instalado en máquinas que no sean el Controller, ejecute el instalador en cada una de esas máquinas. Se recomienda el siguiente orden: License Server, StoreFront y, a continuación, Director.

   Si aún no ha determinado si su servidor de licencias es compatible con la nueva versión (consulte Otras tareas de preparación), es vital que ejecute el instalador en el servidor de licencias antes de actualizar cualquier otro componente principal.

2. Si usa Citrix Provisioning, actualice los dispositivos de destino y los servidores de Citrix Provisioning. Siga las instrucciones indicadas en la documentación de Citrix Provisioning.

3. Ejecute el instalador en las máquinas con agentes VDA. (Consulte el paso 12 si utiliza imágenes maestras y Machine Creation Services.)

4. Ejecute el instalador del producto en la mitad de los Controllers. (Ejecutar el instalador también actualiza los demás componentes principales instalados en esos servidores.) Por ejemplo, si el 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. Puede ocurrir que la capacidad del sitio se vea reducida debido a que 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

5. Si Studio está instalado en otra máquina que no sea una de las actualizadas en el paso anterior, ejecute el instalador en la máquina donde está instalado Studio.
6. Desde el recién actualizado Studio, actualice la base de datos del sitio. Para obtener información más detallada, consulte Actualizar las bases de datos y el sitio.
7. Desde el recién actualizado Studio, seleccione **Citrix Studio** *nombre-de-sitio* en el panel de navegación. Seleccione la ficha **Tareas comunes**. Seleccione **Actualizar los Delivery Controllers restantes**.
8. Una vez completada la actualización y la confirmación, cierre y vuelva a abrir Studio. Es posible que Studio solicite una actualización adicional del sitio para registrar los servicios del Controller en el sitio o para crear un ID de zona si aún no existe.
9. En la sección **Configuración del sitio** de la página **Tareas comunes**, seleccione **Realizar registro**. Registrar los Controllers los convierte en disponibles para el sitio.
10. Una vez que seleccione **Finalizar** tras completarse el proceso de actualización, se le ofrece la oportunidad de inscribirse en los programas de telemetría de Citrix, que recopilan información anónima acerca de la implementación. Esta información se utiliza para mejorar la calidad, la fiabilidad y el rendimiento del producto.
11. Después de actualizar los componentes, la base de datos y el sitio, puede realizar pruebas en el sitio recién actualizado. Desde Studio, seleccione **Citrix Studio** *nombre-de-sitio* en el panel de navegación. Seleccione la ficha **Tareas comunes** y, a continuación, 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 de funcionamiento del sitio puede fallar si hay un Controller instalado en Windows Server 2016, cuando se utiliza una base de datos local SQL Server Express como la base de datos del sitio, si no se inicia el servicio SQL Server Browser. Para evitar este problema, lleve a cabo las siguientes tareas.

    a) Habilite el servicio SQL Server Browser (si fuera necesario) e inícielo.

    b) Reinicie el servicio SQL Server (SQLEXPRESS).
12. Si utiliza Machine Creation Services y quiere actualizar los VDA, después de actualizar y probar la implementación, actualice el VDA que se usa en esas imágenes maestras (si no lo ha hecho aún). Actualice las imágenes maestras que usan esos VDA. Consulte Actualizar o crear una nueva imagen maestra. Luego, actualice los catálogos de máquinas que usan esas imágenes maestras. Después de actualizar los catálogos, actualice los grupos de entrega que usan esos catálogos.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Actualizar las bases de datos y el sitio

Después de actualizar los VDA y los componentes principales, use el recién actualizado Studio para iniciar una actualización manual o automática de la base de datos y del sitio.

Recuerde: Consulte Preparar, indicado más arriba para ver los requisitos de permisos.

- 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.
- Para realizar una actualización manual, el usuario de Studio ejecuta algunos de los scripts generados desde Studio. El Administrador de base de datos ejecuta otros scripts, ya sea desde la herramienta SQLCMD o SQL Server Management Studio en modo SQLCMD. De lo contrario, puede haber errores de inexactitud.

Citrix recomienda encarecidamente que realice una copia de seguridad de la base de datos antes de actualizarla. Consulte CTX135207. Durante la actualización de una base de datos, los servicios del producto están inhabilitados. Tenga en cuenta que, durante ese proceso, los Controllers no pueden actuar como intermediarios o brokers en las nuevas conexiones al sitio.

Una vez actualizada la base de datos y habilitados los servicios de los productos, Studio prueba 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.

Actualizar automáticamente la base de datos y el sitio:

Inicie el recién actualizado Studio. Después de seleccionar el inicio de la actualización del sitio automáticamente y de confirmar que está listo, comienza el proceso de actualización del sitio y de la base de datos.

Actualizar manualmente la base de datos y el sitio:

1. Inicie el recién actualizado Studio. Elija actualizar el sitio manualmente. El asistente comprueba la compatibilidad de License Server y solicita confirmación. Después de confirmar 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 cambia 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 UpgradeLoggingDatabsae.sql no se genera.

2. Ejecute los siguientes scripts en el orden indicado.

   - **DisableServices.ps1:** Script de PowerShell que debe ejecutar el usuario de Studio en un Controller para inhabilitar los servicios del producto.
   - **UpgradeSiteDatabase.sql:** Script de SQL que debe ejecutar el administrador de la base de datos en el servidor que contiene la base de datos del sitio.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **UpgradeMonitorDatabase.sql:** Script de SQL que debe ejecutar el administrador de la base de datos en el servidor que contiene la base de datos de supervisión.
- **UpgradeLoggingDatabase.sql:** Script de SQL que debe ejecutar el administrador de la base de datos 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 una revisión hotfix).
- **EnableServices.ps1:** Script de PowerShell que debe ejecutar el usuario de Studio en un Controller para habilitar los servicios del producto.

3. Después de completar las tareas de la lista de verificación, haga clic en **Finalizar actualización**.

Actualizar un servidor de trabajo XenApp 6.5 a un nuevo VDA

November 29, 2018

Después de migrar una comunidad XenApp 6.5, puede utilizar los servidores XenApp 6.5 que se habían configurado en el modo solo host de sesión (también conocido como servidores de trabajo o solo sesión). Para ello, elimine el software anterior, actualice el SO y, a continuación, instale un nuevo VDA para SO de servidor.

Aunque puede actualizar un servidor de trabajo XenApp 6.5, instalar el software actual de VDA en una máquina limpia ofrece una mayor seguridad.

Para actualizar un servidor de trabajo XenApp 6.5 a un nuevo VDA:

1. Quite Hotfix Rollup Pack 7 para XenApp 6.5 siguiendo las instrucciones descritas en el archivo Léame del hotfix. Consulte CTX202095.
2. Desinstale XenApp 6.5 siguiendo las instrucciones de Eliminar roles y componentes. Este proceso requiere varios reinicios. Si se produce un error durante el proceso de desinstalación, compruebe el registro de errores de desinstalación al que hace referencia el mensaje de error. El archivo de registro se encuentra en la carpeta "%TEMP%\Citrix\XenDesktop Installation\XenApp 6.5 Uninstall Log Files\".
3. Actualice el sistema operativo del servidor a una versión admitida. Para ver una lista de las plataformas respaldadas, consulte la sección de VDA para SO de servidor en Requisitos del sistema.
4. Instale un VDA para SO de servidor mediante un instalador suministrado con esta versión. Consulte Instalar agentes VDA o Instalar desde la línea de comandos.

Después de instalar el nuevo VDA, desde Studio en el nuevo sitio de XenApp, cree catálogos de máquinas (o modifique los existentes) para los servidores de trabajo actualizados.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Solucionar problemas

Falla la eliminación del software de XenApp 6.5. Los registros de desinstalación contienen el mensaje: "Error 25703. An error occurred while plugging XML into Internet Information Server. Setup cannot copy files to your IIS Scripts directory. Please make sure that your IIS installation is correct."

Causa: El problema ocurre en sistemas donde (1) durante el proceso inicial de instalación de XenApp 6.5, usted indicó que Citrix XML Service (CtxHttp.exe) no debe compartir el puerto con IIS, y (2) .NET Framework 3.5.1 está instalado.

Solución:

1. Quite el rol de Servidor web (IIS) usando el asistente para quitar roles del servidor. (Puede volver a instalar el rol de Servidor web (IIS) más tarde.)
2. Reinicie el servidor.
3. Mediante Agregar o quitar programas, desinstale Citrix XenApp 6.5 y Microsoft Visual C++ 2005 Redistributable (x64), versión 8.0.56336.
4. Reinicie el servidor.
5. Instale el VDA para SO de servidor.

Migrar XenApp 6.x

March 14, 2019

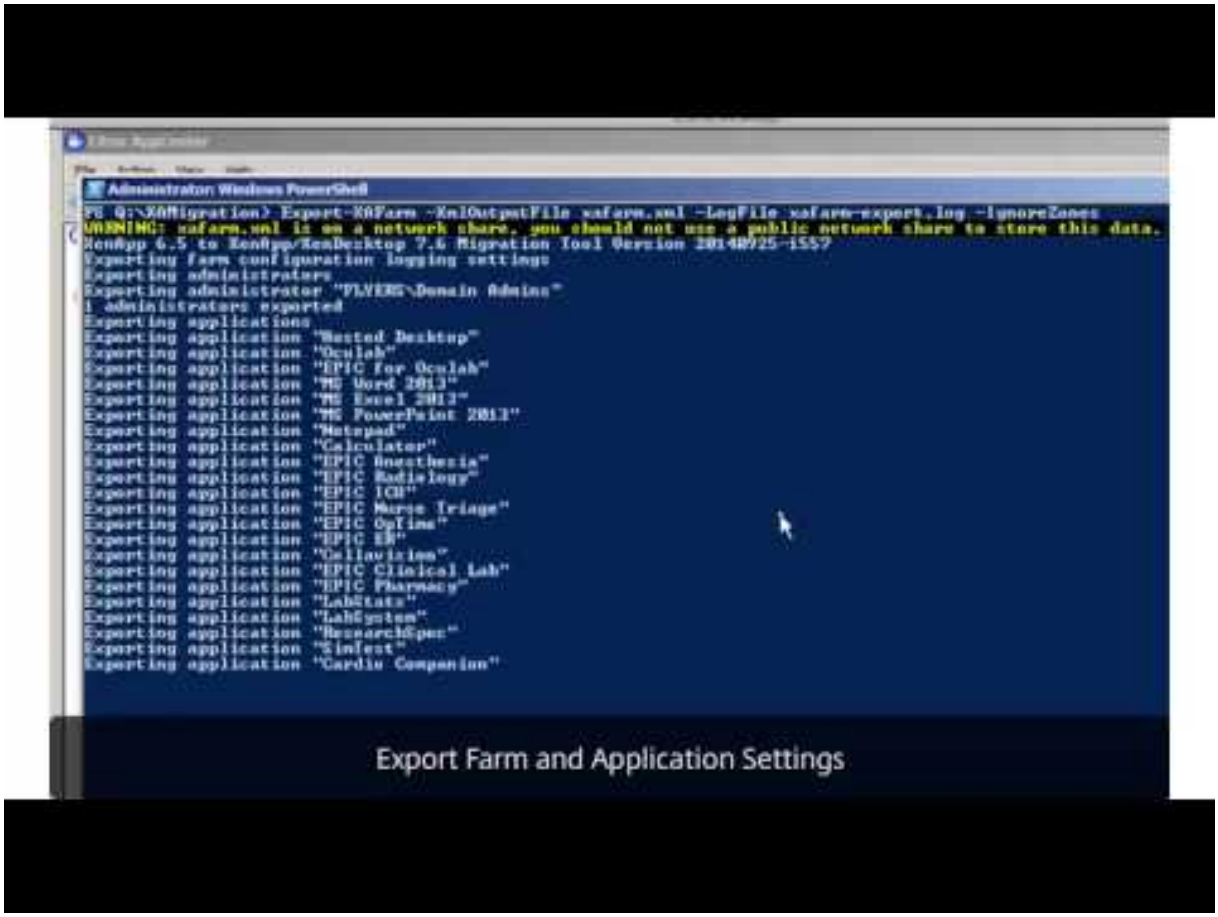
Puede usar la herramienta de migración descrita en este artículo para migrar de XenApp 6.x a XenApp 7.6. Luego, puede actualizar desde XenApp 7.6 a una versión LTSR respaldada o la versión actual de Citrix Virtual Apps and Desktops; consulte Actualizar una implementación.

Herramienta de migración de XenApp 6.x

La herramienta de migración de XenApp 6.x (Migration Tool) es una colección de scripts de PowerShell que contienen cmdlets para migrar los datos de las comunidades y las directivas de XenApp 6.x (6.0 o 6.5). En el servidor del Controller de XenApp 6.x, ejecute los cmdlets de exportación que recopilan dichos datos en archivos XML. A continuación, desde el Controller de XenApp 7.6, ejecute los cmdlets de importación, que crean objetos usando los datos recopilados durante la exportación.

Dispone aquí de un vídeo resumen sobre la herramienta de migración:

© 1999-2019 Citrix Systems, Inc. All rights reserved.



La siguiente secuencia resume el proceso de migración, los detalles se proporcionan más adelante.

1. En un Controller de XenApp 6.0 o 6.5:
   a) Importe los módulos de exportación de PowerShell.
   b) Ejecute los cmdlets de exportación para exportar datos de la comunidad y/o de directivas en archivos XML.
2. Copie los archivos XML (y la carpeta de iconos si eligió no incrustarlos en los archivos XML durante la exportación) en el Controller de XenApp 7.6.
3. En el Controller de XenApp 7.6:
   a) Importe los módulos de importación de PowerShell.
   b) Ejecute los cmdlets de importación para importar los datos de la comunidad (aplicaciones) y/o de directivas, usando los archivos XML como entrada.
4. Complete los pasos posteriores a la migración.

Antes de iniciar una migración real, puede exportar la configuración de XenApp 6.x y, a continuación, realizar una vista previa de la importación en el sitio de XenApp 7.6. La vista previa puede identificar posibles puntos de fallo para que usted pueda resolver los problemas antes de ejecutar la importación en sí. Por ejemplo, una vista previa puede detectar que ya existe una aplicación con el mismo nombre en el nuevo sitio de XenApp 7.6. También puede usar los archivos de registros generados a partir de

© 1999-2019 Citrix Systems, Inc. All rights reserved.

la vista previa como guía para la migración.

A menos que se indique lo contrario, el término 6.x hace referencia a XenApp 6.0 o 6.5.

Paquete de herramienta de migración

La herramienta de migración está disponible en el sitio de descargas de la herramienta de migración de XenApp 7.6. El archivo XAMigration.zip contiene dos paquetes separados:

- **ReadIMA.zip:** Contiene los archivos utilizados para exportar datos desde las comunidades de XenApp 6.x, además de módulos compartidos.

Módulo o archivo	Descripción
ExportPolicy.psm1	Módulo de script de PowerShell para exportar las directivas de XenApp 6.x a un archivo XML.
ExportXAFarm.psm1	Módulo de scripts de PowerShell para exportar la configuración de la comunidad de XenApp 6.x a un archivo XML.
ExportPolicy.psd1	Archivo de manifiesto de PowerShell para el módulo de script ExportPolicy.psm1.
ExportXAFarm.psd1	Archivo de manifiesto de PowerShell para el módulo de script ExportXAFarm.psm1.
LogUtilities.psm1	Módulo de script compartido de PowerShell que contiene las funciones de registro.
XmlUtilities.psd1	Archivo de manifiesto de PowerShell para el módulo de script XmlUtilities.psm1.
XmlUtilities.psm1	Módulo de script compartido de PowerShell que contiene las funciones de XML.

- **ImportFMA.zip:** Contiene los archivos utilizados para importar datos en las comunidades de XenApp 7.6, además de módulos compartidos.

Módulo o archivo	Descripción
ImportPolicy.psm1	Módulo de scripts de PowerShell para importar las directivas en XenApp 7.6.
ImportXAFarm.psm1	Módulo de scripts de PowerShell para importar las aplicaciones en XenApp 7.6.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Módulo o archivo	Descripción
ImportPolicy.psd1	Archivo de manifiesto de PowerShell para el módulo de script ImportPolicy.psm1.
ImportXAFarm.psd1	Archivo de manifiesto de PowerShell para el módulo de script ImportXAFarm.psm1.
PolicyData.xsd	Esquema XML para datos de directivas.
XAFarmData.xsd	Esquema XML para datos de la comunidad XenApp.
LogUtilities.psm1	Módulo de script compartido de PowerShell que contiene las funciones de registro.
XmlUtilities.psd1	Archivo de manifiesto de PowerShell para el módulo de script XmlUtilities.psm1.
XmlUtilities.psm1	Módulo de script compartido de PowerShell que contiene las funciones de XML.

Limitaciones

- No se importan todas las configuraciones de directivas; consulte Configuraciones de directivas que no se importan. Las configuraciones que no son compatibles se ignoran y esto se indica en el archivo de registros.
- Aunque se recopilan detalles de todas las aplicaciones en el archivo XML de salida durante la operación de exportación, solo se importan en el sitio de XenApp 7.6 las aplicaciones instaladas en el servidor. Los escritorios publicados, el contenido y la mayoría de las aplicaciones distribuidas por streaming no reciben respaldo (consulte los parámetros del cmdlet Import-XAFarm en Importar datos: paso a paso para ver las excepciones).
- Los servidores de aplicaciones no se importan.
- Muchas de las propiedades de aplicación no se importan debido a diferencias entre la arquitectura IMA (Independent Management Architecture) de XenApp 6.x y las tecnologías FlexCast Management Architecture (FMA) de XenApp 7.6; consulte Asignación de propiedades de aplicaciones.
- Se crea un grupo de entrega durante la importación. Consulte Uso avanzado para obtener más información sobre cómo usar los parámetros para filtrar lo que se importa.
- Solo se importan las configuraciones de directiva de Citrix creadas con la consola de administración de AppCenter; las configuraciones de directiva de Citrix creadas con objetos de directiva de grupo (GPO) de Windows no se importan.
- Los scripts de migración están diseñados para las migraciones desde XenApp 6.x a XenApp 7.6

© 1999-2019 Citrix Systems, Inc. All rights reserved.

únicamente.
- Studio no respalda el uso de carpetas anidadas a más de cinco niveles de profundidad, por lo que no se importarán. Si la estructura de carpetas de aplicaciones incluye carpetas a más de cinco niveles de profundidad, considere la posibilidad de reducir la cantidad de niveles de anidación de carpetas antes de realizar la importación.

Consideraciones sobre seguridad

Los archivos XML creados por los scripts de exportación pueden contener información confidencial acerca de su entorno y organización, como nombres de usuario, nombres de servidor, y otros datos de configuración de directivas, comunidades y aplicaciones de XenApp. Almacene y gestione estos archivos en entornos seguros.

Repase cuidadosamente los archivos XML antes de usarlos como material para la importación de directivas y aplicaciones, y compruebe que no contienen modificaciones no autorizadas.

Las asignaciones de objeto de directiva (antes conocidas como filtros de directivas) son las que gestionan la forma en que se aplican las directivas. Después de importar las directivas, revise meticulosamente las asignaciones de objeto de cada directiva para comprobar que no haya vulnerabilidades de seguridad a raíz de la importación. Tras la importación, se pueden aplicar a la directiva diferentes conjuntos de usuarios, direcciones IP o nombres de cliente. Después de la importación, es posible que los parámetros “Permitir” o “Denegar” tengan implicaciones diferentes.

Capturar registros y controlar errores

Los scripts ofrecen gran cantidad de registros que hacen un seguimiento de todas las ejecuciones de cmdlets, mensajes informativos, resultados de la ejecución de cmdlets, advertencias y errores.

- Queda registrada la mayor parte del uso de cmdlets de PowerShell de Citrix. Se registran todos los cmdlets de PowerShell en los scripts de importación que crean nuevos objetos del sitio.
- Se registra el progreso de la ejecución de scripts, incluidos los objetos procesados.
- Se registran las principales acciones que afectan al flujo de trabajo, incluidos flujos dirigidos desde la línea de comandos.
- Se registran todos los mensajes que se imprimen en la consola, incluidas las advertencias y los errores.
- Cada línea recibe una marca de hora, con precisión de milésima de segundo.

Citrix recomienda especificar un archivo de registros cuando se ejecute cada uno de los cmdlets de importación y exportación.

Si no se especifica un nombre de archivo de registros, el archivo de registros se almacena en la carpeta principal del usuario (especificada por la variable $HOME de PowerShell) si dicha carpeta existe;

© 1999-2019 Citrix Systems, Inc. All rights reserved.

de lo contrario, se coloca en la carpeta de ejecución del script actual. El nombre predeterminado de los registros es “XFarmYYYYMMDDHHmmSS-xxxxxx” donde los últimos seis dígitos son un número aleatorio.

De forma predeterminada, se muestra toda la información de progreso. Para evitar que se muestre, especifique el parámetro NoDetails en los scripts de exportación e importación.

Por lo general, la ejecución de un script se detiene cuando se encuentra un error, y se puede ejecutar el cmdlet de nuevo después de eliminar las condiciones de error.

Las condiciones que no se consideran errores se registran; muchas se notifican como advertencias, y la ejecución del script continúa. Por ejemplo, los tipos de aplicación sin respaldo se notifican como advertencias y no se importan. Las aplicaciones que ya existen en el sitio de XenApp 7.6 no se importan. Las configuraciones de directiva obsoletas en XenApp 7.6 no se importan.

Los scripts de migración usan muchos cmdlets de PowerShell y puede ser que no se registren todos los errores posibles. Para ver información adicional sobre la cobertura de registros, use la funcionalidad de registros de PowerShell. Por ejemplo, las transcripciones de PowerShell registran todo lo que se imprime en pantalla. Para obtener más información, consulte la ayuda de los cmdlets Start-Transcript y Stop-Transcript.

Requisitos, preparación y procedimientos recomendados

Para migrar, debe usar el SDK de Citrix XenApp 6.5. Descargue ese SDK desde https://www.citrix.com/downloads/xenapp/sdks/powershell-sdk.html.

Consulte este artículo antes de iniciar una migración.

Es necesario comprender los conceptos básicos de PowerShell sobre directiva de ejecución, módulos, cmdlets y scripts. Aunque no es necesario tener una amplia experiencia en creación de scripts, es conveniente entender los cmdlets que hay que ejecutar. Use el cmdlet Get-Help para consultar la ayuda de cada cmdlet de migración antes de ejecutarlo. Por ejemplo: `Get-Help -full Import-XAFarm`.

Especifique un archivo de registros en la línea de comandos y consulte siempre el archivo de registros después de ejecutar el cmdlet. Si un script falla, compruebe y corrija el error identificado en el archivo de registros y, a continuación, ejecute el cmdlet de nuevo.

Tenga en cuenta

- Para facilitar la entrega de aplicaciones mientras hay dos implementaciones ejecutándose (la comunidad de XenApp 6.x y el nuevo sitio de XenApp 7.6), puede realizar un agregado de ambas implementaciones en StoreFront o la Interfaz Web. Consulte la documentación de la versión de StoreFront o la Interfaz Web que esté usando.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Los datos de iconos de las aplicaciones se pueden gestionar de dos formas:
  - Si especifica el parámetro EmbedIconData en el cmdlet Export-XAFarm, los datos de iconos de aplicaciones se incrustan en el archivo XML.
  - Si no especifica el parámetro EmbedIconData en el cmdlet Export-XAFarm, los datos de iconos de aplicaciones exportados se almacenan en una carpeta cuyo nombre se forma añadiendo la cadena "-icons" al nombre básico del archivo XML de salida. Por ejemplo, si el parámetro XmlOutputFile es "FarmData.xml", se creará la carpeta "FarmData-icons" para almacenar los iconos de aplicaciones.

    Los archivos de datos de iconos de esta carpeta son archivos .txt nombrados usando el nombre de explorador de la aplicación publicada (aunque los archivos son .txt, los datos guardados son datos de icono binarios codificados que el script de importación puede leer para volver a crear el icono de la aplicación). Durante la operación de importación, si la carpeta de iconos no se encuentra en la misma ubicación que el archivo XML de importación, se usan iconos genéricos para cada aplicación importada.
- Los nombres de los módulos de script, archivos de manifiesto, módulo compartido y cmdlets son similares. Ponga cuidado al utilizar el procedimiento de completar con tabulador, para evitar errores. Por ejemplo, Export-XAFarm es un cmdlet. ExportXAFarm.psd1 y ExportXAFarm.psm1 son archivos que no se pueden ejecutar.
- En las secciones paso a paso siguientes, la mayoría de los valores de parámetro de <cadena> van entre comillas. Estas son optativas si la cadena solo es de una palabra.

Para exportar desde el servidor XenApp 6.x

- La exportación debe ejecutarse en un servidor XenApp 6.x configurado con el modo de servidor Controller y host de sesión (comúnmente llamado Controller).
- Para ejecutar los cmdlets de exportación, hay que ser un administrador XenApp con permisos para leer objetos. También hay que tener suficientes permisos de Windows para ejecutar scripts de PowerShell; los procedimientos paso a paso siguientes contienen instrucciones.
- Asegúrese de que el estado de integridad de la comunidad XenApp 6.x es correcto antes de comenzar una exportación. Haga una copia de respaldo de la base de datos de la comunidad. Verifique la integridad de la comunidad con la utilidad Citrix IMA Helper (CTX133983). En la ficha IMA Datastore, ejecute Master Check. A continuación, use la opción DSCheck para resolver las entradas no válidas. Repare cualquier problema que haya en la comunidad, antes de realizar la migración, para evitar fallos de exportación. Por ejemplo, si un servidor no se quitó correctamente de la comunidad, es posible que sus datos sigan existiendo en la base de datos; esto puede hacer que fallen los cmdlets del script de exportación (por ejemplo, Get-XAServer -ZoneName). Si los cmdlets fallan, el script falla.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Puede ejecutar los cmdlets de exportación en una comunidad de servidores en ejecución, con conexiones de usuario activas, ya que los scripts de exportación solo leen los datos estáticos de directivas y configuración de la comunidad.

Para importar en el servidor XenApp 7.6

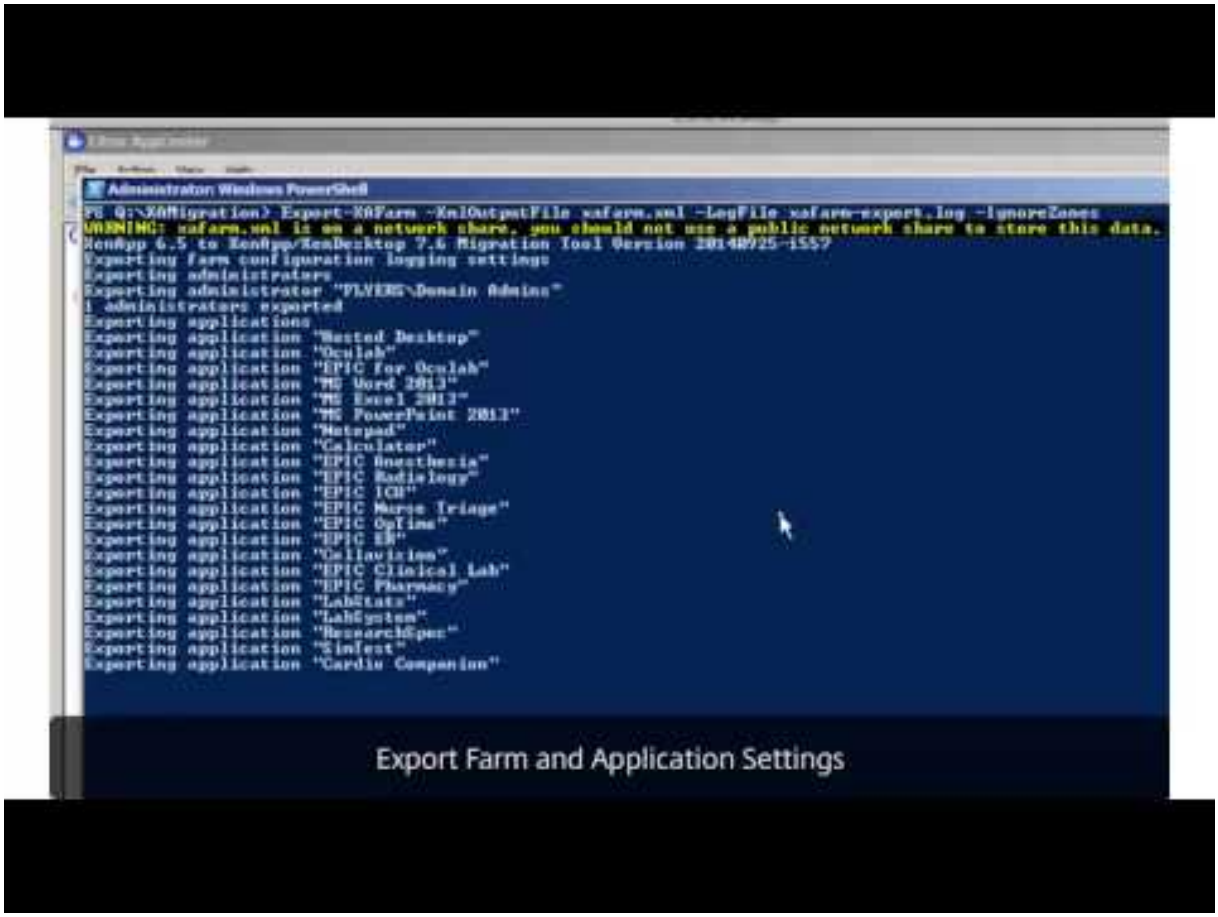
- Puede importar datos a las implementaciones de XenApp 7.6 (y versiones posteriores admitidas). Debe instalar un Controller de XenApp 7.6 y Studio, y crear un sitio, antes de importar los datos exportados desde la comunidad XenApp 6.x. Aunque los VDA no son necesarios para importar configuraciones, permiten que los tipos de archivo de las aplicaciones estén disponibles.
- Para ejecutar los cmdlets de importación de XenApp, debe ser un administrador XenApp con permisos para leer y crear objetos. Un administrador total tiene estos permisos. También hay que tener suficientes permisos de Windows para ejecutar scripts de PowerShell; los procedimientos paso a paso siguientes contienen instrucciones.
- No debe haber otras conexiones de usuario activas durante una importación. Los scripts de importación crean muchos objetos nuevos y pueden producirse interrupciones si hay otros usuarios cambiando la configuración al mismo tiempo.

Recuerde que puede exportar datos y, a continuación, usar el parámetro -Preview con los cmdlets de importación para tener una vista previa de lo que sucedería durante una importación real, sin importar nada todavía. Los registros indicarán exactamente lo que sucedería durante la importación; si se producen errores, resuélvalos antes de iniciar la importación real.

Exportar datos: paso a paso

Dispone aquí de un vídeo sobre el proceso de exportación.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Complete los siguientes pasos para exportar datos desde un Controller de XenApp 6.x a archivos XML.

1. Descargue el paquete de la herramienta de migración XAMigration.zip desde el sitio de descargas de Citrix. Para mayor comodidad, colóquelo en un recurso compartido de archivos en la red, al que tengan acceso tanto la comunidad XenApp 6.x como el sitio XenApp 7.6. Descomprima XAMigration.zip en el recurso compartido de archivos en la red. Se descomprimirá en otros dos archivos zip: ReadIMA.zip e ImportFMA.zip.
2. Inicie la sesión en el Controller de XenApp 6.x como un administrador de XenApp con, al menos, permiso de solo lectura y permisos de Windows para ejecutar scripts de PowerShell.
3. Copie ReadIMA.zip desde el recurso compartido de archivos de la red al Controller de XenApp 6.x. Descomprima y extraiga el contenido de ReadIMA.zip en el Controller en una carpeta (por ejemplo: C:\XAMigration).
4. Abra una consola de PowerShell y establezca como directorio actual el directorio donde se encuentran los scripts. Por ejemplo: `cd C:\XAMigration`.
5. Ejecute `Get-ExecutionPolicy` para consultar la directiva de ejecución de scripts.
6. Establezca la directiva de ejecución de scripts como, al menos, RemoteSigned para permitir que los scripts se ejecuten. Por ejemplo: `Set-ExecutionPolicy RemoteSigned`.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

7. Importe los archivos de definición de módulos ExportPolicy.psd1 y ExportXAFarm.psd1: `Import-Module .\\ExportPolicy.psd1` y `Import-Module .\\ExportXAFarm.psd1`.

   Tenga en cuenta

   - Si va a exportar solo datos de directivas, importe solo el archivo de definición de módulos ExportPolicy.psd1. Del mismo modo, si va a importar solo los datos de la comunidad, importe solo ExportXAFarm.psd1.
   - Al importar los archivos de definición de módulos también se agregan los complementos de PowerShell requeridos.
   - No importe los archivos de script .psm1.

8. Para exportar datos de directiva y datos de comunidad, ejecute los siguientes cmdlets.

Datos de directiva: ejecute `Export-Policy`.

Parámetro	Descripción
-XmlOutputFile “*cadena*.xml”	Nombre del archivo XML resultante; este archivo contendrá los datos exportados. Debe tener la extensión .xml. El archivo no debe existir previamente, pero si se especifica una ruta, la ruta sí debe existir. Valor predeterminado: Ninguno; este parámetro es obligatorio.
-LogFile *cadena*	El nombre del archivo de registros. La extensión es optativa. Si aún no existe, el archivo se creará. Si el archivo existe y se especifica también el parámetro NoClobber, se genera un error; de lo contrario, el contenido del archivo se sobrescribe. Valor predeterminado: Consulte Capturar registros y controlar errores.
-NoLog	No se generan registros. Este parámetro anula el parámetro LogFile si ambos están especificados. Valor predeterminado: False; se generan registros

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Parámetro	Descripción
-NoClobber	No sobrescribir el archivo de registros existente especificado en el parámetro LogFile. Si el archivo de registros no existe, este parámetro no tiene ningún efecto. Valor predeterminado: False; si el archivo de registros ya existe, se sobrescribe
-NoDetails	No enviar a la consola informes detallados acerca de la ejecución de los scripts. Valor predeterminado: False; se envían informes detallados a la consola
-SuppressLogo	No imprimir el mensaje “XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #aaaaMMdd-hhmm#” en la consola. Este mensaje identifica la versión del script y puede resultar útil durante la solución de problemas. Citrix recomienda omitir este parámetro. Valor predeterminado: False; el mensaje se imprime en la consola

Ejemplo: El cmdlet siguiente exporta la información sobre directivas al archivo XML denominado MyPolicies.xml. La operación genera registros que se guardan en el archivo MyPolicies.log.

```
Export-Policy -XmlOutputFile ".\MyPolicies.XML"-LogFile ".\MyPolicies.Log"
```

Datos de comunidad: ejecute `Export-XAFarm`.

Parámetro	Descripción
XmlOutputFile “*cadena*.xml”	Nombre del archivo XML resultante; este archivo contendrá los datos exportados. Debe tener la extensión .xml. El archivo no debe existir previamente, pero si se especifica una ruta, la ruta sí debe existir. Valor predeterminado: Ninguno; este parámetro es obligatorio.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Parámetro	Descripción
-LogFile “*cadena*”	El nombre del archivo de registros. La extensión es optativa. Si aún no existe, el archivo se creará. Si el archivo existe y se especifica también el parámetro NoClobber, se genera un error; de lo contrario, el contenido del archivo se sobrescribe. Valor predeterminado: Consulte Capturar registros y controlar errores.
-NoLog	No se generan registros. Este parámetro anula el parámetro LogFile si ambos están especificados. Valor predeterminado: False; se generan registros
-NoClobber	No sobrescribir el archivo de registros existente especificado en el parámetro LogFile. Si el archivo de registros no existe, este parámetro no tiene ningún efecto. Valor predeterminado: False; si el archivo de registros ya existe, se sobrescribe
-NoDetails	No enviar a la consola informes detallados acerca de la ejecución de los scripts. Valor predeterminado: False; se envían informes detallados a la consola
-SuppressLogo	No imprimir el mensaje “XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #aaaaMMdd-hhmm#” en la consola. Este mensaje identifica la versión del script y puede resultar útil durante la solución de problemas. Citrix recomienda omitir este parámetro. Valor predeterminado: False; el mensaje se imprime en la consola
-IgnoreAdmins	No exportar la información de administradores. Consulte Uso avanzado. Valor predeterminado: False; se exporta la información sobre administradores

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Parámetro	Descripción
-IgnoreApps	No exportar información de aplicaciones. Consulte Uso avanzado. Valor predeterminado: False; se exporta la información sobre aplicaciones
-IgnoreServers	No exportar información de servidores. Valor predeterminado: False; se exporta la información sobre servidores
-IgnoreZones	No exportar información de zonas. Valor predeterminado: False; se exporta la información sobre zonas
-IgnoreOthers	No exportar otros tipos de información como el registro de configuración, los patrones de carga, las directivas de equilibrio de carga, los controladores de impresora y los grupos de trabajo. Valor predeterminado: False; se exportan otros tipos de información. La finalidad de este modificador de línea de comandos es permitir continuar una exportación aunque haya un error, siempre que el error no afecte a los datos en sí utilizados en el proceso de importación o exportación.
-AppLimit *número entero*	Cantidad de aplicaciones a exportar. Consulte Requisitos, preparación y procedimientos recomendados. Valor predeterminado: se exportan todas las aplicaciones
-EmbedIconData	Incrustar los datos de iconos de aplicaciones en el mismo archivo XML donde están los otros objetos. Valor predeterminado: los iconos se guardan por separado. Consulte Requisitos, preparación y procedimientos recomendados.
-SkipApps *número entero*	Cantidad de aplicaciones a omitir. Consulte Uso avanzado. Valor predeterminado: no se omite ninguna aplicación

Ejemplo: El cmdlet siguiente exporta la información sobre la comunidad al archivo XML denominado

© 1999-2019 Citrix Systems, Inc. All rights reserved.

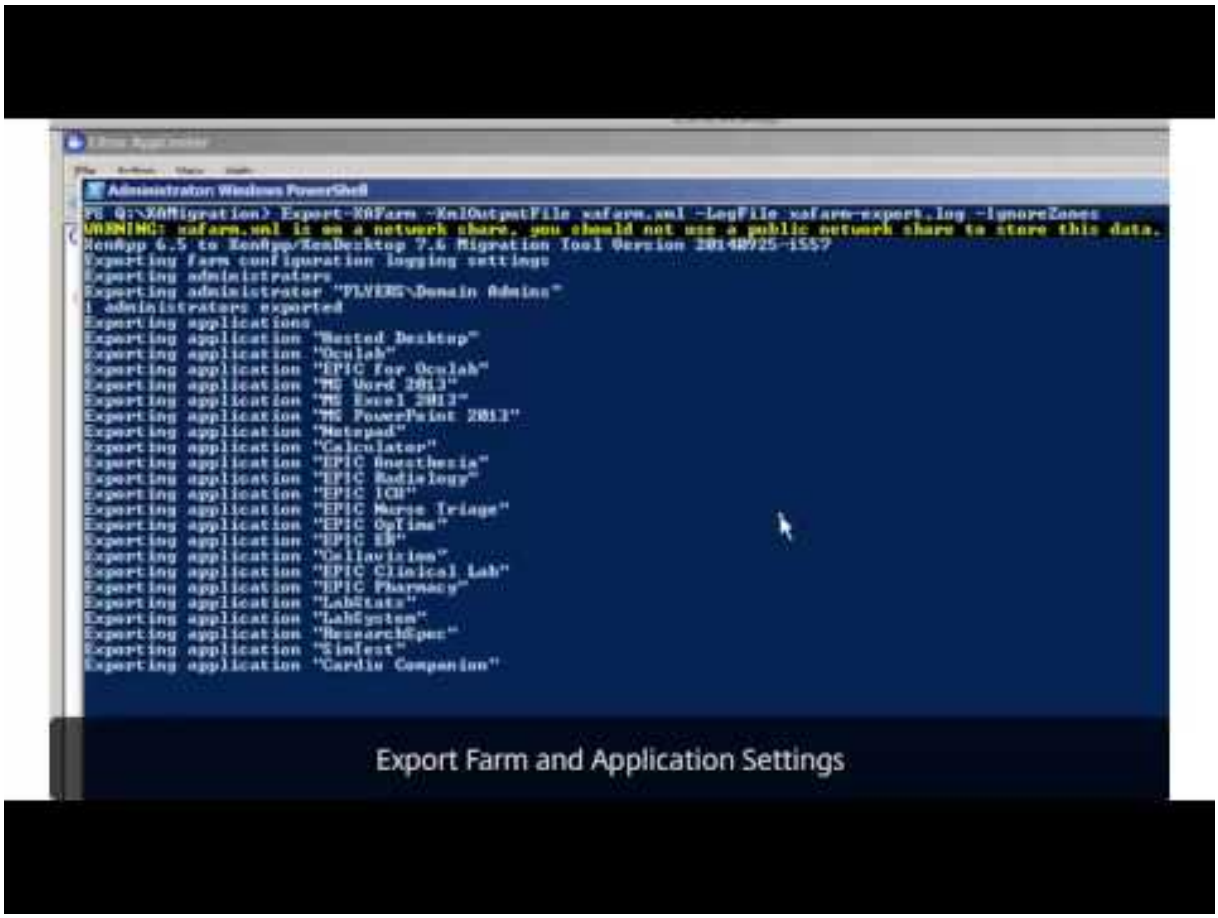
MyFarm.xml. La operación genera registros que se guardan en el archivo MyFarm.log. Se crea una carpeta denominada “MyFarm-icons” para almacenar los archivos de datos de iconos de las aplicaciones; esta carpeta está en la misma ubicación que MyFarm.XML.

```
Export-XAFarm -XmlOutputFile ".\MyFarm.XML"-LogFile ".\MyFarm.Log"
```

Una vez ejecutados los scripts de exportación, los archivos XML especificados en las líneas de comandos contienen los datos de la comunidad XenApp y las directivas. Los archivos de iconos de aplicaciones contienen archivos de datos de icono, y el archivo de registros indica qué ocurrió durante la exportación.

Importar datos: paso a paso

Dispone aquí de un vídeo sobre el proceso de importación.



Recuerde que puede ejecutar una vista previa de la importación (usando los comandos `Import-Policy` o `Import-XAFarm` con el parámetro Preview) y consultar los archivos de registros antes de realizar la importación propiamente dicha.

Complete los siguientes pasos para importar datos a un sitio de XenApp 7.6, usando los archivos XML generados en la exportación.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

1. Inicie una sesión en el Controller de XenApp 7.6 como administrador con permisos de lectura/escritura y con permisos Windows para ejecutar scripts de PowerShell.
2. Si aún no ha descomprimido el paquete de la herramienta de migración XAMigration en el recurso compartido de archivos de la red, descomprímalo ahora. Copie ImportFMA.zip desde el recurso compartido de archivos de la red al Controller de XenApp 7.6. Descomprima y extraiga el contenido de ImportFMA.zip en el Controller en una carpeta (por ejemplo: C:\XAMigration).
3. Copie los archivos XML (los archivos de salida generados durante la exportación) desde el Controller de XenApp 6.x a la misma ubicación del Controller de XenApp 7.6 donde extrajo los archivos de ImportFMA.zip.

   Si eligió no incrustar los datos de iconos de aplicaciones en el archivo XML de salida al ejecutar el cmdlet Export-XAFarm, asegúrese de que copia la carpeta y los archivos de los datos de iconos en la misma ubicación del Controller de XenApp 7.6 donde ya se encuentra el archivo XML de salida que contiene los datos de aplicaciones y los archivos extraídos de ImportFMA.zip.
4. Abra una consola de PowerShell y establezca como directorio actual el directorio donde se encuentran los scripts: `cd C:\XAMigration`.
5. Ejecute `Get-ExecutionPolicy` para consultar la directiva de ejecución de scripts.
6. Establezca la directiva de ejecución de scripts como, al menos, RemoteSigned para permitir que los scripts se ejecuten. Por ejemplo: `Set-ExecutionPolicy RemoteSigned`.
7. Importe los archivos de definición de módulos ImportPolicy.psd1 y ImportXAFarm.psd1: `Import-Module .\\ImportPolicy.psd1` y `Import-Module .\\ImportXAFarm.psd1`.

   Conviene tener en cuenta lo siguiente:

   - Si va a importar solo datos de directivas, importe solo el archivo de definición de módulos ImportPolicy.psd1. Del mismo modo, si va a importar solo los datos de la comunidad, importe solo ImportXAFarm.psd1.
   - Al importar los archivos de definición de módulos también se agregan los complementos de PowerShell requeridos.
   - No importe los archivos de script .psm1.
8. Para importar datos de directiva y datos de comunidad, ejecute los siguientes cmdlets.

Datos de directiva: Ejecute `Import-Policy`. Deberá especificar el archivo XML que contiene los datos exportados de las directivas.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Parámetro	Descripción
-XmlInputFile “*cadena*.xml”	Nombre del archivo XML de entrada; este archivo contiene los datos recopilados tras ejecutar el cmdlet Export-Policy. Debe tener la extensión .xml. Valor predeterminado: Ninguno; este parámetro es obligatorio.
-XsdFile “*cadena*”	Nombre del archivo XSD. Los scripts de importación usan este archivo para validar la sintaxis del archivo XML de entrada. Consulte Uso avanzado. Valor predeterminado: PolicyData.XSD
-LogFile “*cadena*”	El nombre del archivo de registros. Si copió los archivos de registros de exportación en este servidor, use un nombre de archivo distinto para los registros del cmdlet de importación. Valor predeterminado: Consulte Capturar registros y controlar errores.
-NoLog	No se generan registros. Este parámetro anula el parámetro LogFile si ambos están especificados. Valor predeterminado: False; se generan registros
-NoClobber	No sobrescribir el archivo de registros existente especificado en el parámetro LogFile. Si el archivo de registros no existe, este parámetro no tiene ningún efecto. Valor predeterminado: False; si el archivo de registros ya existe, se sobrescribe
-NoDetails	No enviar a la consola informes detallados acerca de la ejecución de los scripts. Valor predeterminado: False; se envían informes detallados a la consola

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Parámetro	Descripción
-SuppressLogo	No imprimir el mensaje “XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #aaaaMMdd-hhmm#” en la consola. Este mensaje identifica la versión del script y puede resultar útil durante la solución de problemas. Citrix recomienda omitir este parámetro. Valor predeterminado: False; el mensaje se imprime en la consola
-Preview	Realizar una vista previa de la importación: leer los datos del archivo XML de entrada, pero sin importar los objetos en el sitio. El archivo de registros y la consola indican qué ocurre durante la vista previa de la importación. La vista previa muestra a los administradores lo que sucedería durante una importación real. Valor predeterminado: False; se produce una importación real

Ejemplo: El cmdlet siguiente importa la información sobre directivas desde el archivo XML denominado MyPolicies.xml. La operación genera registros que se guardan en el archivo MyPolicies.log.

```
Import-Policy -XmlInputFile ”.\MyPolicies.XML”-LogFile ”.\MyPolicies.Log”
```

Aplicaciones: Ejecute `Import-XAFarm`. Deberá especificar un archivo de registros y el archivo XML que contiene los datos exportados de la comunidad de servidores.

Parámetro	Descripción
-XmlInputFile “*cadena*.xml”	Nombre del archivo XML de entrada; este archivo contiene los datos recopilados tras ejecutar el cmdlet Export-XAFarm. Debe tener la extensión .xml. Valor predeterminado: Ninguno; este parámetro es obligatorio.
-XsdFile “*cadena*”	Nombre del archivo XSD. Los scripts de importación usan este archivo para validar la sintaxis del archivo XML de entrada. Consulte Uso avanzado. Valor predeterminado: XAFarmData.XSD

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Parámetro	Descripción
-LogFile “*cadena*”	El nombre del archivo de registros. Si copió los archivos de registros de exportación en este servidor, use un nombre de archivo distinto para los registros del cmdlet de importación. Valor predeterminado: Consulte Capturar registros y controlar errores.
-NoLog	No se generan registros. Este parámetro anula el parámetro LogFile si ambos están especificados. Valor predeterminado: False; se generan registros
-NoClobber	No sobrescribir el archivo de registros existente especificado en el parámetro LogFile. Si el archivo de registros no existe, este parámetro no tiene ningún efecto. Valor predeterminado: False; si el archivo de registros ya existe, se sobrescribe
-NoDetails	No enviar a la consola informes detallados acerca de la ejecución de los scripts. Valor predeterminado: False; se envían informes detallados a la consola
-SuppressLogo	No imprimir el mensaje “XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #aaaaMMdd-hhmm#” en la consola. Este mensaje identifica la versión del script y puede resultar útil durante la solución de problemas. Citrix recomienda omitir este parámetro. Valor predeterminado: False; el mensaje se imprime en la consola

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Parámetro	Descripción
-Preview	Realizar una vista previa de la importación: leer los datos del archivo XML de entrada, pero sin importar los objetos en el sitio. El archivo de registros y la consola indican qué ocurre durante la vista previa de la importación. La vista previa muestra a los administradores lo que sucedería durante una importación real. Valor predeterminado: False; se produce una importación real
-DeliveryGroupName "*cadena*"	Nombre del grupo de entrega para todas las aplicaciones importadas. Consulte Uso avanzado. Valor predeterminado: "<*nombre de la comunidad XenApp*> - Delivery Group"
-MatchFolder "*cadena*"	Importar solo las aplicaciones que se encuentran en carpetas cuyos nombres coinciden con la cadena suministrada. Consulte Uso avanzado. Valor predeterminado: no se realiza ninguna búsqueda de coincidencias.
-NotMatchFolder "*cadena*"	Importar solo las aplicaciones que se encuentran en carpetas cuyos nombres no coinciden con la cadena suministrada. Consulte Uso avanzado. Valor predeterminado: no se realiza ninguna búsqueda de coincidencias.
-MatchServer "*cadena*"	Importar solo las aplicaciones que se encuentran en servidores cuyos nombres coinciden con la cadena suministrada. Consulte Uso avanzado.
-NotMatchServer "*cadena*"	Importar solo las aplicaciones que se encuentran en servidores cuyos nombres no coinciden con la cadena suministrada. Consulte Uso avanzado. Valor predeterminado: no se realiza ninguna búsqueda de coincidencias.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Parámetro	Descripción
-MatchWorkerGroup “*cadena*”	Importar solo las aplicaciones publicadas para grupos de trabajo cuyos nombres coinciden con la cadena suministrada. Consulte Uso avanzado. Valor predeterminado: no se realiza ninguna búsqueda de coincidencias.
-NotMatchWorkerGroup “*cadena*”	Importar solo las aplicaciones publicadas para grupos de trabajo cuyos nombres no coinciden con la cadena suministrada. Consulte Uso avanzado. Valor predeterminado: no se realiza ninguna búsqueda de coincidencias.
-MatchAccount “*cadena*”	Importar solo las aplicaciones publicadas para cuentas de usuarios cuyos nombres coinciden con la cadena suministrada. Consulte Uso avanzado. Valor predeterminado: no se realiza ninguna búsqueda de coincidencias.
-NotMatchAccount “*cadena*”	Importar solo las aplicaciones publicadas para cuentas de usuarios cuyos nombres no coinciden con la cadena suministrada. Consulte Uso avanzado. Valor predeterminado: no se realiza ninguna búsqueda de coincidencias.
-IncludeStreamedApps	Importar aplicaciones del tipo: “StreamedToClientOrServerInstalled”. (No se importan otras aplicaciones de streaming.) Valor predeterminado: las aplicaciones de streaming no se importan.
-IncludeDisabledApps	Importar aplicaciones que se han marcado como inhabilitadas. Valor predeterminado: las aplicaciones inhabilitadas no se importan

Ejemplo: El cmdlet siguiente importa aplicaciones desde el archivo XML denominado MyFarm.xml. La operación genera registros que se guardan en el archivo MyFarm.log.

```
Import-XAFarm -XmlInputFile ".\MyFarm.XML"-LogFile ".\MyFarm.Log"
```

Una vez completada correctamente la migración, hay que realizar las tareas posteriores a la migración.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Tareas posteriores a la migración

Una vez importadas las directivas y la configuración de la comunidad de XenApp 6.x en un sitio de XenApp 7.6, siga las siguientes instrucciones para asegurarse de que los datos se han importado correctamente.

Directivas y configuraciones de directivas

La importación de directivas es fundamentalmente una operación de copia, con la excepción de las directivas y configuraciones que son obsoletas y, por tanto, no se importan. La comprobación posterior a la migración consiste en comparar ambas partes.

1. El archivo de registros enumera todas las directivas y las configuraciones de directiva que se han importado y que se han omitido. Primero, revise el archivo de registros e identifique qué configuraciones y directivas no se importaron.
2. Compare las directivas de XenApp 6.x con las directivas importadas en XenApp 7.6. Los valores de las configuraciones deben quedar igual (excepto en el caso de las configuraciones obsoletas, como se indica en el paso siguiente).
    - Si la cantidad de directivas es pequeña, puede realizar una comparación visual entre las directivas que aparecen en AppCenter en XenApp 6.x y las directivas que aparecen en Studio en XenApp 7.6.
    - Si cuenta con una gran cantidad de directivas, puede que no sea posible hacer una comparación visual. En estos casos, use el cmdlet de exportación de directivas (Export-Policy) para exportar las directivas de XenApp 7.6 a un archivo XML diferente y, a continuación, use una herramienta de comparación de texto (como windiff) para comparar los datos de ese archivo con los datos que aparecen en el archivo XML usado durante la exportación de directivas desde XenApp 6.x.
3. Use la información de la sección Configuraciones de directivas que no se importan para determinar qué puede haber cambiado durante la importación. Si una directiva de XenApp 6.x solo contiene configuraciones obsoletas, la directiva no se importará. Por ejemplo, si una directiva de XenApp 6.x solo contiene configuraciones de pruebas de HMR, dicha directiva se omitirá por completo porque no hay ninguna configuración equivalente respaldada en XenApp 7.6.

   Algunas configuraciones de directiva de XenApp 6.x ya no reciben respaldo, pero la funcionalidad equivalente está implementada en XenApp 7.6. Por ejemplo, en XenApp 7.6, puede configurar una programación de reinicios para las máquinas con sistema operativo de servidor mediante la modificación de un grupo de entrega; esta funcionalidad se implementaba antes mediante configuraciones de directiva.
4. Revise y confirme cómo se aplicarán los filtros al sitio de XenApp 7.6 frente a cómo se usaban

© 1999-2019 Citrix Systems, Inc. All rights reserved.

en XenApp 6.x; las diferencias significativas entre la comunidad XenApp 6.x y el sitio XenApp 7.6 pueden cambiar el efecto de los filtros.

Filtros

Examine con cuidado los filtros para cada directiva. Puede que sea necesario hacer cambios para asegurarse de que funcionen en XenApp 7.6 como funcionaban originalmente en XenApp 6.x.

Filtrar	Consideraciones
Control de acceso	El control de acceso debe tener los mismos valores que los filtros originales de XenApp 6.x y debe funcionar sin necesidad de hacer cambios.
Citrix CloudBridge	Un valor booleano; debe funcionar sin necesidad de hacer cambios. (Ahora, este producto se denomina NetScaler SD-WAN.)
Dirección IP del cliente	Enumera los intervalos de direcciones IP de cliente; cada intervalo se permite o se deniega. El script de importación conserva los valores, pero puede ser necesario hacer cambios si diferentes clientes se conectan a las máquinas VDA de XenApp 7.6.
Nombre del cliente	Al igual que sucede con el filtro de dirección IP de cliente, el script de importación conserva los valores, pero puede ser necesario hacer cambios si diferentes clientes se conectan a las máquinas VDA de XenApp 7.6.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Filtrar	Consideraciones
Unidad organizativa	Los valores pueden conservarse, dependiendo de si las OU se pueden resolver en el momento de la importación. Revise cuidadosamente este filtro, especialmente si las máquinas de XenApp 6.x y de XenApp 7.6 residen en dominios diferentes. Si no se configuran los valores de filtro correctamente, la directiva podría aplicarse a un conjunto incorrecto de unidades organizativas. Las unidades organizativas están representadas solo por nombres, por lo que existe la posibilidad de que el nombre de una unidad organizativa se resuelva incorrectamente con una unidad organizativa distinta que contenga miembros diferentes de unidades organizativas del dominio de XenApp 6.x. Incluso aunque se conserven algunos valores del filtro de unidad organizativa, es necesario revisar cuidadosamente esos valores.
Usuario o grupo	Los valores pueden conservarse, dependiendo de si las cuentas se pueden resolver en el momento de la importación. Al igual que ocurre con las unidades organizativas, las cuentas se resuelven usando solo sus nombres. Por lo tanto, si el sitio de XenApp 7.6 tiene un dominio con el mismo nombre y los mismos nombres de usuario, pero en realidad se trata de dos dominios y conjuntos de usuarios distintos, puede suceder que las cuentas se resuelvan incorrectamente con usuarios diferentes de los usuarios de dominio de XenApp 6.x. Si no se revisan y modifican los valores de los filtros según sea necesario, las directivas pueden aplicarse incorrectamente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Filtrar	Consideraciones
Grupo de trabajo	Los grupos de trabajo no reciben respaldo en XenApp 7.6. Considere la posibilidad de usar filtros de Grupo de entrega, Tipo de grupo de entrega y Etiqueta, que sí reciben respaldo en XenApp 7.6 (no en XenApp 6.x). **Grupo de entrega:** Permite aplicar directivas basadas en grupos de entrega. Cada entrada de filtro especifica un grupo de entrega y puede permitirse o denegarse. **Tipo de grupo de entrega:** Permite aplicar directivas basadas en tipos de grupos de entrega. Cada filtro especifica un tipo de grupo de entrega, que puede permitirse o denegarse. **Etiqueta:** Especifica la aplicación de directivas basándose en etiquetas creadas para las máquinas VDA. Cada etiqueta se puede permitir o denegar.

En resumen, los filtros relacionados con cambios de usuarios de dominio necesitan más atención si la comunidad XenApp 6.x y el sitio XenApp 7.6 están en dominios diferentes. Debido a que el script de importación solo utiliza cadenas de nombres de dominio y de nombres de usuario para resolver los usuarios en el nuevo dominio, algunas de las cuentas pueden resolverse correctamente y otras no. Aunque solo exista una pequeña posibilidad de que los distintos dominios y usuarios tengan los mismos nombres, debe revisar cuidadosamente estos filtros para asegurarse de que contienen los valores correctos.

Aplicaciones

Los scripts de importación de aplicaciones no solo importan aplicaciones, sino que también crean objetos como por ejemplo, grupos de entrega. Si la importación de aplicaciones se realiza en varias iteraciones, la jerarquía de las carpetas de aplicaciones original puede cambiar considerablemente.

1. Primero, lea los archivos de registros de la migración, que contienen detalles sobre qué aplicaciones se importaron y cuáles se omitieron, y los cmdlets que se usaron para crear las aplicaciones.
2. Para cada aplicación:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Compruebe visualmente que se conservaron sus propiedades básicas durante la importación. Use la información de Asignación de propiedades de aplicaciones para determinar qué propiedades se importaron sin cambios, cuáles no se importaron y cuáles se inicializaron con los datos de aplicación de XenApp 6.x.
- Compruebe la lista de usuarios. El script de importación importa automáticamente la lista explícita de usuarios en la lista "Limitar visibilidad" de la aplicación en XenApp 7.6. Compruebe que la lista queda igual.

3. Los servidores de aplicaciones no se importan. Esto significa que no se puede acceder todavía a ninguna de las aplicaciones importadas. Es necesario asignar catálogos de máquinas a los grupos de entrega que contienen estas aplicaciones. Los catálogos contienen las máquinas que tienen las imágenes ejecutables de las aplicaciones publicadas. Para cada aplicación:
    - Asegúrese de que el nombre del archivo ejecutable y el directorio de trabajo hacen referencia a un ejecutable que existe en las máquinas asignadas al grupo de entrega (a través de los catálogos de máquinas).
    - Compruebe un parámetro de línea de comandos (que puede ser cualquier cosa como, por ejemplo, un nombre de archivo, una variable de entorno, o el nombre del ejecutable). Verifique que el parámetro es válido para todas las máquinas de los catálogos de máquinas asignadas al grupo de entrega.

Archivos de registros

Los archivos de registros son el recurso de referencia más importante durante las operaciones de importación y exportación. Esta es la razón por la cual los archivos de registros existentes no se sobrescriben de forma predeterminada y los nombres de los archivos de registros predeterminados son únicos.

Como se indica en Capturar registros y controlar errores, si se quiere usar una captura de registros adicional con los cmdlets de PowerShell `Start-Transcript` y `Stop-Transcript` (que graban todo lo que se escribe y se imprime en la consola), sus resultados, junto con el archivo de registros, ofrecen una referencia completa de toda la actividad de importación y exportación.

Gracias a las marcas de hora incluidas en los archivos de registros se pueden diagnosticar ciertos problemas. Por ejemplo, si una exportación o importación tardó mucho tiempo en ejecutarse, se puede averiguar si la causa fue una conexión de base de datos defectuosa o algún problema al resolver las cuentas de usuario.

Los comandos grabados en los archivos de registros también indican cómo se leen o se crean algunos objetos. Por ejemplo, para crear un grupo de entrega, se ejecutan varios comandos no solo para crear el grupo de entrega propiamente dicho, sino también otros objetos tales como reglas de directivas de acceso que permiten asignar objetos de aplicación al grupo de entrega.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

El archivo de registros se puede usar también para diagnosticar un fallo de importación o exportación. Por lo general, las últimas líneas del archivo de registros indican la causa del fallo; el mensaje de error del fallo también se guarda en el archivo de registros. Junto con el archivo XML, el archivo de registros se puede usar para determinar qué objeto estuvo implicado en el fallo.

Después de revisar y hacer pruebas en la migración:

1. Actualice sus servidores de trabajo XenApp 6.5 con los VDA (Virtual Delivery Agent) actuales ejecutando el instalador de la versión 7.6 en el servidor, lo que quitará el software de XenApp 6.5 e instalará automáticamente el VDA actualizado. Para obtener instrucciones al respecto, consulte Actualización de un servidor de trabajo de XenApp 6.5 a un nuevo VDA para SO de servidor Windows.

   En el caso de servidores de trabajo con XenApp 6.0, es necesario desinstalar manualmente el software de XenApp 6.0 del servidor. A continuación, puede usar el instalador de la versión 7.6 para instalar el VDA actual. No se puede usar el instalador de la versión 7.6 para quitar automáticamente el software de XenApp 6.0.

2. En Studio, en el nuevo sitio de XenApp, cree catálogos de máquinas (o modifique los catálogos existentes) para los servidores de trabajo actualizados.

3. Agregue las máquinas actualizadas desde el catálogo de máquinas a los grupos de entrega que contengan las aplicaciones instaladas en los VDA para SO de servidor Windows.

Uso avanzado

De forma predeterminada, el cmdlet `Export-Policy` exporta todos los datos de directiva a un archivo XML. Del mismo modo, `Export-XAFarm` exporta todos los datos de comunidad a un archivo XML. Se pueden usar parámetros de línea de comandos para controlar con más detalle qué se exporta y se importa.

Exportar aplicaciones parcialmente

Si tiene una gran cantidad de aplicaciones y quiere controlar cuántas de ellas se exportan al archivo XML, use los parámetros siguientes:

- AppLimit: Especifica la cantidad de aplicaciones a exportar.
- SkipApps: Especifica la cantidad de aplicaciones a omitir antes de exportar las aplicaciones subsiguientes.

Puede usar ambos parámetros para exportar una gran cantidad de aplicaciones en fragmentos más manejables. Por ejemplo, supongamos que la primera vez que ejecuta `Export-XAFarm`, quiere exportar solo las primeras 200 aplicaciones; para ello, especifique ese valor en el parámetro AppLimit.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

```
Export-XAFarm -XmlOutputFile "Apps1-200.xml"
```

La siguiente vez que ejecute `Export-XAFarm`, quiere exportar las 100 aplicaciones siguientes; para ello, use el parámetro SkipApps para descartar las aplicaciones que ya exportó antes (las primeras 200) y el parámetro AppLimit para exportar las 100 aplicaciones siguientes.

```
Export-XAFarm -XmlOutputFile "Apps201-300.xml"-AppLimit "100"-SkipApps "200
"
```

No exportar determinados objetos

Algunos objetos pueden omitirse y no es necesario exportarlos, como es el caso, en particular, de los objetos que no se importan. Consulte Configuraciones de directivas que no se importan y Asignación de propiedades de aplicaciones. Utilice los siguientes parámetros para evitar que se exporten objetos innecesarios:

- IgnoreAdmins: No exportar los objetos de administrador
- IgnoreServers: No exportar los objetos de servidor
- IgnoreZones: No exportar los objetos de zona
- IgnoreOthers: No exportar objetos de registro de configuración, patrones de carga, directivas de equilibrio de carga, controladores de impresora y grupos de trabajo
- IgnoreApps: No exportar aplicaciones. Permite exportar otros datos a un archivo XML de salida y, a continuación, ejecutar de nuevo la exportación para exportar las aplicaciones a otro archivo XML de salida distinto.

También se puede usar estos parámetros para solucionar los problemas que podrían provocar el fallo de la exportación. Por ejemplo, si tiene un servidor defectuoso en una zona, la exportación de la zona podría fallar; si incluye el parámetro IgnoreZones, la exportación continúa con otros objetos.

Nombres de grupo de entrega

Si no quiere incluir todas las aplicaciones en un mismo grupo de entrega (por ejemplo, porque acceden a ellas diferentes conjuntos de usuarios y están publicadas en diferentes conjuntos de servidores), puede ejecutar `Import-XAFarm` varias veces, especificando distintas aplicaciones y un grupo de entrega diferente cada vez. Aunque se pueden usar cmdlets de PowerShell para mover las aplicaciones desde un grupo de entrega a otro después de la migración, la importación selectiva en grupos de entrega determinados puede reducir o eliminar el esfuerzo de mover las aplicaciones más tarde.

- Use el parámetro DeliveryGroupName con el cmdlet `Import-XAFarm`. El script crea el grupo de entrega especificado si éste no existe.
- Utilice los siguientes parámetros con expresiones regulares para filtrar las aplicaciones que se importan en el grupo de entrega, en función de carpetas, grupos de trabajo, cuentas

© 1999-2019 Citrix Systems, Inc. All rights reserved.

de usuario y/o nombres de servidores. Se recomienda poner la expresión regular entre comillas simples o dobles. Para obtener información sobre expresiones regulares, consulte https://msdn.microsoft.com/en-us/library/hs600312(v=vs.110).aspx.

- **MatchWorkerGroup** y **NotMatchWorkerGroup:** Por ejemplo, para aplicaciones publicadas en grupos de trabajo, el siguiente cmdlet importa las aplicaciones del grupo de trabajo llamado "Productivity Apps" a un grupo de entrega de XenApp 7.6 con el mismo nombre:

  ```
  Import-XAFarm -XmlInputFile XAFarm.xml -LogFile XAFarmImport.
  log -MatchWorkerGroup 'Productivity Apps' -DeliveryGroupName '
  Productivity Apps'
  ```

- **MatchFolder** y **NotMatchFolder:** Por ejemplo, para aplicaciones organizadas en carpetas, el siguiente cmdlet importa las aplicaciones de la carpeta "Productivity Apps" a un grupo de entrega de XenApp 7.6 con el mismo nombre.

  ```
  Import-XAFarm -XmlInputFile XAFarm.xml -LogFile XAFarmImport.log -
  MatchFolder 'Productivity Apps' -DeliveryGroupName 'Productivity
  Apps'
  ```

  Por ejemplo, el siguiente cmdlet importa en el grupo de entrega predeterminado todas aquellas aplicaciones de cualquier carpeta cuyo nombre contenga "MS Office Apps".

  ```
  Import-XAFarm -XmlInputFile .\TheFarmApps.XML -MatchFolder ".*/MS
  Office Apps/.*"
  ```

- **MatchAccount** y **NotMatchAccount:** Por ejemplo, para aplicaciones publicadas para usuarios y grupos de usuarios de Active Directory, el siguiente cmdlet importa las aplicaciones publicadas para el grupo de usuarios "Finance Group" a un grupo de entrega de XenApp 7.6 llamado "Finance".

  ```
  Import-XAFarm -XmlInputFile XAFarm.xml -LogFile XAFarmImport.log -
  MatchAccount 'DOMAIN\\Finance Group' -DeliveryGroupName 'Finance'
  ```

- **MatchServer** y **NotMatchServer:** Por ejemplo, para las aplicaciones organizadas en servidores, el siguiente cmdlet importa las aplicaciones asociadas con el servidor no llamado "Current" a un grupo de entrega de XenApp llamado "Legacy".

  ```
  Import-XAFarm -XmlInputFile XAFarm.xml -LogFile XAFarmImport.log -
  NotMatchServer 'Current'-DeliveryGroupName 'Legacy'
  ```

Personalización

Los programadores de PowerShell pueden crear sus propias herramientas. Por ejemplo, puede usar el script de exportación como una herramienta de inventario para realizar un seguimiento de los cambios en una comunidad XenApp 6.x. También puede modificar los archivos XSD (o crear sus propios

© 1999-2019 Citrix Systems, Inc. All rights reserved.

archivos XSD) para almacenar datos adicionales o datos en diferentes formatos en los archivos XML. Puede especificar un archivo XSD no predeterminado con cada uno de los cmdlets de importación.

Aunque se pueden modificar los archivos de scripts para ajustarse a requisitos de migración específicos o avanzados, el respaldo se limita a los scripts no modificados. El servicio de asistencia técnica (Citrix Support) le recomendará utilizar los scripts sin modificaciones, para determinar cuál es el comportamiento esperado y ofrecer asistencia técnica, si es necesario.

Solucionar problemas

- Si usa PowerShell 2.0 y agregó el complemento Citrix Group Policy PowerShell Provider o el complemento Citrix Common Commands mediante el cmdlet `Add-PSSnapIn`, puede que aparezca un mensaje de error como el siguiente: "Referencia a objeto no establecida como instancia de un objeto" cuando ejecute los cmdlets de importación o exportación. Este error no afecta a la ejecución del script y puede ignorarse.
- Evite agregar o quitar el complemento Citrix Group Policy PowerShell Provider en la misma sesión de consola donde se usan los módulos de scripts de exportación e importación, porque esos módulos agregan automáticamente el complemento. Si agrega o quita el complemento por separado, puede que vea uno de los siguientes errores:
  - "Ya existe una unidad llamada 'LocalGpo"'. Este error aparece cuando el complemento se agrega dos veces; el complemento intenta montar la unidad LocalGpo cuando se ha cargado y luego notifica el error.
  - "Un parámetro que no se puede encontrar coincide con el nombre de parámetro 'Controller"'. Este error aparece cuando el complemento no ha sido agregado pero el script intenta montar la unidad. El script no tiene constancia de que el complemento se quitó. Cierre la consola e inicie una nueva sesión. En la nueva sesión, importe los módulos de scripts, no agregue ni quite el complemento por separado.
- Al importar los módulos, si hace clic con el botón secundario en un archivo .psd1 y selecciona **Abrir** o **Abrir con PowerShell**, la ventana de la consola de PowerShell se abrirá y se cerrará de nuevo rápidamente hasta que detenga el proceso. Para evitar este error, introduzca el nombre completo del módulo de scripts de PowerShell directamente en la ventana de la consola de PowerShell (por ejemplo, `Import-Module .\\ExportPolicy.psd1`)).
- Si recibe un error de permisos al ejecutar una exportación o importación, asegúrese de que usted es un administrador de XenApp con permisos para leer objetos (para poder exportar), o para leer y crear objetos (para poder importar). También debe tener suficientes permisos de Windows para ejecutar scripts de PowerShell.
- Si la exportación falla, compruebe si la comunidad de XenApp 6.x se encuentra en un estado correcto, ejecutando las utilidades DSMAINT y DSCHECK en el servidor de Controller de XenApp 6.x.
- Si ejecuta una vista previa de la importación y luego ejecuta los cmdlets de importación de

© 1999-2019 Citrix Systems, Inc. All rights reserved.

nuevo para una migración real, pero descubre que no se ha importado nada, compruebe si quitó el parámetro Preview de los cmdlets de importación.

Configuraciones de directivas que no se importan

Las siguientes configuraciones de directiva de usuario y de equipo no se importan porque ya no reciben respaldo. Las directivas sin filtrar nunca se importan. Las funciones y los componentes que dan respaldo a estas configuraciones han sido reemplazadas por otras tecnologías y componentes nuevos, o estas configuraciones ya no se aplican debido a cambios de arquitectura y plataforma.

Configuraciones de directiva de equipo que no se importan

- Control de acceso de las conexiones
- Nivel de administración de CPU de servidor
- Resolución de direcciones DNS
- Nombre de la comunidad
- Almacenamiento completo de iconos en caché
- Supervisión de estado, Pruebas de supervisión de estado
- Nombre de host del servidor de licencias, Puerto del servidor de licencias
- Límite de sesiones de usuario, Límites de sesiones de administrador
- Nombre del patrón de carga
- Registro de sucesos de límites de inicios de sesión
- Porcentaje máximo de servidores con control de inicio de sesión
- Optimización de memoria, Lista de aplicaciones excluidas de la optimización de memoria, Intervalo de optimización de memoria, Programación de la optimización de memoria: día del mes, Programación de la optimización de memoria: día de la semana, Programación de la optimización de memoria: hora
- Confianza en clientes de aplicaciones sin conexión, Registro de sucesos de aplicaciones sin conexión, Periodo de licencias de aplicaciones sin conexión, Usuarios de aplicaciones sin conexión
- Pedir contraseña
- Advertencia personalizada de reinicio, Texto personalizado de advertencia de reinicio, Hora de inhabilitación de inicios de sesión por reinicio, Frecuencia de reinicio programado, Intervalo de selección de hora de reinicio programado, Fecha de comienzo del reinicio programado, Hora del reinicio programado, Intervalo de advertencias de reinicio, Comienzo de advertencias de reinicio, Advertencia de reinicios para los usuarios, Reinicios programados
- Remedo
- Confiar en solicitudes XML (configurada en StoreFront)

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Filtrado de direcciones de adaptador de IP virtual, Lista de programas para compatibilidad con IP virtual, Compatibilidad mejorada de IP virtual, Lista de programas para filtrado de direcciones de adaptador de IP virtual
- Nombre de la carga de trabajo
- Edición del producto XenApp, Modelo del producto XenApp
- Puerto de XML Service

* Reemplazada con Asistencia remota de Windows

Configuraciones de directiva de usuario que no se importan

- Conectar automáticamente puertos COM del cliente, Conectar automáticamente puertos LPT del cliente
- Redirección de puertos COM del cliente, Redirección de puertos LPT del cliente
- Nombres de impresora del cliente
- Límite de sesiones simultáneas
- Entradas de conexiones de remedo *
- Intervalo de temporizador de desconexión de sesión persistente, Intervalo de temporizador de fin de sesión persistente
- Registrar intentos de remedo *
- Notificar al usuario sobre conexiones de remedo pendientes *
- Intervalo de temporizador de desconexión de sesión de preinicio, Intervalo de temporizador de fin de sesión de preinicio
- Importancia de la sesión
- Single Sign-On, Almacén central de Single Sign-On
- Usuarios que pueden remedar a otros usuarios, Usuarios que no pueden remedar a otros usuarios *

* Reemplazada con Asistencia remota de Windows

Tipos de aplicaciones no importados

Los siguientes tipos de aplicación no se importan.

- Escritorios de servidor
- Contenido
- Aplicaciones distribuidas por streaming (App-V es el nuevo método utilizado para la distribución de aplicaciones por streaming)

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Asignación de propiedades de aplicaciones

El script para importar datos de comunidad solo importa aplicaciones. Las siguientes propiedades de aplicación se importan sin cambios.

Propiedad de IMA	Propiedad de FMA
AddToClientDesktop	ShortcutAddedToDesktop
AddToClientStartMenu	ShortcutAddedToStartMenu
ClientFolder	ClientFolder
CommandLineExecutable	CommandLineExecutable
CpuPriorityLevel	CpuPriorityLevel
Description	Description
DisplayName	PublishedName
Habilitada	Habilitada
StartMenuFolder	StartMenuFolder
WaitOnPrinterCreation	WaitForPrinterCreation
WorkingDirectory	WorkingDirectory
FolderPath	AdminFolderName

IMA y FMA tienen restricciones diferentes en cuanto a la longitud de nombre de carpeta. En IMA, el límite para los nombres de carpeta es de 256 caracteres. El límite en FMA es de 64 caracteres. Al realizar la importación, las aplicaciones cuya ruta de acceso contenga un nombre de carpeta de más de 64 caracteres se omitirán. El límite se aplica solamente al nombre de cada carpeta dentro de la ruta de carpetas; la ruta de carpetas entera puede ser más larga que los límites indicados. Para evitar que se omitan aplicaciones durante la importación, Citrix recomienda comprobar la longitud del nombre de las carpetas de las aplicaciones, y acortarlos si es necesario antes de realizar la exportación.

Las siguientes propiedades de aplicación están inicializadas o no inicializadas de forma predeterminada, o están definidas con los valores proporcionados en los datos de XenApp 6.x:

Propiedad de FMA	Valor
Nombre	Inicializada con el nombre completo de la ruta, que contiene las propiedades de IMA FolderPath y DisplayName, pero sin la cadena inicial “Applications\”

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Propiedad de FMA	Valor
ApplicationType	HostedOnDesktop
CommandLineArguments	Inicializada usando argumentos de línea de comandos de XenApp 6.x
IconFromClient	No inicializada; el valor predeterminado es false
IconUid	Inicializada con un objeto de icono creado usando los datos de iconos de XenApp 6.x
SecureCmdLineArgumentsEnabled	No inicializada; el valor predeterminado es true
UserFilterEnabled	No inicializada; el valor predeterminado es false
UUID	Solo lectura, asignado por el Controller
Visible	No inicializada; el valor predeterminado es true

Las siguientes propiedades de aplicación se migran parcialmente:

Propiedad de IMA	Comentarios
FileTypes	Solo se migran los tipos de archivos que ya existen en el nuevo sitio de XenApp. Aquellos tipos de archivo que no existan en el sitio nuevo se omiten. Los tipos de archivo se importan solo después de que se actualicen los tipos de archivo del sitio nuevo.
IconData	Se crean nuevos objetos de icono si los datos de icono se han proporcionado para las aplicaciones exportadas.
Cuentas	Las cuentas de usuario de una aplicación se dividen entre la lista de usuarios para el grupo de entrega y la aplicación. Los usuarios explícitos se usan para inicializar la lista de usuarios para la aplicación. Además, la cuenta “Usuarios de dominio” del dominio de las cuentas de usuario se agrega a la lista de usuarios para el grupo de entrega.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Las siguientes propiedades de XenApp 6.x no se importan:

Propiedad de IMA	Comentarios
ApplicationType	Omitido.
HideWhenDisabled	Omitido.
AccessSessionConditions	Reemplazada por las directivas de acceso de grupos de entrega.
AccessSessionConditionsEnabled	Reemplazada por las directivas de acceso de grupos de entrega.
ConnectionsThroughAccessGatewayAllowed	Reemplazada por las directivas de acceso de grupos de entrega.
OtherConnectionsAllowed	Reemplazada por las directivas de acceso de grupos de entrega.
AlternateProfiles	FMA no respalda aplicaciones distribuidas por streaming.
OfflineAccessAllowed	FMA no respalda aplicaciones distribuidas por streaming.
ProfileLocation	FMA no respalda aplicaciones distribuidas por streaming.
ProfileProgramArguments	FMA no respalda aplicaciones distribuidas por streaming.
ProfileProgramName	FMA no respalda aplicaciones distribuidas por streaming.
RunAsLeastPrivilegedUser	FMA no respalda aplicaciones distribuidas por streaming.
AnonymousConnectionsAllowed	FMA usa una tecnología diferente para dar respaldo a conexiones no autenticadas (anónimas).
ApplicationId, SequenceNumber	Datos exclusivos de IMA.
AudioType	FMA no respalda opciones avanzadas de conexión de cliente.
EncryptionLevel	SecureICA se habilita o inhabilita en los grupos de entrega.
EncryptionRequired	SecureICA se habilita o inhabilita en los grupos de entrega.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Propiedad de IMA	Comentarios
SslConnectionEnabled	FMA usa una implementación de TLS diferente.
ContentAddress	FMA no respalda el contenido publicado.
ColorDepth	FMA no respalda opciones avanzadas de apariencia de ventanas.
MaximizedOnStartup	FMA no respalda opciones avanzadas de apariencia de ventanas.
TitleBarHidden	FMA no respalda opciones avanzadas de apariencia de ventanas.
WindowsType	FMA no respalda opciones avanzadas de apariencia de ventanas.
InstanceLimit	FMA no respalda límites de aplicación.
MultipleInstancesPerUserAllowed	FMA no respalda límites de aplicación.
LoadBalancingApplicationCheckEnabled	FMA usa una tecnología diferente para respaldar el equilibrio de carga.
PreLaunch	FMA usa una tecnología diferente para respaldar el preinicio de sesiones.
CachingOption	FMA usa una tecnología diferente para respaldar el preinicio de sesiones.
ServerNames	FMA usa una tecnología diferente.
WorkerGroupNames	FMA no respalda los grupos de trabajo.

Proteger

January 29, 2019

> **Nota:**
>
> Puede obtener información sobre los cambios en los nombres de producto aquí.

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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 característica 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 respaldan 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Citrix Virtual Apps and Desktops pueden integrarse con muchas soluciones de seguridad de terceros, desde software de gestión de identidades a software antivirus. Puede ver una lista de los productos admitidos en http://www.citrix.com/ready.

Determinadas versiones de Citrix Virtual Apps and Desktops están certificadas para el estándar de Common Criteria. Para obtener una lista de esos estándares, vaya a https://www.commoncriteriaportal.org/cc/.

Recomendaciones y consideraciones de seguridad

January 29, 2019

> **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.

Considere la opción de usar software anti-malware específico para la plataforma, como el Enhanced Mitigation Experience Toolkit (EMET) de Microsoft para máquinas Windows. Algunos organismos recomiendan usar la versión más reciente de EMET respaldada por Microsoft dentro de sus entornos regulados. Tenga en cuenta que, según Microsoft, EMET puede no ser compatible con algunos programas de software, de modo que debe probarlo extensivamente con sus aplicaciones antes de implementarlo en el entorno de producción. Citrix Virtual Apps and Desktops han sido probados con EMET 5.5 en su configuración predeterminada. En estos momentos, no se recomienda usar EMET en una máquina que tenga instalado el Virtual Delivery Agent (VDA).

Proteja todas las máquinas del entorno con firewalls perimetrales, incluido en los límites de enclave, según corresponda.

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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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.

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 utiliza otro firewall, debe configurarlo manualmente.

> **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/).

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.

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.

Administrar privilegios de usuario

Sólo 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 sólo 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 StoreFront, para las cuentas de equipo de otros servidores que se encuentren en el mismo grupo de servidores 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).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 de servidor 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 escritorio, 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): Da respaldo a 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- 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 Service (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): Da respaldo a la administración de StoreFront. (No es parte del componente de StoreFront en sí).
- Citrix Storefront Privileged Administration Service (NT SERVICE\CitrixPrivilegedService): Da respaldo a 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): Da respaldo a 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 pro-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

ceso, Generar auditorías de seguridad y Reemplazar un símbolo (token) de nivel de proceso. No es necesario que cambie estos derechos de usuario. Delivery Controller no utiliza estos privilegios y están inhabilitados automáticamente.

Configurar parámetros de servicios

Excepto Citrix StoreFront Privileged Administration Service y Citrix Telemetry Service, los servicios Windows de Delivery Controller enumerados arriba en la sección Configurar derechos de usuario están configurados para iniciar sesión como la identidad NETWORK SERVICE. No modifique estos parámetros de servicio.

Citrix Storefront Privileged Administration está configurado para iniciar la sesión de sistema local (NT AUTHORITY\SYSTEM). Esto es necesario para las operaciones de StoreFront con Delivery Controller que no están normalmente disponible para los servicios (incluida la creación de sitios de IIS de Microsoft). No modifique estos parámetros de servicio.

Citrix Telemetry Service está configurado para iniciar sesión como su propia identidad específica de servicio.

Si quiere, puede inhabilitar Citrix Telemetry Service. Aparte de este servicio y de los servicios que ya están inhabilitados, no inhabilite ninguno de los otros servicios de Windows de Delivery Controller.

Configurar parámetros de Registro

Ya no es necesario habilitar la creación de carpetas y nombres de archivo 8.3 en el sistema de archivos del VDA. La clave de Registro **NtfsDisable8dot3NameCreation** se puede configurar para inhabilitar la creación de carpetas y nombres de archivo 8.3. También puede configurar este comportamiento mediante el comando **fsutil.exe behavior set disable8dot3**.

Implicaciones de seguridad en los casos de implementación

El entorno de usuario puede contener dispositivos de usuario que la empresa no administra y, por tanto, están bajo el control total del usuario, o bien, dispositivos de usuario que administra totalmente la empresa. En general, las consideraciones de seguridad para estos dos entornos son diferentes.

Dispositivos del usuario administrados

Los dispositivos de usuario administrados permanecen bajo un control administrativo; se encuentran bajo el control del usuario o de otra organización de su confianza. Es posible configurar y suministrar dispositivos del usuario directamente a usuarios. También es posible proporcionar terminales

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 respecto a acceso con Remote PC

El acceso con Remote PC es una función que implementa las siguientes características 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 está respaldado para un solo 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 modificando el Registro.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> **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 modifica el Registro de forma incorrecta, pueden producirse problemas graves, que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Para restringir la asignación automática a un único usuario:

En cada Controller del sitio, configure la siguiente entrada del Registro:

```
HKEY_LOCAL_MACHINE\Software\Citrix|DesktopServer
Nombre: AllowMultipleRemotePCAssignments
Tipo: REG_DWORD
Datos: 0 = Inhabilitar asignaciones múltiples de usuarios, 1 = (Opción
    predeterminada) Habilitar asignaciones múltiples de usuarios.
```

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.

Integrar Citrix Virtual Apps and Desktops con Citrix Gateway

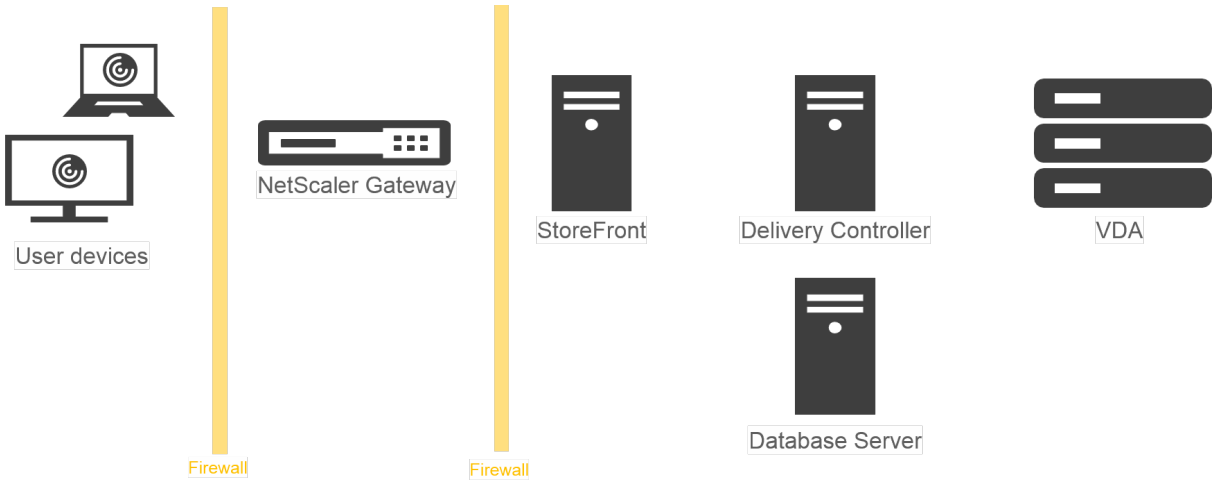
January 25, 2019

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Los servidores StoreFront se implementan y se configuran para administrar el acceso a los datos y los recursos publicados. Para el acceso remoto, se recomienda agregar Citrix Gateway y colocarlo delante de StoreFront.

> **Nota**
>
> Para conocer los pasos detallados de configuración para integrar Citrix Virtual Apps and Desktops con Citrix Gateway, consulte la documentación de StoreFront.

En el siguiente diagrama, se ofrece un ejemplo de una implementación simplificada de Citrix que incluye Citrix Gateway. Citrix Gateway se comunica con StoreFront para proteger las aplicaciones y los datos que entregan Citrix Virtual Apps and Desktops. Los dispositivos de usuario ejecutan la aplicación Citrix Workspace para crear una conexión segura y acceder a las aplicaciones, los escritorios y los archivos.



Los usuarios inician sesiones y se autentican mediante Citrix Gateway. Citrix Gateway se implementa y se protege en la zona DMZ. Se configura la autenticación de dos factores. En función de sus credenciales de usuario, los usuarios reciben los recursos y las aplicaciones que les corresponden. Las aplicaciones y los datos se encuentran en los servidores adecuados (no aparecen en el diagrama). Se utilizan servidores independientes para los datos y las aplicaciones confidenciales de seguridad.

Administración delegada

March 15, 2019

El modelo de administración delegada ofrece flexibilidad para adaptarse al modo en que la organización desee delegar actividades de administración. Para ello, utiliza el control basado en los roles y los objetos. La administración delegada se adapta a implementaciones de todos los tamaños y permite configurar permisos con mucho más detalle a medida que la implementación adquiere complejidad. La administración delegada utiliza tres conceptos: los administradores, los roles y los ámbitos.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **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 del grupo 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 del grupo de entrega y un administrador del catálogo 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, así como información global, pero no puede modificar nada. Por ejemplo, un administrador de solo lectura con Ámbito = Londres puede ver todos los objetos globales (como, por ejemplo, el registro de configuración) y todos los objetos del ámbito Londres (por ejemplo, grupos de entrega de Londres). No obstante, ese administrador no puede ver los objetos del ámbito de Nueva York (a menos que los ámbitos de Londres y Nueva York se superpongan).
Administrador de asistencia técnica	Puede ver los grupos de entrega y administrar las sesiones y las máquinas asociadas con dichos grupos. Puede ver el catálogo de máquinas y la información del host de los grupos de entrega que están bajo supervisión. También puede realizar tareas de administración de sesiones y de administración de energía de las máquinas de esos grupos de entrega.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Rol	Permisos
Administrador de catálogo 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 grupo 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:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Administrador	Roles	Ámbitos
dominio/Fred	Administrador total	Todo (el rol de administrador total siempre tiene el ámbito Todo)
dominio/Rob	Administrador de solo lectura	Todos
dominio/Heidi	Administrador de solo lectura, administrador de asistencia técnica	Todo Ventas
dominio/adminalmacén	Administrador de asistencia técnica	Almacén
dominio/Miguel	Administrador del grupo de entrega, administrador del catálogo 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 total del 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, todas las tareas recaen en un administrador o un número reducido de ellos; no se delega nada. En este caso, cree a cada administrador con el rol integrado de administrador total, cuyo ámbito es Todo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- 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 ámbitos adicionales, 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 nuevos 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 nuevo 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 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. Es decir, no se elimina el rol o el ámbito, ni tampoco afecta a ningún otro administrador configurado con esa pareja de rol y ámbito.

Para administrar a los administradores, haga clic en Configuración > Administradores en el panel de navegación de Studio y, a continuación, haga clic en la ficha Administradores en el panel central superior.

- Para crear un administrador, haga clic en Crear nuevo administrador en el panel Acciones. Escriba o vaya al nombre de la cuenta de usuario, seleccione o cree un ámbito, y seleccione un

© 1999-2019 Citrix Systems, Inc. All rights reserved.

rol. El nuevo administrador se habilita de forma predeterminada, aunque puede modificar este valor.

- Para copiar un administrador, selecciónelo en el panel central y, a continuación, haga clic en Copiar administrador en el panel Acciones. Escriba o vaya al nombre de la cuenta de usuario. Puede seleccionar y, a continuación, modificar o eliminar las parejas de rol y ámbito, así como agregar otras nuevas. El nuevo administrador se habilita de forma predeterminada, aunque puede modificar este valor.
- Para modificar un administrador, selecciónelo en el panel central y, a continuación, haga clic en Modificar administrador en el panel Acciones. Puede modificar o eliminar las parejas de rol y ámbito, así como agregar otras nuevas.
- Para eliminar un administrador, selecciónelo en el panel central y, a continuación, haga clic en Eliminar administrador en el panel Acciones. No se puede eliminar un administrador si se trata del único administrador total habilitado en ese momento.

Crear y gestionar roles

Los nombres de rol pueden contener un máximo de 64 caracteres Unicode. 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), > (flecha derecha), | (barra vertical, [ ](corchete izquierdo o derecho), () (paréntesis izquierdo o derecho), “ (comillas dobles) y ‘ (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 usando.

> **Nota:**
>
> Solo algunas ediciones de producto admiten los roles personalizados. Las ediciones donde no se respaldan los roles personalizados no contienen las opciones correspondientes en el panel Acciones.

Para administrar los roles, haga clic en Configuración > Administradores en el panel de navegación de Studio y, a continuación, haga clic en la ficha Roles en el panel central superior.

- Para ver información detallada de un rol, selecciónelo en el panel central. La parte inferior del panel central muestra los tipos de objeto y los permisos asociados con el rol. Haga clic en la ficha Administradores en el panel inferior para mostrar una lista de los administradores que actualmente tienen ese rol.
- Para crear un rol personalizado, haga clic en Crear nuevo rol en el panel Acciones. Escriba un nombre y una descripción. Seleccione los tipos de objeto y los permisos pertinentes.
- Para copiar un rol, selecciónelo en el panel central y, a continuación, haga clic en Copiar rol en el panel Acciones. Cambie el nombre, la descripción, los tipos de objeto y los permisos, según

© 1999-2019 Citrix Systems, Inc. All rights reserved.

sea necesario.

- Para modificar un rol personalizado, selecciónelo en el panel central y, a continuación, haga clic en Modificar rol en el panel Acciones. Cambie el nombre, la descripción, los tipos de objeto y los permisos, según sea necesario.
- Para eliminar un rol personalizado, selecciónelo en el panel central y, a continuación, haga clic en Eliminar rol en el panel Acciones. Cuando se le solicite, confirme la eliminación.

Crear y gestionar ámbitos

Cuando se crea un sitio, el único ámbito disponible es el ámbito 'Todo', que no se puede eliminar.

Puede crear ámbitos mediante el siguiente procedimiento. También puede crear ámbitos al tiempo que crea un administrador; cada administrador debe estar asociado con 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 no incluibles en ámbitos específicos se incluyen en el ámbito 'Todo'. (Los administradores totales siempre tienen asociado el ámbito Todo.) Las máquinas, las acciones de energía, los escritorios y las sesiones no se pueden incluir directamente en un ámbito; se puede asignar permisos sobre estos objetos a los administradores a través de los catálogos de máquinas o grupos de entrega asociados.

Los nombres de ámbito pueden contener un máximo de 64 caracteres Unicode. 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), > (flecha derecha), | (barra vertical, [ ] (corchete izquierdo o derecho), () (paréntesis izquierdo o derecho), " (comillas dobles) y ' (apóstrofe). Las descripciones pueden contener un máximo de 256 caracteres Unicode.

Al copiar o modificar un ámbito, tenga en cuenta que eliminar objetos del ámbito puede tener como consecuencia que el administrador no pueda acceder a ellos. Si el ámbito modificado está emparejado con uno o varios roles, compruebe que los cambios que haga en el ámbito no hagan que la pareja de rol y ámbito quede inutilizable.

Para administrar ámbitos, haga clic en "Configuración > Administradores" en el panel de navegación de Studio y, a continuación, haga clic en la ficha "Ámbitos" en el panel central superior.

- Para crear un ámbito, haga clic en Crear nuevo ámbito en el panel Acciones. Escriba un nombre y una descripción. Para incluir todos los objetos de un tipo concreto (por ejemplo, grupos de entrega), seleccione el tipo de objeto. Para incluir objetos concretos, expanda el tipo y, a continuación, seleccione objetos individualmente (por ejemplo, grupos de entrega individuales utilizados por el equipo de Ventas).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Para copiar un ámbito, selecciónelo en el panel central y, a continuación, haga clic en Copiar ámbito en el panel Acciones. Escriba un nombre y una descripción. Cambie los objetos y los tipos de objeto, según sea necesario.
- Para modificar un ámbito, selecciónelo en el panel central y, a continuación, haga clic en Modificar ámbito en el panel Acciones. Cambie el nombre, la descripción, los tipos de objeto y los objetos, según sea necesario.
- Para eliminar un ámbito, selecciónelo en el panel central y, a continuación, haga clic en Eliminar ámbito en el panel Acciones. Cuando se le solicite, confirme la eliminación.

Crear informes

Puede generar dos tipos de informes de administración delegada:

- Un informe HTML que ofrece una lista de las parejas de rol y ámbito asociadas con un administrador, además de los permisos individuales de cada tipo de objeto (por ejemplo, grupos de entrega y catálogos de máquinas). Este informe se genera desde Studio.

  Para crear este informe, haga clic en Configuración > Administradores en el panel de navegación. Seleccione un administrador en el panel central y, a continuación, haga clic en Crear informe en el panel Acciones.

  También puede solicitar este informe al crear, copiar o modificar un administrador.

- Un informe HTML o CSV donde figuran todas las asignaciones de roles integrados y personalizados con sus correspondientes permisos. Este informe se genera al ejecutar un script de PowerShell denominado OutputPermissionMapping.ps1.

  Para ejecutar este script, es necesario ser un administrador total, un administrador de solo lectura, o un administrador personalizado que cuente con permiso para leer roles. El script se encuentra en: *Archivos de programa\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Scripts*.

  Sintaxis:

  ```
  OutputPermissionMapping.ps1 [-Help] [-Csv] [-Path \<string>] [-AdminAddress
   \<string>] [-Show] [\<CommonParameters>]
  ```

Parámetro	Descripción
-Help	Muestra la ayuda del script.
-Csv	Especifica la salida CSV. Valor predeterminado = HTML
-Path <cadena>	Destino de escritura de los resultados. Valor predeterminado = stdout

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Parámetro	Descripción
-AdminAddress <cadena>	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.
	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.

```
pre codeblock
& "$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.

```
pre codeblock
& "$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:

```
pre codeblock
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'
-CSV -Path Roles.csv"
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Tarjetas inteligentes

March 8, 2019

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.

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 del respaldo que reciben 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- 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 simplemente en el equipo del usuario. Esos certificados digitales no son estrictamente equivalentes a tarjetas inteligentes.

El respaldo para tarjetas inteligentes de Citrix Virtual Apps and Desktops está basado en las especificaciones estándar Personal Computer/Smart Card (PC/SC) de Microsoft. Requisito mínimo: las tarjetas inteligentes y los dispositivos de tarjeta inteligente deben ser compatibles con el sistema operativo Windows subyacente y deben estar aprobados por Microsoft Windows Hardware Quality Labs (WHQL) para utilizarse en equipos con sistemas operativos Windows válidos. Consulte la documentación de Microsoft para obtener más información sobre el cumplimiento normativo de hardware de PC/SC. Existen otros tipos de dispositivos de usuario que pueden cumplir el estándar PS/SC. Para obtener más información, consulte el programa Citrix Ready.

Por lo general, se necesita un controlador de dispositivo independiente para la tarjeta inteligente o equivalente de cada proveedor. Sin embargo, si las tarjetas inteligentes cumplen un estándar como Personal Identity Verification (PIV) de NIST, se puede usar un solo controlador de dispositivo para una gama de tarjetas inteligentes. El controlador del dispositivo debe instalarse tanto en el dispositivo del usuario como en Virtual Delivery Agent (VDA). Ese controlador de dispositivo se incluye a menudo en el paquete de middleware de la tarjeta inteligente, disponible de un socio de Citrix. Ese paquete ofrece funciones avanzadas. El controlador del dispositivo también puede describirse como un 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
ActivClient 7.0 (modo DoD habilitado)	Tarjeta DoD CAC
ActivClient 7.0 en modo PIV	Tarjeta NIST PIV
Minicontrolador de Microsoft	Tarjeta NIST PIV

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Middleware	Tarjetas válidas
Minicontrolador GemAlto para tarjeta .NET	GemAlto .NET v2+
Controlador nativo de Microsoft	Tarjetas inteligentes virtuales (TPM)

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 está respaldado solo para el acceso remoto a PC físicos de oficina con Windows 10, Windows 8 o Windows 7; no se admiten tarjetas inteligentes para PC de oficina con Windows XP.

Las siguientes tarjetas inteligentes se han probado con el acceso con Remote PC:

Middleware	Tarjetas válidas
Minicontrolador GemAlto .NET	Gemalto .NET v2+
ActivIdentity ActivClient 6.2	NIST PIV
ActivIdentity ActivClient 6.2	CAC
Minicontrolador de Microsoft	NIST PIV
Controlador nativo de Microsoft	Tarjetas inteligentes virtuales

Tarjeta inteligente rápida

La tarjeta inteligente rápida es una mejora con respecto a la redirección HDX existente de tarjetas inteligentes basada en PC/SC. Mejora el rendimiento cuando se usan tarjetas inteligentes en redes WAN con latencia alta.

La tarjeta inteligente rápida está habilitada de manera predeterminada en los hosts que ejecutan Windows Server 2012, Windows Server 2016 o Windows 10 (versión mínima). En el lado del cliente, para habilitar la tarjeta inteligente rápida, incluya el siguiente parámetro en el archivo *default.ica* del sitio StoreFront asociado:

```
[WFClient]
SmartCardCryptographicRedirection=On
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Limitaciones:

- Solo Citrix Receiver para Windows admite las tarjetas inteligentes rápidas. Si configura tarjetas inteligentes rápidas en el archivo default.ica, los Citrix Receivers que no son para Windows seguirán funcionando con la redirección existente de PC/SC.
- Los únicos casos de doble salto donde se admiten las tarjetas inteligentes rápidas son ICA > ICA con la tarjeta inteligente rápida habilitada en ambos saltos. Como la tarjeta inteligente rápida no admite casos de doble salto ICA> RDP, esas situaciones no funcionan.
- La tarjeta inteligente rápida no es compatible con Cryptography Next Generation. Por lo tanto, la tarjeta inteligente rápida no admite tarjetas inteligentes de criptografía de curva elíptica (Elliptic Curve Cryptography o ECC).
- La tarjeta inteligente rápida solo admite operaciones de contenedor de claves de solo lectura. Por ejemplo, una tarjeta inteligente no puede registrarse con una tarjeta inteligente rápida.
- La tarjeta inteligente rápida no admite el cambio del PIN de la tarjeta inteligente.

Tipos de lectores de tarjetas inteligentes

El lector de tarjetas inteligentes se puede integrar en el dispositivo del usuario, o bien se puede conectar al dispositivo del usuario (normalmente mediante USB o Bluetooth). Se admiten los lectores de tarjetas con contacto que cumplen con la especificación de los dispositivos de interfaz de tarjetas inteligentes/chips USB (CCID). Contienen una ranura donde el usuario debe introducir o pasar la tarjeta inteligente. El estándar (Deutsche Kreditwirtschaft DK) define cuatro clases de lectores de tarjetas con contacto.

- Los lectores de tarjetas inteligentes de clase 1 son los más comunes, y normalmente solo contienen una ranura. Por norma general, los lectores de tarjetas inteligentes de clase 1 se admiten con un controlador de dispositivo CCID estándar que se suministra con el sistema operativo.
- Los lectores de tarjetas inteligentes de clase 2 constan, además, de un teclado seguro al que no se puede acceder desde el dispositivo de usuario. Los lectores de tarjetas inteligentes de clase 2 pueden estar integrados en un teclado que contenga a su vez un teclado numérico seguro. Para lectores de tarjetas inteligentes de clase 2, póngase en contacto con su representante de Citrix. Puede ser necesario un controlador de dispositivo específico del lector para habilitar la función de teclado numérico seguro.
- Los lectores de tarjetas inteligentes de clase 3 contienen, además, una pantalla segura. Los lectores de tarjetas inteligentes de clase 3 no se respaldan.
- 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 respaldan.

> **Nota:**
>
> La clase que tenga el lector de tarjetas inteligentes no tiene que ver con la clase de dispositivo

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> USB.

Los lectores de tarjetas inteligentes deben instalarse con el controlador de dispositivo correspondiente en el dispositivo de usuario.

Para obtener información sobre los lectores admitidos de tarjetas inteligentes, consulte la documentación de la aplicación Citrix Workspace que utilice. En la documentación de la aplicación Citrix Workspace, las versiones admitidas suelen incluirse en el artículo de tarjetas inteligentes o en el artículo de requisitos del sistema.

Experiencia de usuario

El respaldo para tarjetas inteligentes está integrado 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 USB genérica para lectores de tarjetas inteligentes. Esta funcionalidad está inhabilitada de forma predeterminada para lectores de tarjetas inteligentes y no se respalda si se habilita.

Es posible utilizar varias tarjetas inteligentes y varios lectores en el mismo dispositivo de usuario, pero si la autenticación PassThrough se encuentra en uso solo debe insertarse una tarjeta inteligente cuando el usuario inicia un escritorio virtual o una aplicación. Cuando se utiliza una tarjeta inteligente en una aplicación (por ejemplo, para las funciones de cifrado o firma digital), es posible que aparezcan solicitudes adicionales para insertar una tarjeta inteligente o introducir un PIN. Esto puede suceder cuando se inserta más de una tarjeta inteligente al mismo tiempo.

- Si se les solicita a los usuarios que inserten una tarjeta inteligente cuando la tarjeta inteligente ya se encuentra en el lector, deben seleccionar Cancelar.
- Si se solicita el PIN a los usuarios, deben introducirlo de nuevo.

Puede restablecer los PIN con un sistema de administración de tarjetas o alguna herramienta del proveedor.

> **Importante:**
>
> En una sesión de Citrix Virtual Apps o Citrix Virtual Desktops, no se admite el uso de una tarjeta inteligente con la aplicación Conexión a Escritorio remoto de Microsoft. Esto a veces se describe como un uso de “doble salto”.

Antes de implementar tarjetas inteligentes

- Obtenga un controlador de dispositivo para el lector de tarjetas inteligentes e instálelo en el dispositivo de usuario. Muchos lectores de tarjetas inteligentes pueden usar el controlador de dispositivo CCID que proporciona Microsoft.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Obtenga un controlador de dispositivo y el software de proveedor de servicios de cifrado (CSP) del proveedor de la tarjeta inteligente e instálelos en los dispositivos de usuario y escritorios virtuales. El controlador y el software CSP deben ser compatibles con Citrix Virtual Apps and Desktops; consulte la documentación del proveedor para comprobarlo. Para los escritorios virtuales con tarjetas inteligentes que admiten y usan el modelo de minicontroladores, esos minicontroladores de tarjeta inteligente deberían descargarse automáticamente, aunque pueden obtenerse del proveedor o en http://catalog.update.microsoft.com. Además, si se necesita middleware de PKCS #11, puede obtenerlo del proveedor de tarjetas.
- Importante: Se recomienda instalar y probar los controladores y el software CSP en un equipo físico antes de instalar el software de Citrix.
- Agregue la URL de Citrix Receiver para Web a la lista de sitios de confianza para los usuarios que trabajan con tarjetas inteligentes en Internet Explorer con Windows 10. En Windows 10, Internet Explorer no se ejecuta en el modo protegido de forma predeterminada para los sitios de confianza.
- Asegúrese de que la infraestructura de clave pública (PKI) está configurada correctamente. Esto incluye comprobar que la asignación de certificados a cuentas está configurada correctamente para el entorno de Active Directory y que la validación de certificados de usuario puede realizarse correctamente.
- Compruebe que su implementación cumple los requisitos del sistema de los demás componentes de Citrix utilizados con tarjetas inteligentes, incluidos la aplicación Citrix Workspace y StoreFront.
- Compruebe que tiene acceso a los siguientes servidores de su sitio:
  - El controlador de dominio de Active Directory para la cuenta de usuario que está asociada con 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Paso 4: Habilite StoreFront para el uso de tarjetas inteligentes. Para obtener más información, consulte Configuración de la autenticación con tarjeta inteligente en la documentación de StoreFront.

Paso 5: Habilite Citrix Gateway o Access Gateway para el uso de tarjetas inteligentes. Para obtener más información, consulte Configuración de la autenticación y la autorización y Configuración del acceso de tarjetas inteligentes con la Interfaz Web en la documentación de NetScaler.

Paso 6: Habilite agentes VDA para el uso de tarjetas inteligentes.

- Compruebe que el VDA tiene las aplicaciones y las actualizaciones necesarias.
- Instale el middleware.
- Configure la comunicación remota con tarjetas inteligentes, habilite la comunicación de datos de la tarjeta inteligente entre la aplicación Citrix Workspace presente en un dispositivo de usuario y una sesión de escritorio virtual.

Paso 7: Habilite los dispositivos de usuario (incluidas las máquinas que estén o no estén unidas a un dominio) para el uso de tarjetas inteligentes. Para obtener más información, consulte Configuración de la autenticación con tarjeta inteligente en la documentación de StoreFront.

- Importe el certificado raíz y el certificado de emisión de la entidad de certificación en el almacén de claves del dispositivo.
- Instale el middleware del proveedor de la tarjeta inteligente.
- Instale y configure la aplicación Citrix Workspace para Windows; importe icaclient.adm mediante la Consola de administración de directivas de grupo y habilite la autenticación con tarjeta inteligente.

Paso 8: Realice pruebas en la implementación. Compruebe que la implementación está correctamente configurada iniciando un escritorio virtual con la tarjeta inteligente de un usuario de prueba. Pruebe todos los mecanismos de acceso posibles (por ejemplo, el acceso al escritorio a través de Internet Explorer y la aplicación Citrix Workspace).

Implementaciones de tarjeta inteligente

October 3, 2018

Los siguientes tipos de implementaciones de tarjeta inteligente reciben respaldo en esta versión del producto y en entornos mixtos que contengan esta versión. Hay otras configuraciones que pueden funcionar, pero no reciben respaldo.

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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Tipo	Conectividad con StoreFront
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 características del dispositivo del usuario al que está conectado el lector de tarjetas inteligentes:

- Si el dispositivo está unido a un dominio o no.
- Cómo se conecta el dispositivo con StoreFront.
- Qué software se usa para ver las aplicaciones y los escritorios virtuales.

Además, las aplicaciones habilitadas para tarjeta inteligente, tales como Microsoft Word y Microsoft Excel, también se pueden utilizar en estas implementaciones. Esas aplicaciones permiten a los usuarios firmar o cifrar documentos digitalmente.

Autenticación bimodal

Cuando es posible en cada una de estas implementaciones, Receiver admite la autenticación bimodal, que ofrece al usuario la posibilidad de elegir si quiere autenticarse con tarjeta inteligente o con nombre de usuario y contraseña. Esto resulta útil cuando no se puede usar la tarjeta inteligente por alguna razón (por ejemplo, si el usuario la olvidó en casa o el certificado de inicio de sesión caducó).

Como los usuarios de dispositivos que no pertenecen a un dominio inician sesión en Receiver para Windows directamente, puede permitir que los usuarios recurran a la autenticación explícita. Si configura la autenticación bimodal, a los usuarios se les solicita que inicien sesión con una tarjeta inteligente y su PIN, pero tienen la opción de seleccionar la autenticación explícita si tienen problemas con las tarjetas inteligentes.

Si implementa Citrix Gateway, los usuarios inician sesión en sus dispositivos y Receiver para Windows les pedirá autenticarse en Citrix Gateway. Esto se aplica a dispositivos unidos a un dominio y a dispositivos que no pertenecen a ningún dominio. Los usuarios pueden iniciar sesión en Citrix Gateway con

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 respalda 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 reciben respaldo.

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.

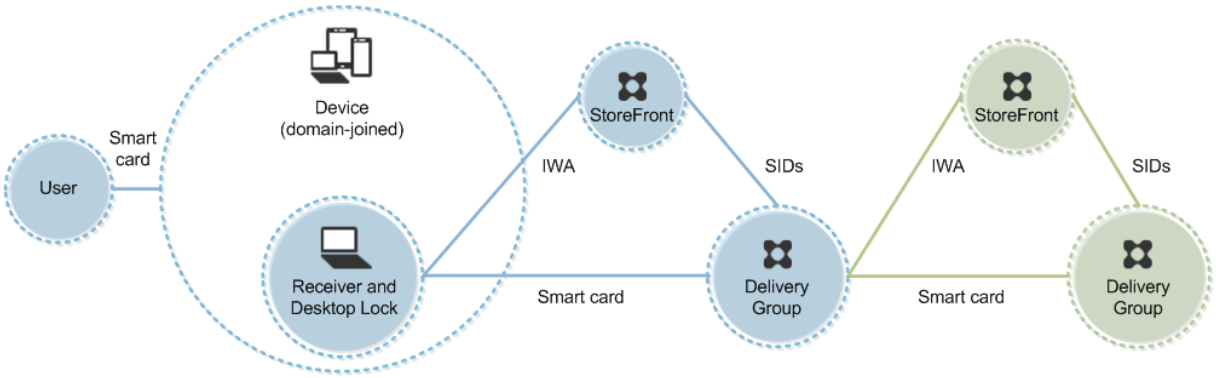
© 1999-2019 Citrix Systems, Inc. All rights reserved.

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.



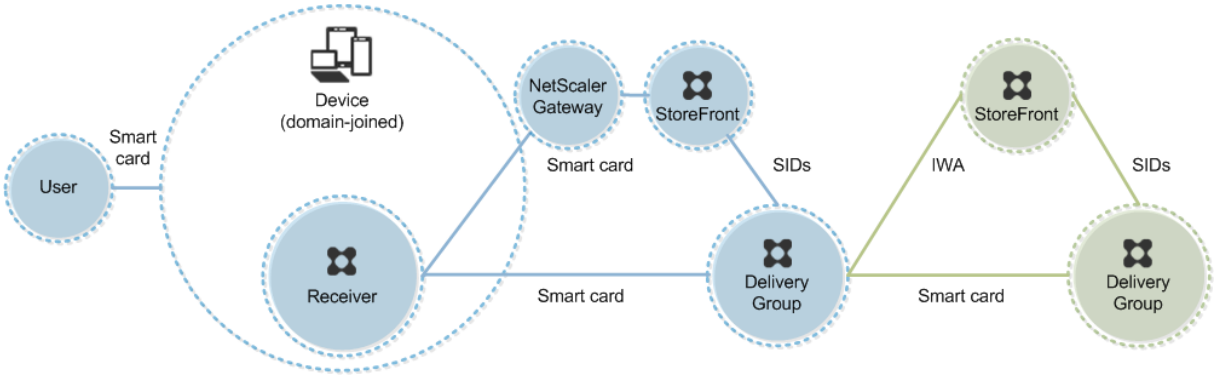
El usuario inicia sesión en un dispositivo usando una tarjeta inteligente y un PIN. Receiver autentica al usuario en un servidor StoreFront mediante la autenticación integrada de Windows (IWA). StoreFront pasa los identificadores de seguridad del usuario (SID) a Citrix Virtual Apps o Citrix Virtual Desktops. 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 StoreFront y un servidor que aloja aplicaciones. Un Receiver desde el escritorio virtual se autentica en el segundo servidor 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



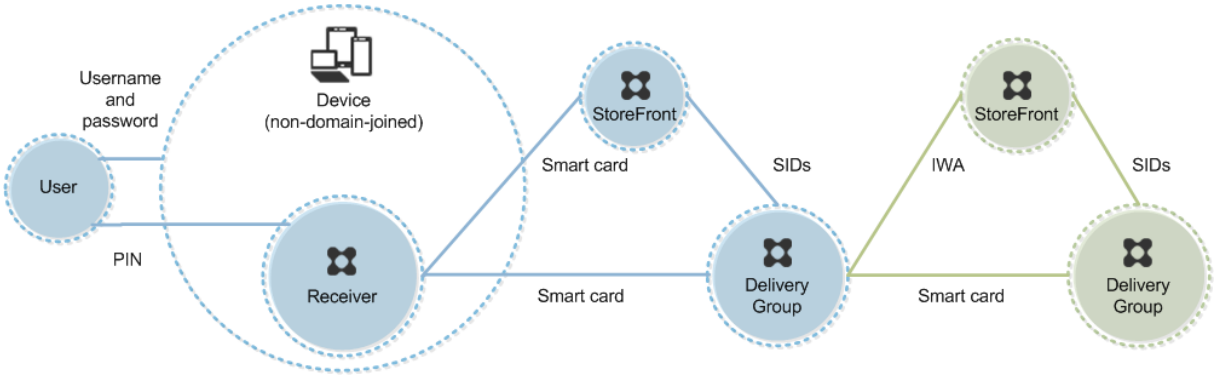
El usuario inicia sesión en un dispositivo con una tarjeta inteligente y un PIN. A continuación, inicia otra sesión en Citrix Gateway o Access Gateway. Este segundo inicio de sesión puede realizarse con la tarjeta inteligente y el PIN, o con un nombre de usuario y una contraseña, porque Receiver permite 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 StoreFront y un servidor que aloja aplicaciones. Un Receiver desde el escritorio virtual se autentica en el segundo servidor 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

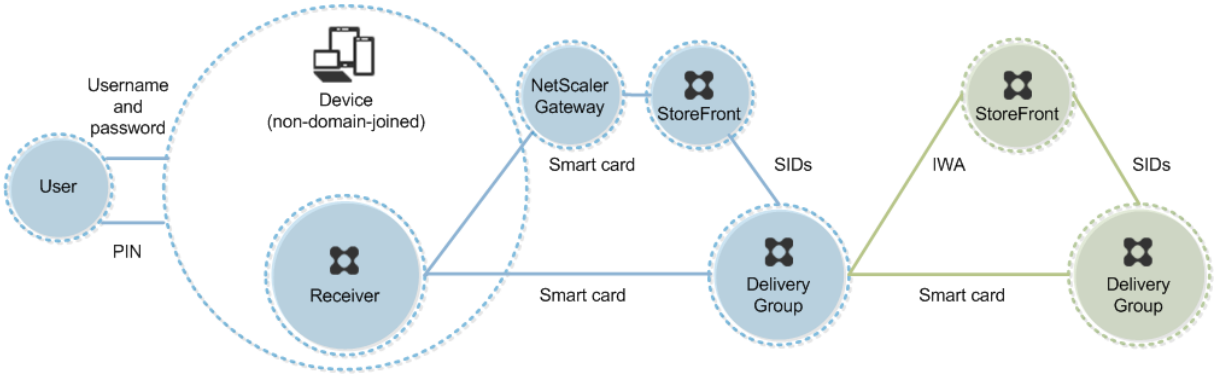
sesión son optativas. Como la autenticación bimodal es posible en esta implementación, Receiver pide al usuario una tarjeta inteligente y un PIN, o un nombre de usuario y una contraseña. A continuación, Receiver se autentica en StoreFront.

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 StoreFront y un servidor que aloja aplicaciones. Un Receiver desde el escritorio virtual se autentica en el segundo servidor 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 StoreFront y un servidor que aloja aplicaciones. Un Receiver desde el escritorio virtual se autentica en el segundo servidor StoreFront. Con esta segunda conexión se puede usar

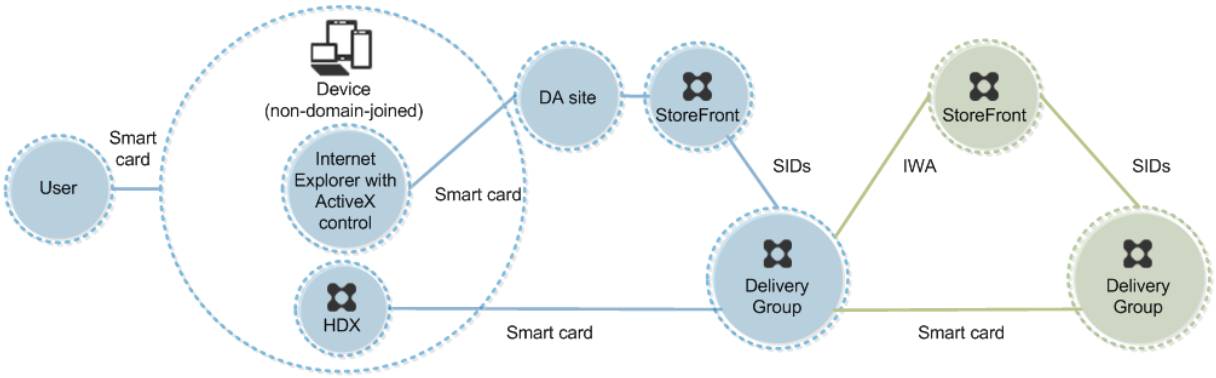
© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 usando 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.

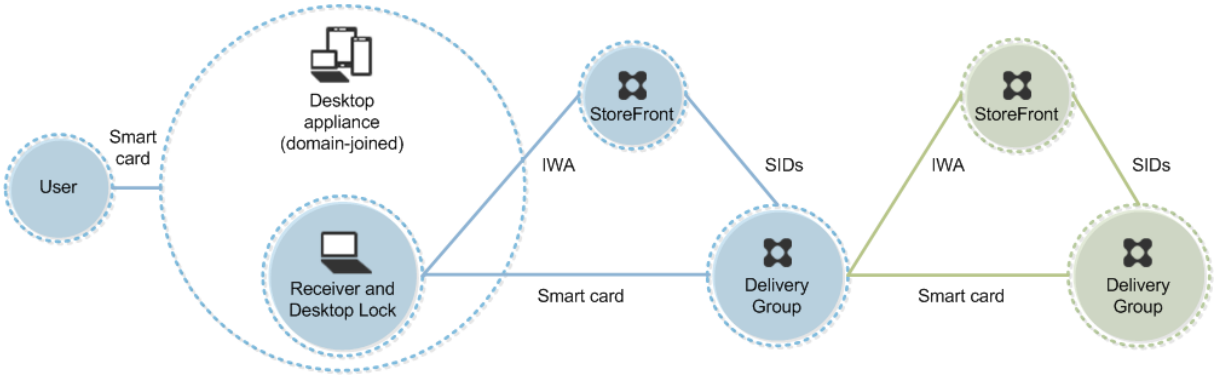
Esta implementación se puede ampliar a una configuración de doble salto con la incorporación de un segundo servidor StoreFront y un servidor que aloja aplicaciones. Un Receiver desde el escritorio virtual se autentica en el segundo servidor StoreFront. Con esta segunda conexión se puede usar cualquier 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 usando una tarjeta inteligente y un PIN. Si Desktop Lock se está ejecutando en el dispositivo, autentica al usuario en un servidor 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 StoreFront y un servidor que aloja aplicaciones. Un Receiver desde el escritorio virtual se autentica en el segundo servidor StoreFront. Con esta segunda conexión se puede usar cualquier método de autenticación. La configuración que se muestra para el primer salto se puede volver a utilizar en el segundo salto o usarse en el segundo salto solamente.

Autenticación PassThrough y Single Sign-On con tarjetas inteligentes

January 29, 2019

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Autenticación mediante paso de credenciales (PassThrough)

La autenticación PassThrough con tarjeta inteligente en los escritorios virtuales se admite en los dispositivos de usuario con Windows 10, Windows 8 y Windows 7 SP1, ediciones Enterprise y Professional.

La autenticación PassThrough con tarjeta inteligente en aplicaciones alojadas está respaldada en servidores que ejecutan Windows Server 2016, Windows Server 2012 R2, Windows Server 2012 y Windows Server 2008 R2 SP1.

Para utilizar la autenticación PassThrough con tarjeta inteligente en aplicaciones alojadas, asegúrese de habilitar el uso de Kerberos cuando configure PassThrough con tarjeta inteligente como el método de autenticación para el sitio.

Nota: La disponibilidad de la autenticación PassThrough con tarjeta inteligente depende de varios factores, incluidos, entre otros:

- Las directivas de seguridad de la organización respecto a la autenticación PassThrough.
- El tipo y la configuración del middleware.
- Los tipos de lectores de tarjetas inteligentes.
- Las directivas de caché de PIN en el middleware.

La autenticación PassThrough con tarjeta inteligente se configura en Citrix StoreFront. Consulte la documentación de StoreFront para obtener más información.

Single Sign-On

Single Sign-On es una función de Citrix que implementa la autenticación PassThrough en el inicio de escritorios virtuales y aplicaciones. Puede utilizar esta característica 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 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 al inicio de sesión único.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- 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)

March 14, 2019

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 desea, 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- 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:

  * La habilitación de conexiones TLS entre los usuarios y los VDA solo es válida para los sitios de XenApp 7.6 y XenDesktop 7.6 y versiones posteriores respaldadas.
  * 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 lo modifica de forma incorrecta, pueden producirse problemas graves que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Para obtener información acerca de la habilitación de TLS para la base de datos del sitio, consulte CTX137556.

Instalar certificados de servidor TLS en los Controllers

Para HTTPS, XML Service admite las funciones de TLS cuando se usan certificados de servidor, no cuando se usan certificados de cliente. Para obtener, instalar y registrar un certificado en un Controller y para configurar un puerto con el certificado TLS:

Si el Controller tiene IIS instalado, siga las instrucciones indicadas en https://technet.microsoft.com/en-us/library/cc771438%28v=ws.10%29.aspx.

Si el Controller no tiene IIS instalado, he aquí un método de configuración del certificado:

1. Obtenga un certificado de servidor TLS e instálelo en el Controller siguiendo las instrucciones de http://blogs.technet.com/b/pki/archive/2009/08/05/how-to-create-a-web-server-ssl-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

certificate-manually.aspx. Para obtener información sobre la herramienta certreq, consulte http://technet.microsoft.com/en-us/library/cc736326(WS.10).aspx.

2. Configure un puerto con el certificado; consulte http://msdn.microsoft.com/en-us/library/ms733791%28v=vs.110%29.aspx.

Si el Controller está instalado en Windows Server 2016 y StoreFront está instalado en Windows Server 2012, es necesario cambiar la configuración en el Controller, para cambiar el orden de los conjuntos de cifrado TLS.

> **Nota:**
>
> Este cambio de configuración no es necesario para Controller ni StoreFront con otras combinaciones de versiones de Windows Server.

La lista ordenada de los conjuntos de cifrado debe incluir el conjunto de cifrado TLS_ECDHE_RSA_WITH_AES_256*CBC_SHA384 o TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (o ambos), y estos conjuntos deben preceder cualquier conjunto de cifrado TLS_DHE*.

> **Nota:**
>
> Windows Server 2012 no admite estos conjuntos de cifrado GCM: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA38 o TLS_ECDHE_RSA_WITH_AES_128_GCM _SHA256.

1. Desde el editor de directivas de grupo de Microsoft, vaya a Configuración del equipo > Plantillas administrativas > Red > Opciones de configuración SSL.
2. Modifique la directiva “Orden de conjuntos de cifrado SSL”. De manera predeterminada, esta directiva está establecida en “No configurada”. Habilite esta directiva.
3. Ordene los conjuntos de cifrado; quite aquellos conjuntos que no quiera usar.

Compruebe que ni TLS_ECDHE_RSA_WITH_AES_256*CBC_SHA384 ni TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 preceden conjuntos de cifrado TLS_DHE*.

En Microsoft MSDN, también puede consultar Prioritizing Schannel Cipher Suites.

Cambiar puertos HTTP o HTTPS

De forma predeterminada, el XML Service en el Controller escucha en los puertos 80 para el tráfico HTTP y 443 para el tráfico HTTPS. Aunque se pueden utilizar otros puertos distintos de los predeterminados, tenga en cuenta los riesgos de seguridad que implica la exposición de un Controller a redes que no son de confianza. Antes que cambiar los valores predeterminados, es preferible implementar un servidor StoreFront independiente.

Para cambiar los puertos HTTP o HTTPS predeterminados que usa el Controller, ejecute el comando siguiente en Studio:

BrokerService.exe -WIPORT <*puerto http*> -WISSLPORT <*puerto https*>

© 1999-2019 Citrix Systems, Inc. All rights reserved.

<*puerto http*> es el número de puerto para el tráfico HTTP y <*puerto https*> es el número de puerto para el tráfico HTTPS.

> **Nota:**
>
> Después de cambiar de un puerto, Studio puede mostrar un mensaje acerca de la actualización y la compatibilidad de licencias. Para resolver el problema, vuelva a registrar las instancias de servicio mediante esta secuencia de cmdlet de PowerShell:

```
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 XmlServicesEnableNonSsl y déle 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 deben permitirse.**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> **Importante:**
>
> Citrix recomienda revisar el uso de SSL 3 y volver a configurar las implementaciones para quitar el respaldo a SSL 3 donde corresponda. Consulte CTX200238.

Las versiones respaldadas del protocolo TLS siguen una jerarquía (de menor a mayor): SSL 3.0, TLS 1.0, TLS 1.1 y TLS 1.2. Debe especificar la versión mínima permitida; se permitirán todas las conexiones que usen esa versión del protocolo o una versión más alta.

Por ejemplo, si especifica TLS 1.1 como la versión mínima, se permitirán conexiones con TLS 1.1 y TLS 1.2. Si elige SSL 3.0 como la versión mínima, se permitirán conexiones con todas las versiones respaldadas. Si especifica TLS 1.2 como la versión mínima, solo se permiten conexiones con TLS 1.2.

DTLS 1.0 corresponde a TLS 1.1, mientras que DTLS 1.2 corresponde a TLS 1.2.

- **¿Qué conjuntos de cifrado TLS 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 respaldados, 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	TODO	COM	GOB	TODO	COM	GOB
Modo FIPS	No	No	No	Sí	Sí	Sí
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384**	X		X	X		X
TLS_ECDHE_	X	X	X	X	X	X
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	X		X	X		X
TLS_ECDHE_	X	X	X	X	X	X
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	X		X	X		X
TLS_ECDHE_	X	X	X	X	X	X
TLS_RSA_WITH_AES_256_GCM_SHA384	X		X	X		X

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Conjunto de cifrado TLS/DTLS	TODO	COM	GOB	TODO	COM	GOB
TLS_RSA_WIT	X	X	X	X	X	X
TLS_RSA_WITH	X_AES_256_CBC_SHA256		X	X		X
TLS_RSA_WIT	X	X	X	X	X	X
TLS_RSA_WITH	X_AES_256_CBC_SHA		X	X		X
TLS_RSA_WIT	X	X	X	X	X	X
TLS_RSA_WITH	X_3DES_EDE_CBC_SHA		X***	X		X***
TLS_RSA_WIT	X**	X**				
TLS_RSA_WITH	X_RC4_128_MD5	X**				

* DTLS no admite estos conjuntos de cifrado.

** Estos conjuntos de cifrado no se admiten en Windows Server 2012 R2.

*** 3DES está inhabilitado de forma predeterminada en el conjunto de cifrado GOV.

De forma predeterminada, ** RC4-MD5 está inhabilitado.

> **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.

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 “<huella digital>” [–SSLPort <puerto>] [-SSLMinVersion “<versión mínima de SSL>”] [-SSLCipherSuite”<conjunto de cifrado>”]‘

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Parámetro	Descripción
CertificateThumbPrint “<huella digital>”	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>	Puerto TLS. Valor predeterminado: 443
SSLMinVersion “”	Versión mínima del protocolo TLS, entre comillas. Valores válidos: “SSL_3.0”, “TLS_1.0” (valor predeterminado), “TLS_1.1” y “TLS_1.2”. **Importante:** Citrix recomienda que los clientes revisen su uso de SSL 3 y tomen las medidas necesarias para reconfigurar sus implementaciones con el fin de quitar el respaldo para SSL 3 donde corresponda. Consulte CTX200238.
-SSLCipherSuite “<conjunto de cifrado>”	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_1.2”
 - SSLCipherSuite ”GOV”
```

El siguiente script inhabilita la escucha de TLS en el VDA.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

```
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 escritorio Windows o NT SERVICE\TermService para un VDA de SO de servidor 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 déle acceso de lectura:

- Para un VDA de SO de escritorio Windows, “PORTICASERVICE”
- Para un VDA de SO de servidor Windows, “TERMSERVICE”

PASO 5. Haga doble clic en el certificado TLS instalado. En el cuadro de diálogo del certificado, seleccione la ficha Detalles y desplácese 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 Editar valor binario (por ejemplo, ‘0000’ y los caracteres especiales).
2. Edite la clave SSLEnabled y cambie el valor DWORD a 1. (Para inhabilitar SSL más adelante, cambie el valor DWORD a 0.)
3. Si desea cambiar la configuración predeterminada (optativo), use lo siguiente en la misma ruta de Registro:

   SSLPort DWORD – número de puerto SSL. Valor predeterminado: 443.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

SSLMinVersion DWORD – 1 = SSL 3.0, 2 = TLS 1.0, 3 = TLS 1.1, 4 = TLS 1.2. Valor predeterminado: 2 (TLS 1.0).

SSLCipherSuite DWORD – 1 = GOV, 2 = COM, 3 = ALL. Valor predeterminado: 3 (ALL).

PASO 7. Compruebe que los puertos UDP y TCP de TLS están abiertos en el Firewall de Windows, si no son el predeterminado 443. (Cuando cree la regla de entrada en el Firewall de Windows, compruebe que tenga seleccionadas las entradas “Permitir la conexión” y “Habilitada” en las propiedades.)

Paso 8. Asegúrese de que no hay otros servicios o aplicaciones (por ejemplo, IIS) que estén usando el puerto TCP de TLS.

PASO 9. Para los VDA para SO de servidor Windows, reinicie la máquina para que los cambios tengan efecto. (No es necesario reiniciar las máquinas que contienen los VDA para SO de escritorio Windows.)

> **Importante:**
>
> Se necesita un paso adicional si el VDA está en Windows Server 2012 R2, Windows Server 2016, o bien, en Windows 10 Anniversary Edition o una versión posterior respaldada. 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 Server 2012 R2, Windows Server 2016 o Windows 10 Anniversary Edition o versiones posteriores), mediante el Editor de directivas de grupo, vaya a “Configuración del equipo > 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_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> **Nota:**
>
> Los cuatro 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 de TLS en el 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**.

Solucionar 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 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 posterior, Receiver para Mac 12.8 o posterior o Receiver para iOS 7.5 o posterior;
- actualice Citrix Gateway a una versión que admita DTLS al VDA;
- actualice el VDA a la versión 7.16 o 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 conseguirlo, se colocan dos certificados personalizados en el almacén de certificados presente en el VDA.

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.

> **Nota:**
>
> Si no tiene intención de utilizar la redirección de vídeo HTML5 ni la redirección de contenido del explorador Web, le recomendamos eliminar los dos certificados contenidos en el almacén de certificados del equipo local.
>
> Esos certificados son:
>
> - Para la CA (raíz): **Citrix XenApp/XenDesktop HDX In-Product CA** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX In-Product CA)
>   Ubicación: Certificados (Equipo local) > Entidades de certificación raíz de confianza > Certificados.
> - Para la entidad final (hoja): **Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX Service)
>   Ubicación: Certificados (Equipo local) > Personal > Certificados.
>
> Recomendamos configurar el servicio Citrix HDX HTML5 Video Redirection Service para que no se inicie automáticamente.
> La detención de este servicio también elimina los certificados.

Para obtener más información sobre la redirección de vídeos HTML5, consulte Configuraciones de directiva de Multimedia.

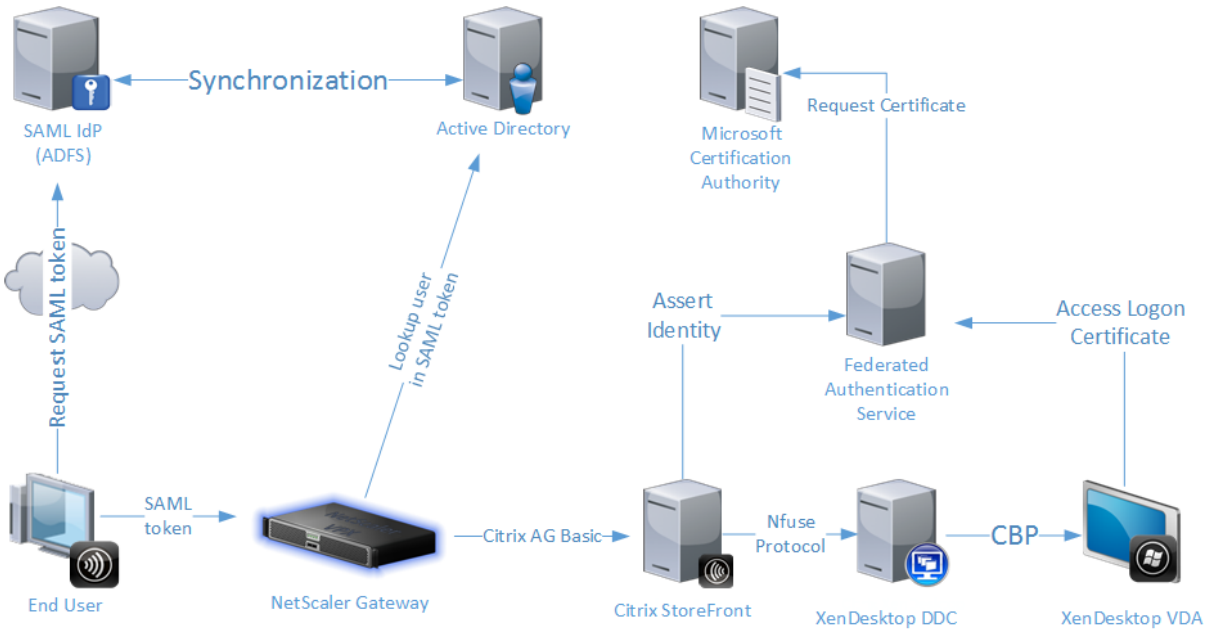
Servicio de autenticación federada

March 8, 2019

© 1999-2019 Citrix Systems, Inc. All rights reserved.

El servicio de autenticación federada (Federated Authentication Service) de Citrix es un componente con privilegios diseñado para integrarlo con el Servicio de Certificados de Active Directory. Emite certificados para los usuarios de forma dinámica, lo que les permite iniciar sesiones en un entorno de Active Directory como si tuvieran una tarjeta inteligente. Esto permite a StoreFront usar una gama más amplia de opciones de autenticación, tales como aserciones SAML (Security Assertion Markup Language). SAML se usa normalmente como alternativa a las cuentas de usuario tradicionales de Windows en Internet.

El siguiente diagrama muestra el Servicio de autenticación federada integrado con una entidad de certificación de Microsoft y ofreciendo servicios de respaldo para StoreFront y los agentes Virtual Delivery Agent (VDA) de Citrix Virtual Apps and Desktops.



Los servidores StoreFront de confianza contactan con el servicio de autenticación federada (Federated Authentication Service, FAS) a medida que los usuarios solicitan acceso a los entornos Citrix. El servicio FAS concede un tíquet que permite que una sola de sesión de Citrix Virtual Apps o Citrix Virtual Desktops se autentique con un certificado para esa sesión. Cuando un agente VDA debe autenticar a un usuario, se conecta al servicio FAS y canjea el tíquet. Solo el servicio FAS tiene acceso a la clave privada del certificado del usuario; el VDA debe enviar al servicio FAS cada operación de firma y descifrado que necesita llevar a cabo con el certificado.

Requisitos

El servicio de autenticación federada se admite en servidores Windows (Windows Server 2008 R2 o una versión posterior).

- Citrix recomienda la instalación del servicio FAS en un servidor que no contenga ningún otro

© 1999-2019 Citrix Systems, Inc. All rights reserved.

componente de Citrix.
- El servidor de Windows debe ser seguro. Este servidor tendrá acceso a un certificado de autorización de registro y una clave privada que permitirá emitir certificados para los usuarios del dominio y tendrá acceso a esos certificados de usuario y sus claves privadas.

En el sitio de Citrix Virtual Apps o Citrix Virtual Desktops:

- Los Delivery Controllers deben ser de la versión 7.9 como mínimo.
- El VDA debe ser como mínimo de la versión 7.9. Compruebe que la configuración de directiva de grupo del servicio de autenticación federada se ha aplicado correctamente para los VDA antes de crear el catálogo de máquinas de la forma habitual; consulte la sección Configurar la directiva de grupo para obtener más detalles.
- El servidor StoreFront debe ser como mínimo de la versión 3.6 (esta es la versión suministrada en la imagen ISO de XenApp y XenDesktop 7.9).

Al planificar la implementación de este servicio, revise la sección Consideraciones de seguridad.

Referencias:

- Servicios de certificados de Active Directory

https://technet.microsoft.com/en-us/library/hh831740.aspx

- Configuración de Windows para el inicio de sesión con certificados

http://support.citrix.com/article/CTX206156

Secuencia de instalación y configuración

1. Instalar el Servicio de autenticación federada
2. Habilitar el plug-in del Servicio de autenticación federada en los servidores StoreFront
3. Configurar la directiva de grupo
4. Use la consola de administración del Servicio de autenticación federada para: (a) Implementar las plantillas suministradas, (b) Configurar entidades de certificación y (c) Autorizar al Servicio de autenticación federada a usar su entidad de certificación
5. Configurar reglas de usuario

Instalar el Servicio de autenticación federada

Por motivos de seguridad, Citrix recomienda que el Servicio de autenticación federada (FAS) esté instalado en un servidor dedicado que sea seguro, y esté protegido del mismo modo que un controlador de dominio o una entidad de certificación. El servicio FAS se puede instalar con el botón **Servicio de autenticación federada** en la pantalla de autoejecución que aparece cuando se abre la imagen ISO.

Se instalarán los siguientes componentes:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Servicio de autenticación federada
- Cmdlets del complemento de PowerShell para configurar de forma remota el servicio de autenticación federada
- Consola de administración del Servicio de autenticación federada
- Plantillas de directiva de grupo del Servicio de autenticación federada (CitrixFederatedAuthenticationService.admx/adml)
- Archivos de plantilla de certificado para una configuración simple de la entidad de certificación
- Contadores de rendimiento y registros de eventos

Habilitar el plug-in del Servicio de autenticación federada en un almacén de StoreFront

Para habilitar la integración del Servicio de autenticación federada en un almacén de StoreFront, ejecute los siguientes cmdlets de PowerShell con una cuenta de administrador. Si tiene más de un almacén, o si el almacén tiene otro nombre, la ruta indicada aquí puede ser distinta de la suya.

```
1 Get-Module "Citrix.StoreFront.*" -ListAvailable | Import-Module
2 $StoreVirtualPath = "/Citrix/Store"
3 $store = Get-STFStoreService -VirtualPath $StoreVirtualPath
4 $auth = Get-STFAuthenticationService -StoreService $store
5 Set-STFClaimsFactoryNames -AuthenticationService $auth -
     ClaimsFactoryName "FASClaimsFactory"
6 Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider "
     FASLogonDataProvider"
```

Para dejar de usar el servicio FAS, use el siguiente script de PowerShell:

```
1 Get-Module "Citrix.StoreFront.*" -ListAvailable | Import-Module
2 $StoreVirtualPath = "/Citrix/Store"
3 $store = Get-STFStoreService -VirtualPath $StoreVirtualPath
4 $auth = Get-STFAuthenticationService -StoreService $store
5 Set-STFClaimsFactoryNames -AuthenticationService $auth -
     ClaimsFactoryName "standardClaimsFactory"
6 Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider ""
```

Configurar el Delivery Controller

Para usar el Servicio de autenticación federada, configure el Delivery Controller de Citrix Virtual Apps o Citrix Virtual Desktops para que confíe en los servidores StoreFront que pueden conectarse a él: ejecute el cmdlet de PowerShell **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

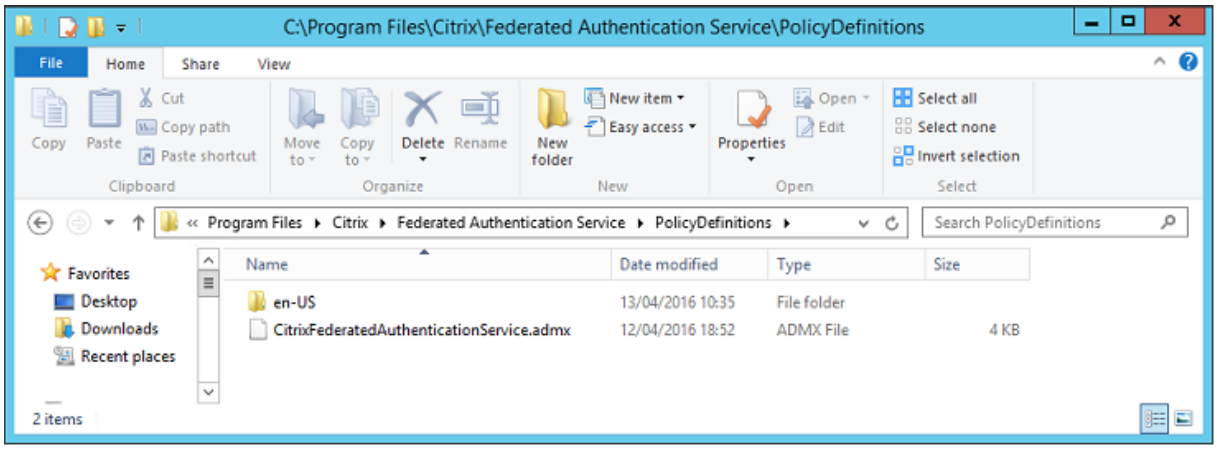
Configurar la directiva de grupo

Después de instalar el Servicio de autenticación federada, se deben especificar las direcciones DNS completas de los servidores del servicio FAS en Directiva de grupo usando las plantillas de directiva de grupo suministradas en la instalación.

> **Importante:**
>
> Compruebe que los servidores StoreFront que solicitan tíquets y los VDA que canjean los tíquets tienen una configuración idéntica de direcciones DNS, incluida la numeración automática de los servidores que aplica el objeto de directiva de grupo.

Para simplificar la tarea, los siguientes ejemplos configuran una sola directiva en el nivel de dominio que se aplica a todas las máquinas; sin embargo, esto no es necesario. El servicio FAS funcionará siempre que los servidores StoreFront, los VDA y la máquina que ejecuta la consola de administración de FAS vean la misma lista de direcciones DNS. Tenga en cuenta que el objeto de directiva de grupo agrega un número de índice a cada entrada, que también debe coincidir cuando se usan varios objetos.

Paso 1: En el servidor donde instaló el servicio FAS, busque el archivo C:\Archivos de programa\Citrix\Federated Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.admx y la carpeta en-US.



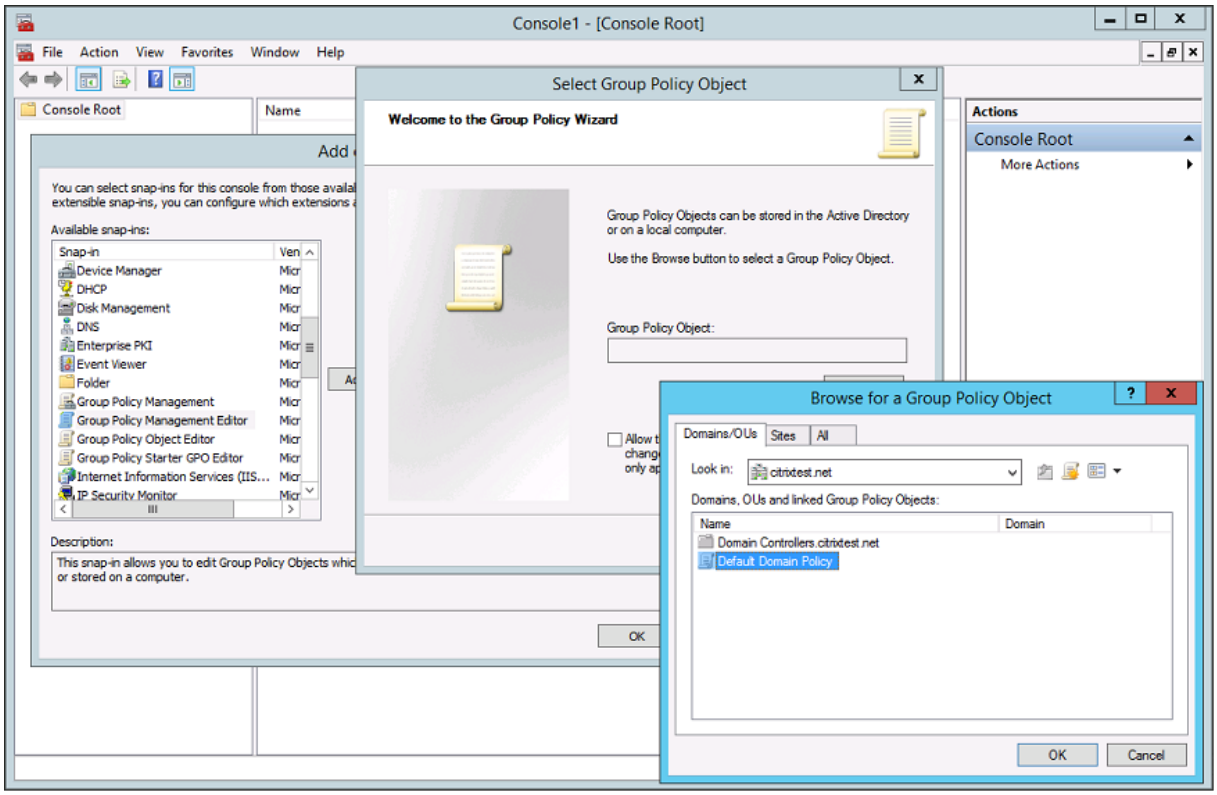
Paso 2: Cópielos en el controlador de dominio y colóquelos en la unidad C:\Windows\PolicyDefinitions y en la subcarpeta en-US.

Paso 3: Ejecute Microsoft Management Console (mmc.exe desde la línea de comandos). En la barra de menús, seleccione **Archivo > Agregar o quitar complemento**. Agregue el **Editor de administración de directivas de grupo**.

Cuando se le solicite un objeto de directiva de grupo, seleccione **Examinar** y, a continuación, seleccione **Directiva predeterminada de dominio**. De forma alternativa, puede crear y seleccionar un objeto de directiva adecuado para el entorno, mediante las herramientas de su elección. La direc-

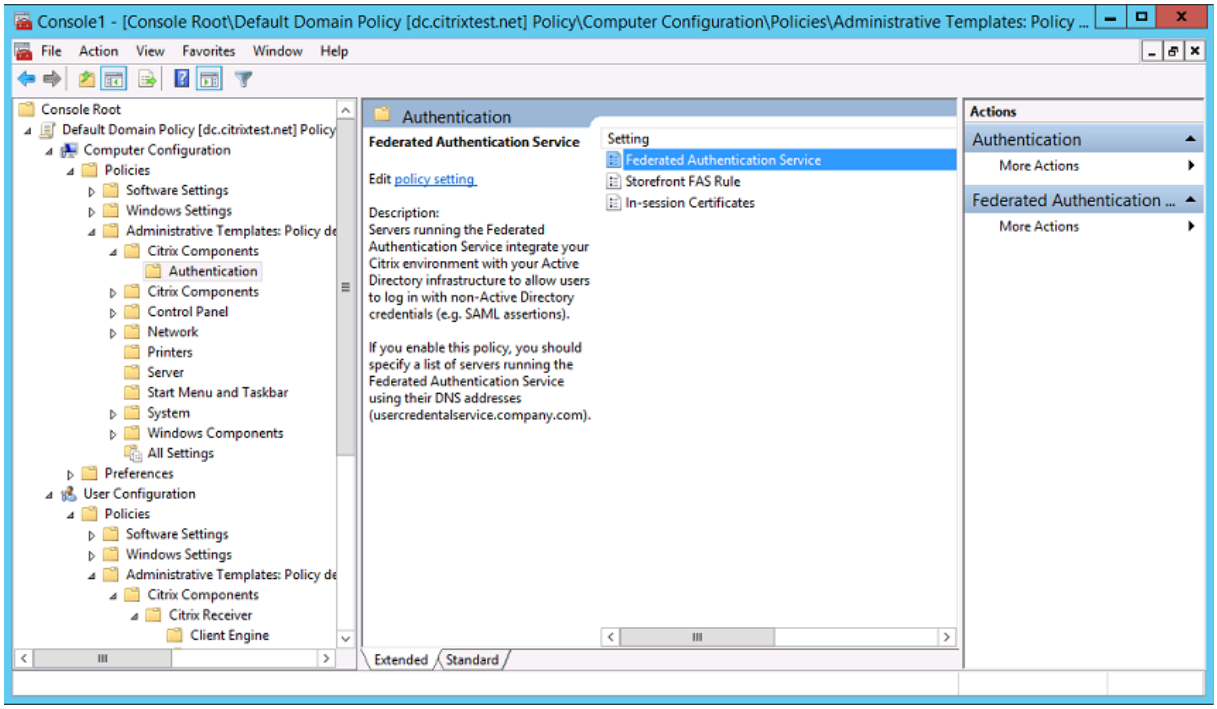
© 1999-2019 Citrix Systems, Inc. All rights reserved.

tiva debe aplicarse a todas las máquinas que ejecutan el software de Citrix afectado (VDA, servidores StoreFront, herramientas de administración).



Paso 4: Vaya a la directiva de Servicio de autenticación federada (Federated Authentication Service) en Configuración del equipo/Directivas/Plantillas administrativas/Citrix Components/Authentication.

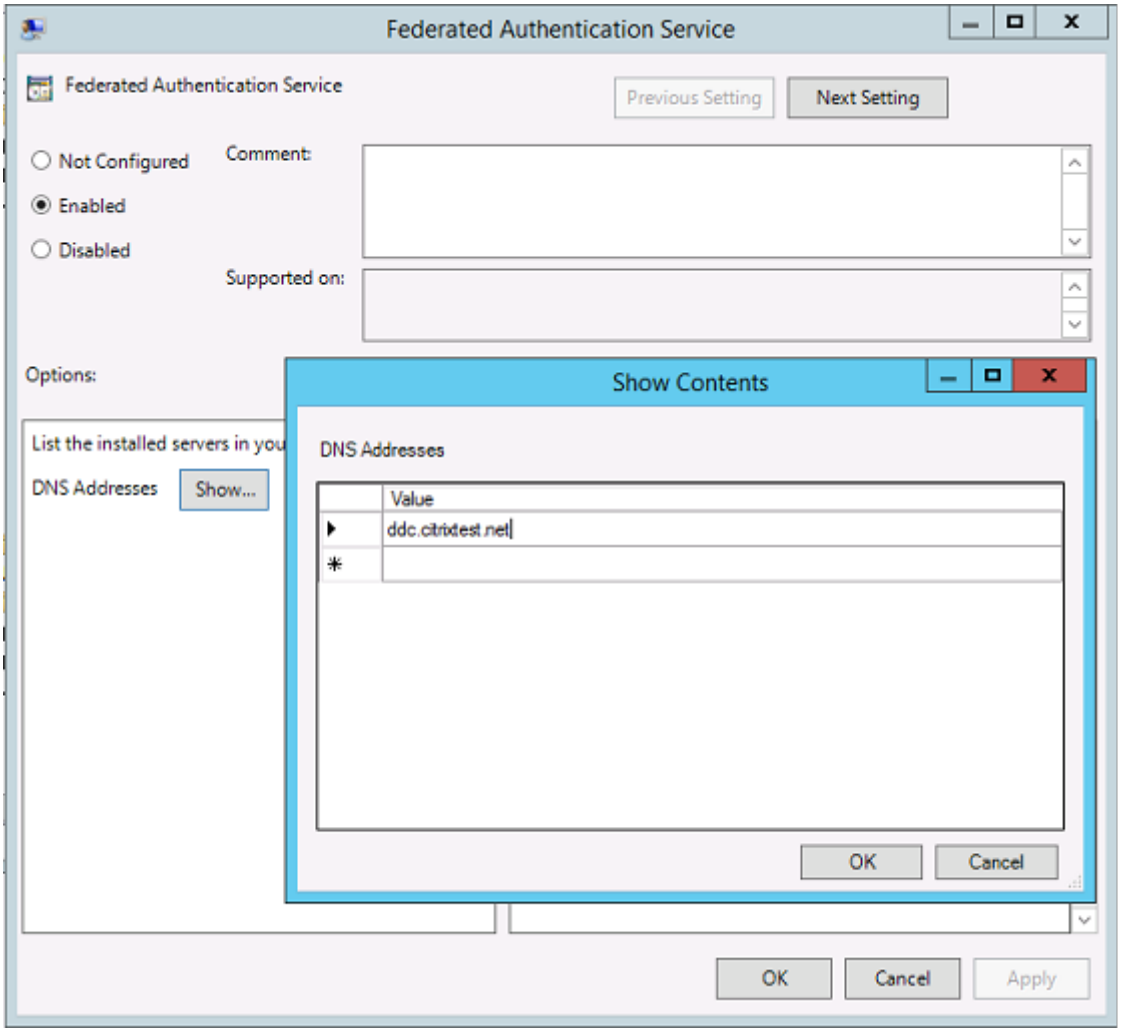
© 1999-2019 Citrix Systems, Inc. All rights reserved.



> **Nota:**
>
> La configuración de directiva del Servicio de autenticación federada de Citrix solo está disponible en el GPO del dominio cuando agrega el archivo de plantilla CitrixBase.admx o CitrixBase.adml a la carpeta \policyDefinitions. Una vez agregada, la configuración de directiva del Servicio de autenticación federada aparece en la carpeta Plantillas administrativas > Componentes Citrix > Autenticación.

Paso 5: Abra la directiva Federated Authentication Service y seleccione **Habilitada**. Esto le permite seleccionar el botón **Mostrar** con el que puede configurar las direcciones DNS de servidores del servicio FAS.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Paso 6: Escriba las direcciones DNS de los servidores que alojan el Servicio de autenticación federada.

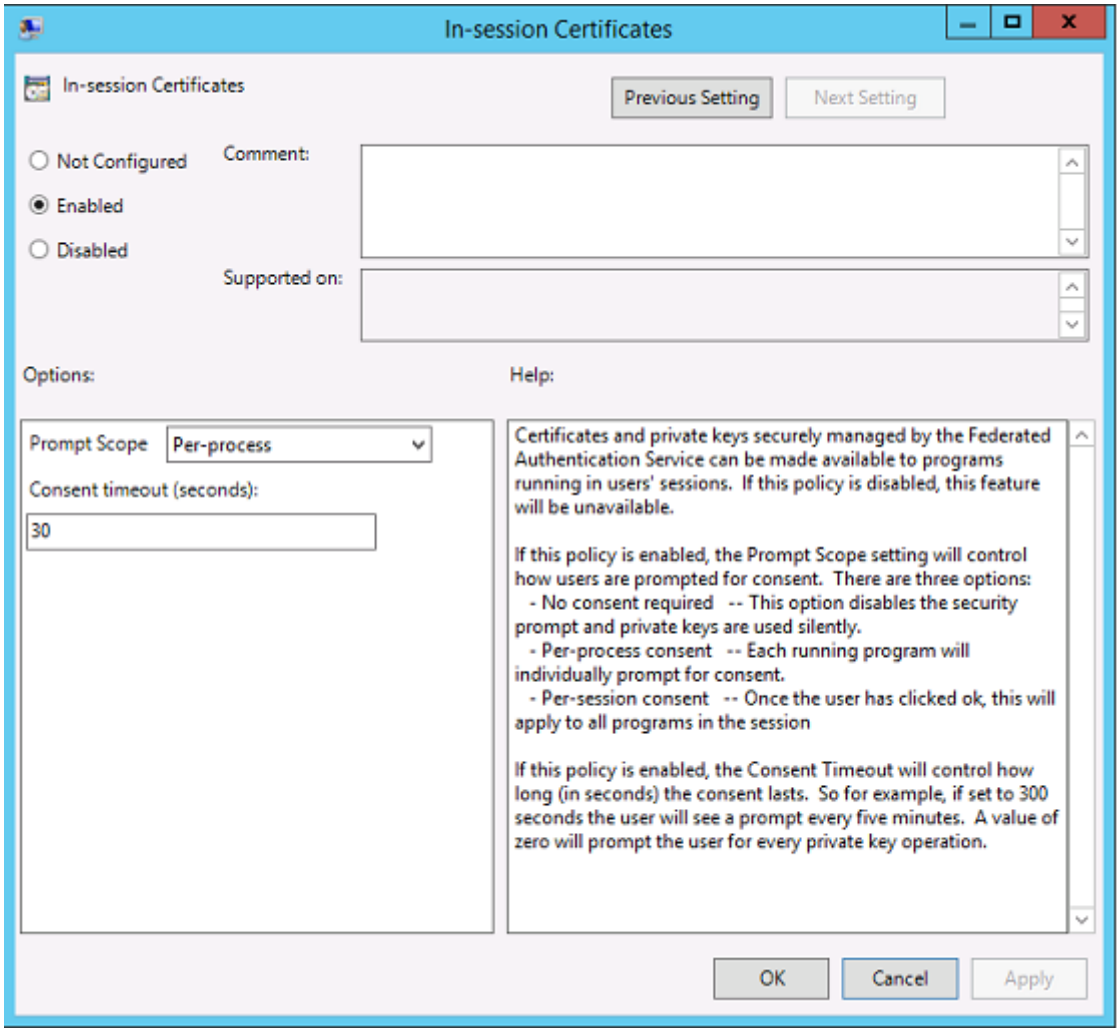
Recuerde: Si escribe varias direcciones, el orden de la lista debe ser coherente entre los servidores de StoreFront y los VDA. Esto incluye las entradas en blanco y las entradas de no utilizadas de la lista.

Paso 7: Haga clic en **Aceptar** para salir del asistente de directivas de grupo y aplicar los cambios de la directiva de grupo. Es posible que tenga que reiniciar las máquinas (o ejecutar **gpupdate /force** desde la línea de comandos) para que el cambio surta efecto.

Habilitar el respaldo a certificados en la sesión

La plantilla de directiva de grupo incluye respaldo para configurar el sistema para usar certificados de la sesión. Esto coloca los certificados en el almacén de certificados personal del usuario después del inicio de sesión para el uso de aplicaciones. Por ejemplo, si necesita usar autenticación TLS en los servidores Web dentro de la sesión de VDA, Internet Explorer puede usar el certificado. De forma predeterminada, los VDA no permitirán el acceso a los certificados después de iniciar la sesión.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

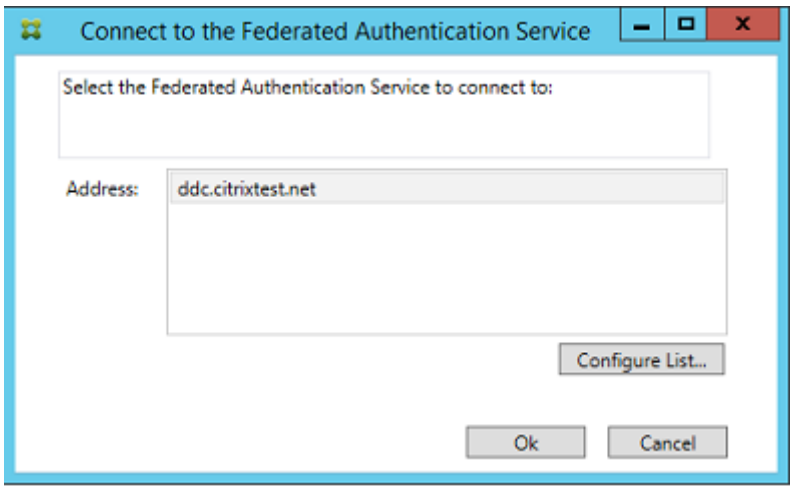


Usar la consola de administración de los Servicios de autenticación federada

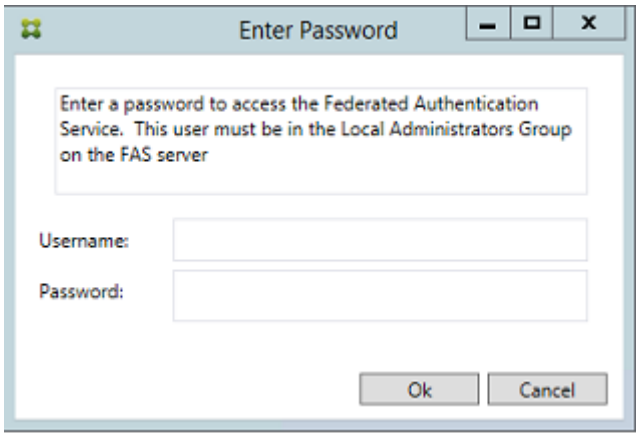
La consola de administración del Servicio de autenticación federada se instala como parte del servicio de autenticación federada. Se coloca el icono Citrix Federated Authentication Service en el menú Inicio.

La consola intenta encontrar automáticamente los servidores del servicio FAS del entorno mediante la configuración de directiva de grupo. Si esto falla, consulte la sección Configurar la directiva de grupo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

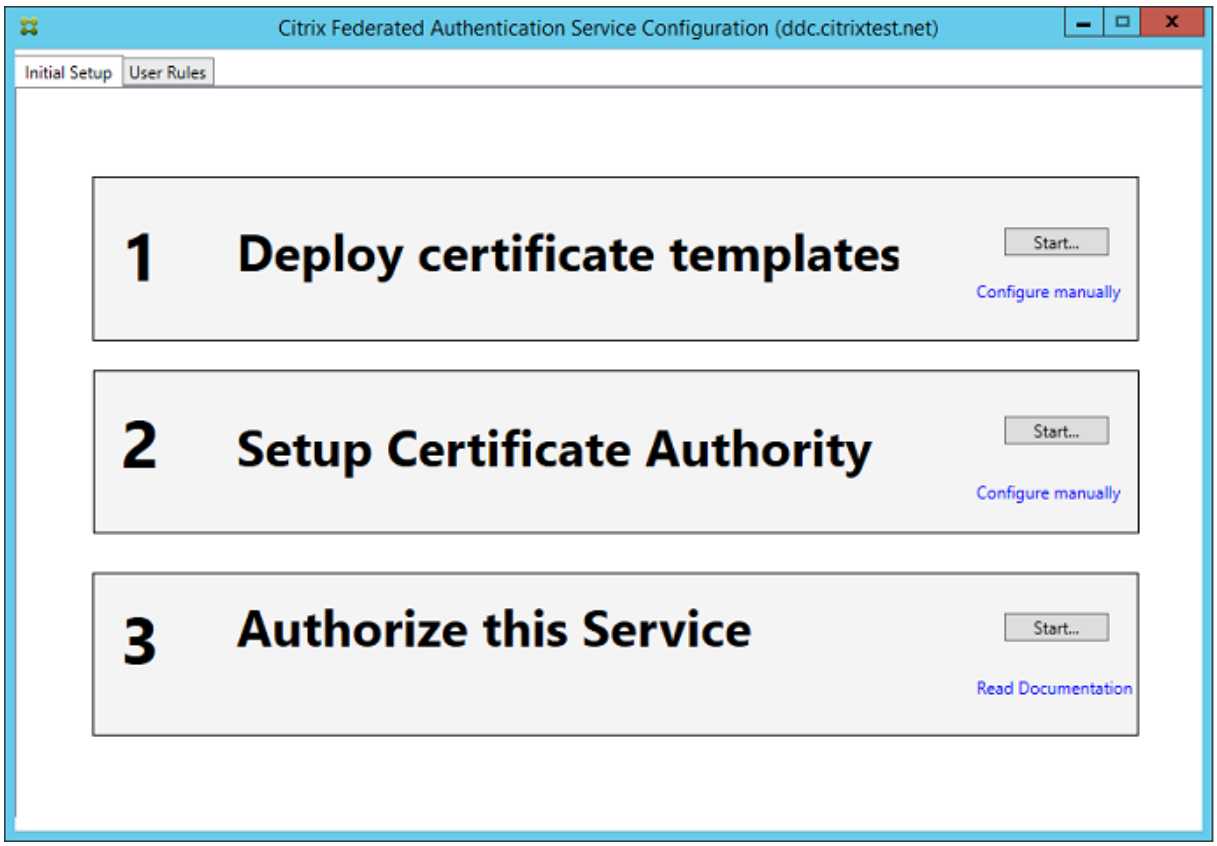


Si la cuenta de usuario no es miembro del grupo Administradores en el equipo que ejecuta el Servicio de autenticación federada, se le solicitará que introduzca las credenciales.



La primera vez que se utiliza la consola de administración, se le guiará a través de un proceso de tres pasos que implementa las plantillas de certificado, establece la entidad de certificación y autoriza al Servicio de autenticación federada para usar la entidad de certificación. Algunos de los pasos pueden completarse manualmente mediante herramientas de configuración del sistema operativo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



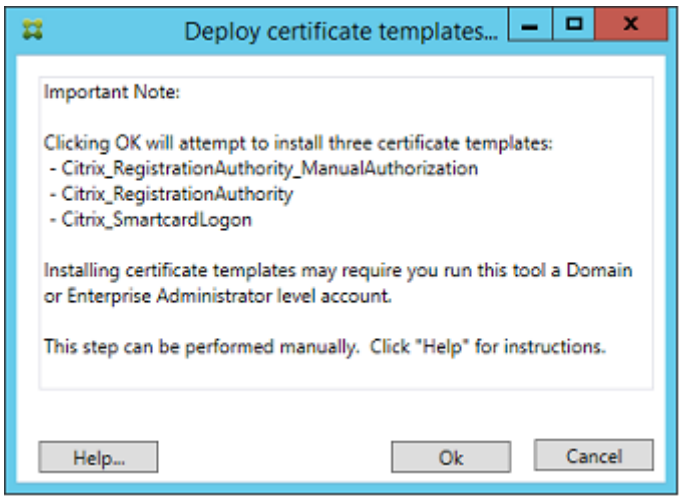
Implementar plantillas de certificado

Para evitar problemas de interoperabilidad con otros programas de software, el Servicio de autenticación federada proporciona tres plantillas de certificado de Citrix para su propio uso.

- Citrix_RegistrationAuthority_ManualAuthorization
- Citrix_RegistrationAuthority
- Citrix_SmartcardLogon

Estas plantillas deben registrarse con Active Directory. Si la consola no puede encontrarlas, se pueden instalar con la herramienta **Implementar plantillas de certificado**. Esta herramienta debe ejecutarse con una cuenta que tenga permisos para administrar el bosque de AD de su empresa.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



La configuración de las plantillas se encuentra en los archivos XML con la extensión .certificatetemplate. Estos archivos se instalan con el Servicio de autenticación federada en:

C:\Archivos de programa\Citrix\Federated Authentication Service\CertificateTemplates

Si no dispone de permiso para instalar estos archivos de plantilla, déselas al administrador de Active Directory.

Para instalar manualmente las plantillas, pueden usar los siguientes comandos de PowerShell:

```
$template = [System.IO.File]::ReadAllBytes("$Pwd\Citrix_SmartcardLogon.certificatetemplate")
$CertEnrol = New-Object -ComObject X509Enrollment.CX509EnrollmentPolicyWebService
$CertEnrol.InitializeImport($template)
$comtemplate = $CertEnrol.GetTemplates().ItemByIndex(0)
$writabletemplate = New-Object -ComObject X509Enrollment.CX509CertificateTemplateADWritable
$writabletemplate.Initialize($comtemplate)
$writabletemplate.Commit(1, $NULL)
```

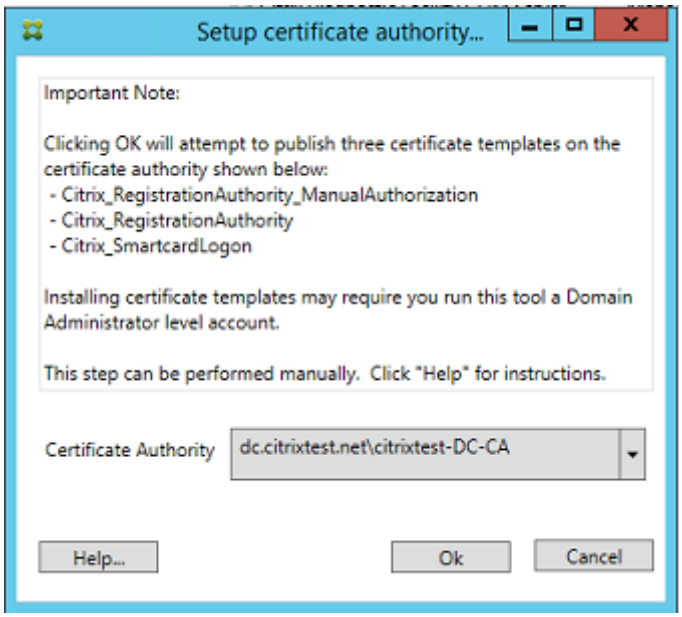
Configurar los Servicios de certificados de Active Directory

Después de instalar las plantillas de certificado de Citrix, deben publicarse en uno o varios servidores de entidad de certificación de Microsoft. Consulte la documentación de Microsoft acerca de cómo implementar Servicios de certificados de Active Directory.

Si las plantillas no se publican en, al menos, un servidor, la herramienta **Setup certificate authority** solicita publicarlas. Debe ejecutar esta herramienta como un usuario que tenga permisos para administrar la entidad de certificación.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

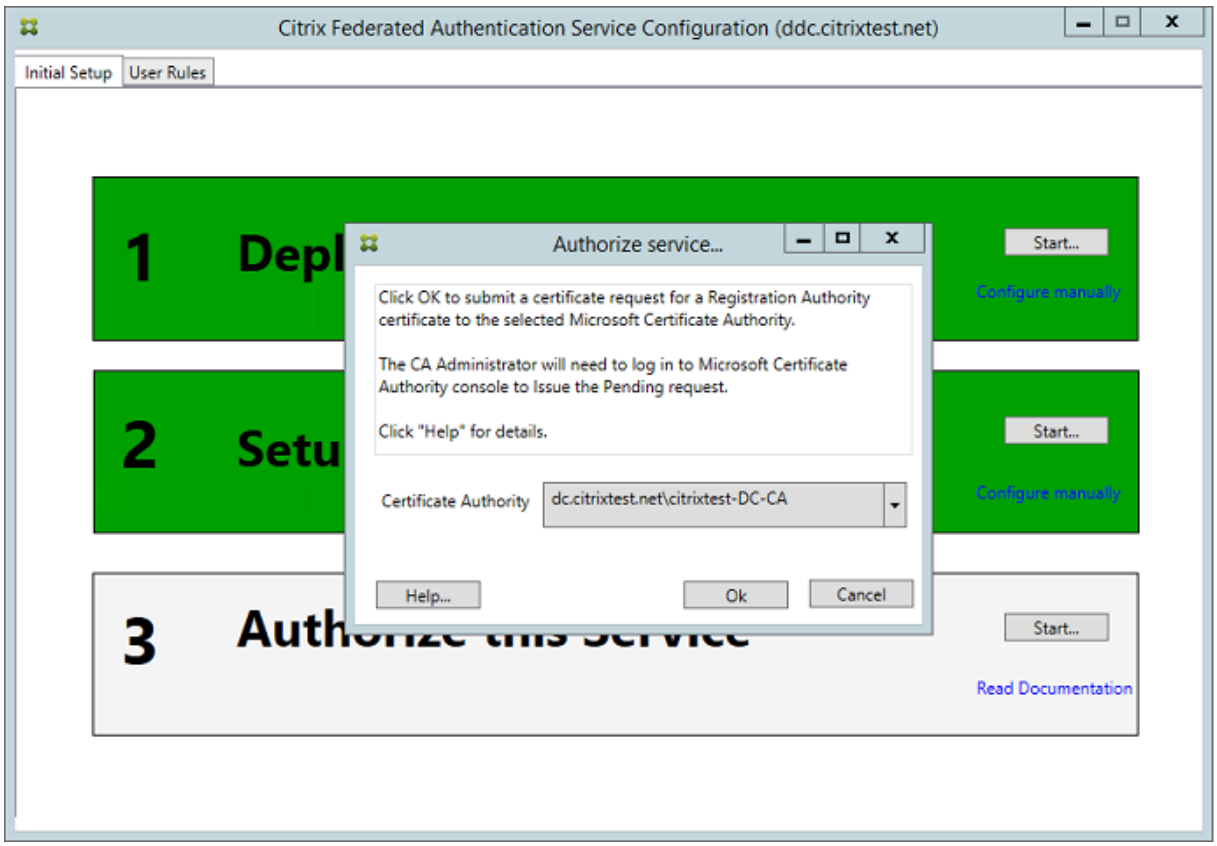
(También se pueden publicar plantillas de certificado mediante la consola de Entidad de certificación de Microsoft.)



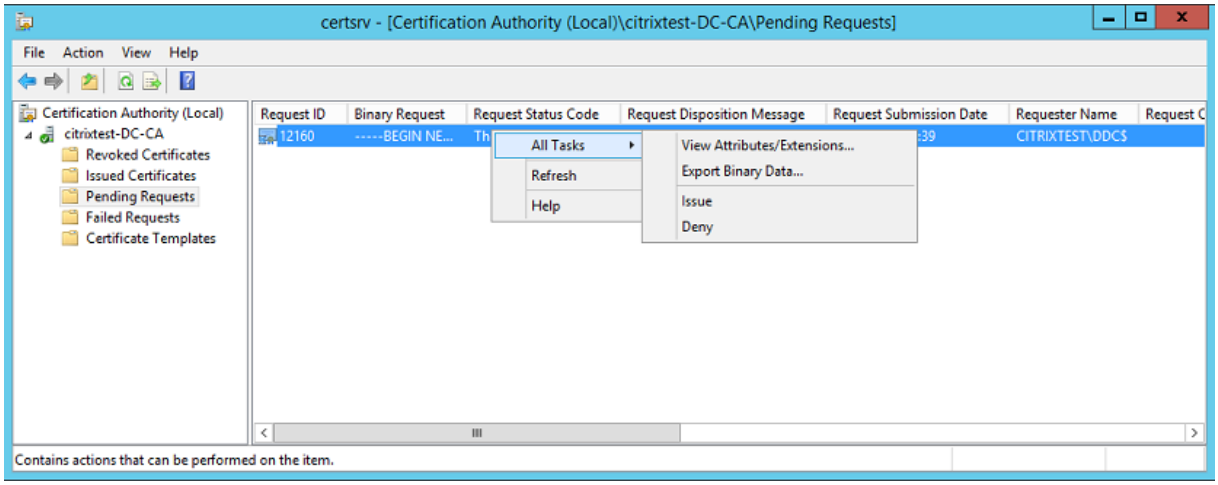
Autorizar el Servicio de autenticación federada

El paso final de configuración en la consola inicia la autorización del Servicio de autenticación federada. La consola de administración utiliza la plantilla Citrix_RegistrationAuthority_ManualAuthorization para generar una solicitud de certificado y, a continuación, lo envía a una de las entidades de certificación que publican esa plantilla.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

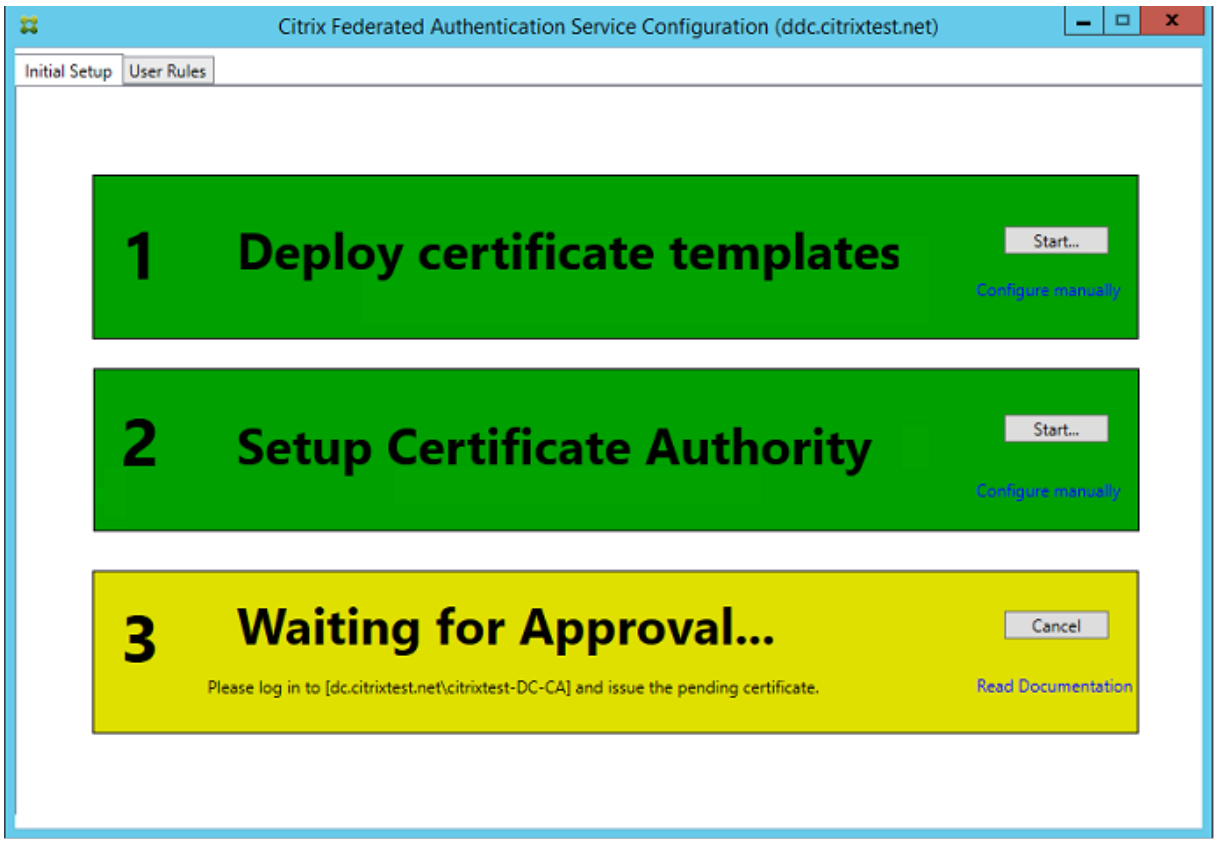


Después de enviarse la solicitud, aparecerá en la lista de **Solicitudes pendientes** de la consola de la entidad de certificación de Microsoft. El administrador de la entidad de certificación debe elegir entre **Emitir** o **Rechazar** la solicitud antes de que la configuración del servicio de autenticación federada pueda continuar. Tenga en cuenta que la solicitud de autorización se muestra como una **Solicitud pendiente** desde la cuenta de equipo de FAS.



Haga clic con el botón secundario en **Todas las tareas** y, a continuación, seleccione **Emitir** o **Rechazar** la solicitud de certificado. La consola de administración del Servicio de autenticación federada detecta automáticamente cuando se completa el proceso. Esto puede tardar unos minutos.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

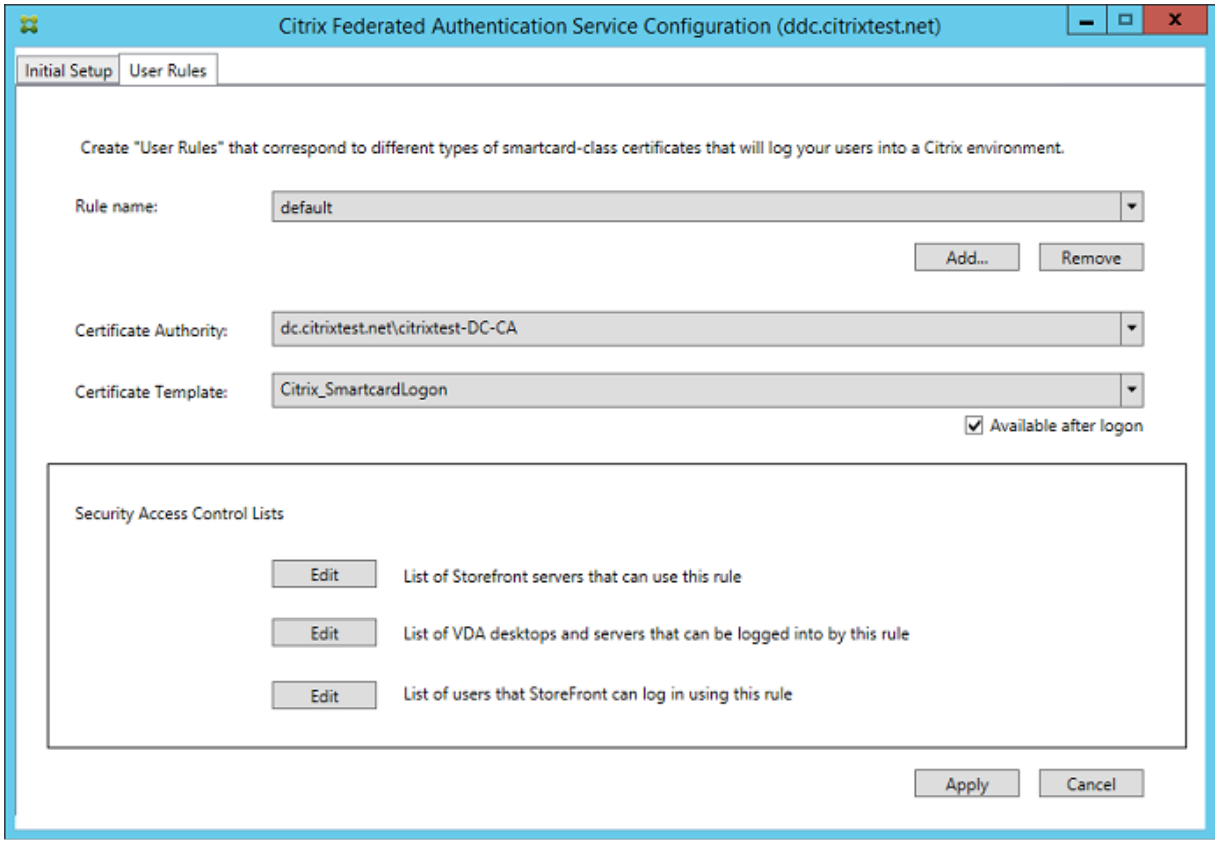


Configurar reglas de usuario

Una regla de usuario autoriza la emisión de certificados para el inicio de sesión en los VDA y uso dentro de sesiones, según lo indique StoreFront. Cada regla especifica los servidores StoreFront que son de confianza para solicitar certificados, el conjunto de usuarios para los que pueden ser solicitados y el conjunto de máquinas VDA a las que se les permite usarlos.

Para completar la instalación del Servicio de autenticación federada, el administrador debe definir la regla predeterminada. Para ello, debe ir a la ficha User Rules de la consola de administración del servicio FAS, seleccionar una entidad de certificación donde esté publicada la plantilla Citrix_SmartcardLogon y editar la lista de servidores StoreFront. La lista de VDA incluye de forma predeterminada los Equipos del dominio y la lista de usuario incluye de forma predeterminada los Usuarios del dominio, pero esto puede cambiarse si estos valores predeterminados no son los adecuados.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Campos:

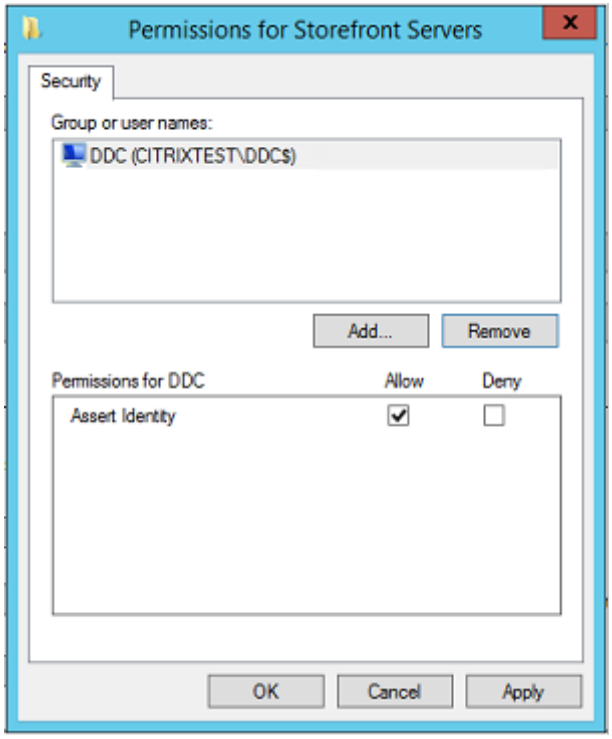
Certificate Authority and Certificate Template: La plantilla de certificado y la entidad de certificación que se van a usar para emitir certificados de usuario. Esta debe ser la plantilla Citrix_SmartcardLogon, o una copia modificada de ella, en una de las entidades de certificación donde esté publicada esta plantilla.

El servicio FAS respalda varias entidades de certificación para la conmutación por error y el equilibrio de carga, y esto es configurable mediante comandos de PowerShell. Del mismo modo, se pueden configurar opciones de generación de certificados más avanzadas mediante la línea de comandos y los archivos de configuración. Consulte las secciones PowerShell y Módulos de seguridad de hardware.

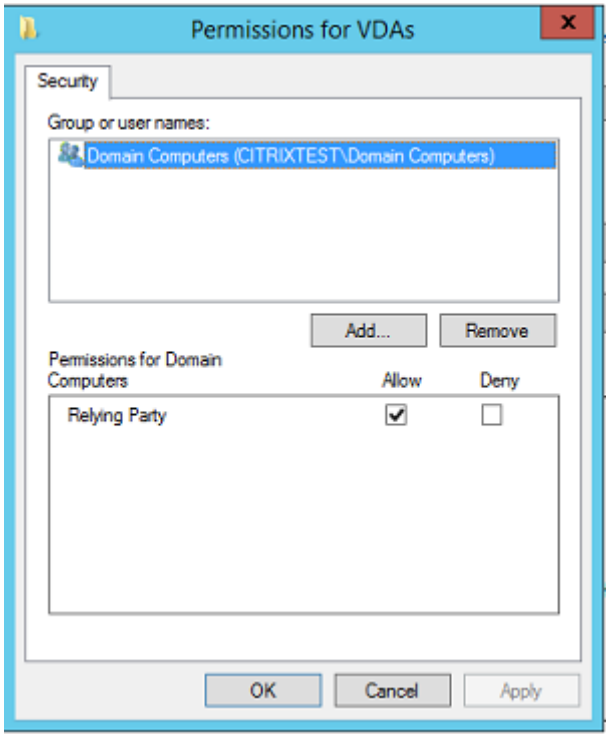
In-Session Certificates: La casilla **Available after logon** controla si un certificado puede usarse también como certificado de la sesión. Si la casilla no está marcada, el certificado se usará solo para el inicio de sesión o la reconexión y el usuario no tendrá acceso al certificado después de autenticarse.

List of StoreFront servers that can use this rule: La lista de máquinas de servidor StoreFront de confianza que están autorizadas para solicitar certificados para el inicio de sesión o la reconexión de usuarios. Tenga en cuenta que este parámetro es fundamental para la seguridad y es necesario configurarlo muy cuidadosamente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



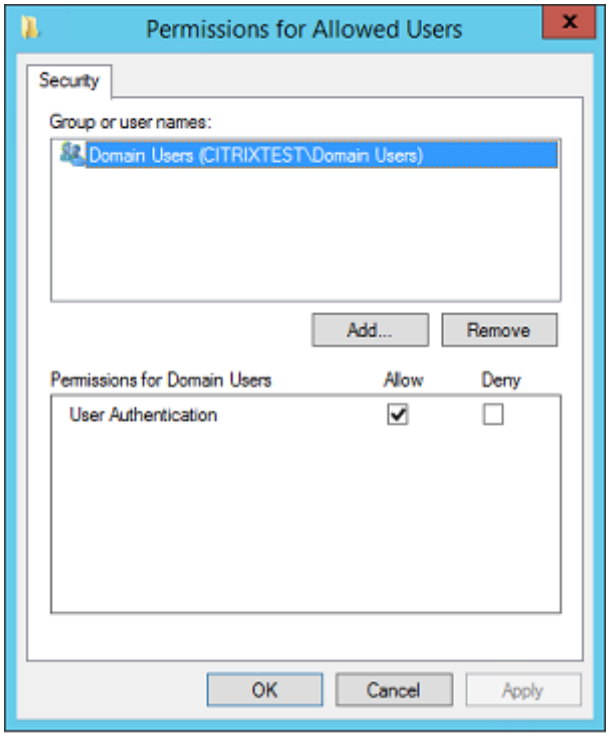
List of VDA desktops and servers that can be logged into by this rule: La lista de las máquinas VDA donde los usuarios pueden iniciar sesiones mediante el sistema del Servicio de autenticación federada.



List of users that StoreFront can log in using this rule: Lista de los usuarios para los que se pueden

© 1999-2019 Citrix Systems, Inc. All rights reserved.

emitir certificados a través del Servicio de autenticación federada.



Uso avanzado

Puede crear reglas adicionales para hacer referencia a otras plantillas de certificado y entidades de certificación, que pueden haberse configurado con propiedades y permisos diferentes. Estas reglas se pueden configurar para ser utilizadas por distintos servidores StoreFront, que a su vez deberán configurarse para solicitar la nueva regla por su nombre. De forma predeterminada, StoreFront solicita la regla predeterminada **default** al contactar con el Servicio de autenticación federada. Esto se puede cambiar mediante las opciones de configuración de la directiva de grupo.

Para crear una nueva plantilla de certificado, cree un duplicado de la plantilla Citrix_SmartcardLogon en la consola de la entidad de certificación de Microsoft, cámbiele el nombre (por ejemplo, Citrix_SmartcardLogon2) y modifíquela según sea necesario. Cree una nueva regla, haciendo clic en **Add** para que haga referencia a la nueva plantilla de certificado.

Consideraciones sobre la actualización

- Todos los parámetros de servidor del Servicio de autenticación federada se conservan cuando se realiza una actualización en contexto.
- Actualice el Servicio de autenticación federada mediante el instalador de producto completo de Virtual Apps and Desktops.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Antes de actualizar el Servicio de autenticación federada, actualice el Controller y los VDA (y otros componentes principales) a la versión requerida.
- La consola del Servicio de autenticación federada debe estar cerrada antes de actualizar el Servicio de autenticación federada.
- Al menos un servidor del Servicio de autenticación federada debe estar disponible en todo momento. Si un servidor StoreFront habilitado para el Servicio de autenticación federada no puede establecer contacto con ningún servidor, los usuarios no podrán iniciar sesión ni iniciar aplicaciones.

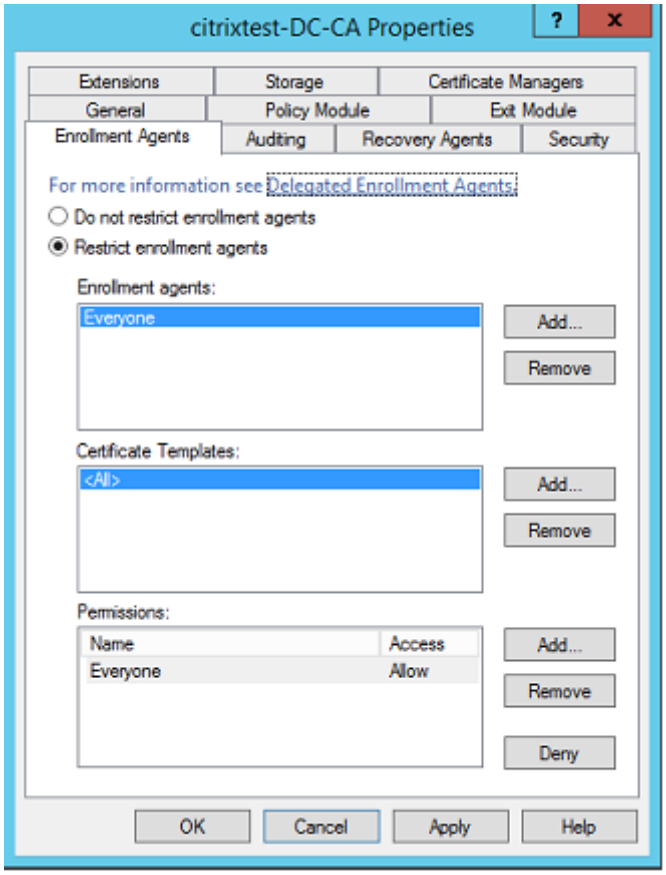
Consideraciones sobre seguridad

El Servicio de autenticación federada (FAS) tiene un certificado de autorización de registro que le permite emitir certificados de forma autónoma en nombre de los usuarios de dominio. Como consecuencia, es muy importante desarrollar e implementar una directiva de seguridad para proteger los servidores del servicio FAS y restringir sus permisos.

Agentes de inscripción delegada

La entidad de certificación de Microsoft permite controlar qué plantillas puede usar el servidor del servicio FAS, así como limitar para qué usuarios puede emitir certificados dicho servidor.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Citrix recomienda configurar estas opciones de modo que el Servicio de autenticación federada solo pueda emitir certificados para los usuarios apropiados. Por ejemplo, es una buena práctica impedir que el Servicio de autenticación federada emita certificados para los usuarios incluidos en un grupo de Administración o de Usuarios protegidos.

Configurar una lista de control de acceso

Como se describe en la sección Configurar roles de usuario, debe configurar una lista de servidores StoreFront con la confianza necesaria para la aserción de identidades de usuario de cara al Servicio de autenticación federada cuando se emiten certificados. Del mismo modo, puede restringir para qué usuarios se pueden emitir certificados y en qué máquinas VDA se pueden autenticar. Esto es adicional a las funciones de seguridad estándar de la entidad de certificación o de Active Directory.

Parámetros de firewall

Todas las comunicaciones con los servidores del servicio FAS usan conexiones de red Kerberos de Windows Communication Foundation (WCF) a través del puerto 80, con autenticación mutua.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Supervisar el registro de eventos

El Servicio de autenticación federada y el VDA escriben información en el registro de eventos de Windows. Esto se puede utilizar para ver información de supervisión y auditoría. En la sección Registros de eventos, se ofrece una lista de las entradas del Registro de eventos que pueden generarse.

Módulo de seguridad de hardware

Todas las claves privadas, incluidas las de los certificados de usuario emitidos por el Servicio de autenticación federada, se almacenan como claves privadas no exportables con la cuenta de Servicio de red. El Servicio de autenticación federada admite el uso de un módulo de seguridad de hardware de cifrado, si su directiva de seguridad así lo requiere.

La configuración criptográfica de bajo nivel está disponible en el archivo FederatedAuthenticationService.exe.config. Estos parámetros se aplican cuando las claves privadas se crean por primera vez. Por lo tanto, se pueden usar parámetros diferentes para las claves privadas de autoridad de registro (por ejemplo, 4096 bits, protegido por TPM) y de los certificados de usuario en tiempo de ejecución.

Parámetro	Descripción
ProviderLegacyCsp	Cuando tiene el valor True, el servicio FAS usará el Microsoft CryptoAPI (CAPI). De lo contrario, el servicio FAS usará Microsoft Cryptography Next Generation API (CNG).
ProviderName	Nombre del proveedor de CAPI o CNG que se va a usar.
ProviderType	Se refiere a Microsoft KeyContainerPermissionAccessEntry.ProviderType Property PROV_RSA_AES 24. Debe ser siempre 24 a menos que esté usando un HSM con CAPI y el proveedor de HSM especifique otra cosa.
KeyProtection	Controla la marca “Exportable” de las claves privadas. También permite el uso del almacenamiento de claves TPM (Trusted Platform Module), si lo admite el hardware.
KeyLength	Longitud de clave para las claves privadas de RSA. Los valores admitidos son 1024, 2048 y 4096 (predeterminado: 2048).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

SDK de PowerShell

Aunque la consola de administración del Servicio de autenticación federada es adecuada para implementaciones simples, la interfaz de PowerShell ofrece opciones más avanzadas. Cuando use opciones que no estén disponibles en la consola, Citrix recomienda utilizar solo PowerShell para la configuración.

El siguiente comando agrega los cmdlets de PowerShell:

```
1 Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
```

Use **Get-Help** <*nombre del cmdlet*> para ver la ayuda de uso de los cmdlet. La siguiente tabla muestra algunos comandos donde * representa un verbo estándar de PowerShell (tales como New, Get, Set, Remove).

Comandos	Información general
*-FasServer	Muestra y reconfigura los servidores del servicio FAS en el entorno actual.
*-FasAuthorizationCertificate	Administra el certificado de autoridad de registro.
*-FasCertificateDefinition	Controla los parámetros que usa el servicio FAS para generar certificados.
*-FasRule	Administra las reglas de usuario configuradas en el Servicio de autenticación federada.
*-FasUserCertificate	Muestra y administra certificados almacenados en caché por el Servicio de autenticación federada.

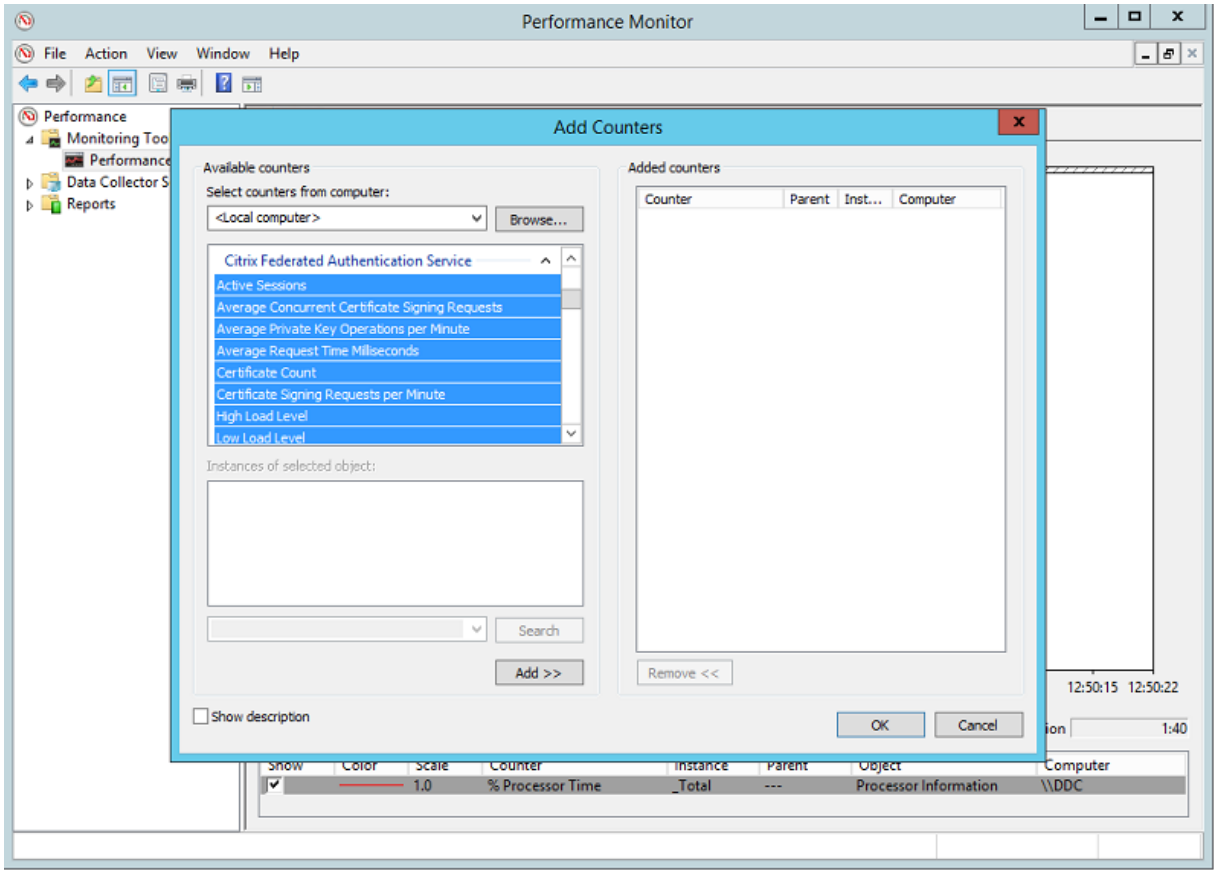
Se pueden usar cmdlets de PowerShell de forma remota especificando la dirección de un servidor del servicio FAS.

También puede descargar un archivo zip que contiene todos los archivos de ayuda de cmdlets de PowerShell para FAS; consulte el artículo PowerShell SDK.

Contadores de rendimiento

El Servicio de autenticación federada incluye un conjunto de contadores de rendimiento para el seguimiento de la carga.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



En la siguiente tabla se muestran los contadores disponibles. La mayoría de estos contadores muestran la media calculada cada cinco minutos.

Nombre	Descripción
Sesiones activas	Cantidad de conexiones con seguimiento del Servicio de autenticación federada.
Concurrent CSRs (Solicitudes de firma de certificado concurrentes)	Cantidad de solicitudes de certificado procesadas al mismo tiempo.
Private Key ops (Operaciones de clave privada)	Cantidad de operaciones de clave privada realizadas por minuto.
Request time (Tiempo de la solicitud)	Tiempo tomado para generar y firmar un certificado.
Certificate Count (Recuento de certificados)	Cantidad de certificados en caché en el Servicio de autenticación federada.
CSR per minute (CSR por minuto)	Cantidad de solicitudes de certificados (CSR) procesadas por minuto.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre	Descripción
Low/Medium/High (Baja, media o alta)	Estimaciones de la carga que el Servicio de autenticación federada puede aceptar en términos de “Solicitudes de certificado (CSR) por minuto”. Si se supera el umbral “Carga alta”, el lanzamiento de sesiones puede fallar.

Registros de eventos

En las siguientes tablas se enumeran las entradas de registro de eventos generadas por el Servicio de autenticación federada.

Eventos de administración

[Origen del evento: Citrix.Authentication.FederatedAuthenticationService]

Estos eventos se registran como respuesta a un cambio de configuración en el servidor del Servicio de autenticación federada.

Códigos de registro
[S001] ACCESS DENIED: User [{0}] is not a member of Administrators group
[S002] ACCESS DENIED: User [{0}] is not an Administrator of Role [{1}]
[S003] Administrator [{0}] setting Maintenance Mode to [{1}]
[S004] Administrator [{0}] enrolling with CA [{1}] templates [{2} and {3}]
[S005] Administrator [{0}] de-authorizing CA [{1}]
[S006] Administrator [{0}] creating new Certificate Definition [{1}]
[S007] Administrator [{0}] updating Certificate Definition [{1}]
[S008] Administrator [{0}] deleting Certificate Definition [{1}]
[S009] Administrator [{0}] creating new Role [{1}]
[S010] Administrator [{0}] updating Role [{1}]
[S011] Administrator [{0}] deleting Role [{1}]
[S012] Administrator [{0}] creating certificate [upn: {0} sid: {1} role: {2}][Certificate Definition: {3}]
[S013] Administrator [{0}] deleting certificates [upn: {0} role: {1} Certificate Definition: {2}]

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Códigos de registro
[S401] Performing configuration upgrade – [From version {0}][to version {1}]
[S402] ERROR: The Citrix Federated Authentication Service must be run as Network Service [currently running as: {0}]
[S404] Forcefully erasing the Citrix Federated Authentication Service database
[S405] An error occured while migrating data from the registry to the database: [\{0\}]
[S406] Migration of data from registry to database is complete (note: user certificates are not migrated)
[S407] Registry-based data was not migrated to a database since a database already existed

Crear aserciones de identidad [Servicio de autenticación federada]

Estos sucesos se registran durante el tiempo de ejecución en el servidor del Servicio de autenticación federada cuando un servidor de confianza realiza una aserción de un inicio de sesión de usuario.

Códigos de registro
[S101] Server [{0}] is not authorized to assert identities in role [{1}]
[S102] Server [{0}] failed to assert UPN [{1}] (Exception: {2}{3})
[S103] Server [{0}] requested UPN [{1}] SID {2}, but lookup returned SID {3}
[S104] Server [{0}] failed to assert UPN [{1}] (UPN not allowed by role [{2}])
[S105] Server [{0}] issued identity assertion [upn: {0}, role {1}, Security Context: [{2}]
[S120] Issuing certificate to [upn: {0} role: {1} Security Context: [{2}]]
[S121] Issuing certificate to [upn: {0} role: {1}] on behalf of account {2}
[S122] Warning: Server is overloaded [upn: {0} role: {1}][Requests per minute {2}].

Actúa como usuario de confianza [Servicio de autenticación federada]

Estos sucesos se registran durante el tiempo de ejecución en el servidor del Servicio de autenticación federada cuando un VDA inicia la sesión de un usuario.

Códigos de registro
[S201] Relying party [{0}] does not have access to a password.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Códigos de registro
[S202] Relying party [{0}] does not have access to a certificate.
[S203] Relying party [{0}] does not have access to the Logon CSP
[S204] Relying party [{0}] accessing the Logon CSP [Operation: {1}]
[S205] Calling account [{0}] is not a relying party in role [{1}]
[S206] Calling account [{0}] is not a relying party
[S207] Relying party [{0}] asserting identity [upn: {1}] in role: [{2}]
[S208] Private Key operation failed [Operation: {0}][upn: {1} role: {2} certificateDefinition {3}][Error {4} {5}].

Servidor de certificados de sesión [Servicio de autenticación federada]

Estos sucesos se registran en el servidor del Servicio de autenticación federada cuando un usuario utiliza un certificado de sesión.

Códigos de registro
[S301] Access Denied: User [{0}] does not have access to a Virtual Smart Card
[S302] User [{0}] requested unknown Virtual Smart Card [thumbprint: {1}]
[S303] User [{0}] does not match Virtual Smart Card [upn: {1}]
[S304] User [{1}] running program [{2}] on computer [{3}] using Virtual Smart Card [upn: {4} role: {5}] for private key operation: [{6}]
[S305] Private Key operation failed [Operation: {0}][upn: {1} role: {2} containerName {3}][Error {4} {5}].

Iniciar sesión [VDA]

[Origen del evento: Citrix.Authentication.IdentityAssertion]

Estos sucesos se registran en el VDA durante la fase de inicio de sesión.

Códigos de registro
[S101] Identity Assertion Logon failed. Unrecognised Federated Authentication Service [id: {0}]
[S102] Identity Assertion Logon failed. Could not lookup SID for {0} [Exception: {1}{2}]

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Códigos de registro
[S103] Identity Assertion Logon failed. User {0} has SID {1}, expected SID {2}
[S104] Identity Assertion Logon failed. Failed to connect to Federated Authentication Service: {0} [Error: {1} {2}]
[S105] Identity Assertion Logon. Logging in [Username: {0}][Domain: {1}]
[S106] Identity Assertion Logon. Logging in [Certificate: {0}]
[S107] Identity Assertion Logon failed. [Exception: {1}{2}]
[S108] Identity Assertion Subsystem. ACCESS_DENIED [Caller: {0}]

Certificados de sesión [VDA]

Estos sucesos se registran en el VDA cuando un usuario intenta usar un certificado de sesión.

Códigos de registro
[S201] Virtual Smart Card Authorized [User: {0}][PID: {1} Name:{2}][Certificate {3}]
[S202] Virtual Smart Card Subsystem. No smart cards available in session {0}
[S203] Virtual Smart Card Subsystem. Access Denied [caller: {0}, session {1}, expected: {2}]
[S204] Virtual Smart Card Subsystem. Smart card support disabled.

Solicitud de certificado y códigos de generación [Servicio de autenticación federada]

[Origen del evento: Citrix.Authentication.FederatedAuthenticationService]

Estos eventos de bajo nivel se registran cuando el Servicio de autenticación federada realiza operaciones criptográficas de bajo nivel.

Códigos de registro
[S11001]TrustArea::TrustArea: Installed certificate chain
[S11002]TrustArea::Join: Callback has authorized an untrusted certificate
[S11003]TrustArea::Join: Joining to a trusted server
[S11004]TrustArea::Maintain: Renewed certificate
[S11005]TrustArea::Maintain: Retrieved new certificate chain

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Códigos de registro
[S11006]TrustArea::Export: Exporting private key
[S11007]TrustArea::Import: Importing Trust Area
[S11008]TrustArea::Leave: Leaving Trust Area
[S11009]TrustArea::SecurityDescriptor: Setting Security Descriptor
[S11010]CertificateVerification: Installing new trusted certificate
[S11011]CertificateVerification: Uninstalling expired trusted certificate
[S11012]TrustFabricHttpClient: Attempting single sign-on to {0}
[S11013]TrustFabricHttpClient: Explicit credentials entered for {0}
[S11014]Pkcs10Request::Create: Created PKCS10 request
[S11015]Pkcs10Request::Renew: Created PKCS10 request
[S11016]PrivateKey::Create
[S11017]PrivateKey::Delete
[S11018]TrustArea::TrustArea: Waiting for Approval
[S11019]TrustArea::Join: Delayed Join
[S11020]TrustArea::Join: Delayed Join
[S11021]TrustArea::Maintain: Installed certificate chain

Códigos de registro
[S0101]TrustAreaServer::Create root certificate
[S0102]TrustAreaServer::Subordinate: Join succeeded
[S0103]TrustAreaServer::PeerJoin: Join succeeded
[S0104]MicrosoftCertificateAuthority::GetCredentials: Authorized to use {0}
[S0104]MicrosoftCertificateAuthority::SubmitCertificateRequest Error {0}
[S0105]MicrosoftCertificateAuthority::SubmitCertificateRequest Issued cert {0}
[S0106]MicrosoftCertificateAuthority::PublishCRL: Published CRL
[S0107]MicrosoftCertificateAuthority::ReissueCertificate Error {0}
[S0108]MicrosoftCertificateAuthority::ReissueCertificate Issued Cert {0}
[S0109]MicrosoftCertificateAuthority::CompleteCertificateRequest - Still waiting for approval

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Códigos de registro
[S0110]MicrosoftCertificateAuthority::CompleteCertificateRequest - Pending certificate refused
[S0111]MicrosoftCertificateAuthority::CompleteCertificateRequest Issued certificate
[S0112]MicrosoftCertificateAuthority::SubmitCertificateRequest - Waiting for approval
[S0120]NativeCertificateAuthority::SubmitCertificateRequest Issued cert {0}
[S0121]NativeCertificateAuthority::SubmitCertificateRequest Error
[S0122]NativeCertificateAuthority::RootCARollover New root certificate
[S0123]NativeCertificateAuthority::ReissueCertificate New certificate
[S0124]NativeCertificateAuthority::RevokeCertificate
[S0125]NativeCertificateAuthority::PublishCRL

Información relacionada

- Las implementaciones más comunes del servicio FAS se resumen en Información general de las arquitecturas del Servicio de autenticación federada.
- En el artículo Administrar y configurar el Servicio de autenticación federada, se indican otros artículos de procedimientos.

Introducción a las arquitecturas del Servicio de autenticación federada

October 3, 2018

Introducción

El servicio de autenticación federada FAS (Federated Authentication Service) es un componente de Citrix que se integra con su entidad de certificación (CA) de Active Directory, lo que permite a los usuarios autenticarse de manera imperceptible dentro de un entorno Citrix. Este documento describe diversas arquitecturas de autenticación que pueden ser apropiadas para su implementación.

Cuando está habilitado, el servicio FAS delega las decisiones de autenticación de usuarios en servidores StoreFront de confianza. StoreFront tiene un amplio conjunto de opciones de autenticación integrado con tecnologías Web modernas, y es fácilmente ampliable con el SDK de StoreFront o complementos de IIS de terceros. El objetivo básico del diseño es conseguir que cualquier tecnología de autenticación que pueda autenticar a un usuario en un sitio Web se pueda usar para iniciar sesión en una implementación de Citrix Virtual Apps o Citrix Virtual Desktops.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Este documento cubre algunos ejemplos de implementación de nivel superior, con una complejidad cada vez mayor.

- Implementación interna
- Implementación de NetScaler Gateway
- SAML de ADFS
- Asignación de cuentas B2B
- Unión a Azure AD de Windows 10

Se proporcionan enlaces a artículos relativos al servicio FAS. Para todas las arquitecturas, el artículo Servicio de autenticación federada es la referencia principal para la instalación y la configuración de este servicio.

Funcionamiento

El servicio FAS está autorizado para emitir certificados de tarjeta inteligente automáticamente de parte de los usuarios de Active Directory que son autenticados por StoreFront. Esto usa interfaces API similares a las herramientas que permiten a los administradores aprovisionar tarjetas inteligentes físicas.

Cuando un broker gestiona el acceso de un usuario a un Virtual Delivery Agent (VDA) de Citrix Virtual Apps o Citrix Virtual Desktops, el certificado se conecta a la máquina, y el dominio de Windows detecta el inicio de sesión como una acción de autenticación con tarjeta inteligente estándar.

Implementación interna

El servicio FAS permite que los usuarios se autentiquen de forma segura en StoreFront usando una gran variedad de opciones de autenticación (incluido el inicio de sesión Single Sign-on de Kerberos) y se conecten con una sesión Citrix HDX con autenticación completa.

Esto permite la autenticación de Windows sin diálogos para introducir las credenciales de usuario o el PIN de tarjeta inteligente, y sin tener que usar la función del tipo “administración de contraseñas guardadas”, tales como Single Sign-On Service. Puede utilizarse para reemplazar las funciones de inicio de sesión que ofrezca la Delegación limitada de Kerberos, disponible en versiones anteriores de Citrix Virtual Apps.

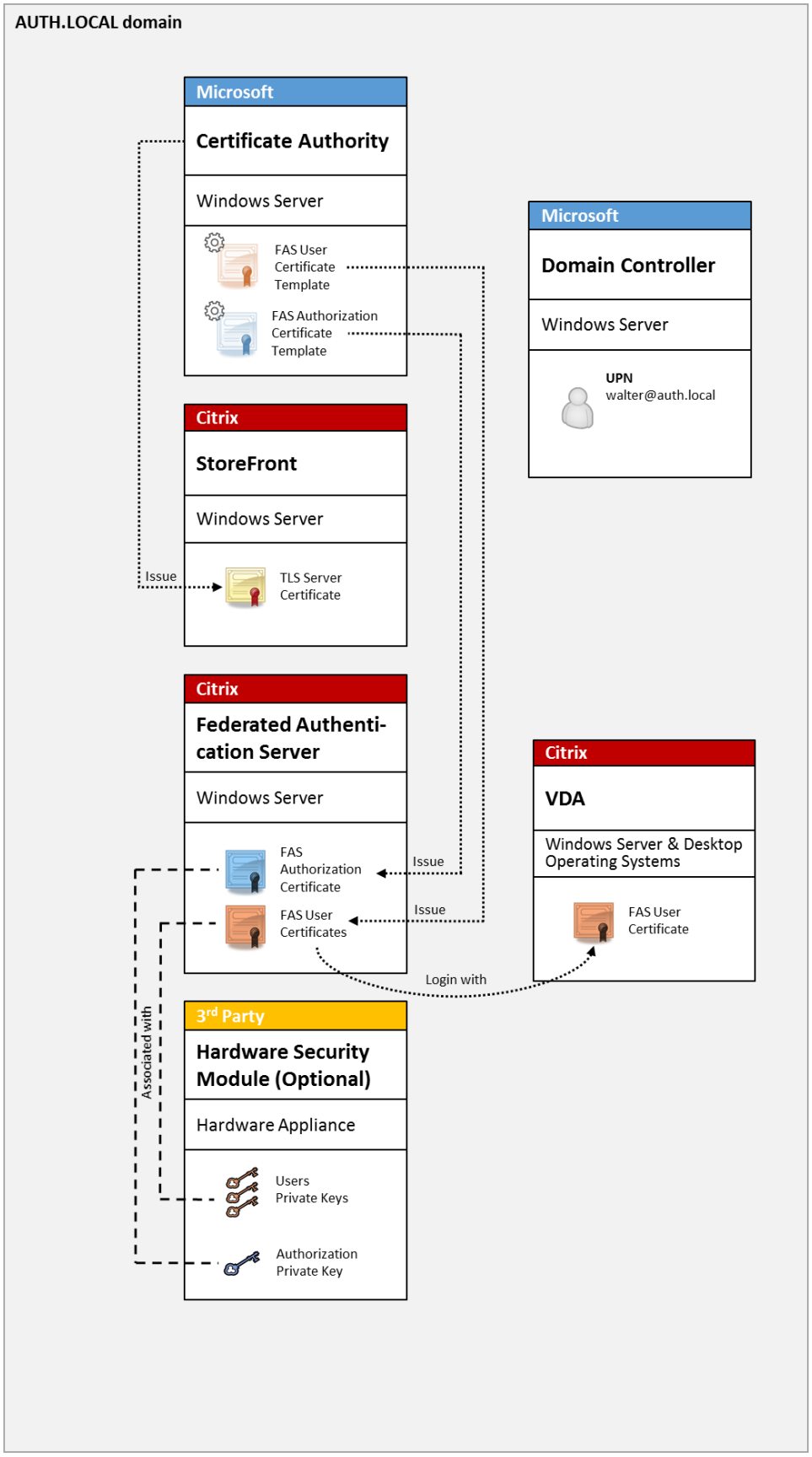
Todos los usuarios tienen acceso a certificados de infraestructura de clave pública (PKI) dentro de su sesión, independientemente de si inician sesión en los dispositivos de punto final con una tarjeta inteligente o no. Esto permite una migración sin problemas a modelos de autenticación de dos factores, incluso desde dispositivos como smartphones y tabletas que no tienen un lector de tarjeta inteligente.

Esta implementación agrega un nuevo servidor en el que se ejecuta el servicio FAS, que está autorizado para emitir certificados de clase de tarjeta inteligente en nombre de los usuarios. Estos certifi-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

cados se utilizan después para conectar con sesiones de usuario en un entorno de Citrix HDX como si se estuviera utilizando un inicio de sesión con tarjeta inteligente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

El entorno de Citrix Virtual Apps o Citrix Virtual Desktops debe estar configurado de manera similar al inicio de sesión con tarjeta inteligente, que se describe en CTX206156.

En una implementación existente, esto normalmente solo implica asegurarse de que haya una entidad de certificación (CA) de Microsoft disponible y de que los controladores de dominio tengan asignados certificados de controlador de dominio. (Consulte la sección "Issuing Domain Controller Certificates" en el artículo CTX206156.)

Información relacionada:

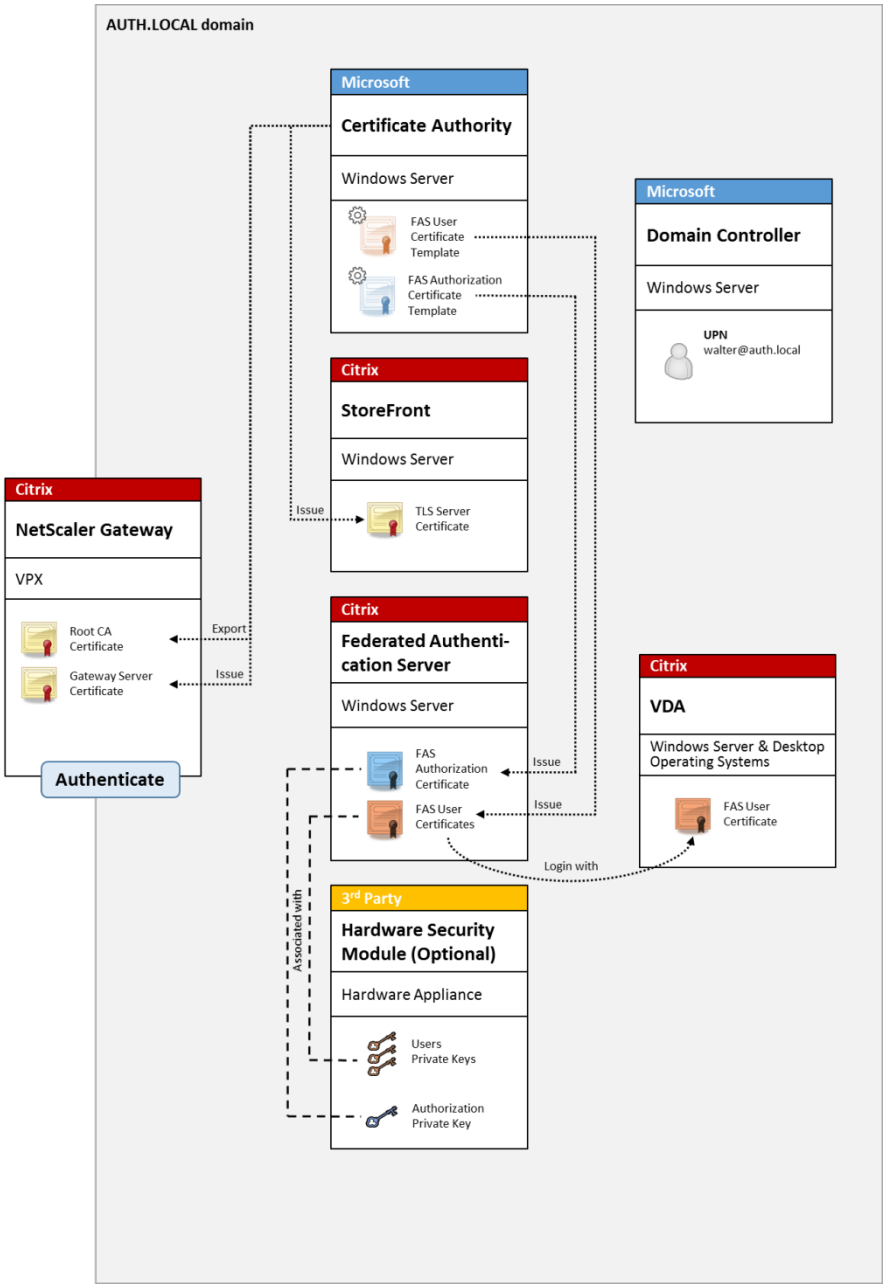
- Las claves se pueden almacenar en un módulo de seguridad de hardware (HSM) o en un módulo de plataforma de confianza (TPM) integrado. Para obtener más información, consulte el artículo Protección de claves privadas para el Servicio de autenticación federada.
- El artículo de Servicio de autenticación federada describe cómo instalar y configurar el FAS.

Implementación de NetScaler Gateway

La implementación de NetScaler es similar a la implementación interna, pero agrega Citrix NetScaler Gateway emparejado con StoreFront, moviendo el punto de autenticación principal al propio NetScaler. Citrix NetScaler incluye opciones muy sofisticadas de autenticación y autorización que se pueden usar para el acceso remoto seguro a los sitios Web de una empresa.

Esta implementación se puede utilizar para evitar la aparición de varias solicitudes de PIN que ocurren al autenticarse primero en NetScaler y, a continuación, iniciar sesión en una sesión de usuario. También permite el uso de las tecnologías de autenticación avanzada de NetScaler, sin necesidad de pedir adicionalmente contraseñas de Active Directory o tarjetas inteligentes.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



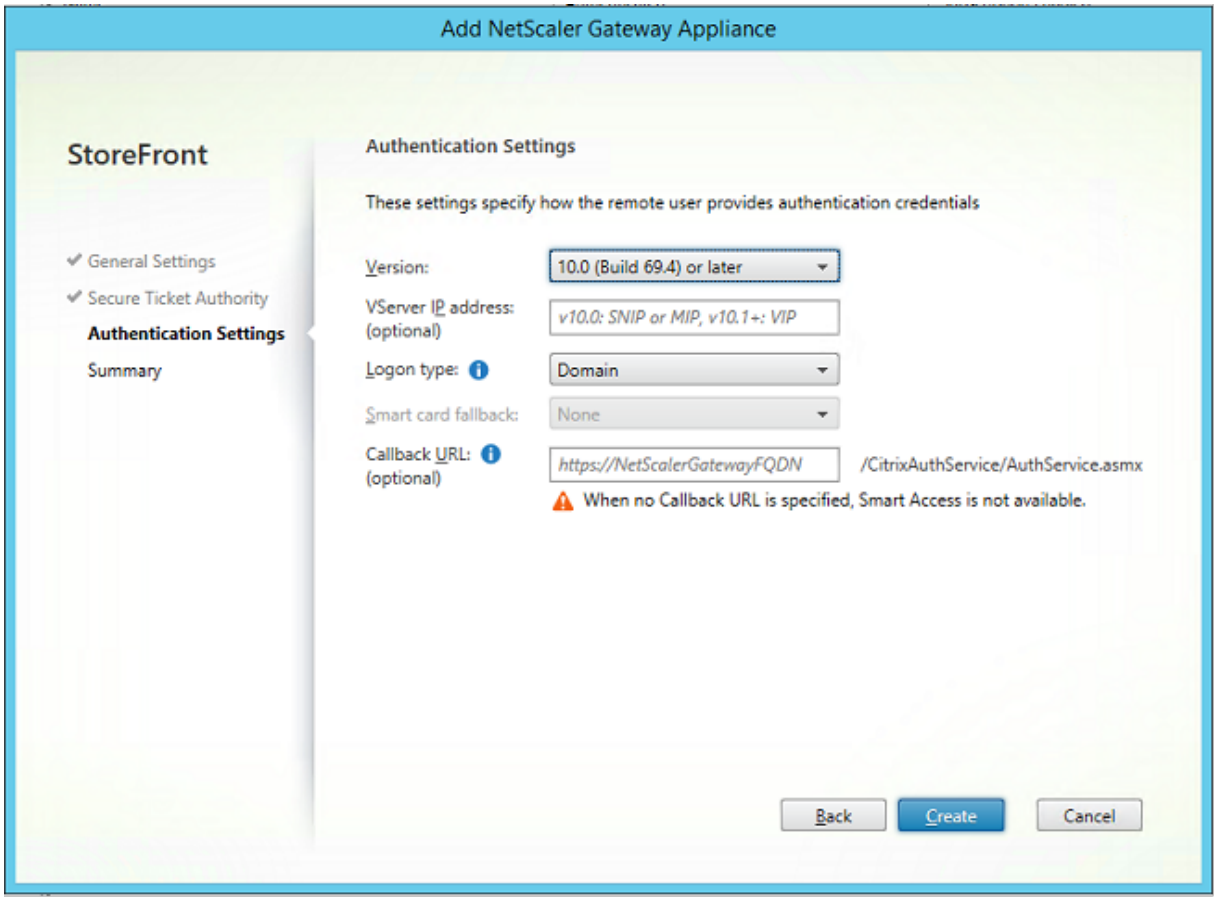
El entorno de Citrix Virtual Apps o Citrix Virtual Desktops debe estar configurado de manera similar al inicio de sesión con tarjeta inteligente, que se describe en CTX206156.

En el caso de una implementación existente, esto normalmente solo implica asegurarse de que haya una entidad de certificación (CA) de Microsoft disponible y de que los controladores de dominio tengan asignados certificados de controlador de dominio. (Consulte la sección “Issuing Domain Controller Certificates” en el artículo CTX206156.)

Al configurar NetScaler como el sistema de autenticación principal, asegúrese de que todas las conexiones entre NetScaler y StoreFront están protegidas con TLS. En concreto, asegúrese de que la dirección URL de respuesta está configurada correctamente para que apunte al servidor NetScaler, ya que

© 1999-2019 Citrix Systems, Inc. All rights reserved.

esto puede usarse para autenticar el servidor NetScaler en esta implementación.



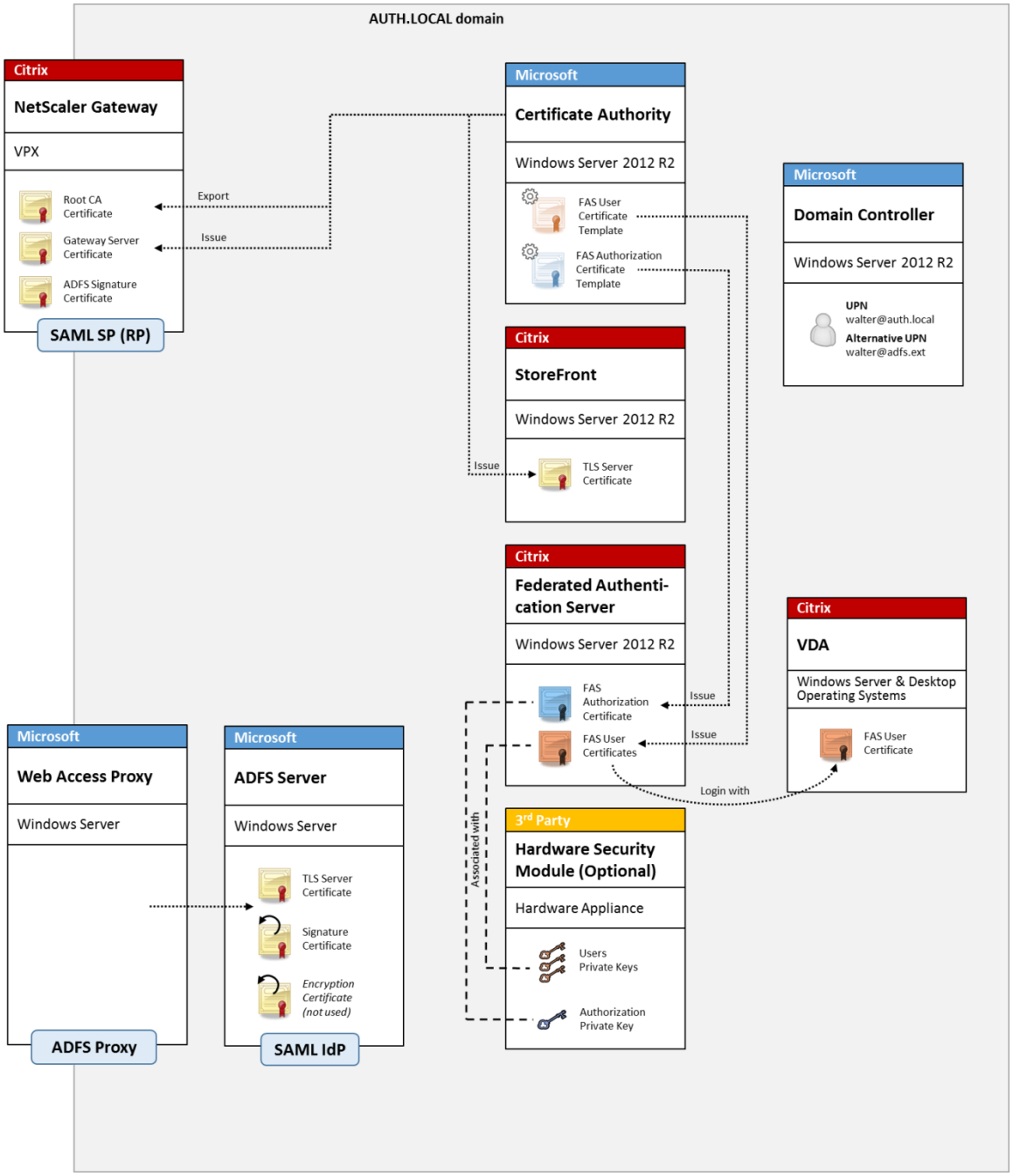
Información relacionada:

- Para configurar NetScaler Gateway (ahora Citrix Gateway), consulte "Cómo configurar NetScaler Gateway 10.5 para usarlo con StoreFront 3.6 y Citrix Virtual Desktops 7.6".
- El artículo de Servicio de autenticación federada describe cómo instalar y configurar el FAS.

Implementación de SAML de ADFS

Una tecnología de autenticación clave de NetScaler permite la integración con Microsoft ADFS, que puede funcionar como un proveedor de identidades (IdP) SAML. Una aserción SAML es un bloque XML firmado criptográficamente, emitido por un IdP de confianza, que autoriza a un usuario a iniciar sesión en un sistema informático. Eso significa que el servidor FAS ahora permite delegar la autenticación de un usuario al servidor ADFS de Microsoft (o a otro IdP habilitado para SAML).

© 1999-2019 Citrix Systems, Inc. All rights reserved.



ADFS se usa normalmente para autenticar a los usuarios con seguridad de forma remota en los recursos de la empresa a través de Internet, por ejemplo, se usa para la integración de Office 365.

Información relacionada:

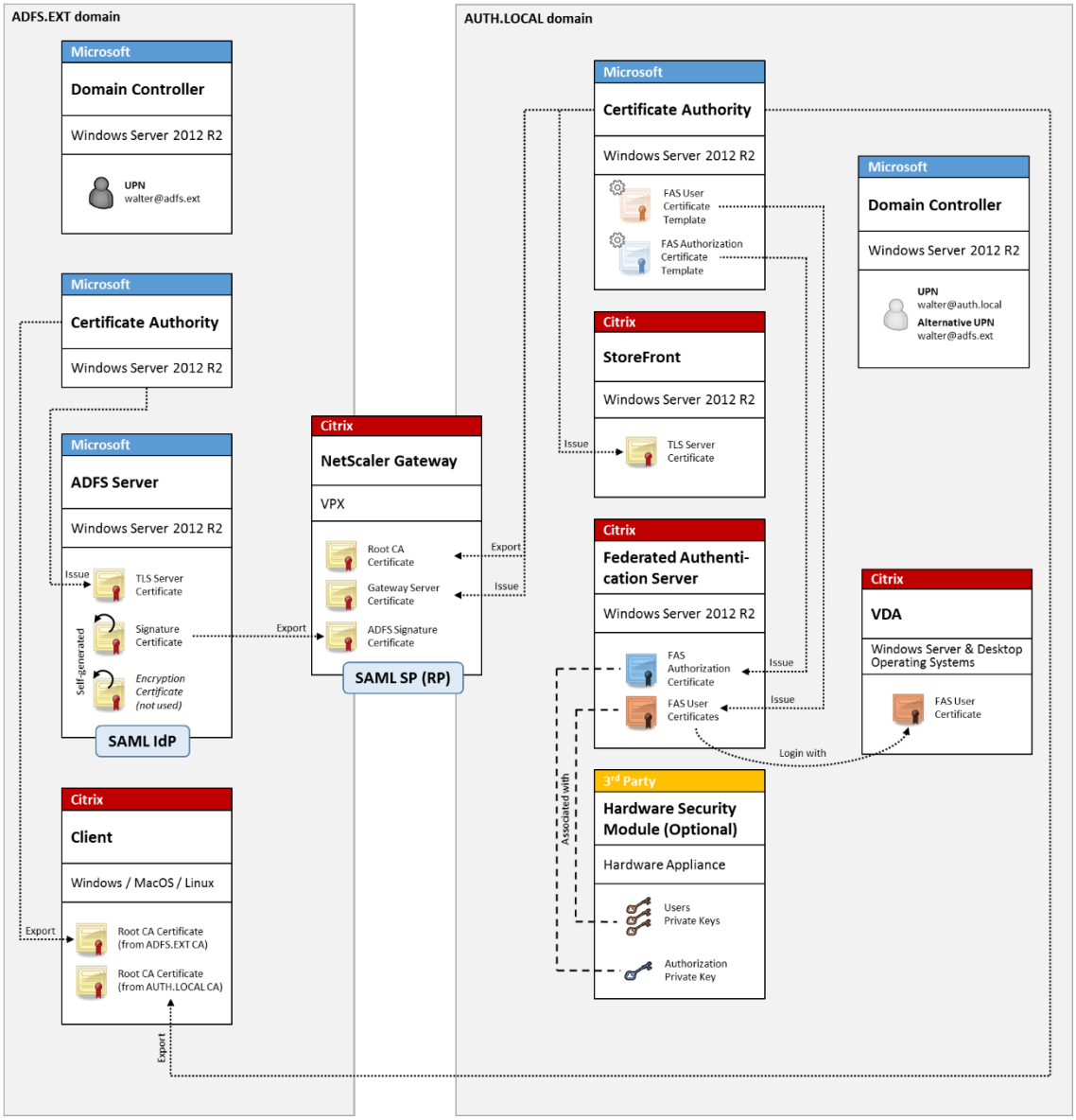
- El artículo Implementar ADFS y el Servicio de autenticación federada contiene información al respecto.
- En el artículo Servicio de autenticación federada se describe cómo instalar y configurar FAS.
- La sección Implementación de NetScaler Gateway en este artículo contiene información acerca

© 1999-2019 Citrix Systems, Inc. All rights reserved.

de la configuración.

Asignación de cuentas B2B

Si dos empresas quieren compartir los sistemas informáticos entre ellas, una opción común es configurar un servidor ADFS (Servicio de federación de Active Directory) con una relación de confianza. Eso permite que los usuarios de una empresa se autentiquen en el entorno de Active Directory (AD) de la otra, de manera imperceptible. Al iniciar sesión, cada usuario utiliza las credenciales de su propia empresa; ADFS las asigna automáticamente a una “cuenta sombra” en el entorno de AD de la otra empresa.



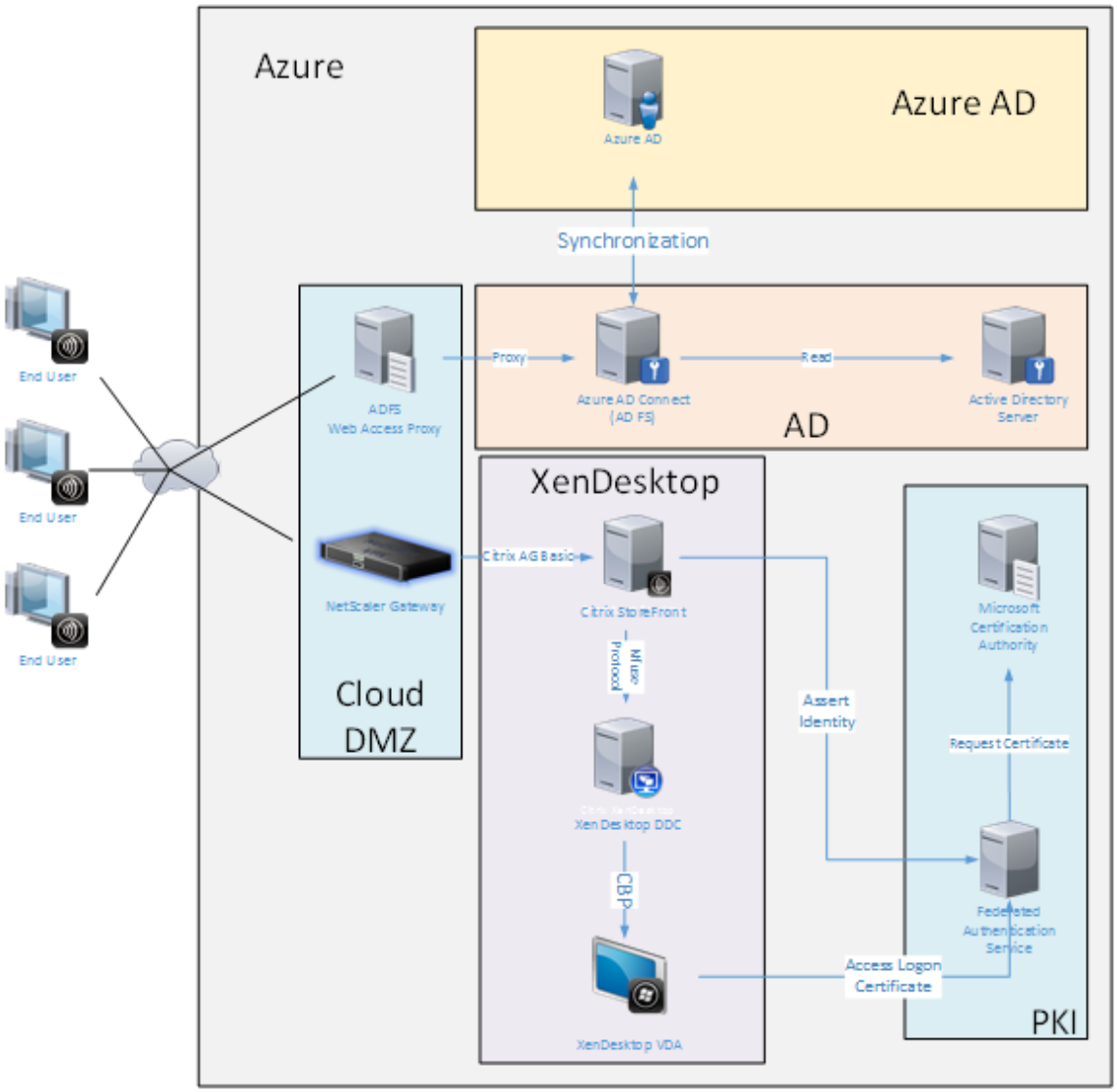
Información relacionada:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- En el artículo Servicio de autenticación federada se describe cómo instalar y configurar FAS.

Unión a Azure AD de Windows 10

Windows 10 introdujo el concepto de "Unión a Azure AD", que es conceptualmente similar a la unión a un dominio Windows tradicional, solo que destinado a casos a través de Internet. Este sistema funciona bien con equipos portátiles y tabletas. Al igual que al unirse a un dominio de Windows tradicional, Azure AD tiene funciones para permitir modelos de inicio de sesión Single Sign-On en recursos y sitios Web de la empresa. Estos pueden funcionar con Internet, por lo que funcionarán desde cualquier ubicación que esté conectada a Internet, no solo la red LAN de la oficina.



Esta implementación es un ejemplo donde no existe el concepto de "usuarios finales en la oficina". Los equipos portátiles se inscriben y se autentican totalmente en Internet con las funciones modernas de

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Azure AD.

Tenga en cuenta que la infraestructura en esta implementación se puede ejecutar en cualquier donde haya una dirección IP: en las propias oficinas, en un proveedor alojado, Azure o en otro proveedor de nube. El sincronizador de Azure AD Connect se conectará automáticamente a Azure AD. El gráfico de ejemplo utiliza máquinas virtuales de Azure para simplificar la tarea.

Información relacionada:

- En el artículo Servicio de autenticación federada se describe cómo instalar y configurar FAS.
- El artículo Integrar Azure AD y el Servicio de autenticación federada contiene información al respecto.

Implementar ADFS y el Servicio de autenticación federada

January 29, 2019

Introducción

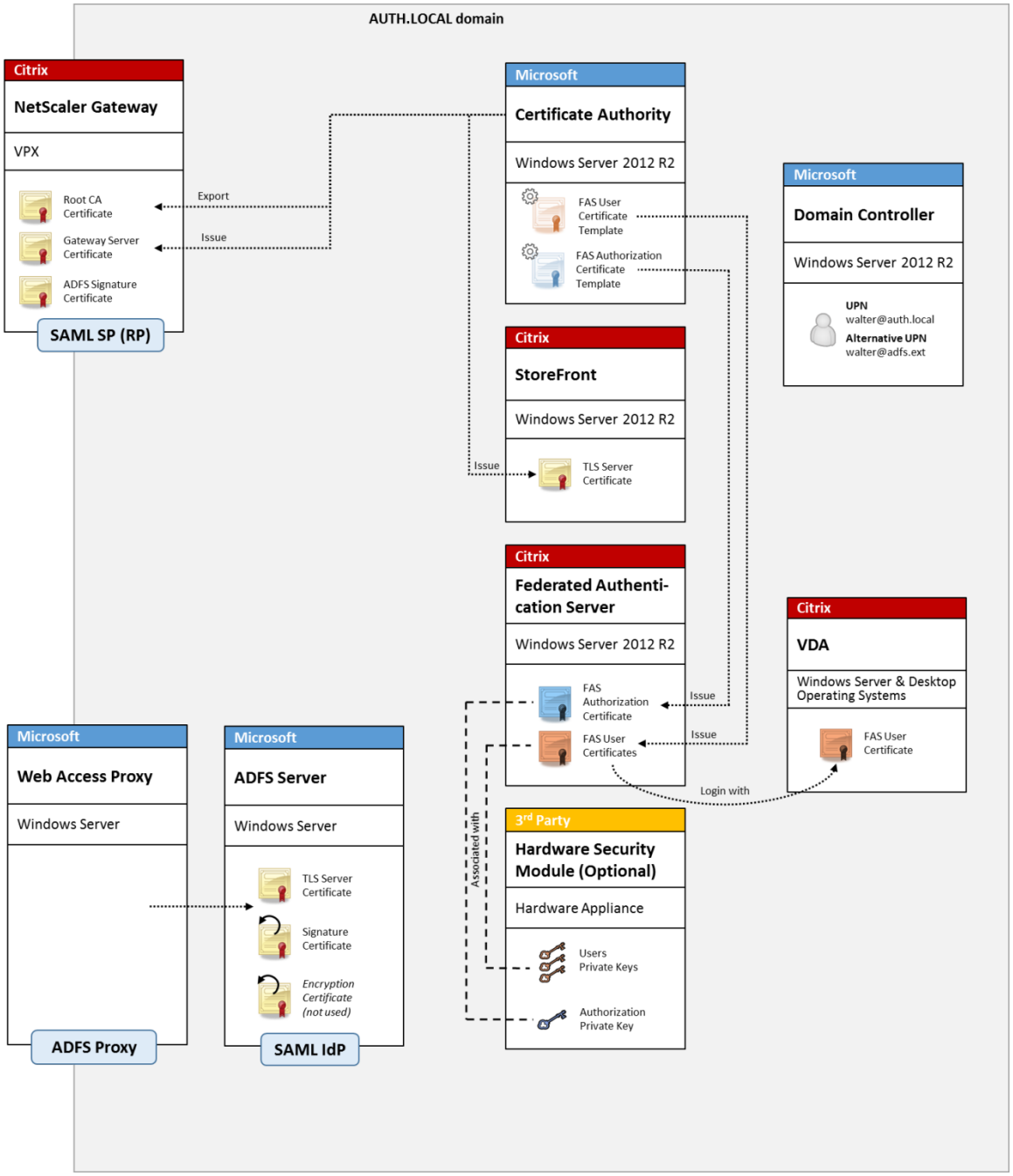
Este documento describe cómo integrar un entorno de Citrix con Microsoft ADFS.

Muchas organizaciones usan ADFS para administrar el acceso seguro de los usuarios a los sitios Web que requieren un único punto de autenticación. Por ejemplo, una empresa puede tener descargas y contenido adicionales disponibles para los empleados; estas ubicaciones deben estar protegidas con credenciales de inicio de sesión estándar de Windows.

El Servicio de autenticación federada (FAS) también permite integrar Citrix NetScaler y Citrix StoreFront en el sistema de inicio de sesión de ADFS, lo que disminuye el riesgo de confusión para el personal de la empresa.

Esta implementación integra NetScaler como un usuario de confianza en Microsoft ADFS.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Descripción general de SAML

Security Assertion Markup Language (SAML) es un sistema sencillo de inicio de sesión con explorador Web para “redirigir a la página de inicio de sesión”. La configuración incluye los siguientes elementos:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Dirección URL de redirección [URL del servicio Single Sign-On]

Cuando NetScaler detecta que un usuario tiene que autenticarse, indica al explorador Web del usuario que haga un envío HTTP POST a la página Web de inicio de sesión de SAML en el servidor ADFS. Esta suele ser una dirección `https://` en el formato: `https://adfs.mycompany.com/adfs/ls`.

Este POST a la página Web incluye información adicional, incluida la dirección de devolución adonde ADFS llevará al usuario cuando se complete el inicio de sesión.

Identificador [Nombre del emisor/ID de entidad o EntityID]

El ID de entidad (EntityID) es un identificador único que NetScaler incluye en los datos de POST enviados a ADFS. Eso informa al servicio ADFS acerca del servicio en el que intenta iniciar sesión el usuario, para aplicar distintas directivas de autenticación según corresponda. Si se emite, el XML de autenticación de SAML solo servirá para iniciar sesión en el servicio identificado por EntityID.

Normalmente, el EntityID es la dirección URL de la página de inicio de sesión del servidor NetScaler, pero puede ser cualquier cosa, siempre que NetScaler y ADFS lo acuerden: `https://ns.mycompany.com/application/logonpage`.

Dirección de devolución [URL de respuesta]

Si la autenticación se realiza correctamente, ADFS indica al explorador Web del usuario que envíe con POST un XML de autenticación de SAML de vuelta a una de las URL de respuesta que están configuradas para EntityID. Esta suele ser una dirección `https://` en el servidor NetScaler original con el formato: `https://ns.mycompany.com/cgi/samlauth`.

Si hay más de una dirección URL de respuesta configurada, NetScaler puede elegir uno en su POST original para ADFS.

Certificado de firma [Certificado IDP]

ADFS firma criptográficamente los objetos blob (Binary Large Object) de XML de autenticación de SAML usando su clave privada. Para validar la firma, NetScaler debe estar configurado para comprobar las firmas usando una clave pública que se incluye en un archivo de certificado. El archivo de certificado es normalmente un archivo de texto obtenido del servidor ADFS.

URL de Single Sign-Out [URL de cierre de sesión único]

ADFS y NetScaler respaldan un sistema de “cierre de sesión central”. Se trata de una dirección URL que NetScaler sondea ocasionalmente para comprobar que el blob XML de autenticación SAML aún

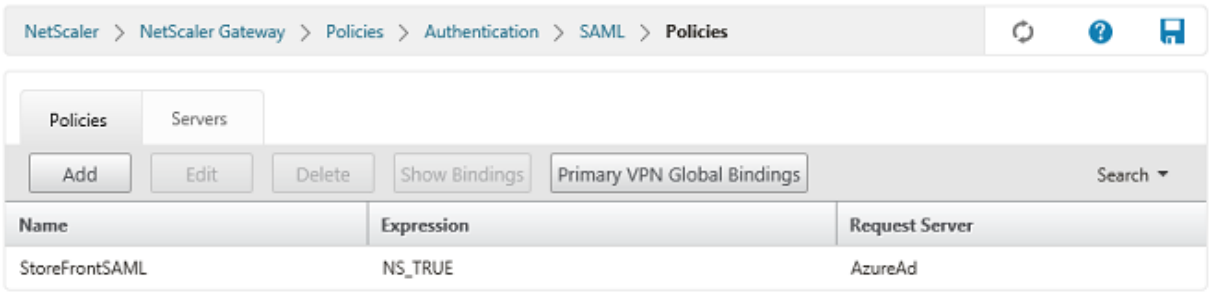
© 1999-2019 Citrix Systems, Inc. All rights reserved.

representa una sesión conectada.

Esta es una característica optativa, no es necesario que esté configurada. Esta suele ser una dirección `https://` en el formato: `https://adfs.mycompany.com/adfs/logout`. (Tenga en cuenta que puede ser la misma que la dirección URL de inicio de sesión único.)

Configuración

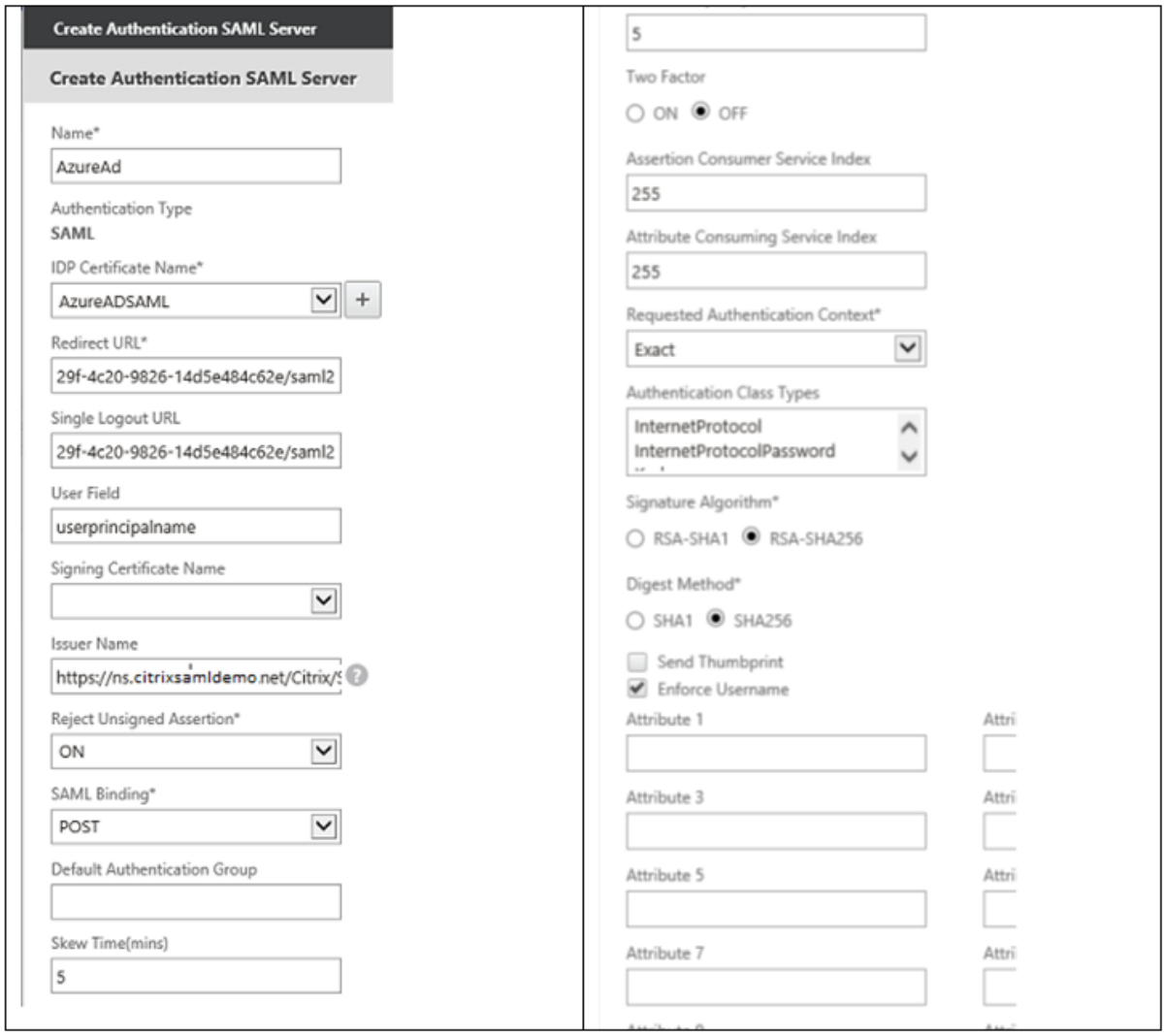
En la sección Implementar NetScaler Gateway del artículo Arquitecturas de Servicios de autenticación federada, se describe cómo configurar Citrix Gateway para gestionar opciones de autenticación LDAP estándar, con el Asistente de instalación de NetScaler de XenApp y XenDesktop. Una vez completado correctamente, se puede crear una nueva directiva de autenticación en NetScaler que permita la autenticación SAML. Después, esto puede reemplazar la directiva LDAP predeterminada utilizada en el asistente de instalación de NetScaler.



Rellenar la directiva de SAML

Configure el nuevo servidor de proveedor de identidades SAML usando la información tomada anteriormente de la consola de administración de ADFS. Cuando se aplica esta directiva, NetScaler redirige al usuario a ADFS para el inicio de sesión y a su vez acepta el token de autenticación de SAML firmado por ADFS.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Información relacionada

- El artículo Servicio de autenticación federada (FAS - Federated Authentication Service) es la referencia principal para la instalación y la configuración de este servicio.
- Las implementaciones más comunes del servicio FAS se resumen en el artículo Información general de las arquitecturas del Servicio de autenticación federada.
- En el artículo Administrar y configurar el Servicio de autenticación federada, se indican otros artículos de procedimientos.

Integrar Azure AD y el Servicio de autenticación federada

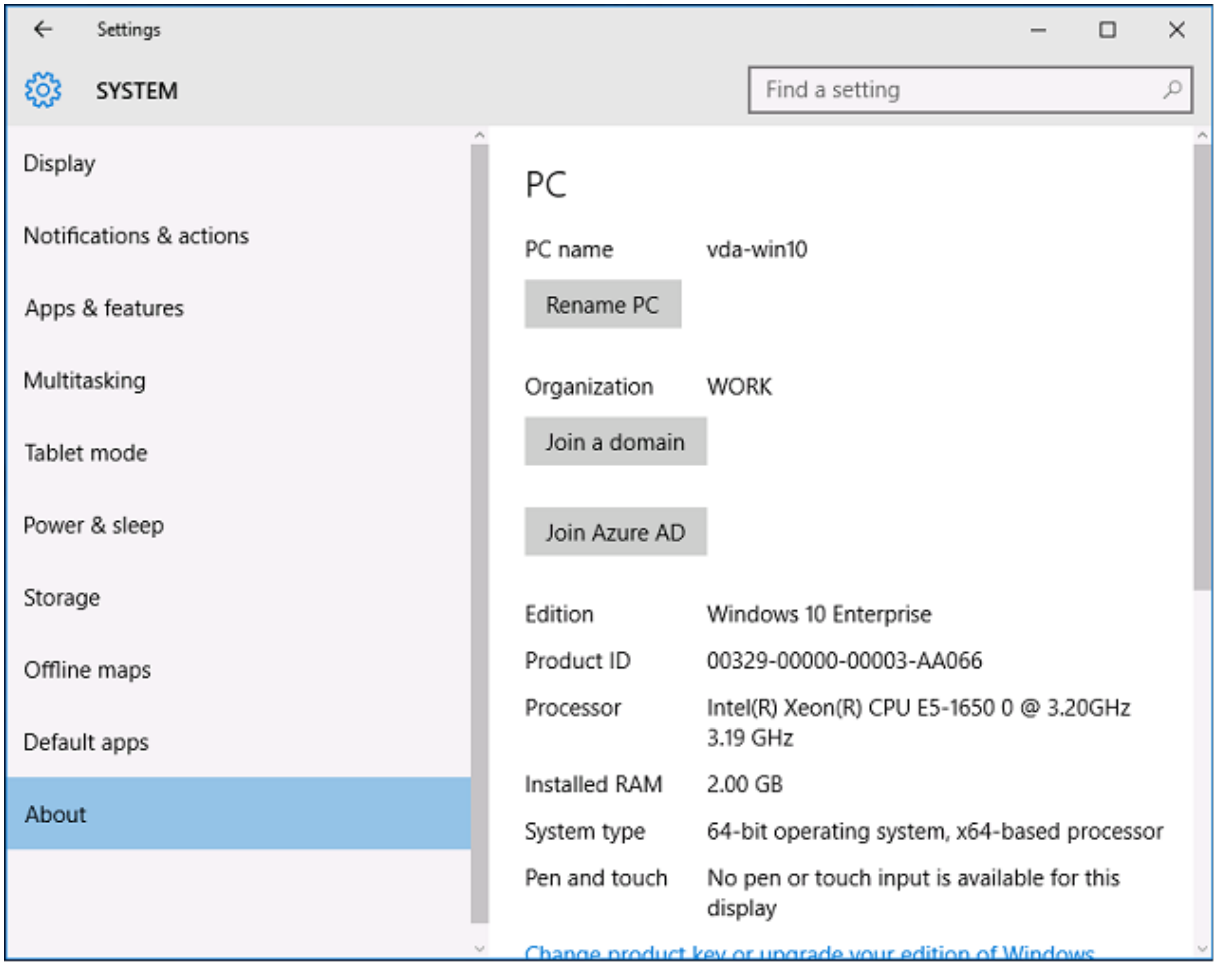
March 8, 2019

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Introducción

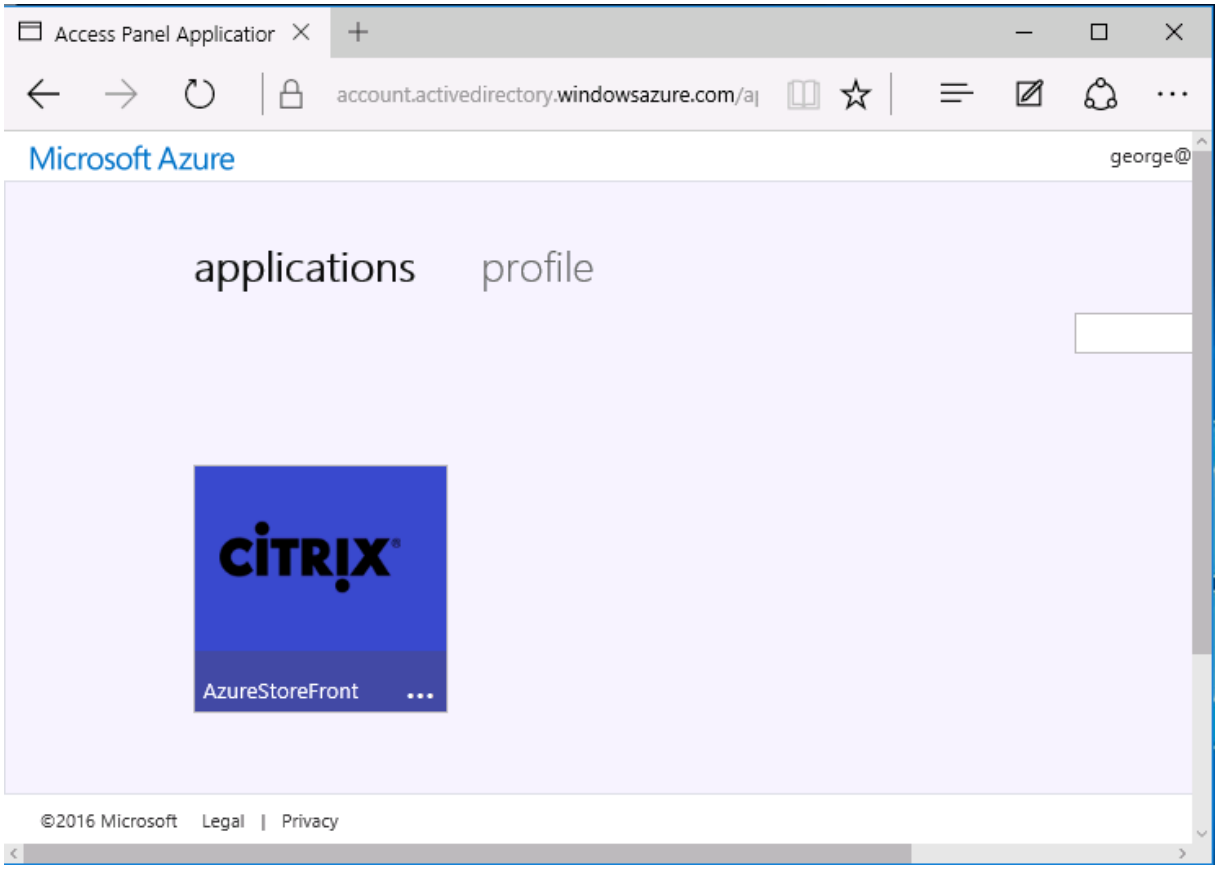
Este documento describe cómo integrar un entorno de Citrix con la funcionalidad de Azure AD de Windows 10. Windows 10 introdujo Azure AD, que es un nuevo modelo para unirse a dominios, por el cual los portátiles móviles pueden unirse a un dominio de empresa a través de Internet con fines de administración y Single Sign-on.

El ejemplo de implementación en este documento describe un sistema donde TI proporciona a los nuevos usuarios una dirección de correo electrónico de la empresa y un código de inscripción para sus portátiles Windows 10 personales. Los usuarios acceden a este código desde la opción **Sistema > Acerca de > Unirse a Azure AD** en el panel **Configuración**.



Una vez inscrito el portátil, el explorador Web Microsoft Edge inicia sesión automáticamente en los sitios Web de la empresa y las aplicaciones publicadas de Citrix a través de la página Web de aplicaciones SaaS de Azure, con otras aplicaciones de Azure, como Office 365.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

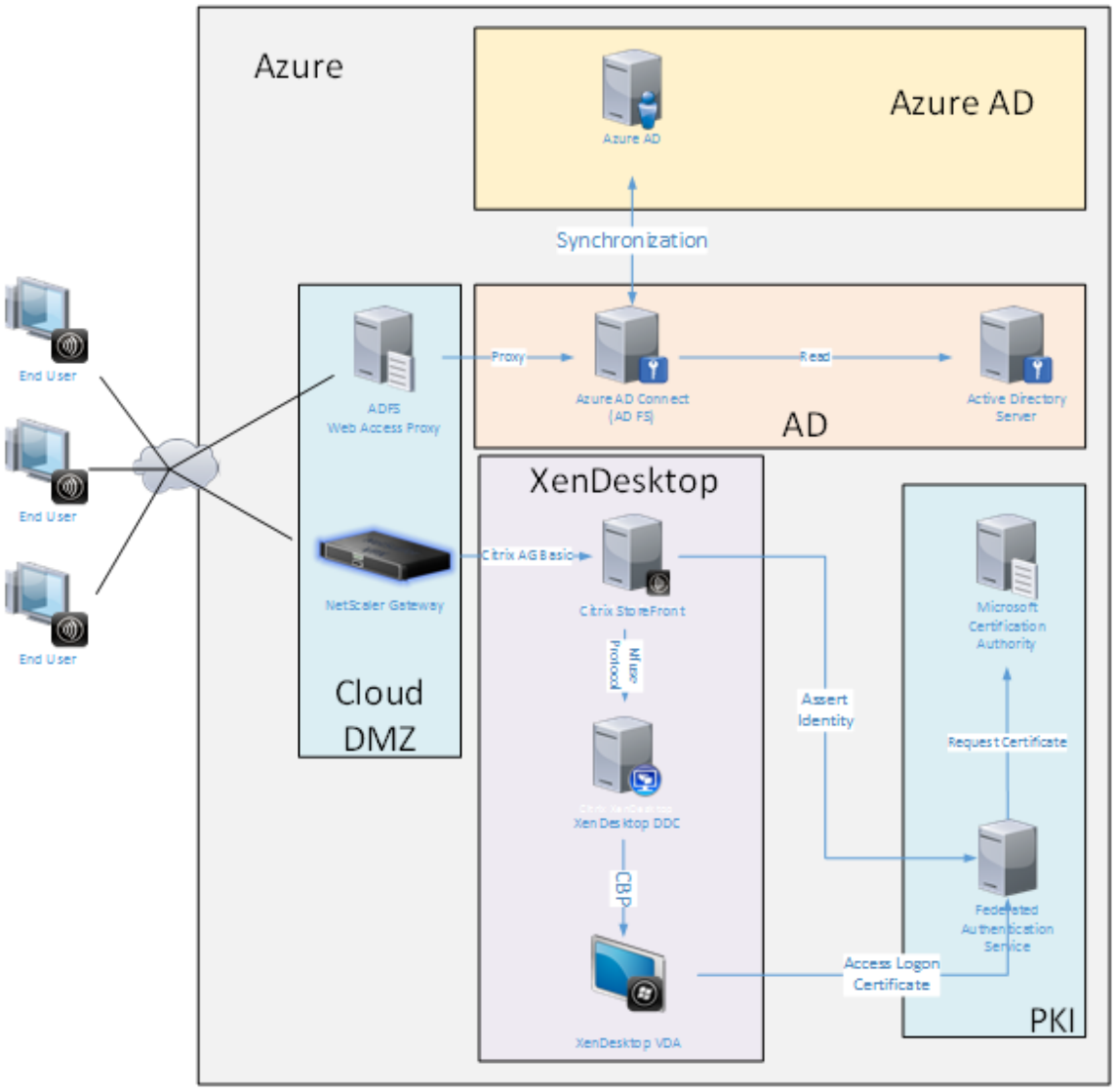


Arquitectura

Esta arquitectura replica una red de empresa tradicional incluida totalmente dentro de Azure, integrada con tecnologías de nube modernas, tales como Azure AD y Office 365. Los usuarios finales se consideran todos trabajadores remotos, sin concepto de estar en una intranet de la oficina.

El modelo se puede aplicar a las empresas con sistemas existentes en las propias sedes, porque Azure Connect Synchronization puede establecer un puente con Azure a través de Internet.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Las conexiones seguras y Single Sign-On, que tradicionalmente se habrían establecido con autenticación Kerberos/NLTM y LAN con firewall, se sustituyen en esta arquitectura con conexiones TLS hacia Azure y SAML. Se crean nuevos servicios a medida que nuevas aplicaciones de Azure se unen a Azure AD. Las aplicaciones que requieren Active Directory (por ejemplo, una base de datos de SQL Server) se pueden ejecutar mediante una VM estándar de servidor de Active Directory en la porción de IAAS del Servicio de nube de Azure.

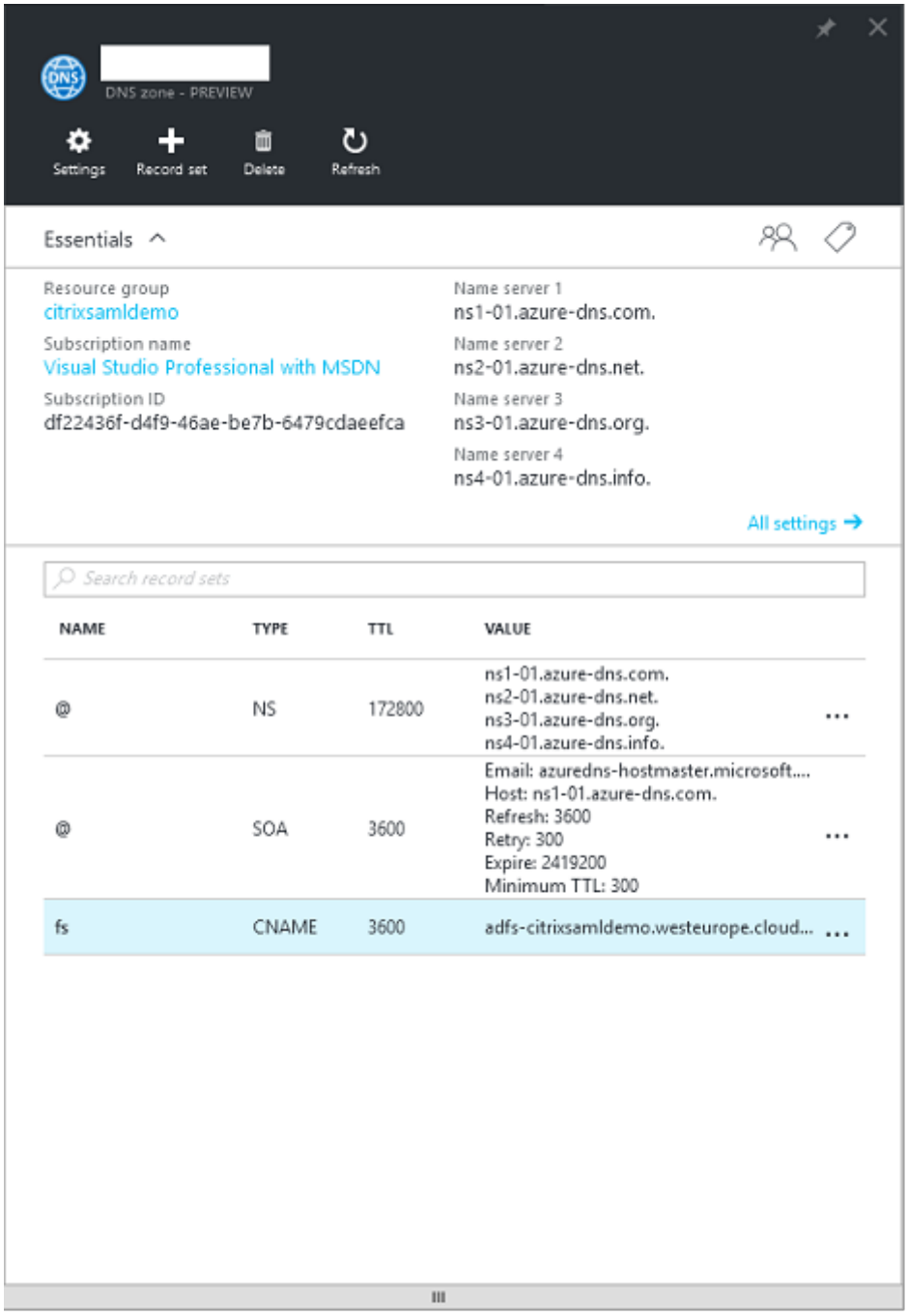
Cuando un usuario inicia una aplicación tradicional, el acceso tiene lugar usando aplicaciones publicadas de Citrix Virtual Apps and Desktops. Los diferentes tipos de aplicaciones se intercalan a través de la página **Aplicaciones de Azure** del usuario con la ayuda de las funciones Single Sign-On de Microsoft Edge. Microsoft también proporciona aplicaciones de iOS y Android que pueden enumerar e iniciar aplicaciones de Azure.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Crear una zona DNS

Azure AD requiere que el administrador haya registrado una dirección DNS pública y controla la zona de delegación para el sufijo de nombre de dominio. Para realizar esta acción, el administrador puede usar la función de zona DNS en Azure.

En este ejemplo, se usa la zona DNS con el nombre *citrixsamldemo.net*.



La consola muestra los nombres de los servidores DNS de Azure. Estos deben constar en las entradas

© 1999-2019 Citrix Systems, Inc. All rights reserved.

NS del registrador DNS de la zona (por ejemplo: `citrixsamldemo.net. NS n1-01.azure-dns.com`).

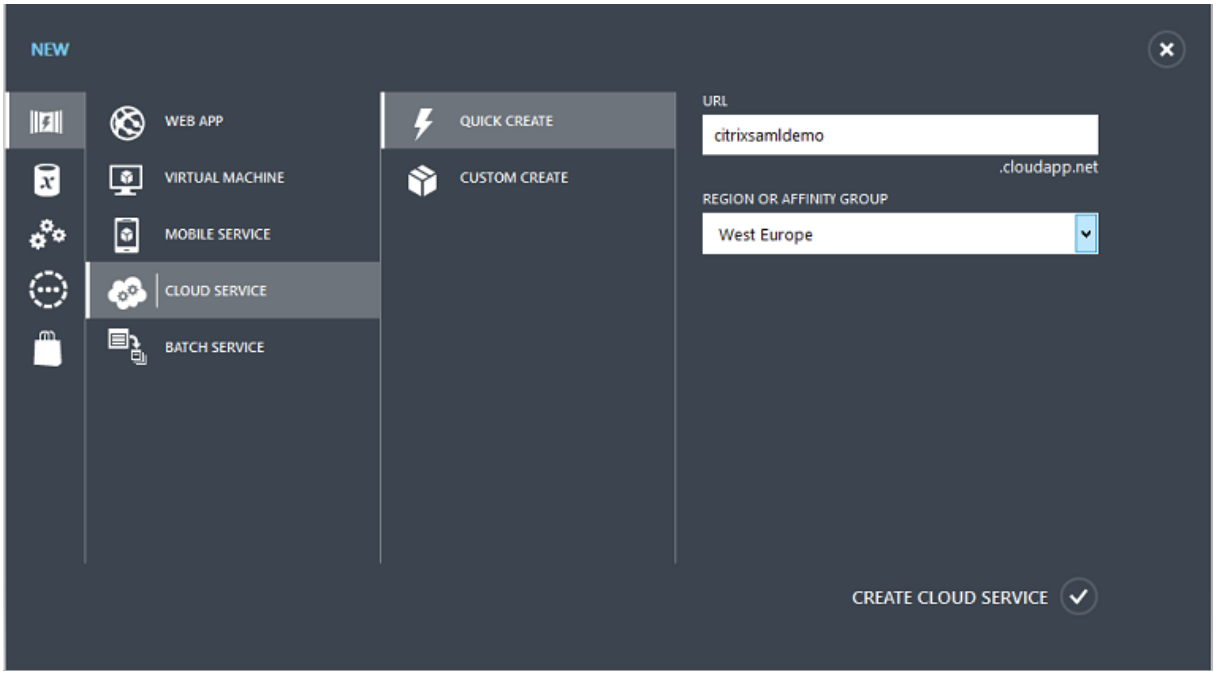
Al agregar referencias a las VM ejecutadas en Azure, lo más sencillo es usar un puntero CNAME que apunte al registro DNS administrado por Azure para la VM. Si la dirección IP de la VM cambia, no será necesario actualizar manualmente el archivo de zona DNS.

Los sufijos de ambas direcciones DNS interna y externa coincidirán en esta implementación. El dominio es citrixsamldemo.net y usan DNS dividido (10.0.0.* internamente).

Agregue una entrada “fs.citrixsamldemo.net” que haga referencia al servidor Proxy de aplicación Web. Este es el Servicio de federación para esta zona.

Crear un servicio de nube

En este ejemplo, se configura un entorno Citrix, que incluye un entorno AD con un servidor ADFS ejecutándose en Azure. Se crea un servicio de nube llamado “citrixsamldemo”.



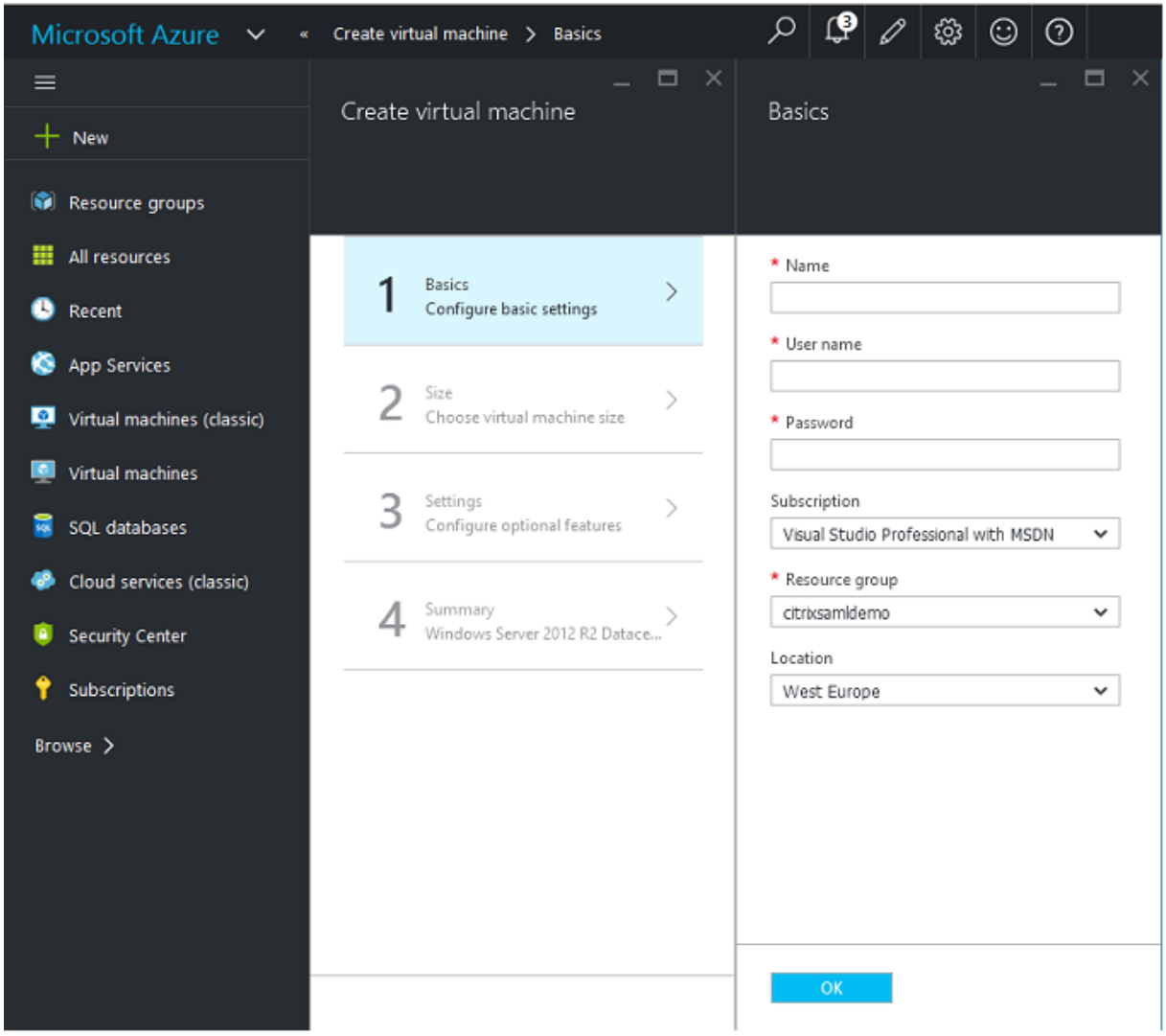
Crear máquinas virtuales de Windows

Cree cinco máquinas virtuales Windows ejecutándose en el servicio de nube:

- Controlador de dominio (domaincontrol)
- Servidor ADFS de Azure Connect (adfs)
- Proxy de acceso Web de ADFS (proxy de aplicación Web, no unido a dominio)
- Delivery Controller (ddc) de Citrix Virtual Desktops

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Virtual Delivery Agent (VDA) de Citrix Virtual Desktops



Controlador de dominio

- Agregue los roles **Servidor DNS** y **Servicios de dominio de Active Directory** para crear una implementación estándar de Active Directory (en este ejemplo, citrixsamldemo.net). Una vez completada la promoción de dominio, agregue el rol **Servicios de certificados de Active Directory**.
- Cree una cuenta de usuario normal para las pruebas (por ejemplo, Jorge@ citrixsamldemo.net).
- Dado que este servidor ejecutará DNS interno, todos los servidores deben hacer referencia a este servidor para la resolución de DNS. Se logra desde la página **Configuración DNS** de Azure. (Para obtener más información, consulte el Apéndice en este documento.)

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Controlador ADFS y servidor proxy de aplicaciones Web

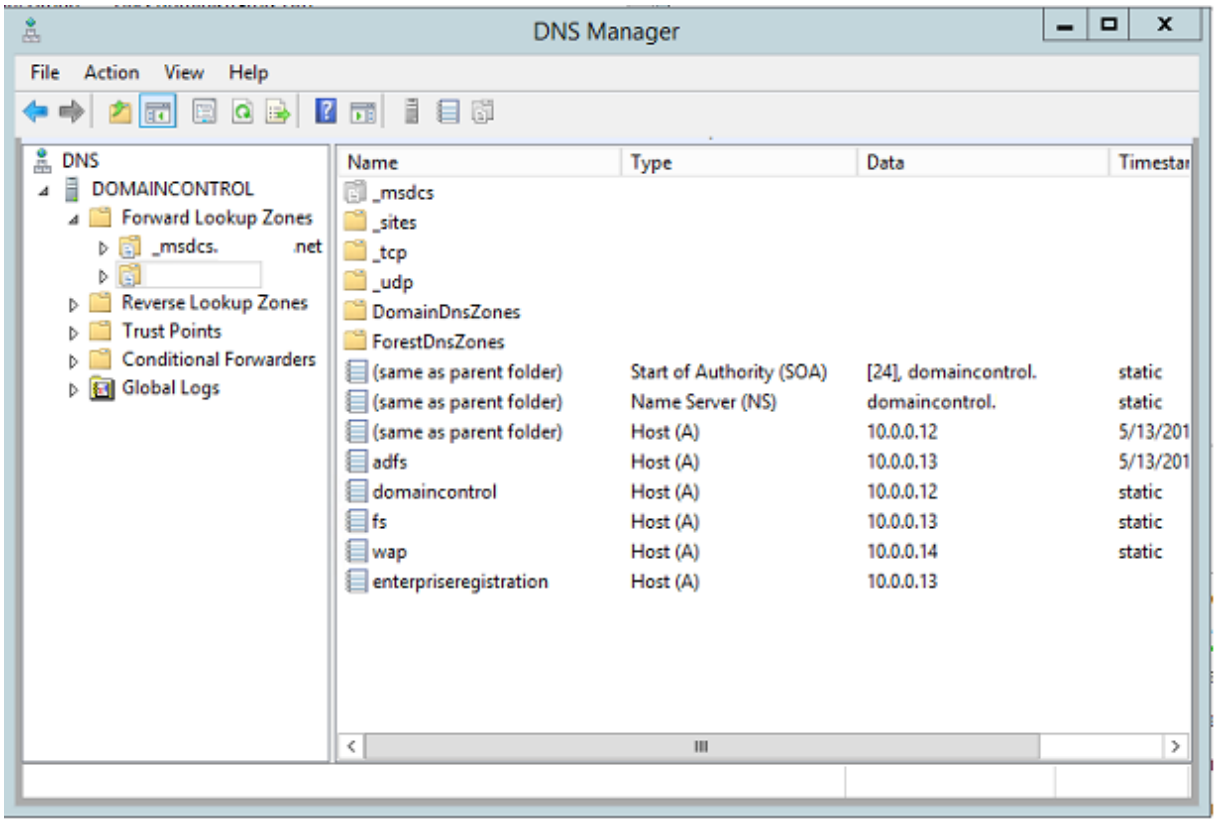
- Una el servidor ADFS al dominio citrixsamldemo. El servidor proxy de aplicaciones Web debe estar en un grupo de trabajo aislado, por lo que debe registrar manualmente una dirección DNS con el DNS de AD.
- Ejecute el cmdlet **Enable-PSRemoting – Force** en estos servidores, para permitir la comunicación remota de PS a través de firewalls desde la herramienta Azure AD Connect.

VDA y Delivery Controller de Citrix Virtual Desktops

- Instale el Delivery Controller y el VDA de Citrix Virtual Apps o Citrix Virtual Desktops en los dos servidores Windows restantes unidos a citrixsamldemo.

Configurar un DNS interno

Después de que el controlador de dominio está instalado, configure el servidor DNS para controlar la vista de citrixsamldemo.net y actuar como un reenviador a un servidor DNS externo (por ejemplo: 8.8.8.8).

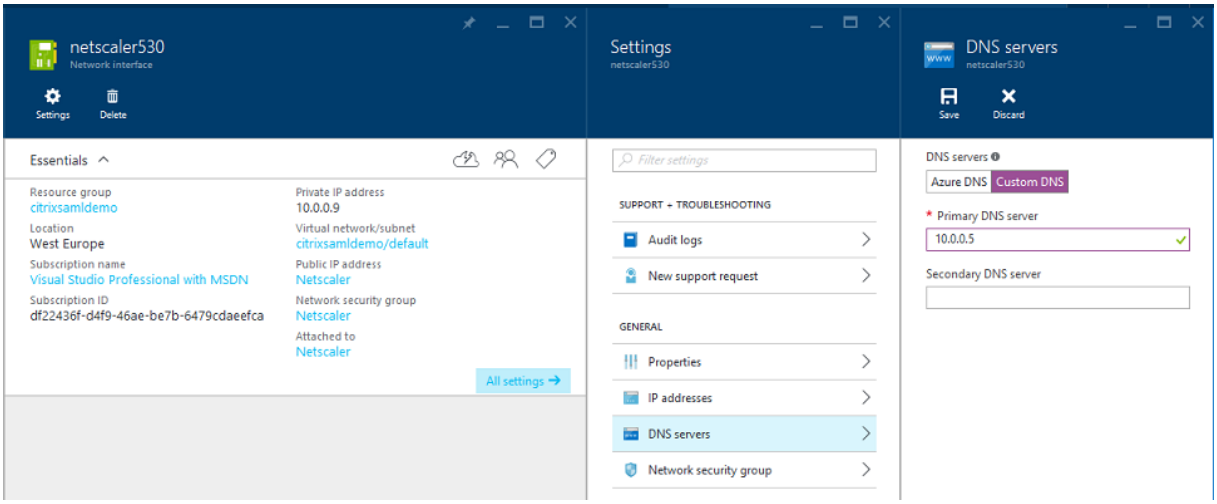


Agregue un registro estático para:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- wap.citrixsamldemo.net [la VM de proxy de aplicaciones Web no estará unida a ningún dominio]
- fs.citrixsamldemo.net [dirección de servidor de federación interno]
- enterpriseregistration.citrixsaml.net [igual que fs.citrixsamldemo.net]

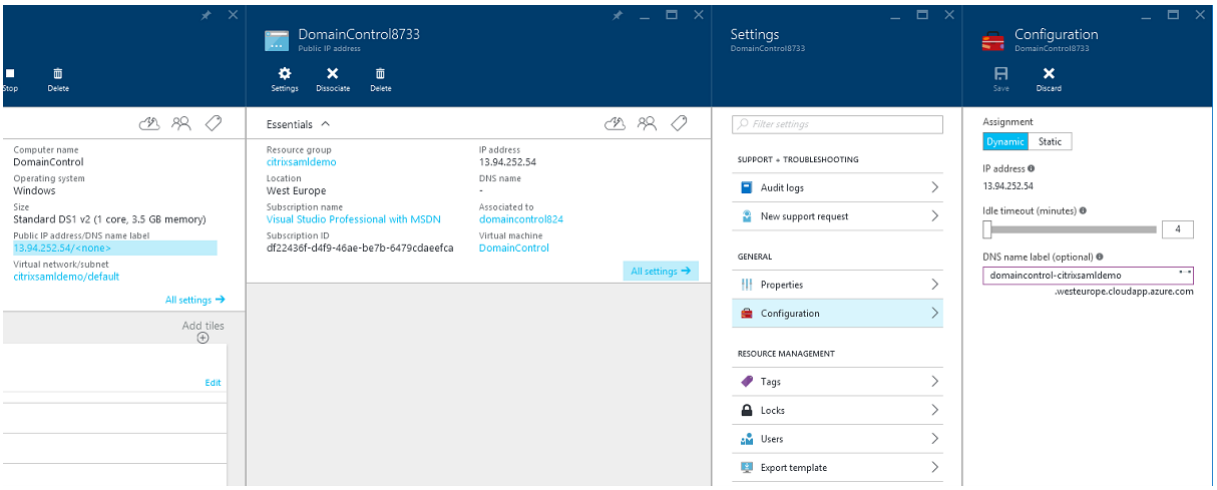
Todas las VM que se ejecutan en Azure deben estar configuradas para usar solo este servidor DNS. Puede hacerlo a través de la GUI de interfaz de red.



De forma predeterminada, la dirección IP interna (10.0.0.9) se asigna dinámicamente. Puede usar el parámetro de direcciones IP para asignar permanentemente la dirección IP. Esto debe hacerse para el servidor proxy de aplicaciones Web y el controlador de dominio.

Configurar una dirección DNS externa

Cuando se está ejecutando una VM, Azure mantiene su propio servidor de zona DNS que apunta a la dirección IP pública actual asignada a la VM. Habilitar esta función resulta muy útil porque Azure asigna direcciones IP cuando cada VM se inicia, de manera predeterminada.



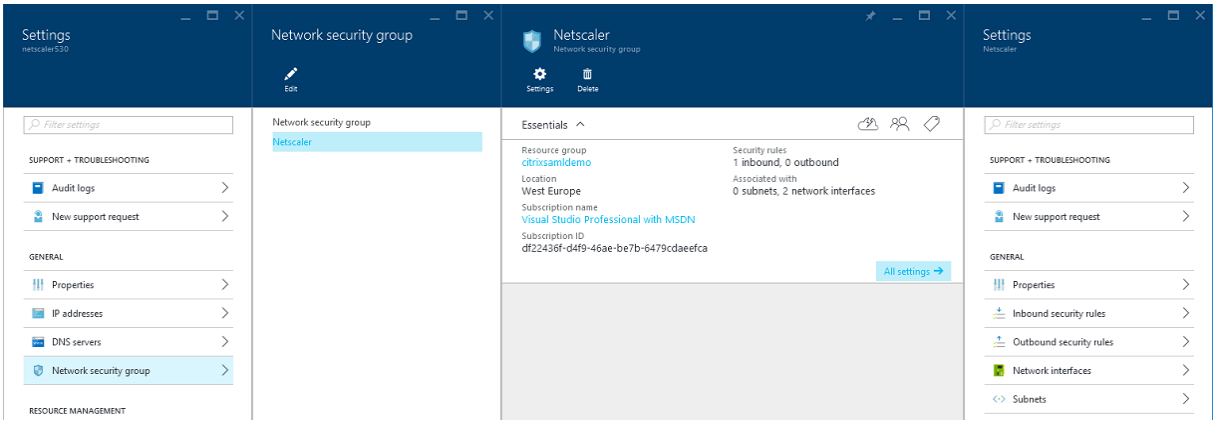
© 1999-2019 Citrix Systems, Inc. All rights reserved.

Este ejemplo asigna una dirección DNS de domaincontrol-citrixsamldemo.westeurope.cloudapp.azure.com al controlador de dominio.

Tenga en cuenta que cuando se complete la configuración remota, solo las VM del proxy de aplicaciones Web y de NetScaler deben tener direcciones IP públicas habilitadas. (Durante la configuración, la dirección IP pública se usa para el acceso RDP al entorno).

Configurar grupos de seguridad

La nube de Azure administra las reglas de firewall para el acceso TCP/UDP en las VM desde Internet utilizando grupos de seguridad. De forma predeterminada, todas las VM permiten el acceso RDP. Los servidores de NetScaler y el proxy de aplicaciones Web deben permitir TLS en el puerto 443.



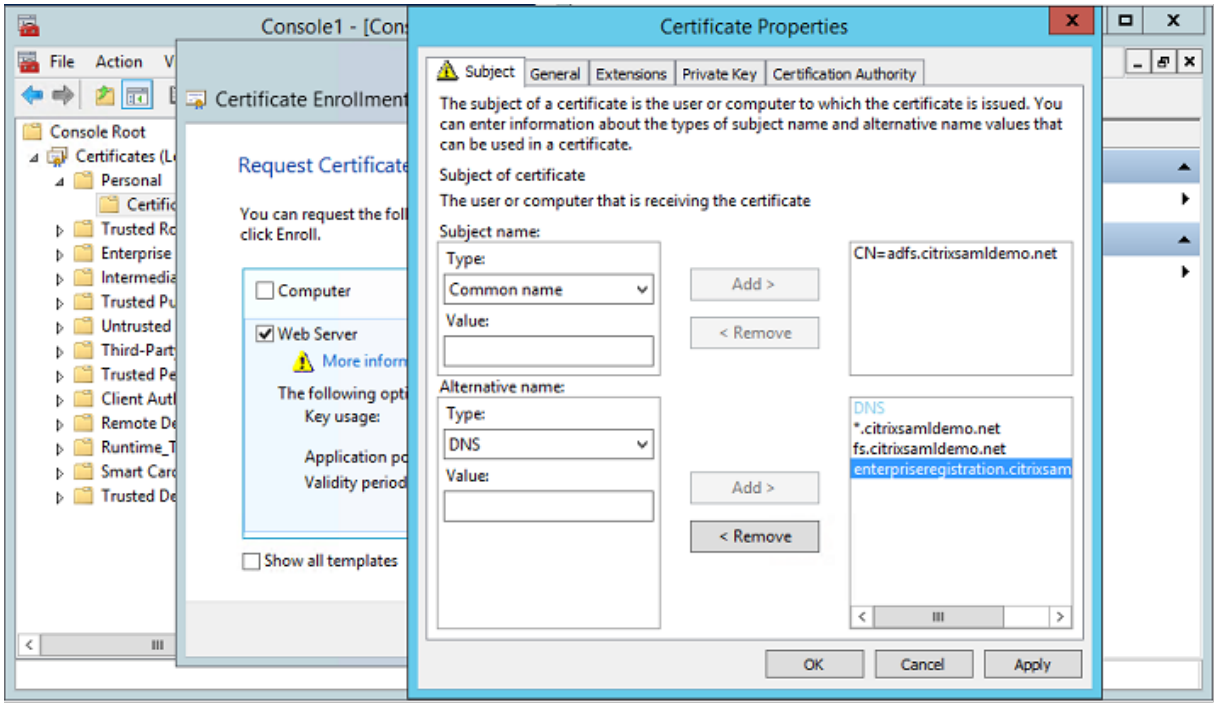
Crear un certificado ADFS

Habilite la plantilla de certificado **Servidor Web** en la entidad de certificación (CA) de Microsoft. Esto permite la creación de un certificado con direcciones DNS personalizadas que se pueden exportar (incluida la clave privada) a un archivo .pfx. Debe instalar este certificado en tanto en el servidor proxy de aplicaciones Web como en el servidor ADFS, por lo que un archivo PFX es la opción preferida.

Emita un certificado de servidor Web con los siguientes nombres de sujeto:

- Commonname:
  - adfs.citrixsamldemo.net [nombre del equipo]
- SubjectAltname:
  - *.citrixsamldemo.net [nombre de la zona]]
  - fs.citrixsamldemo.net [entrada en DNS]
  - enterpriseregistration.citrixsamldemo.net

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Exporte el certificado a un archivo PFX, incluida una clave privada protegida por contraseña.

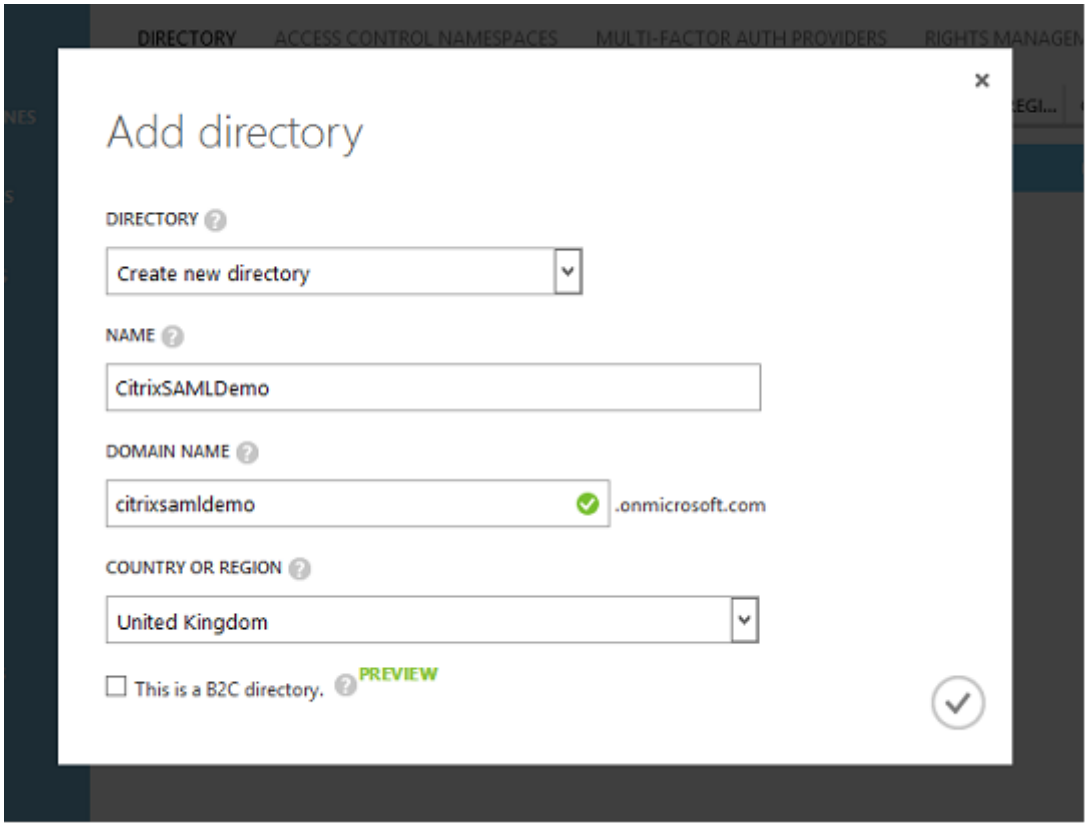
Configurar Azure AD

Esta sección detalla el proceso de configuración de una nueva instancia de Azure AD y la creación de identidades de usuario que se pueden usar para unir Windows 10 a Azure AD.

Crear un directorio nuevo

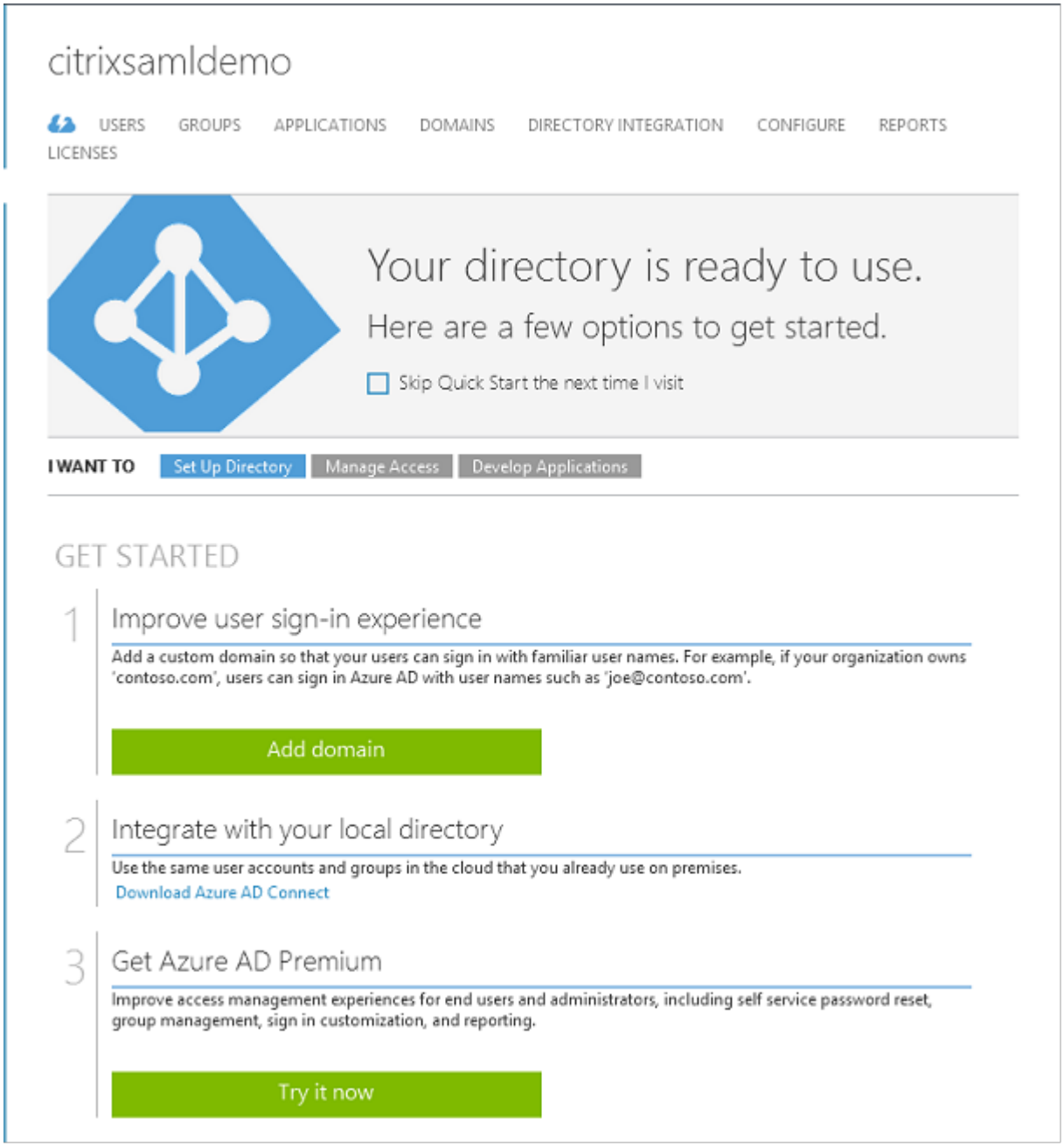
Inicie sesión en el portal Azure clásico y cree un directorio nuevo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Una vez completado, aparece una página de resumen.

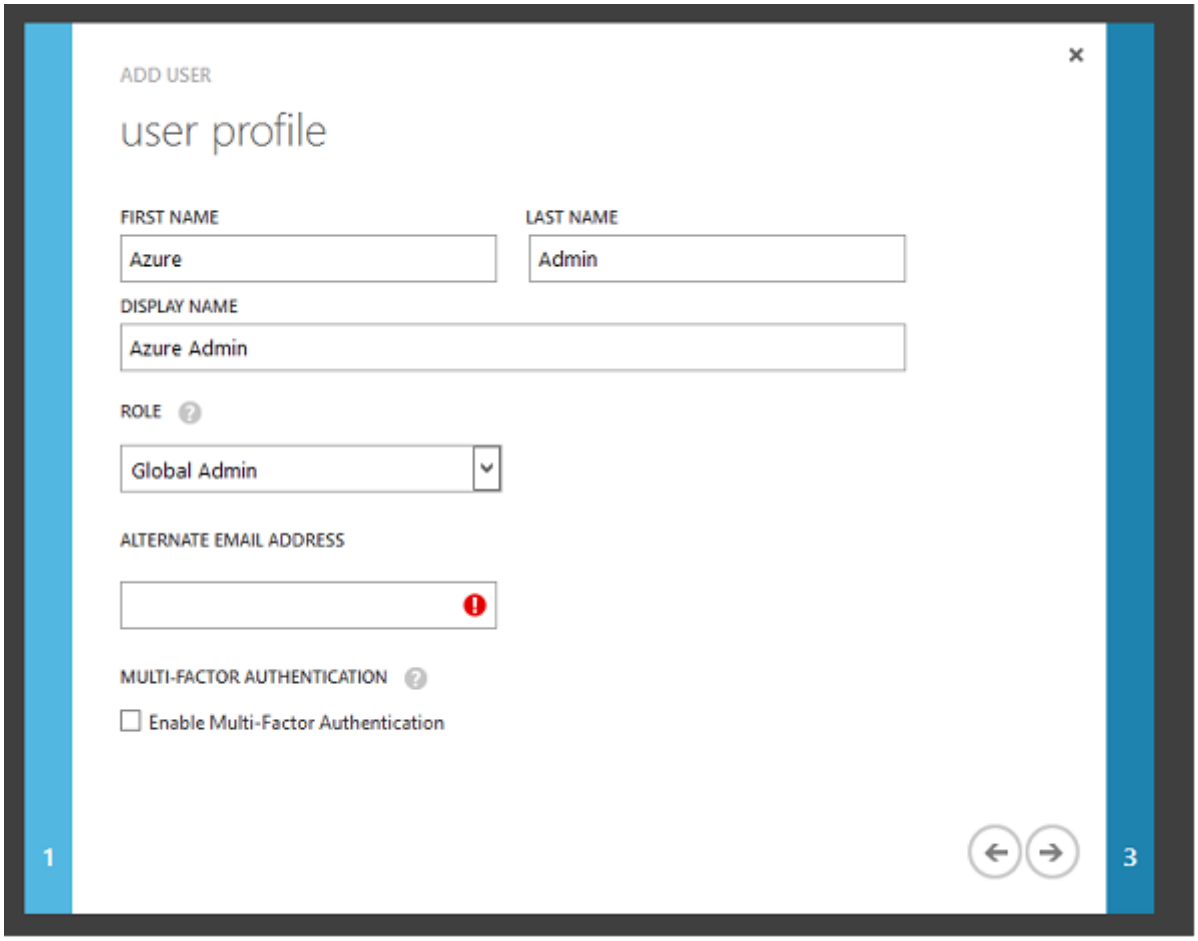
© 1999-2019 Citrix Systems, Inc. All rights reserved.



Crear un usuario administrador global (AzureAdmin)

Cree un administrador global en Azure (en este ejemplo, `AzureAdmin@citrixsamldemo.onmicrosoft.com`) e inicie sesión con la nueva cuenta para configurar una contraseña.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Registrar su dominio en Azure AD

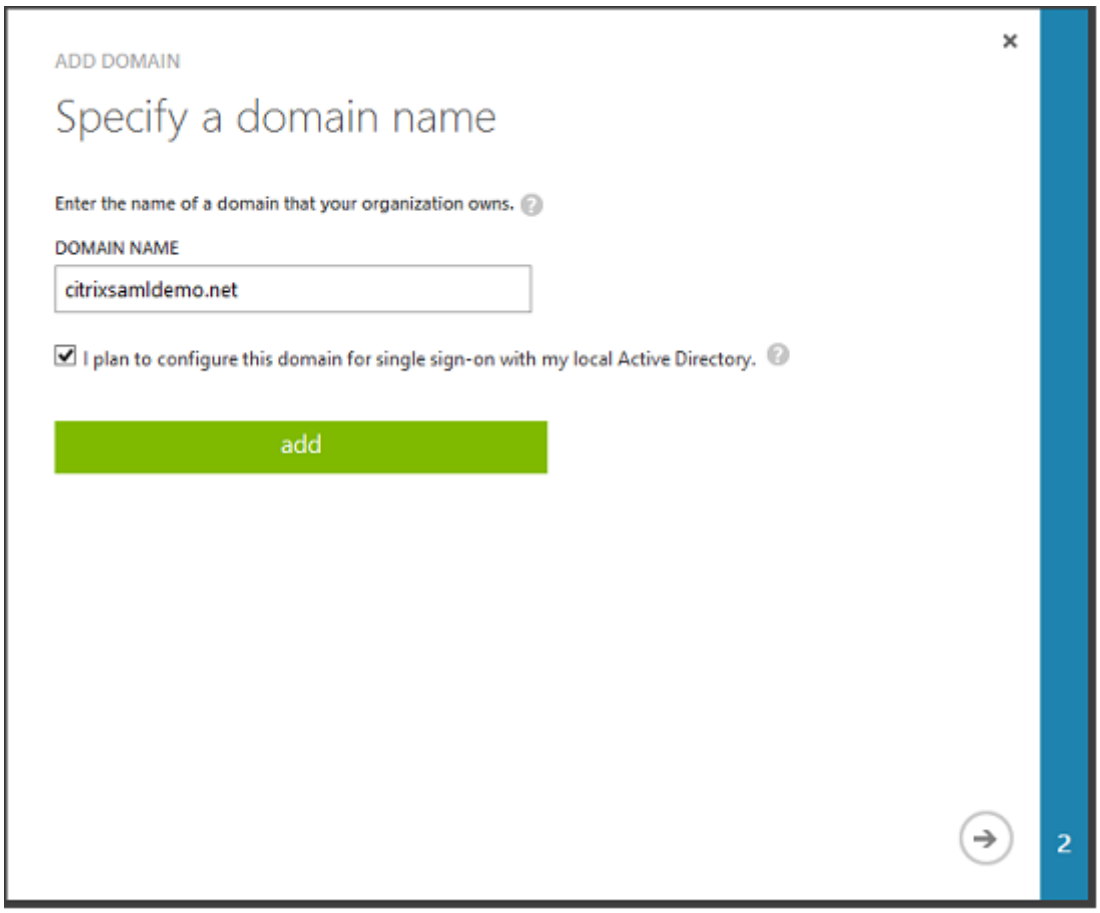
De forma predeterminada, los usuarios se identifican mediante una dirección de correo electrónico en el formato: `<user.name>@<company>.onmicrosoft.com`.

Aunque esto funciona sin configuración adicional, se prefiere un formato estándar para la dirección de correo electrónico; preferiblemente, es mejor que coincida con el formato de la cuenta de correo electrónico del usuario final: `<user.name>@<company>.com`.

La acción **Agregar dominio** configura una redirección desde el dominio real de su empresa. En el ejemplo se usa `citrixsamldemo.net`.

Si quiere configurar ADFS para el inicio de sesión único Single Sign-on, marque la casilla correspondiente.

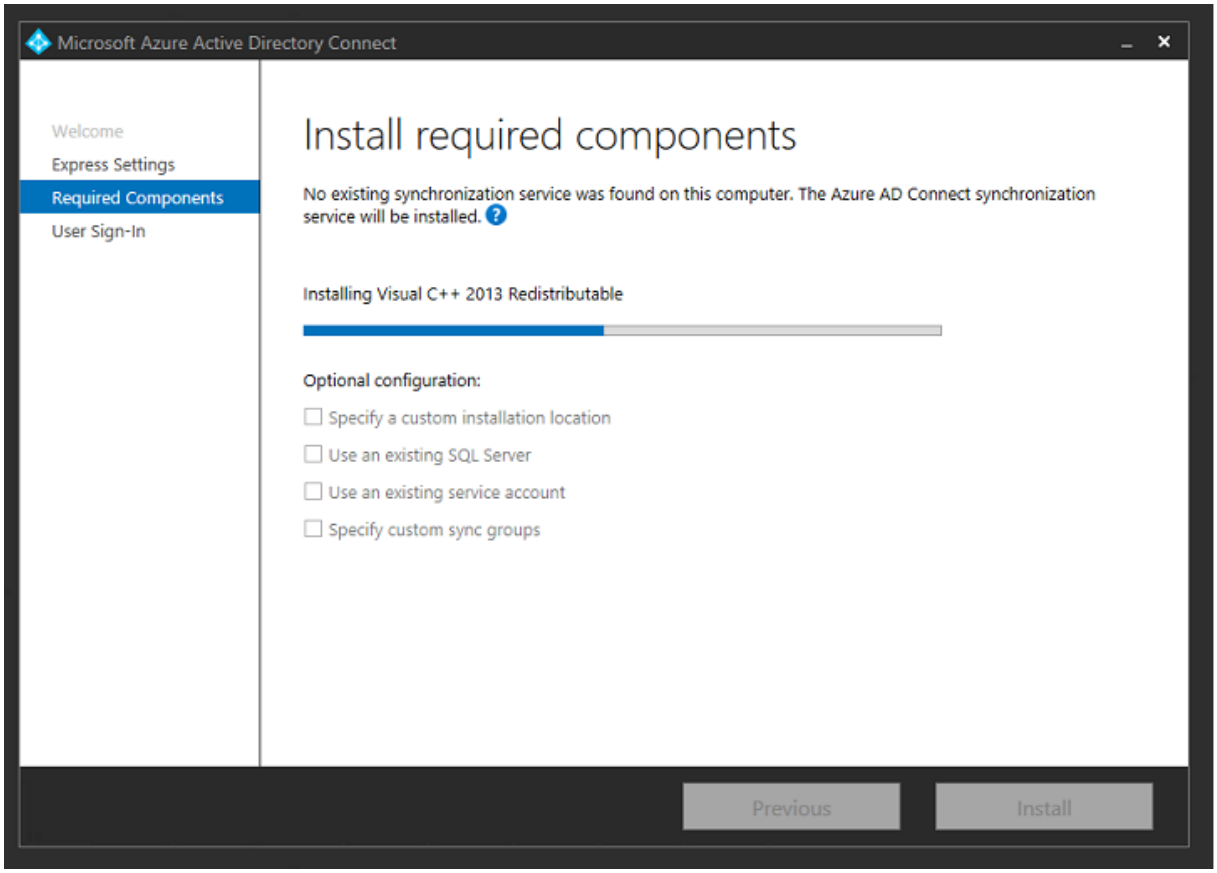
© 1999-2019 Citrix Systems, Inc. All rights reserved.



Instalar Azure AD Connect

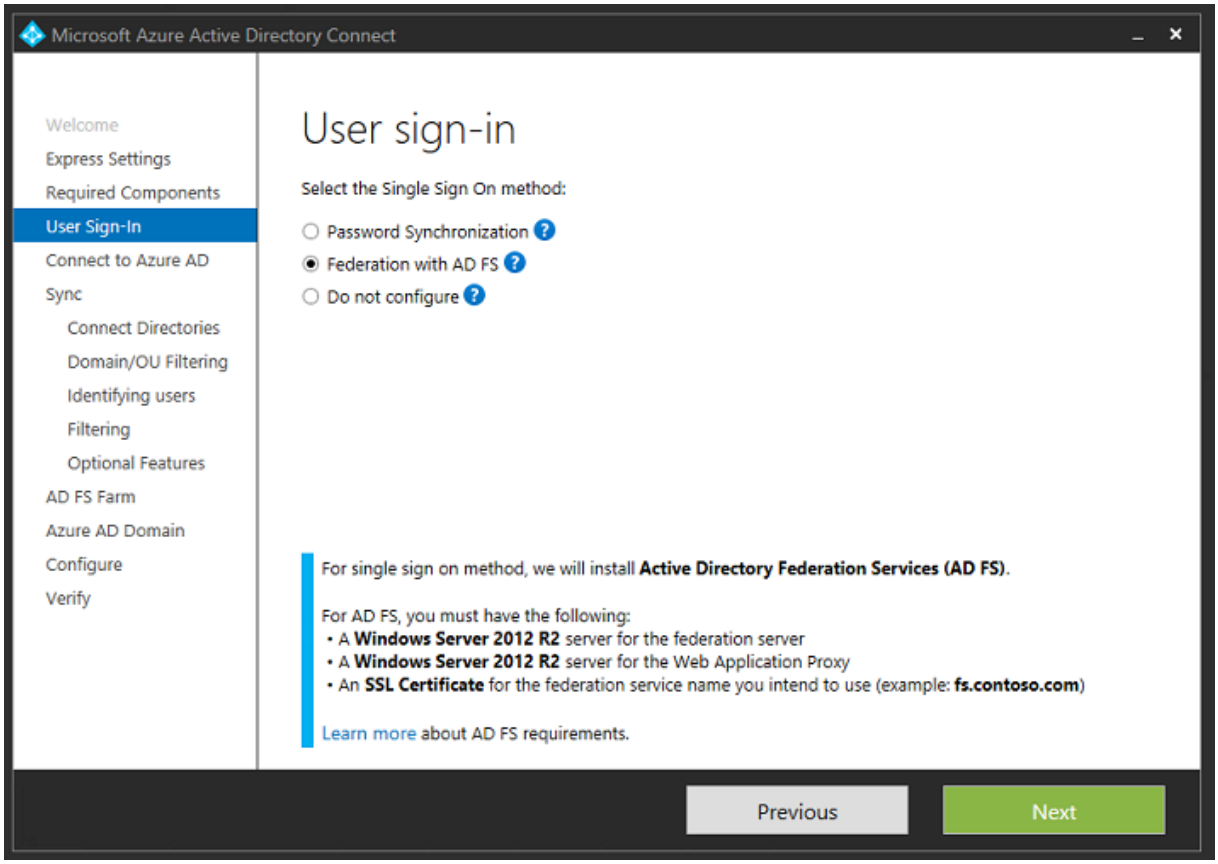
El paso 2 de la interfaz de usuario de configuración de Azure AD le redirige a la página de descarga de Microsoft de Azure AD Connect. Instale esto en la VM de ADFS. Use **Instalación personalizada**, en lugar de **Configuración rápida**, para poder acceder a las opciones de ADFS.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



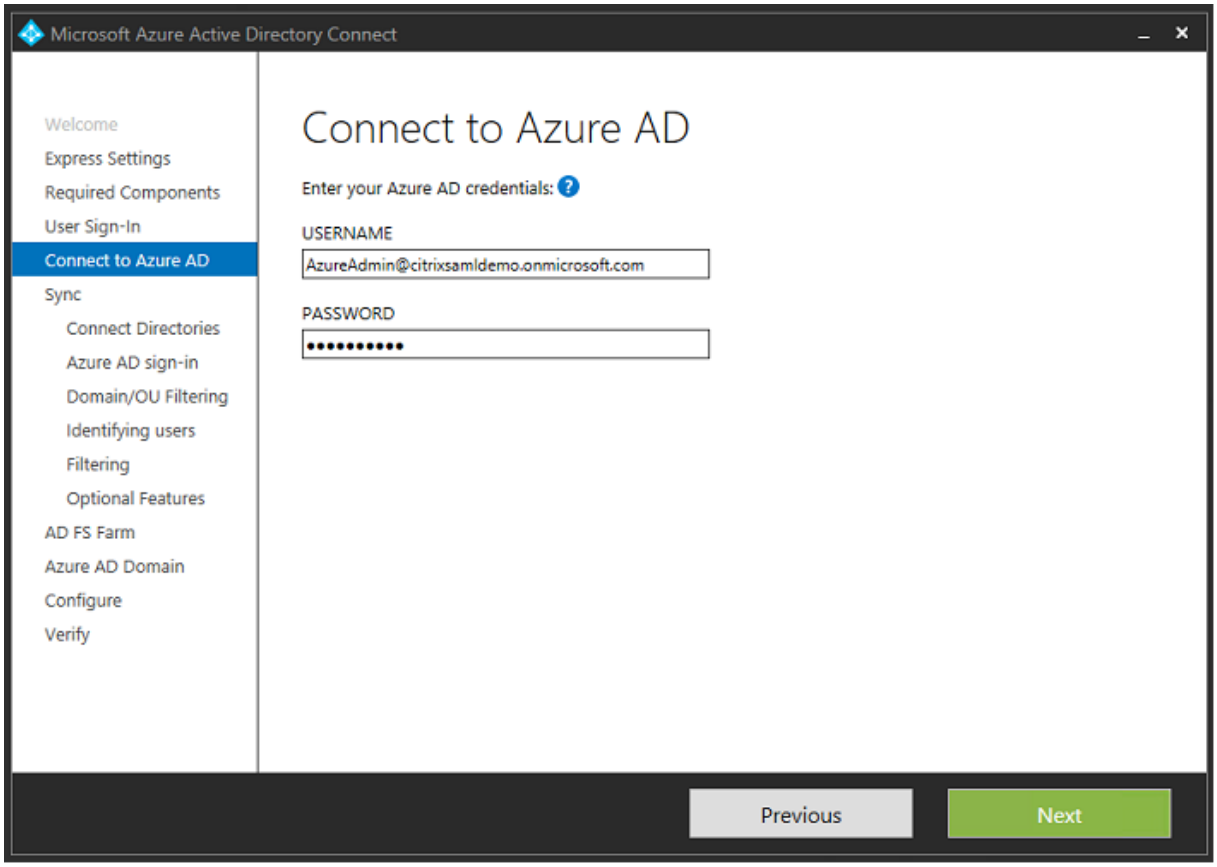
Seleccione la opción **Federación con AD FS** como método SSO.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



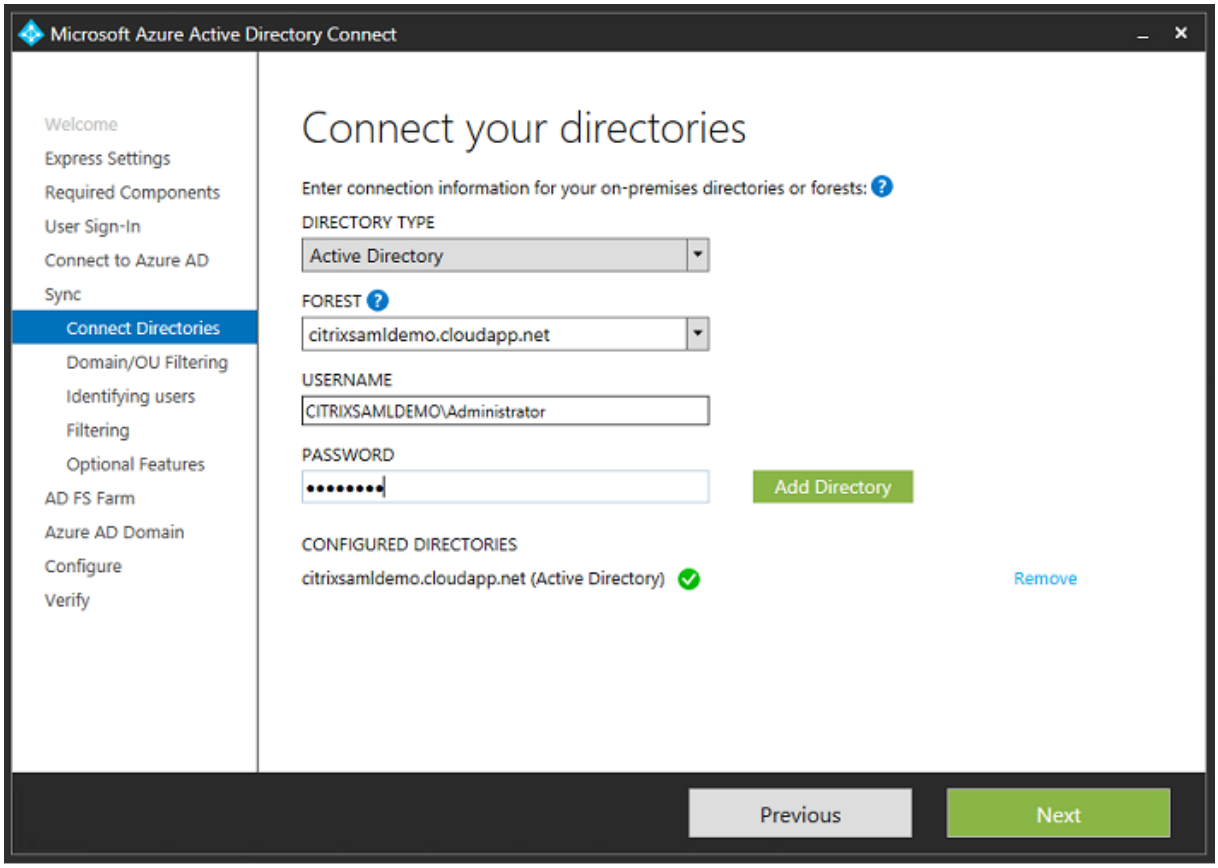
Conéctese a Azure con la cuenta de administrador que ha creado anteriormente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



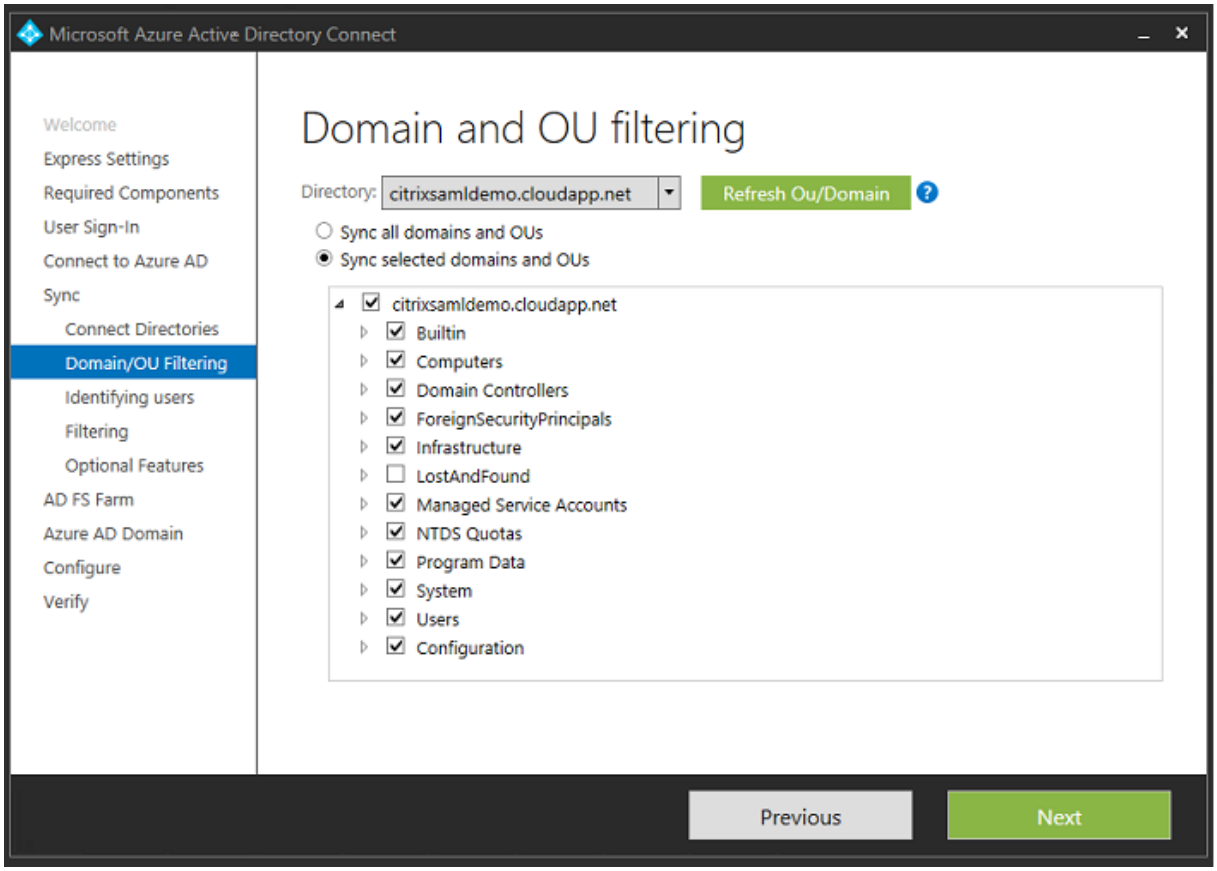
Seleccione el bosque de AD interno.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



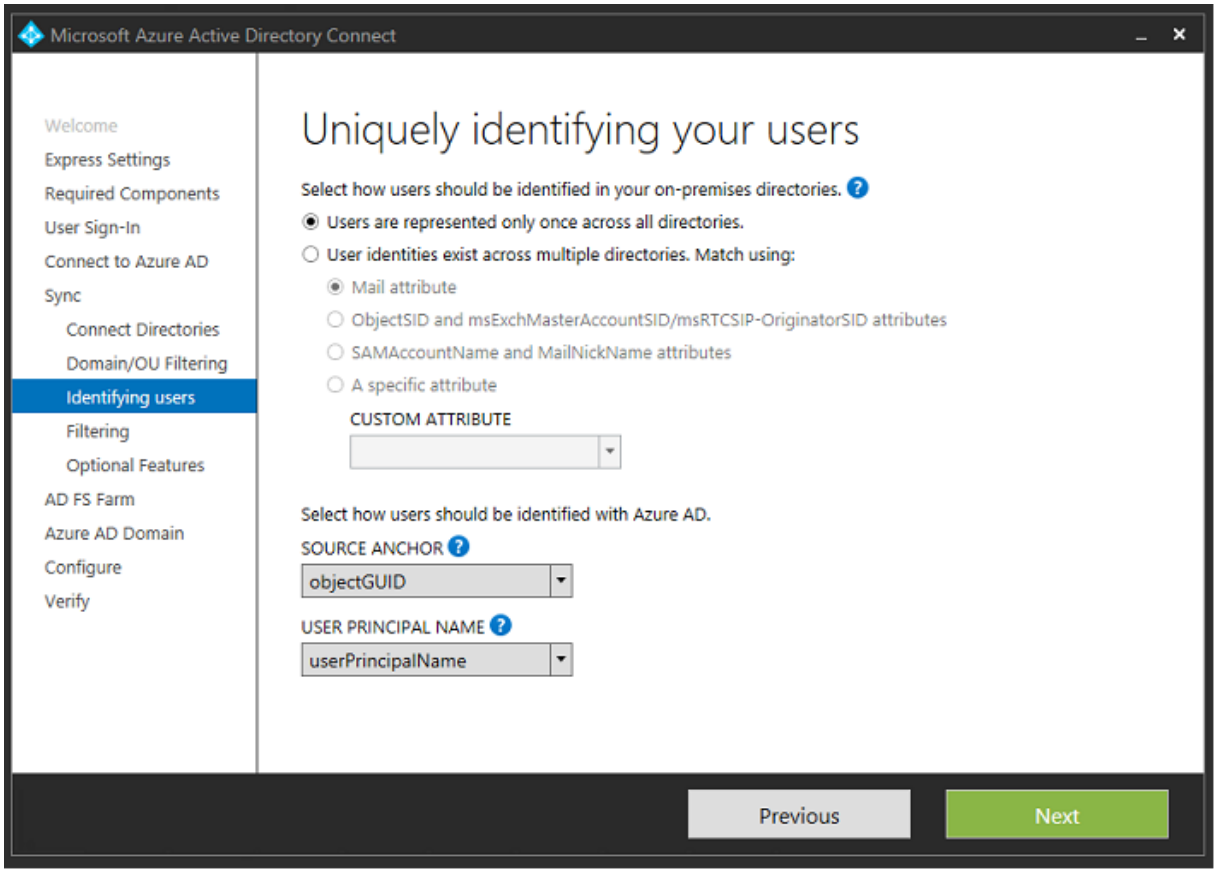
Sincronice todos los objetos de Active Directory antiguos con Azure AD.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



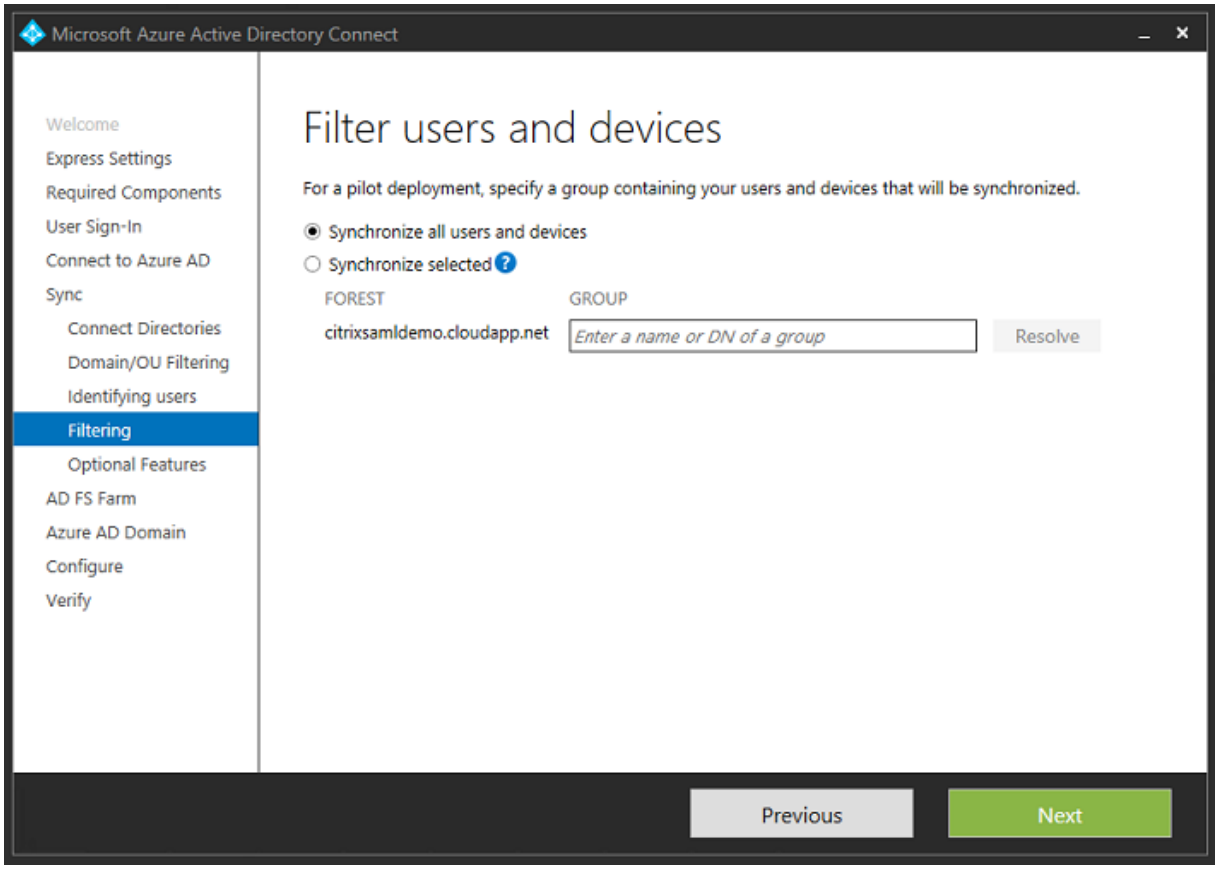
Si la estructura de directorio es sencilla, puede asumir que los nombres de usuario serán lo suficientemente únicos para identificar al usuario que inicia una sesión.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



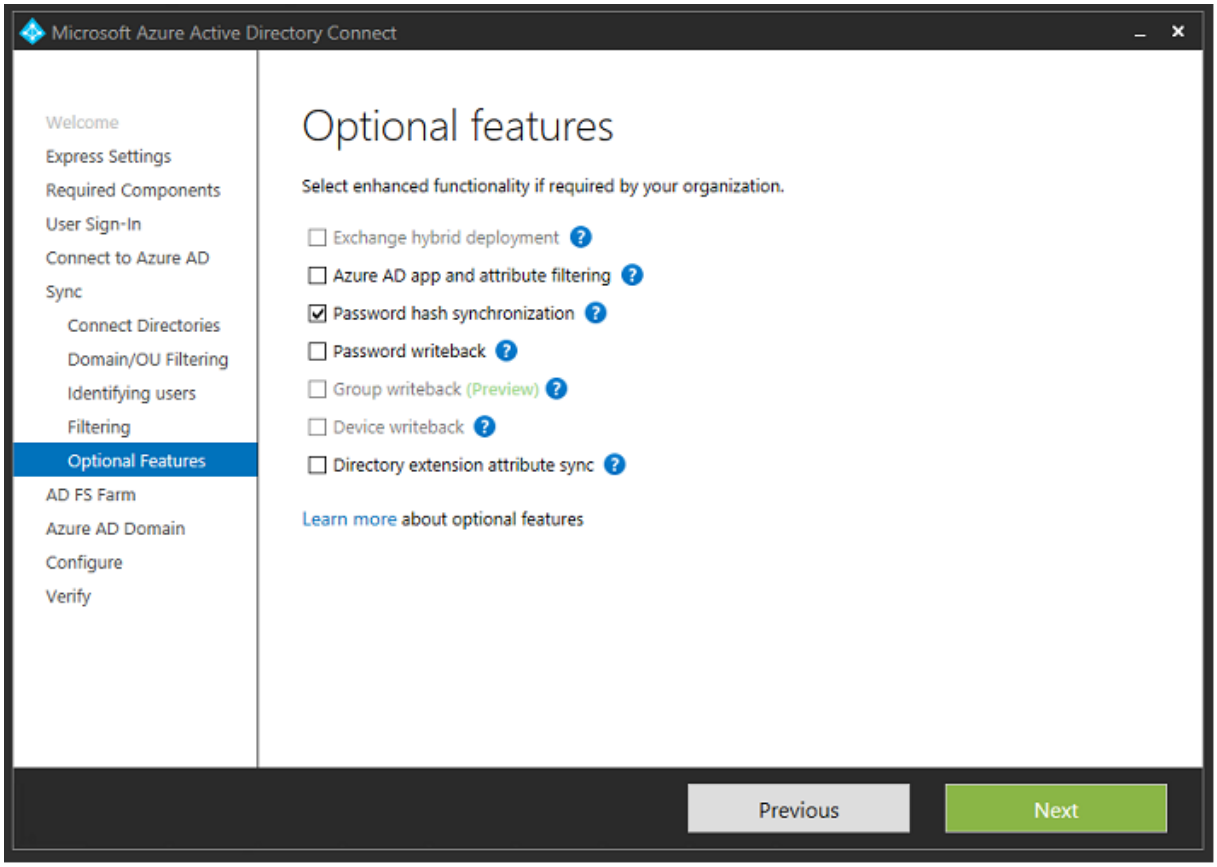
Acepte las opciones de filtrado predeterminadas, o restrinja usuarios y dispositivos a un conjunto de grupos determinado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



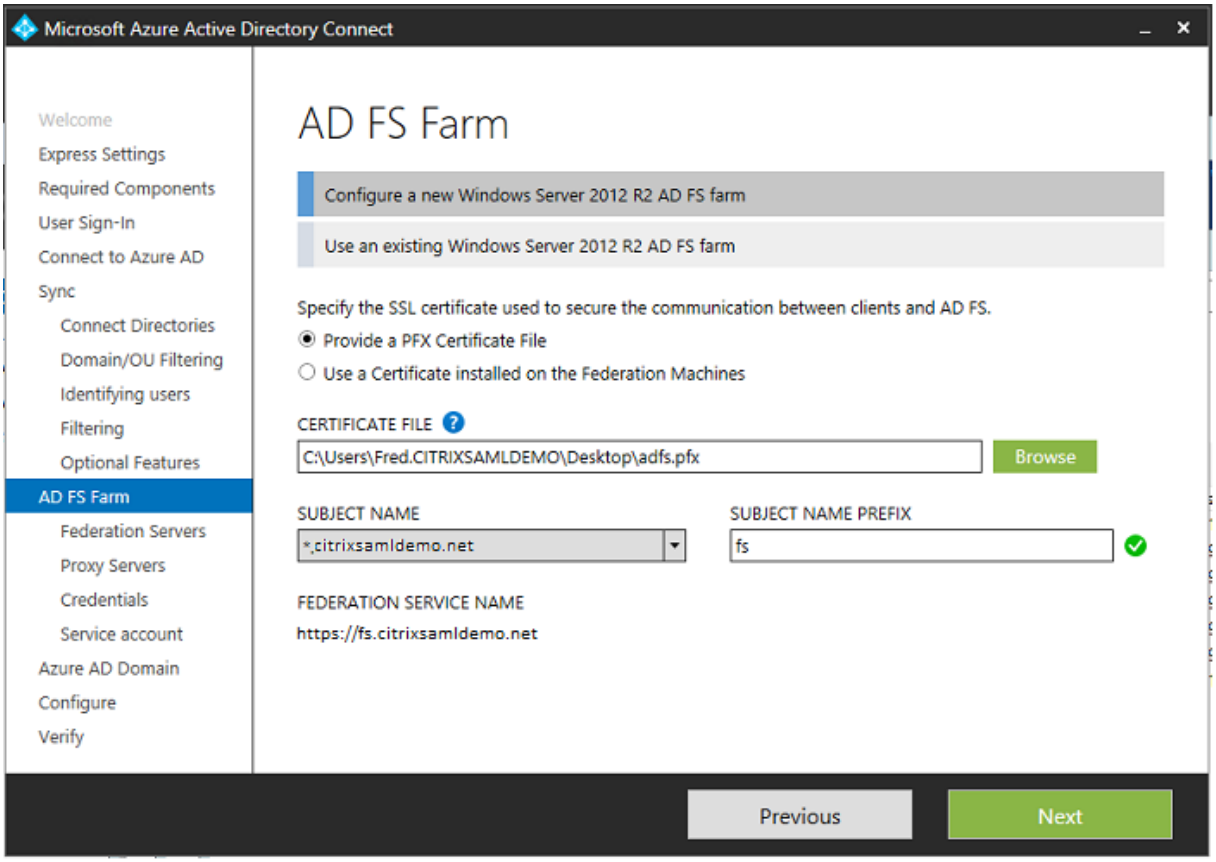
Si lo desea, puede sincronizar las contraseñas de Azure AD con Active Directory. Esto normalmente no es necesario para la autenticación basada en ADFS.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



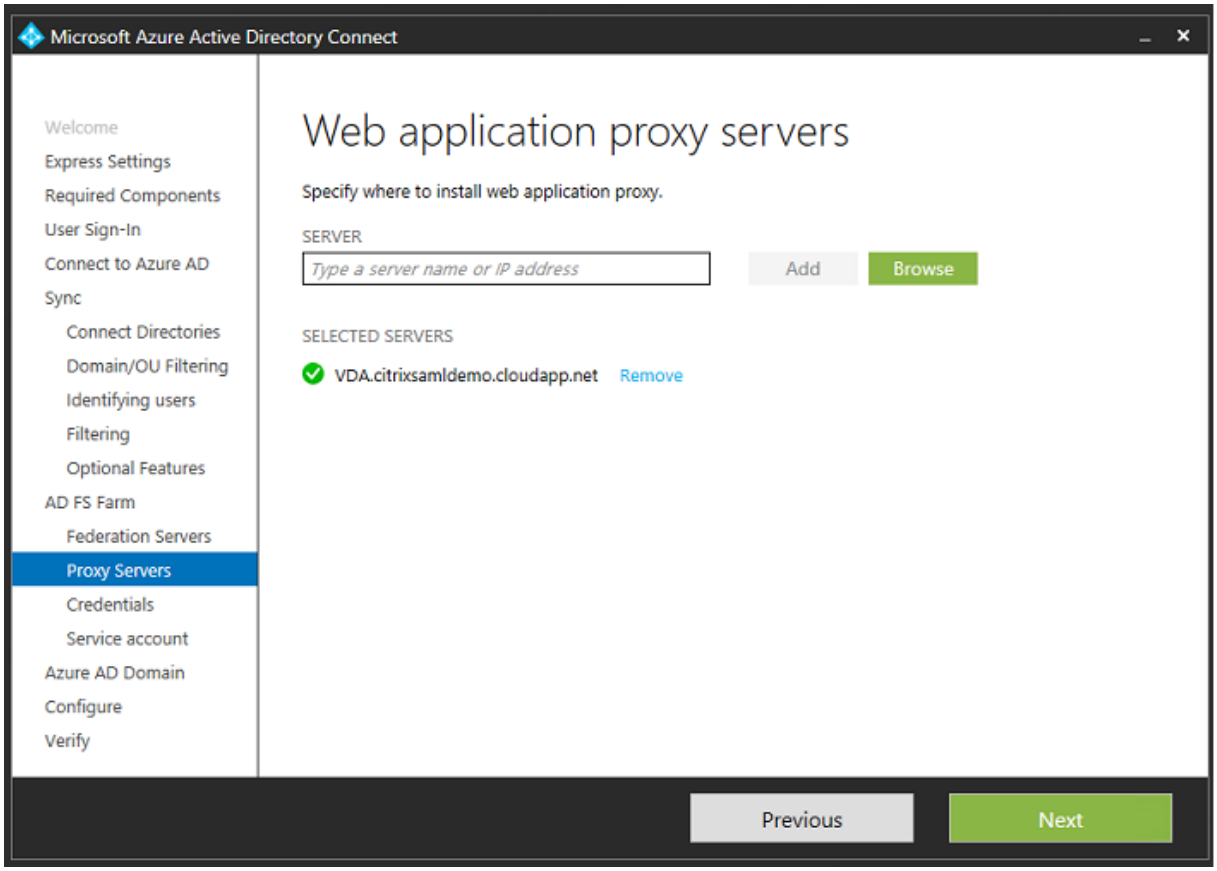
Seleccione el archivo de certificado PFX que se va a usar en ADFS, especificando fs.citrixsamldemo.net como nombre DNS.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Cuando se le pida seleccionar un servidor proxy, escriba la dirección del servidor wap.citrixsamldemo.net. Puede que deba ejecutar el cmdlet **Enable-PSRemoting – Force** como administrador en el servidor proxy de aplicaciones web, para que Azure AD Connect pueda configurarlo.

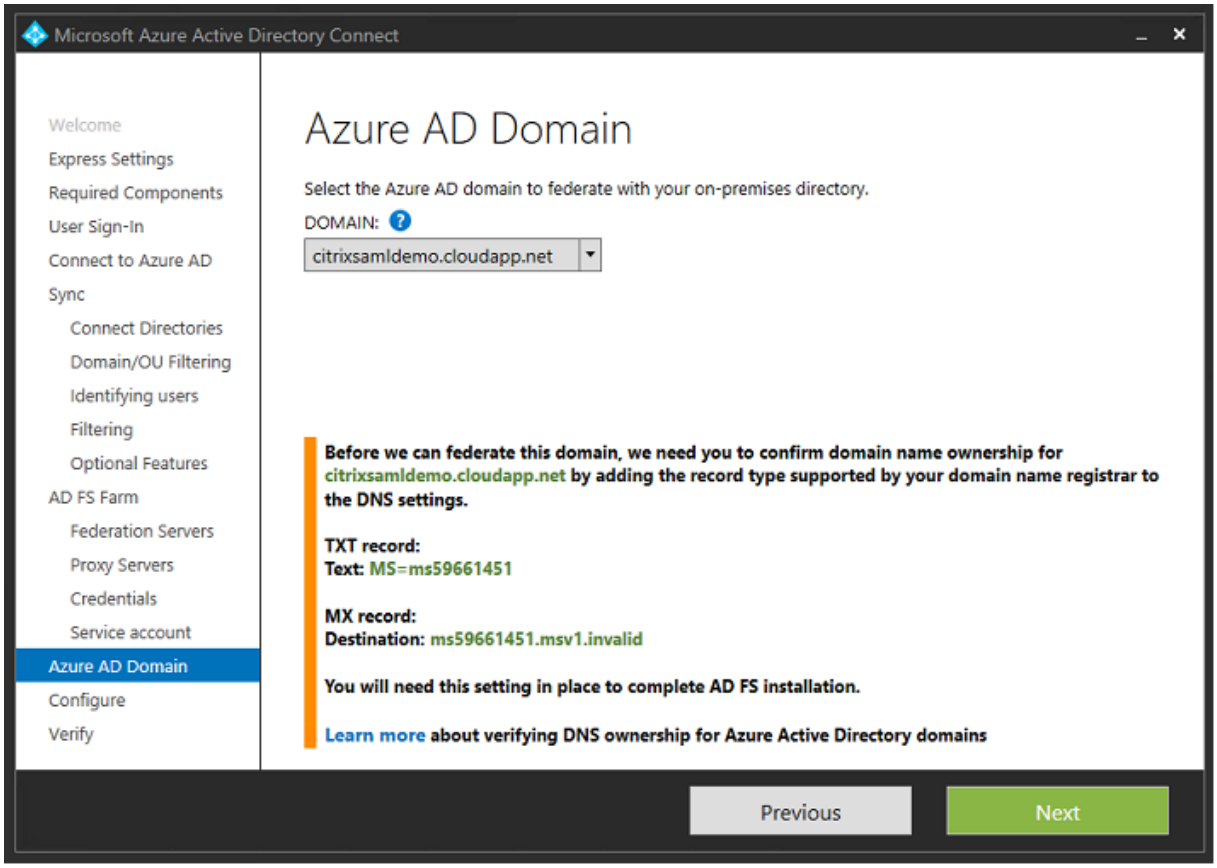
© 1999-2019 Citrix Systems, Inc. All rights reserved.



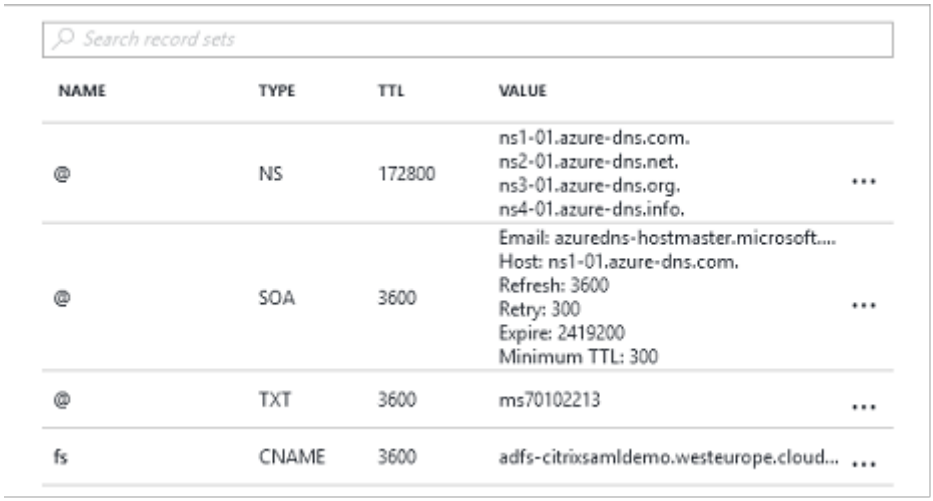
> **Nota:**
>
> Si este paso falla debido a problemas de confianza con el PowerShell remoto, una el servidor proxy de aplicaciones Web al dominio.

Para los pasos restantes del asistente, use las contraseñas estándar de administrador y cree una cuenta de servicio de ADFS. Azure AD Connect pedirá validar el propietario de la zona DNS.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

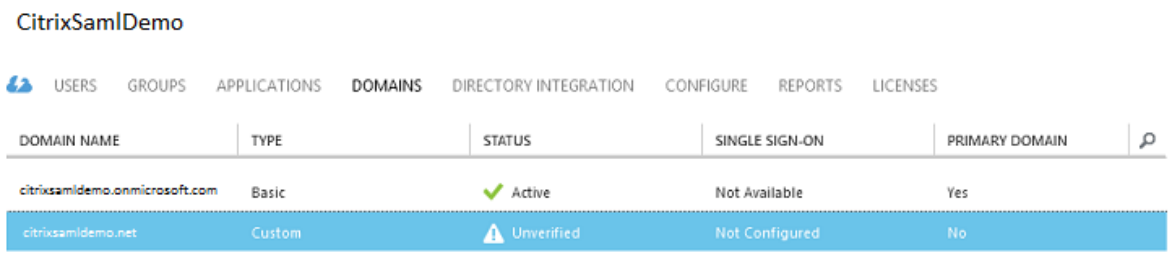


Agregue los registros TXT y MX a los registros de direcciones DNS en Azure.



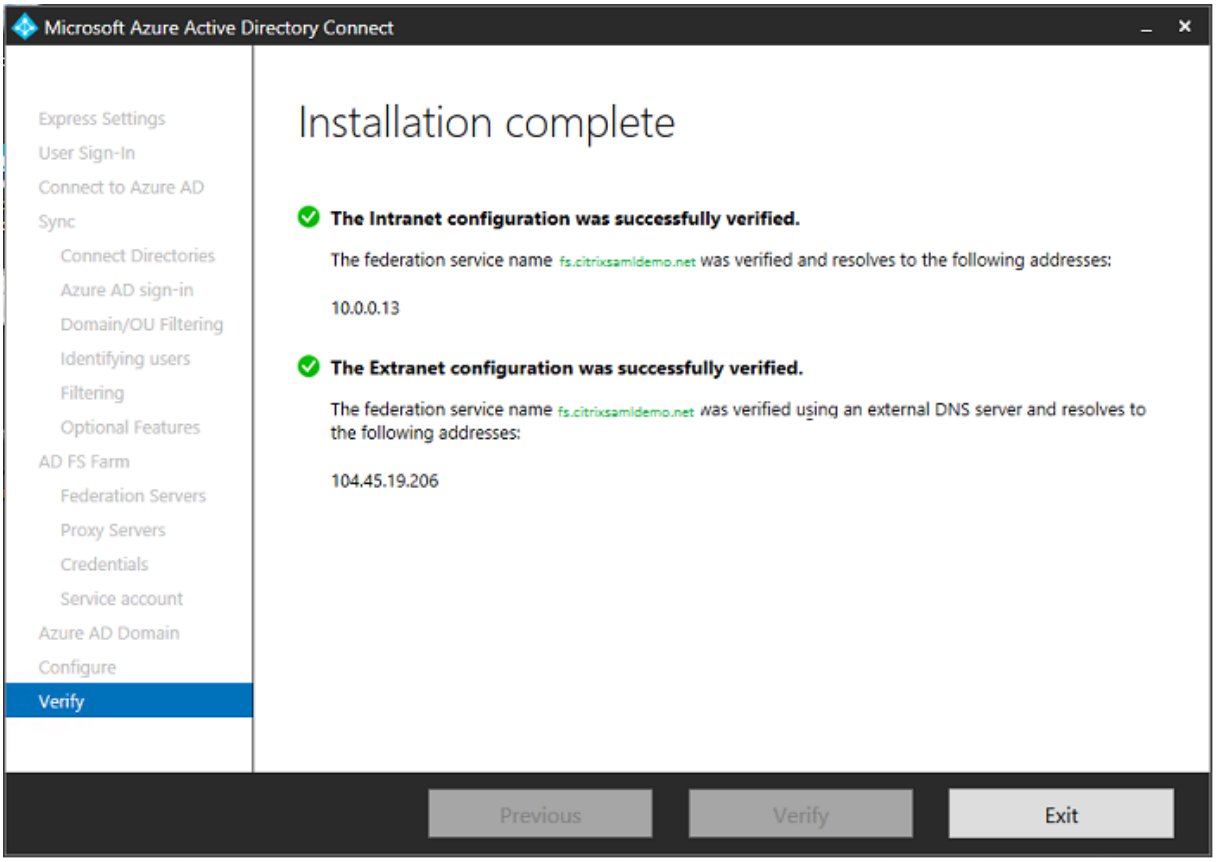
Haga clic en **Verificar** en la consola de administración de Azure.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



> **Nota:**
>
> Si este paso falla, puede verificar el dominio antes de ejecutar Azure AD Connect.

Una vez completado, se contacta con la dirección externa fs.citrixsamldemo.net a través del puerto 443.

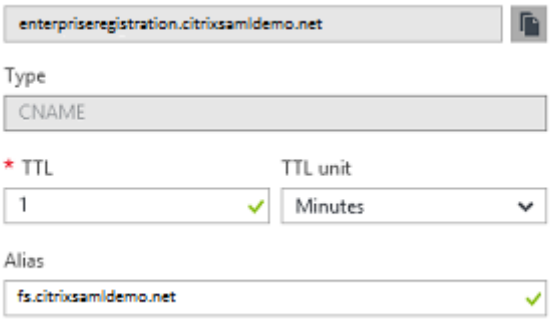


Habilitar la función Unirse a Azure AD

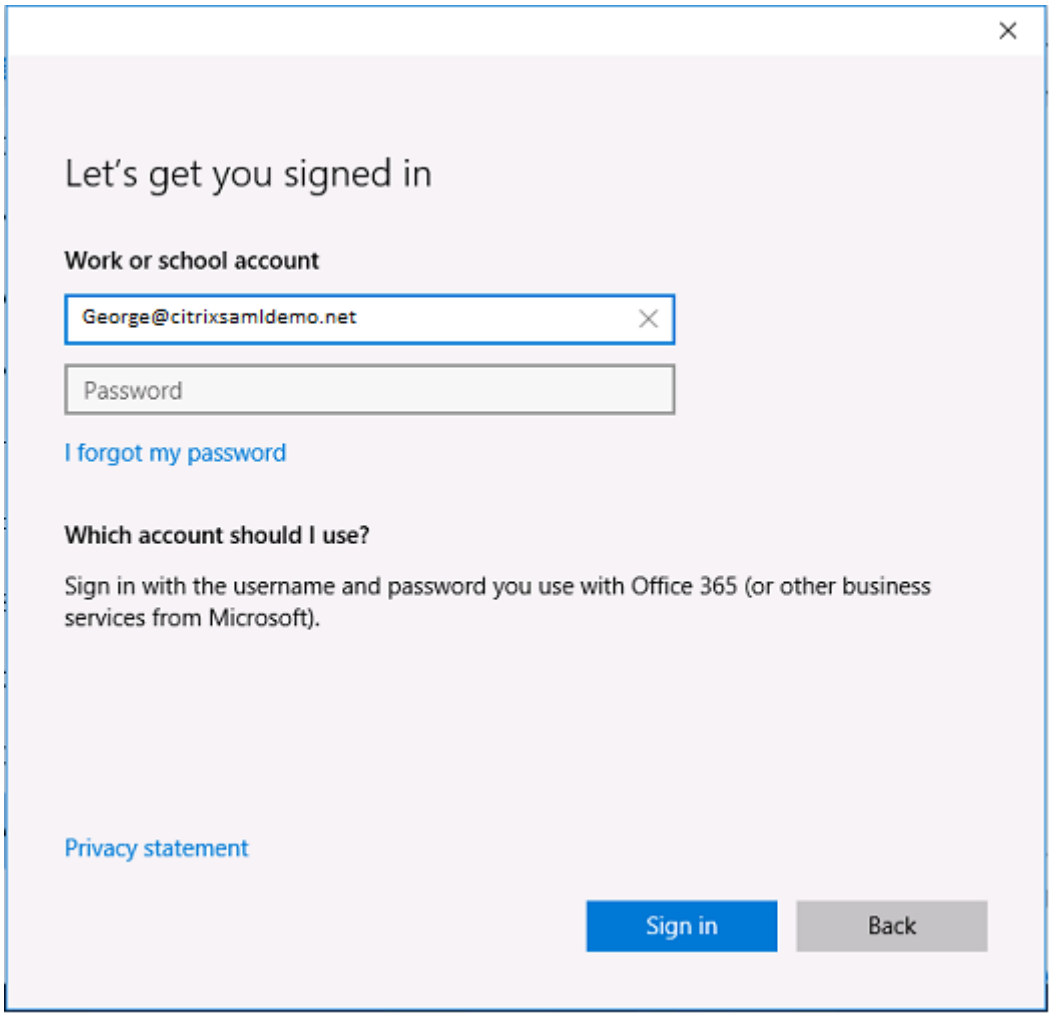
Cuando un usuario introduce una dirección de correo electrónico para que Windows 10 pueda unirse a Azure AD, se usa el sufijo DNS para crear un registro DNS CNAME que debe apuntar a ADFS: enterpriseregistration.<*sufijoUPN*>.

En el ejemplo, es `fs.citrixsamldemo.net`.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

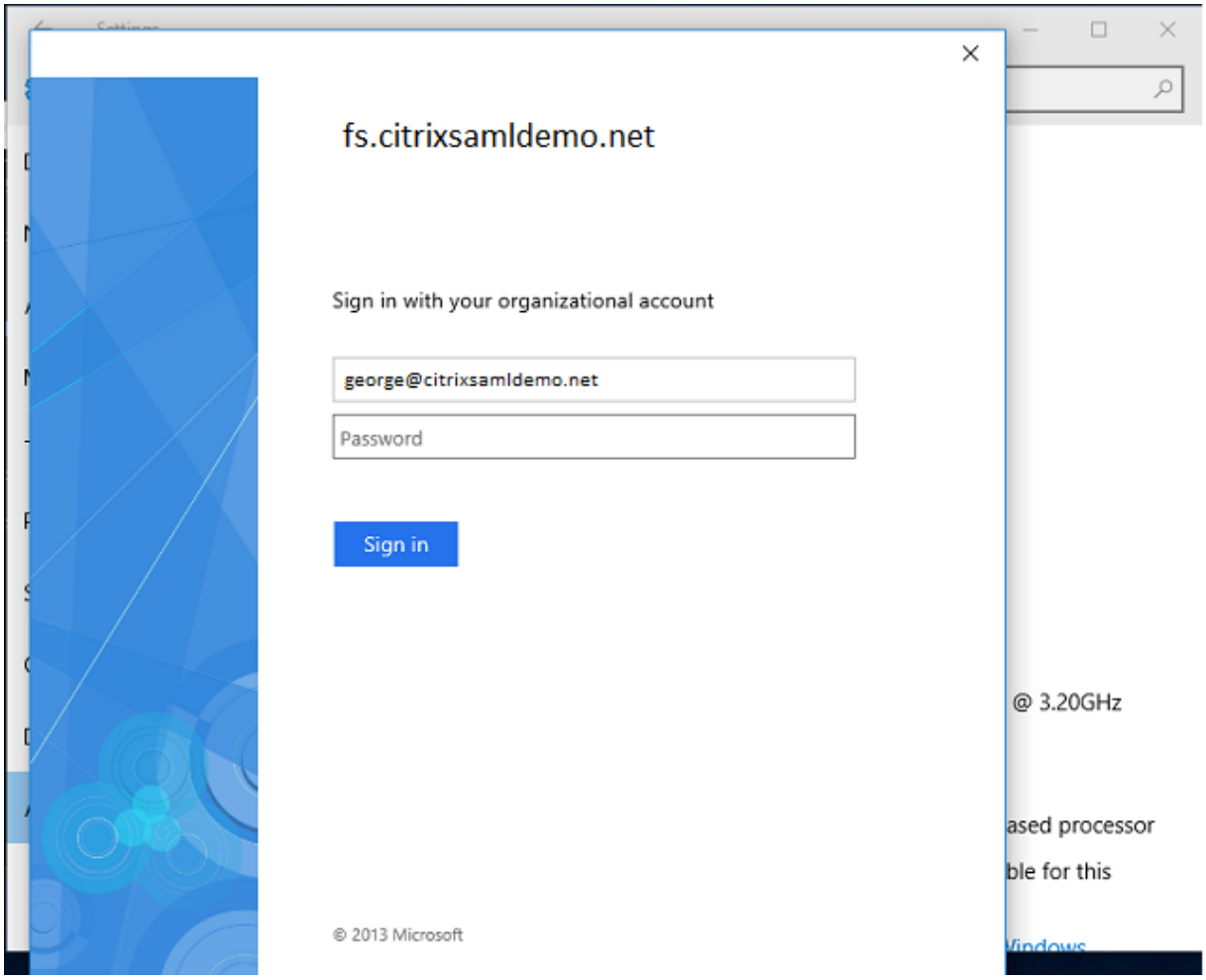


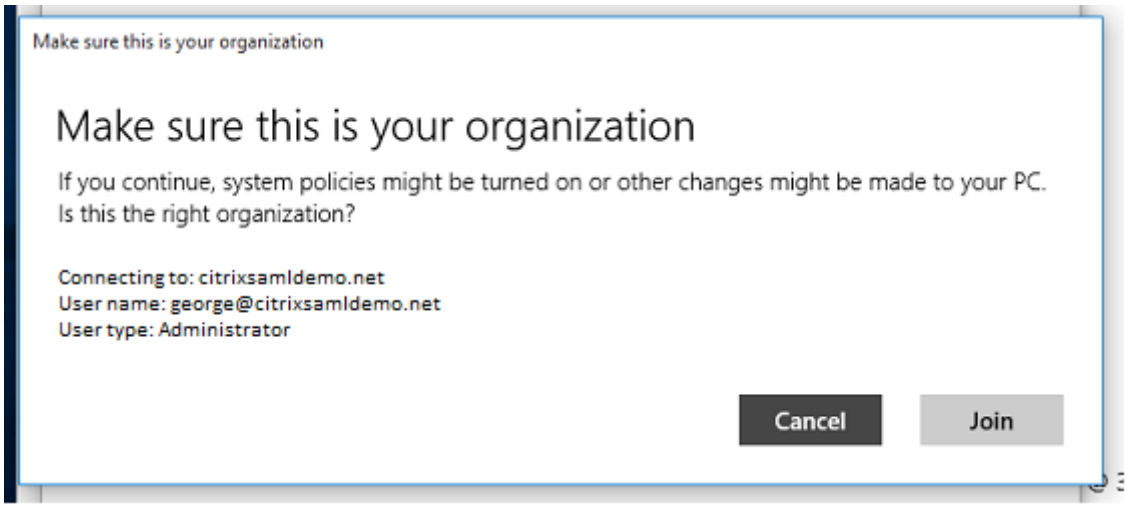
Si no está usando una entidad de certificación CA pública, asegúrese de que el certificado raíz de ADFS está instalado en el equipo con Windows 10 de modo que Windows confié en el servidor ADFS. Realice la unión con el dominio de Azure AD utilizando la cuenta de usuario estándar generada anteriormente.



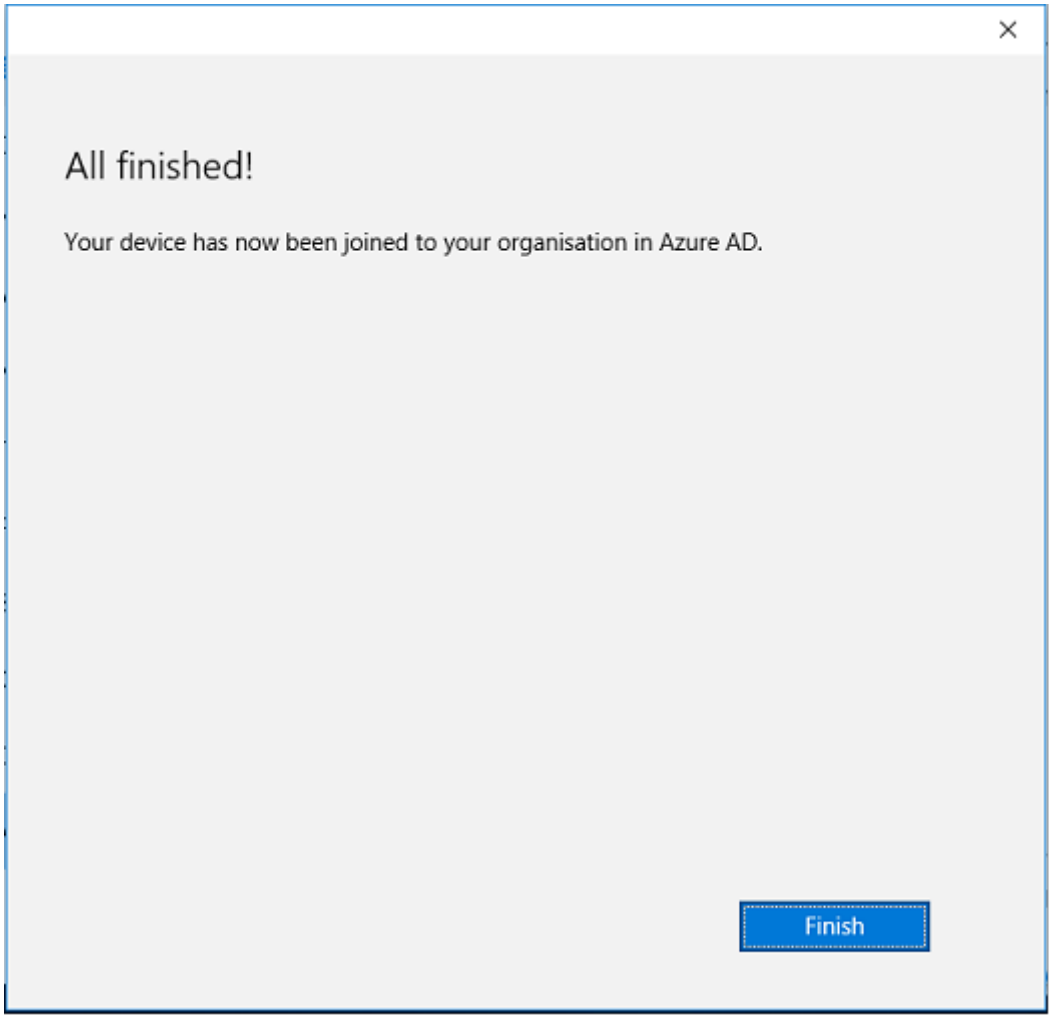
Tenga en cuenta que el nombre UPN debe coincidir con el nombre UPN reconocido por el controlador de dominio de ADFS.

© 1999-2019 Citrix Systems, Inc. All rights reserved.





© 1999-2019 Citrix Systems, Inc. All rights reserved.



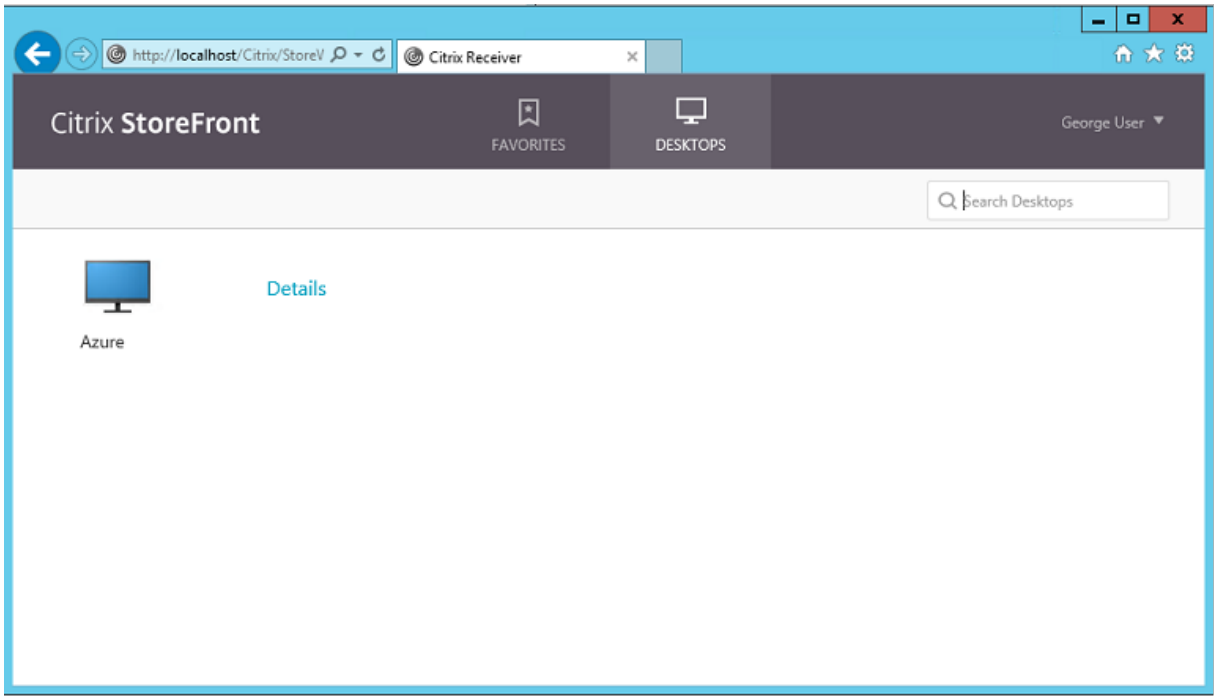
Verifique que la máquina se ha unido al dominio de Azure AD. Para ello, reinicie la máquina e inicie sesión usando la dirección de correo electrónico del usuario. Una vez iniciada la sesión, abra Microsoft Edge y conéctese a http://myapps.microsoft.com. El sitio web debe utilizar Single Sign-On automáticamente.

Instalar Citrix Virtual Apps o Citrix Virtual Desktops

Puede instalar las máquinas virtuales del Delivery Controller y los VDA directamente en Azure desde la imagen ISO de Citrix Virtual Apps o Citrix Virtual Desktops de la forma habitual.

En este ejemplo, StoreFront se instala en el mismo servidor que el Delivery Controller. El VDA se instala como una máquina de trabajo Windows 2012 R2 RDS independiente, sin integración con Machine Creation Services (aunque esto puede configurarse si se prefiere). Compruebe que el usuario Jorge@citrixsamldemo.net se puede autenticar con una contraseña, antes de continuar.

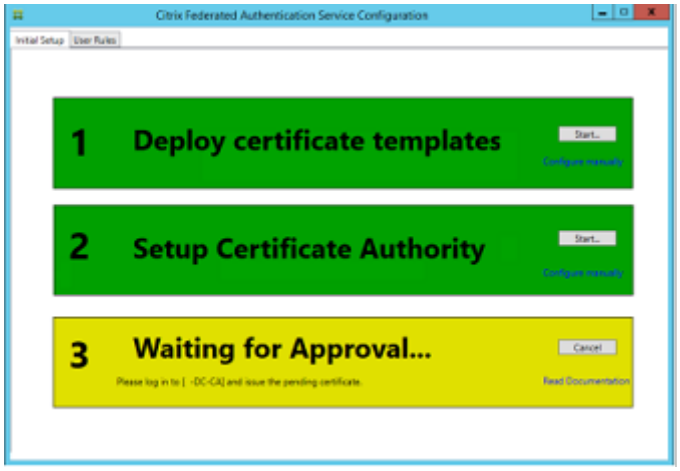
© 1999-2019 Citrix Systems, Inc. All rights reserved.



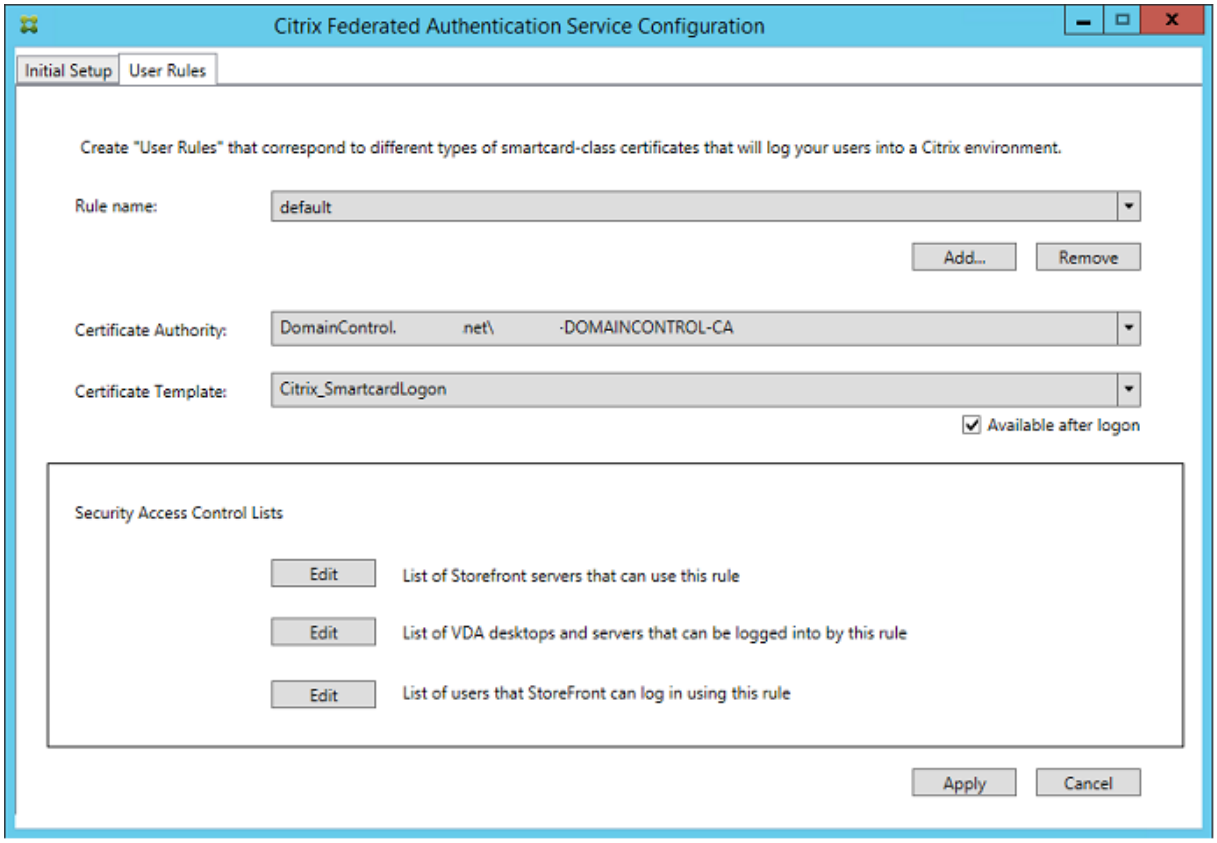
Ejecute el cmdlet **Set-BrokerSite –TrustRequestsSentToTheXmlServicePort $true** de PowerShell en el Controller para permitir que StoreFront se autentique sin las credenciales de los usuarios.

Instalar el Servicio de autenticación federada

Instale el componente del Servicio de autenticación federada FAS (Federated Authentication Service) en el servidor ADFS y configure una regla para que el Controller actúe como un StoreFront de confianza.



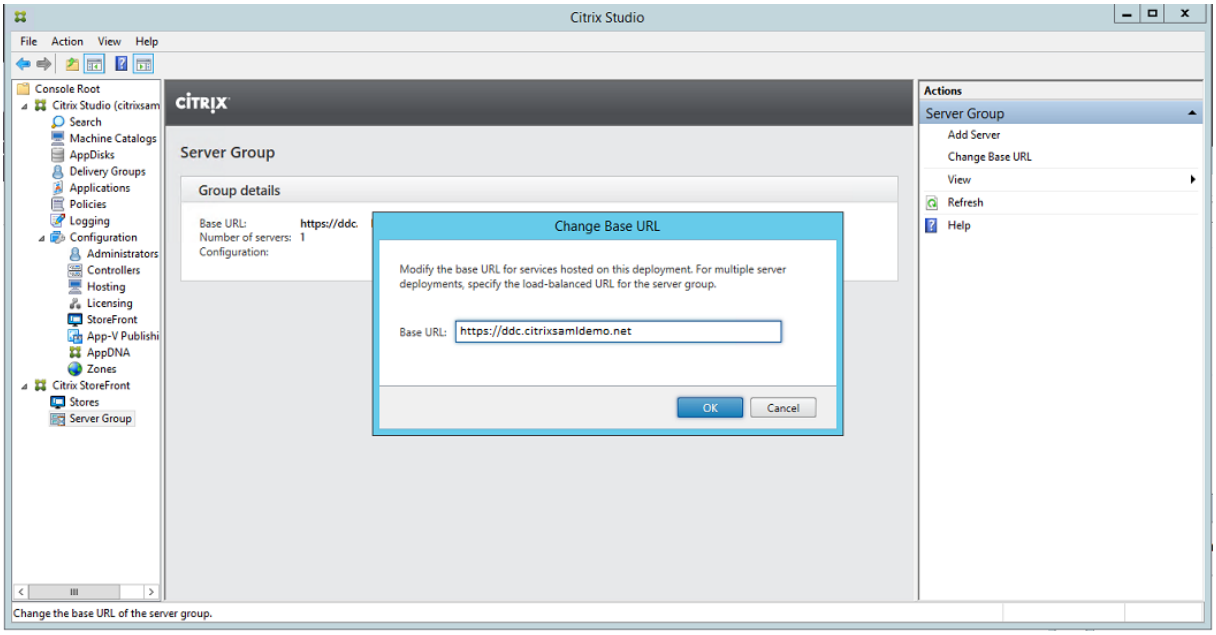
© 1999-2019 Citrix Systems, Inc. All rights reserved.



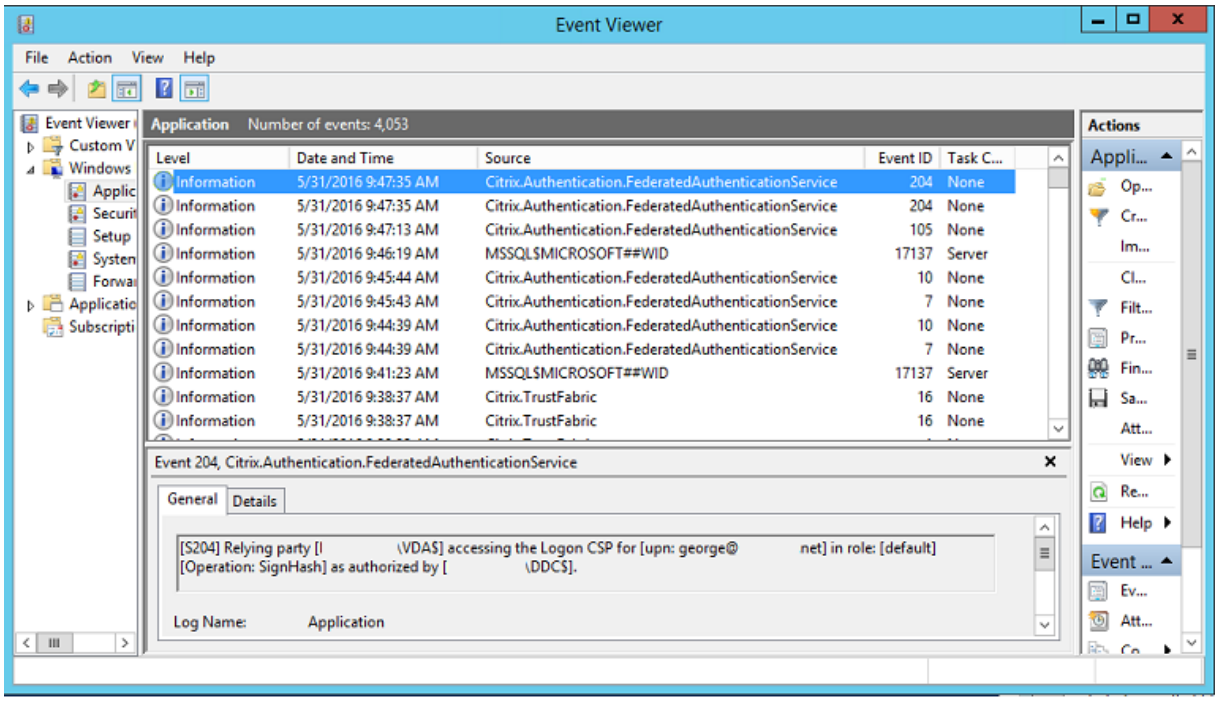
Configurar StoreFront

Solicite un certificado de equipo para el Delivery Controller y configure IIS y StoreFront para usar HTTPS estableciendo un enlace de IIS para el puerto 443 y cambiando la dirección de base de datos de StoreFront a https:.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



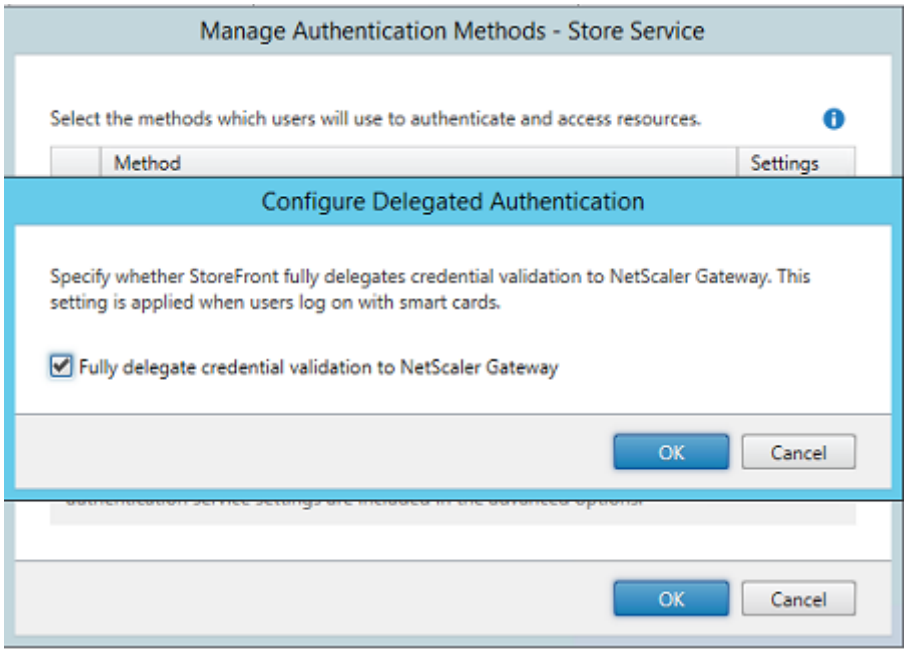
Configure StoreFront para usar el servidor de FAS (use el script de PowerShell en el artículo Servicio de autenticación federada), y haga pruebas internamente dentro de Azure, para asegurarse de que el inicio de sesión usa el servicio FAS consultando el visor de eventos en el servidor FAS.



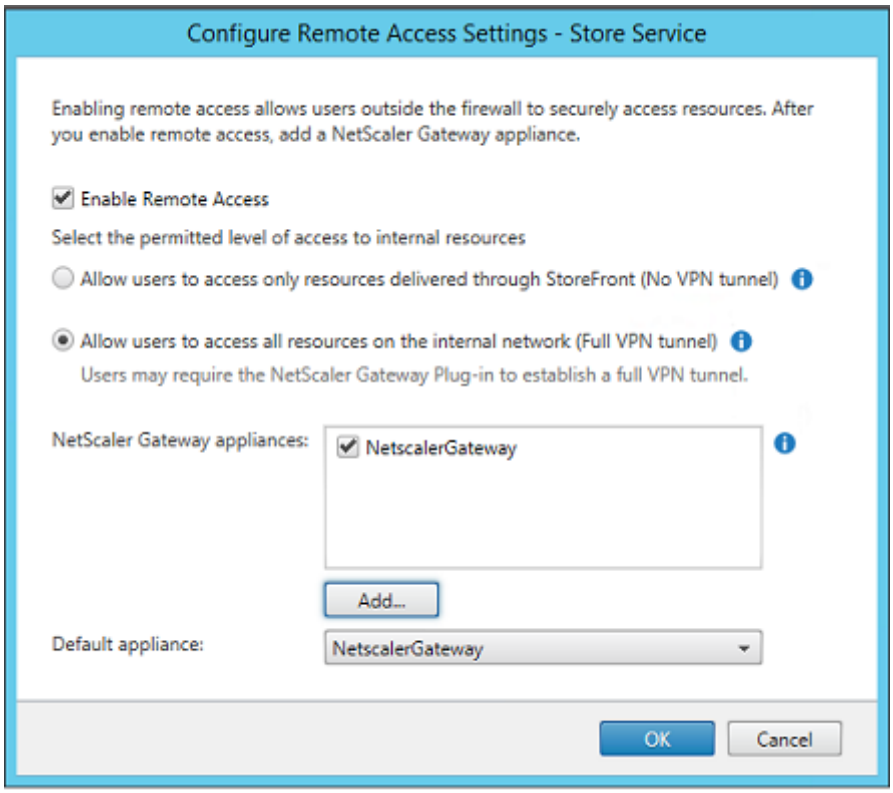
Configurar StoreFront para usar NetScaler

Mediante la interfaz de usuario de **Administrar métodos de autenticación** en la consola de administración de StoreFront, configure StoreFront para que utilice NetScaler para realizar la autenticación.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



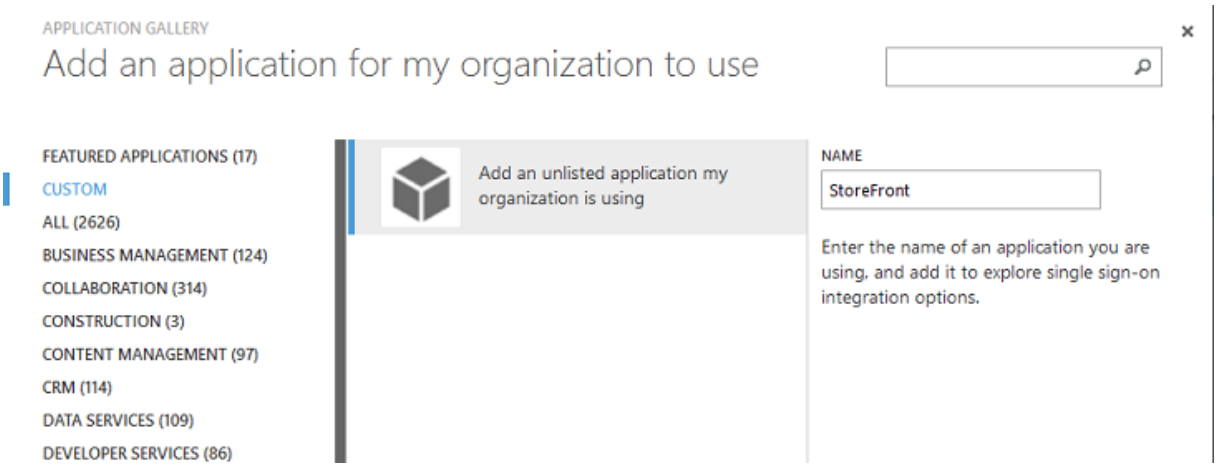
Para integrar las opciones de autenticación de NetScaler, configure Secure Ticket Authority (STA) y configure la dirección de NetScaler Gateway.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurar una nueva aplicación de Azure AD para inicios Single Sign-On en StoreFront

En esta sección se usan las funciones de Single Sign-on de Azure AD SAML 2.0, que actualmente requieren una suscripción de Azure Active Directory Premium. En la herramienta de administración de Azure AD, seleccione **Nueva aplicación** y elija **Agregar una aplicación de la galería**.



Seleccione **Personalizado > Agregar una aplicación que no figura en la lista que mi organización está usando** para crear una nueva aplicación personalizada para los usuarios.

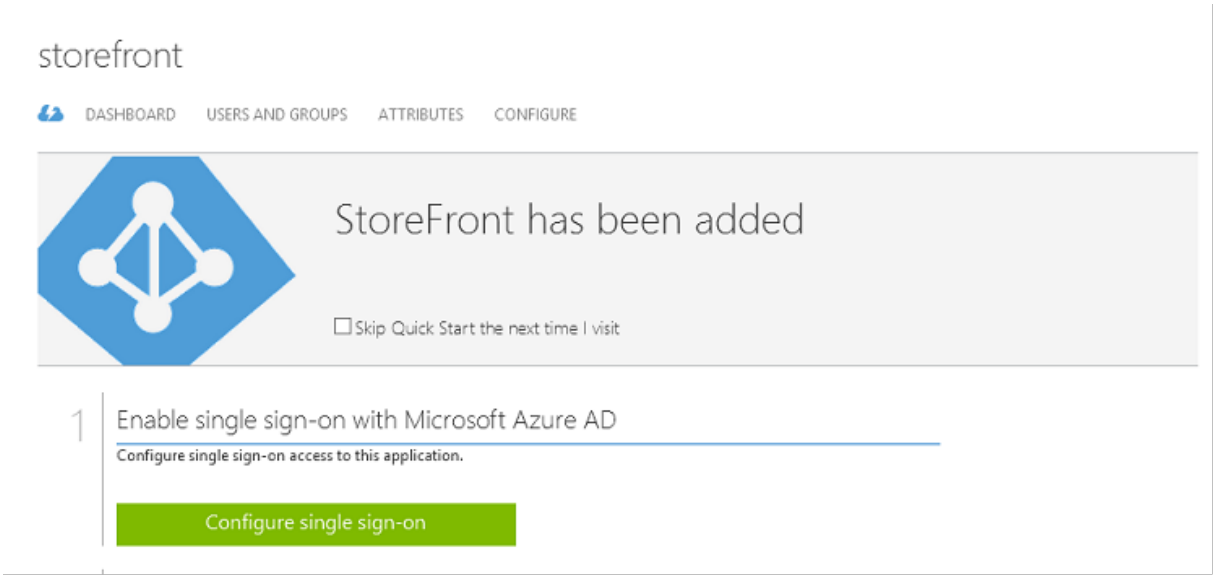
Configurar un icono

Cree una imagen de 215 x 215 píxeles de tamaño y cárguela en la página CONFIGURAR para usarla como icono de la aplicación.

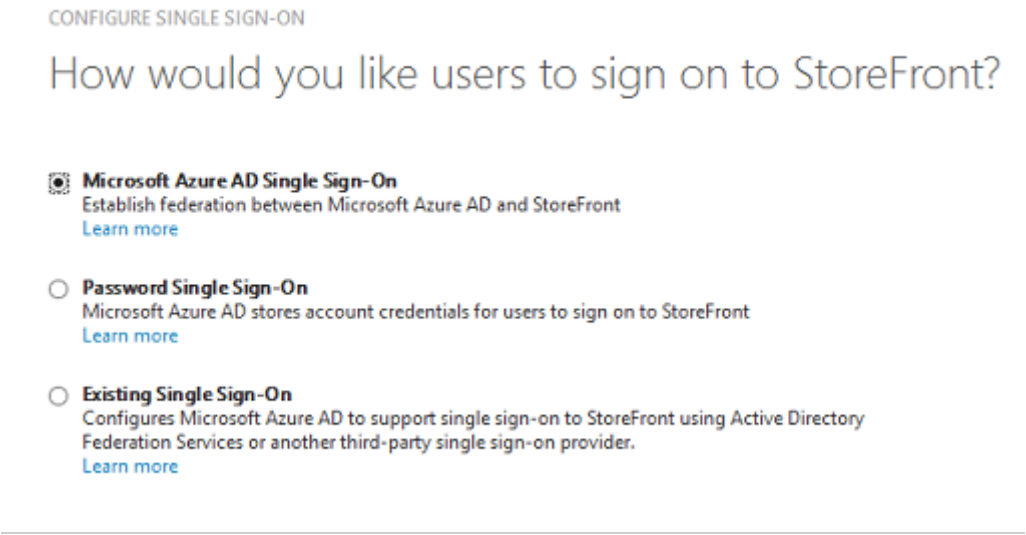
Configurar la autenticación SAML

Vuelva a la página introductoria Panel de la aplicación y seleccione **Configurar Single Sign-On**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

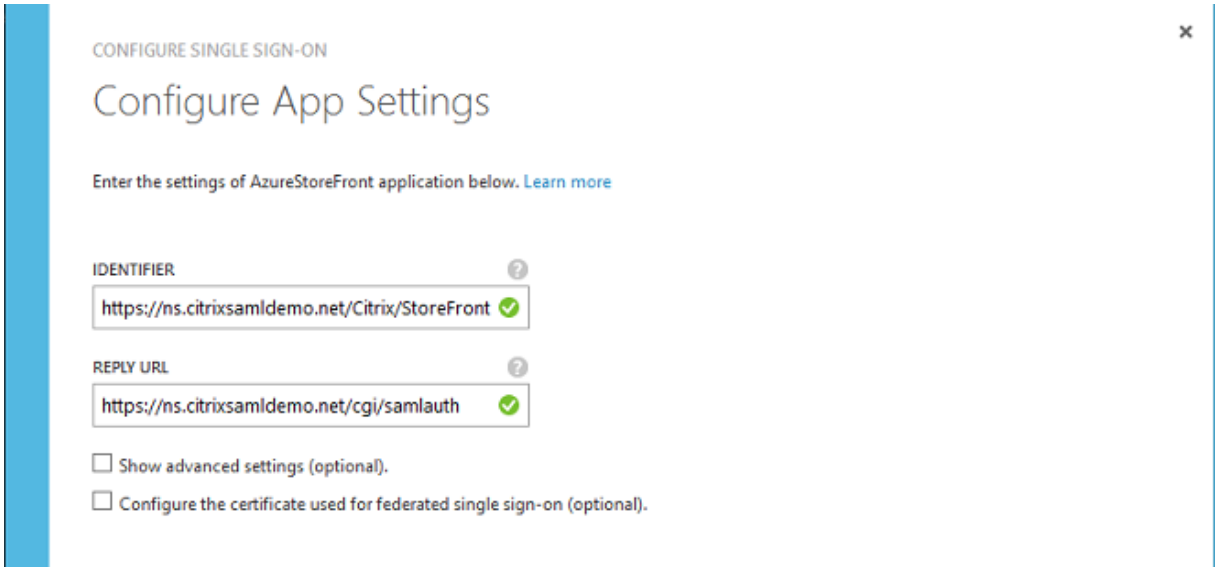


Esta implementación utilizará la autenticación SAML 2.0, que corresponde a **Microsoft Azure AD Single Sign-On**.

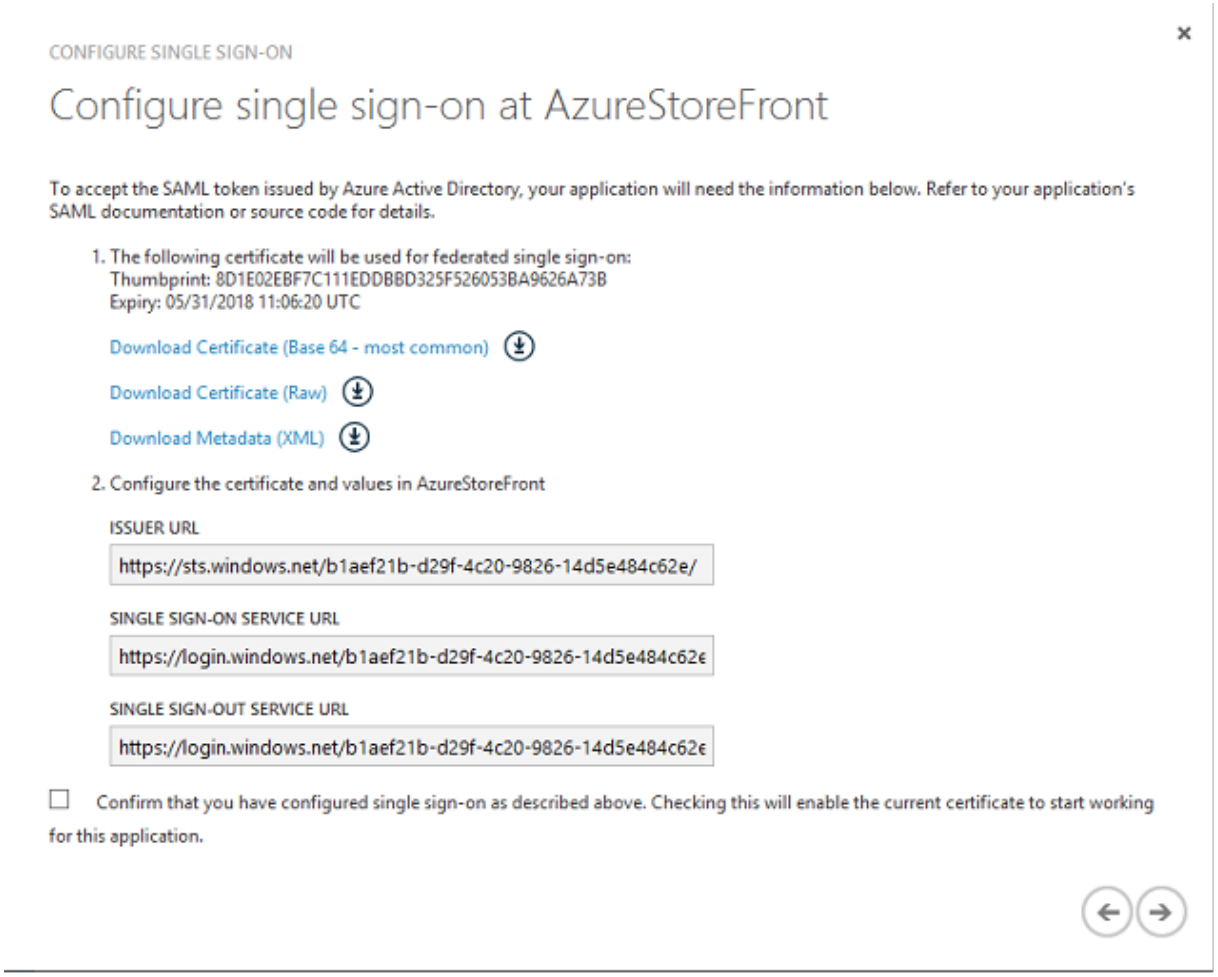


La cadena de identificación **Identifier** puede ser una cadena arbitraria (debe coincidir con la configuración suministrada a NetScaler); en este ejemplo, la **URL de respuesta**, Reply URL, es */cgi/samlauth* en el servidor NetScaler.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



La siguiente página contiene información que se usa para configurar NetScaler como una parte de confianza para Azure AD.



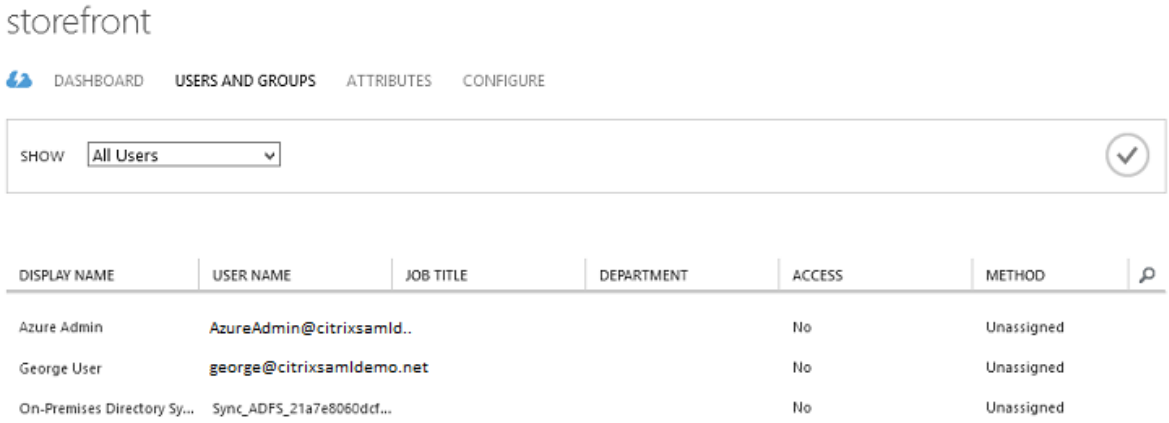
Descargue el certificado de firma de confianza de base 64 y copie las URL de inicio y cierre de sesión.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Pegará estas URL en las pantallas de configuración de NetScaler más adelante.

Asignar la aplicación a los usuarios

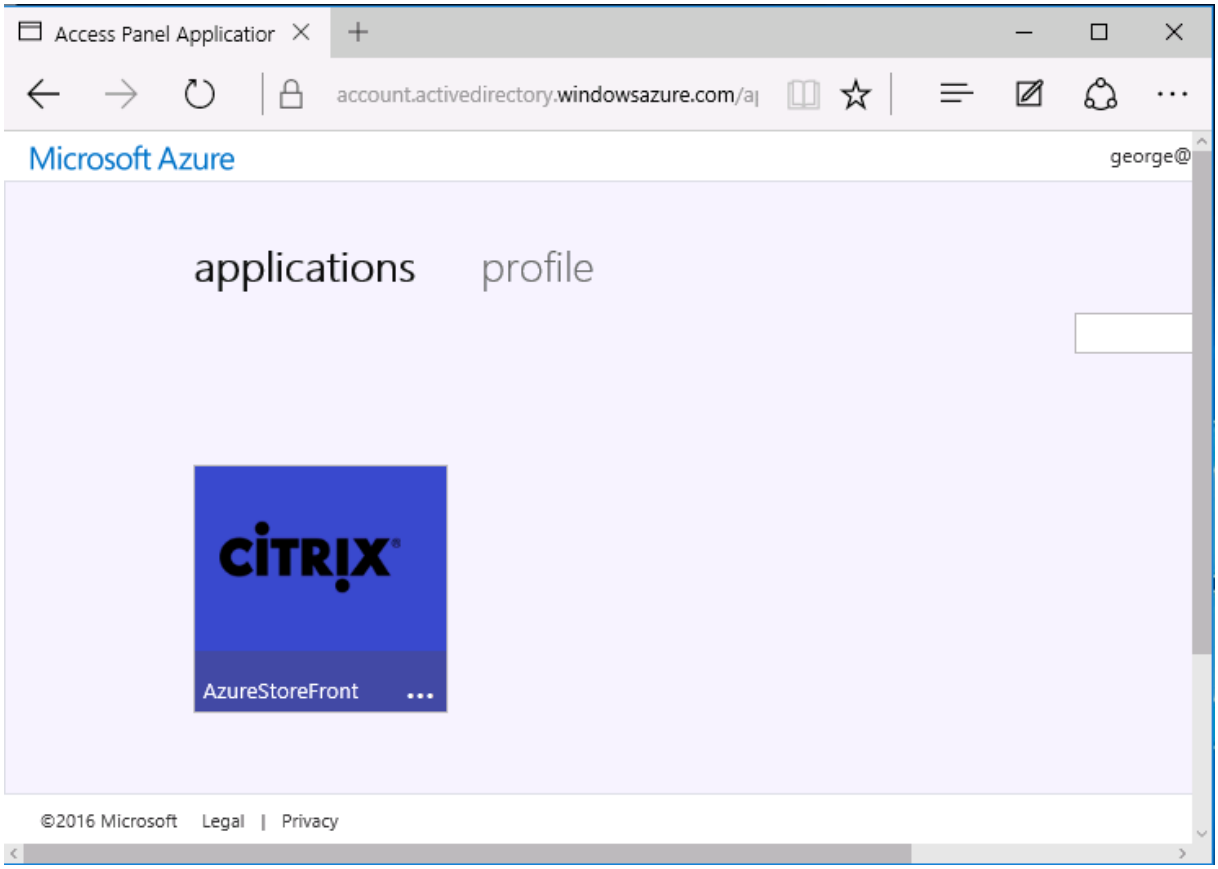
El paso final es habilitar la aplicación de modo que aparezca en la página de control “myapps.microsoft.com” de los usuarios. Esto se realiza en la página Usuarios y grupos. Asigne acceso para las cuentas de usuarios de domino sincronizadas por Azure AD Connect. También puede usar otras cuentas, pero deben estar explícitamente asignadas, porque no cumplen el formato <usuario>@<dominio>.



Página MyApps

Cuando la aplicación se ha configurado, aparece en las listas de los usuarios de las aplicaciones de Azure cuando visitan https://myapps.microsoft.com.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

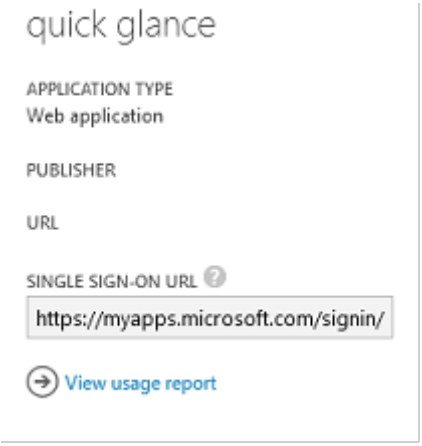


Cuando está unido a Azure AD, Windows 10 admite el inicio de sesión único Single Sign-on en las aplicaciones de Azure para el usuario que inicie sesión. Al hacer clic en el icono, el explorador va a la página de SAML cgi/samlauth que se configuró anteriormente.

URL de Single Sign-on

Vuelva a la aplicación en el panel de mandos de Azure AD. Ahora hay una URL de Single Sign-on disponible para la aplicación. Esta dirección URL se utiliza para proporcionar enlaces de explorador Web o crear accesos directos del menú Inicio que llevan a los usuarios directamente a StoreFront.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Pegue la dirección URL en un explorador Web para asegurarse de que Azure AD le redirige a la página Web de NetScaler cgi/samlauth configurada anteriormente. Este sistema funciona solamente para los usuarios que se han asignado y ofrecerá inicio de sesión único Single Sign-on solo para sesiones de inicio de sesión en Windows 10 unido a Azure AD. (A otros usuarios se les pedirán credenciales de Azure AD.)

Instalar y configurar NetScaler Gateway

Para acceder de manera remota a la implementación, en este ejemplo se utiliza una VM independiente que ejecuta NetScaler. Esta VM se puede adquirir en Azure Store. En este ejemplo, se usa la opción “Bring your own License” de NetScaler 11.0.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

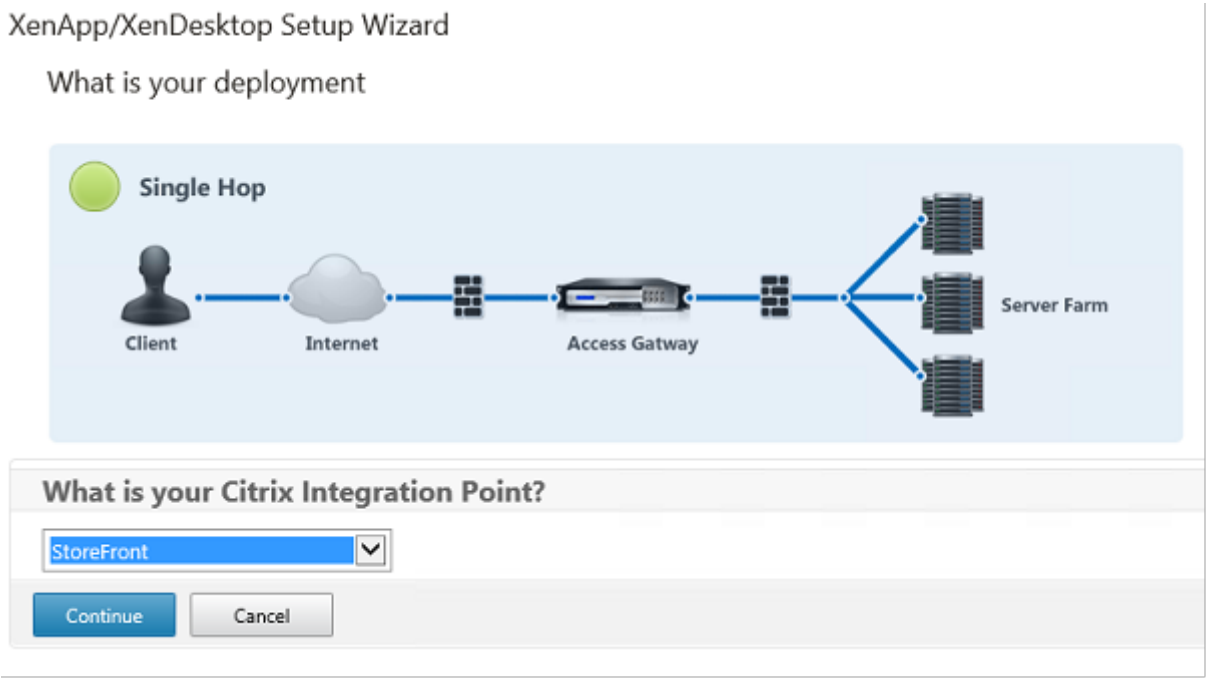
Inicie sesión en la VM de NetScaler, apuntando el explorador Web a la dirección IP interna, usando las credenciales especificadas cuando el usuario se autenticó. Tenga en cuenta que se debe cambiar la contraseña del usuario nsroot en una VM de Azure AD.

Agregue licencias, seleccionando **reboot** después de agregar cada una de ellas, y apunte la resolución DNS al controlador de dominio de Microsoft.

Ejecutar el asistente de configuración de Citrix Virtual Apps and Desktops

Este ejemplo empieza configurando una integración simple de StoreFront sin SAML. Una vez que esta implementación está funcionando, agrega una directiva de inicio de sesión de SAML.

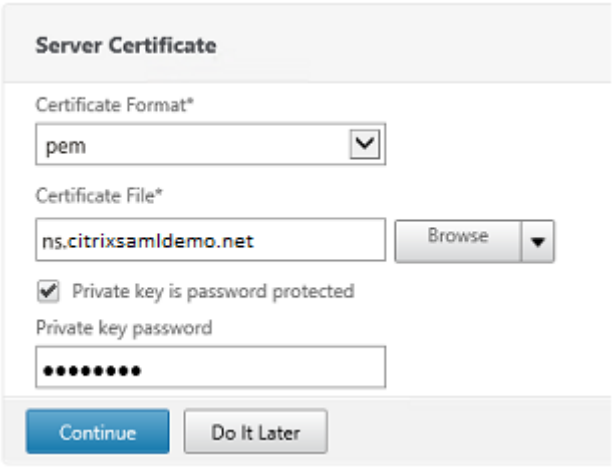
© 1999-2019 Citrix Systems, Inc. All rights reserved.



Seleccione los parámetros estándar de NetScaler de StoreFront. Para usarlo en Microsoft Azure, en este ejemplo se configura el puerto 4433, en lugar del puerto 443. De forma alternativa, puede redirigir el puerto o reasignar el sitio Web de administración de NetScaler.

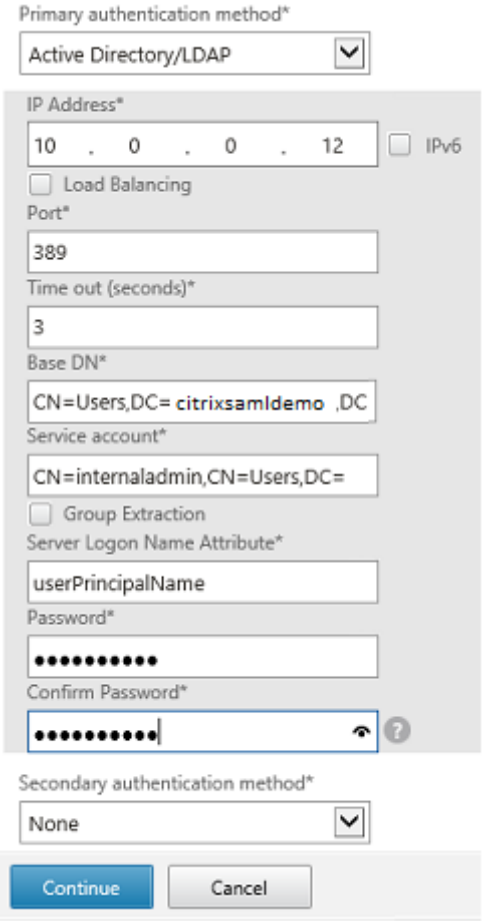
Para simplificar las tareas, el ejemplo carga un certificado de servidor existente y una clave privada guardada en un archivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Configurar el controlador de dominio para la administración de cuentas de AD

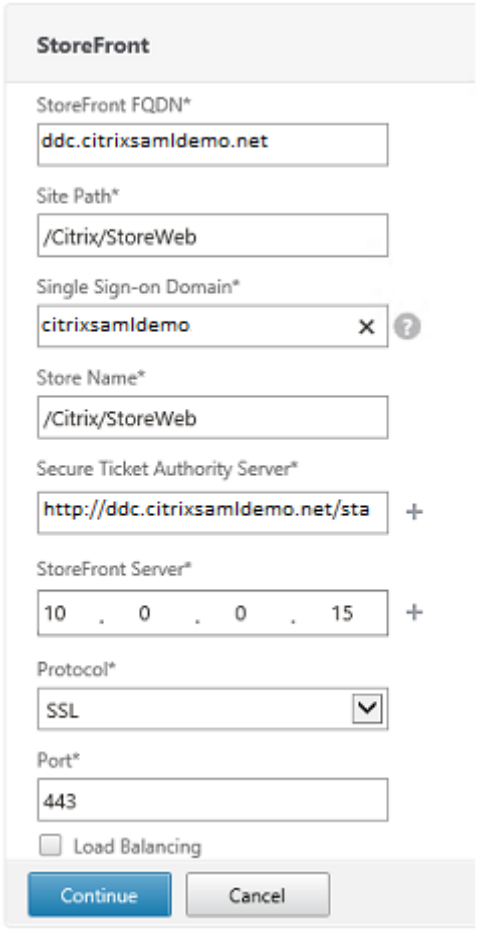
El controlador de dominio se usará para la resolución de cuentas, por lo que hay que agregar su dirección IP en el método de autenticación principal. Tenga en cuenta el formato esperado en cada campo en el cuadro de diálogo.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

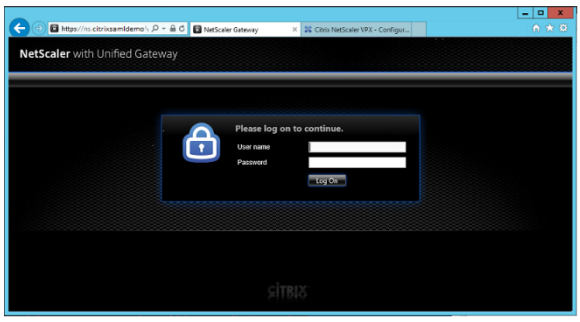
Configurar la dirección de StoreFront

En este ejemplo, StoreFront se ha configurado usando HTTPS, por lo tanto, seleccione las opciones de protocolo SSL.



Verificar la implementación de NetScaler

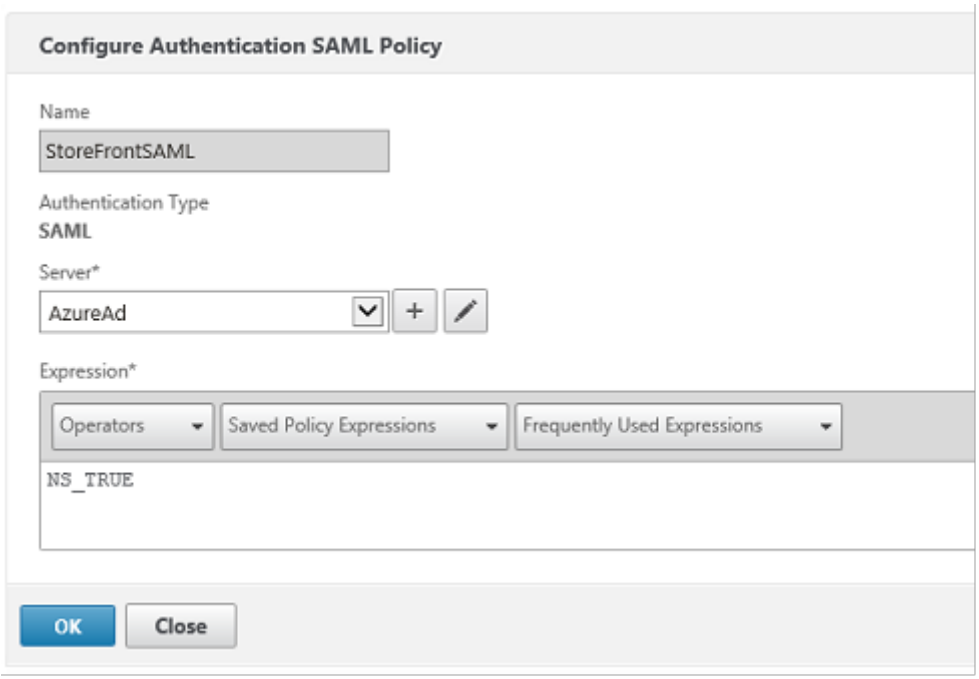
Conéctese a NetScaler y compruebe que la autenticación y el inicio se realizan correctamente con el nombre de usuario y la contraseña.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

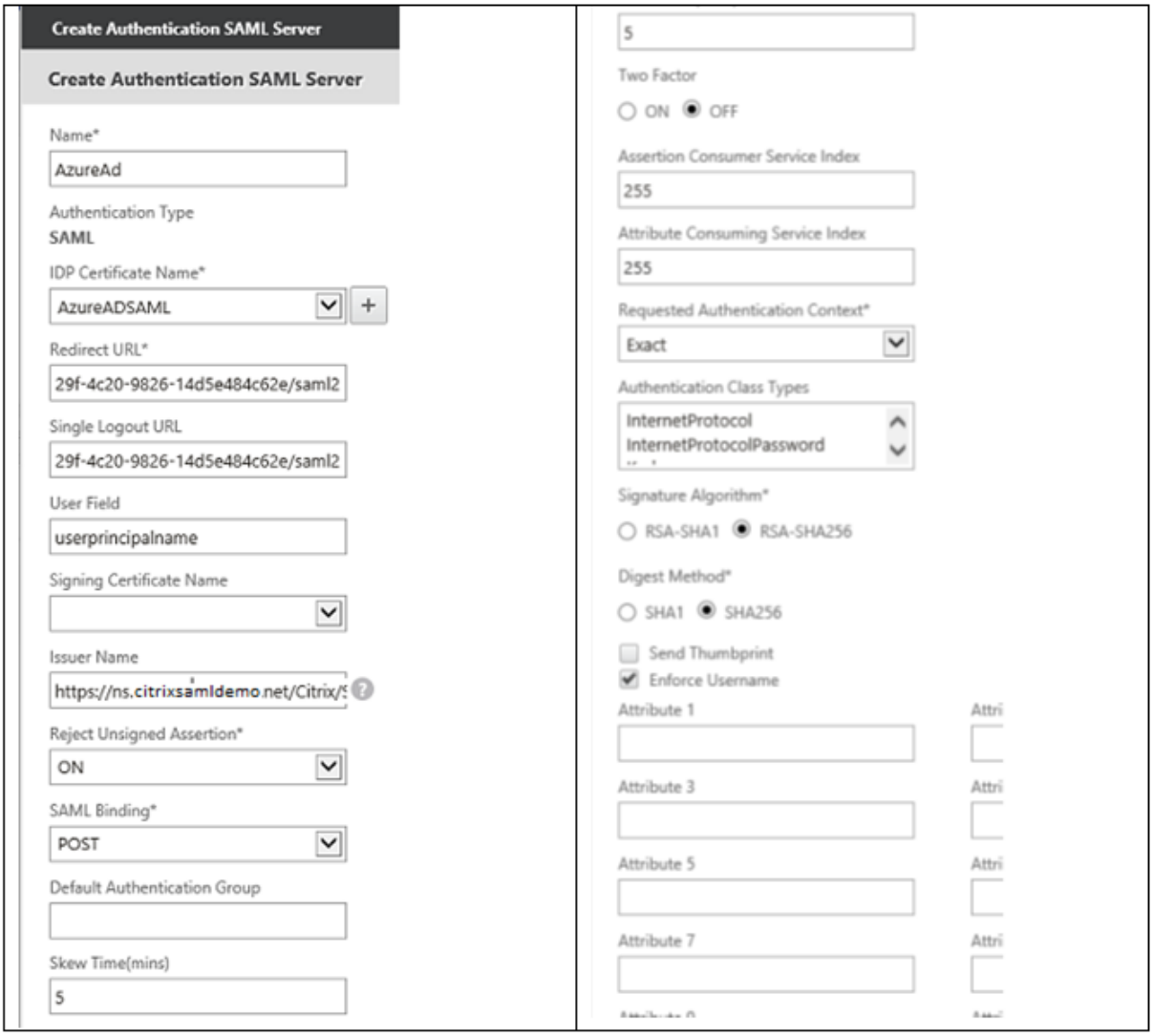
Habilitar el respaldo para la autenticación SAML

El uso de SAML con StoreFront es similar al uso de SAMI con otros sitios Web. Agregue una nueva directiva de SAML, con una expresión de **NS_TRUE**.



Configurar el servidor de identidades SAML, mediante la información obtenida de Azure AD previamente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

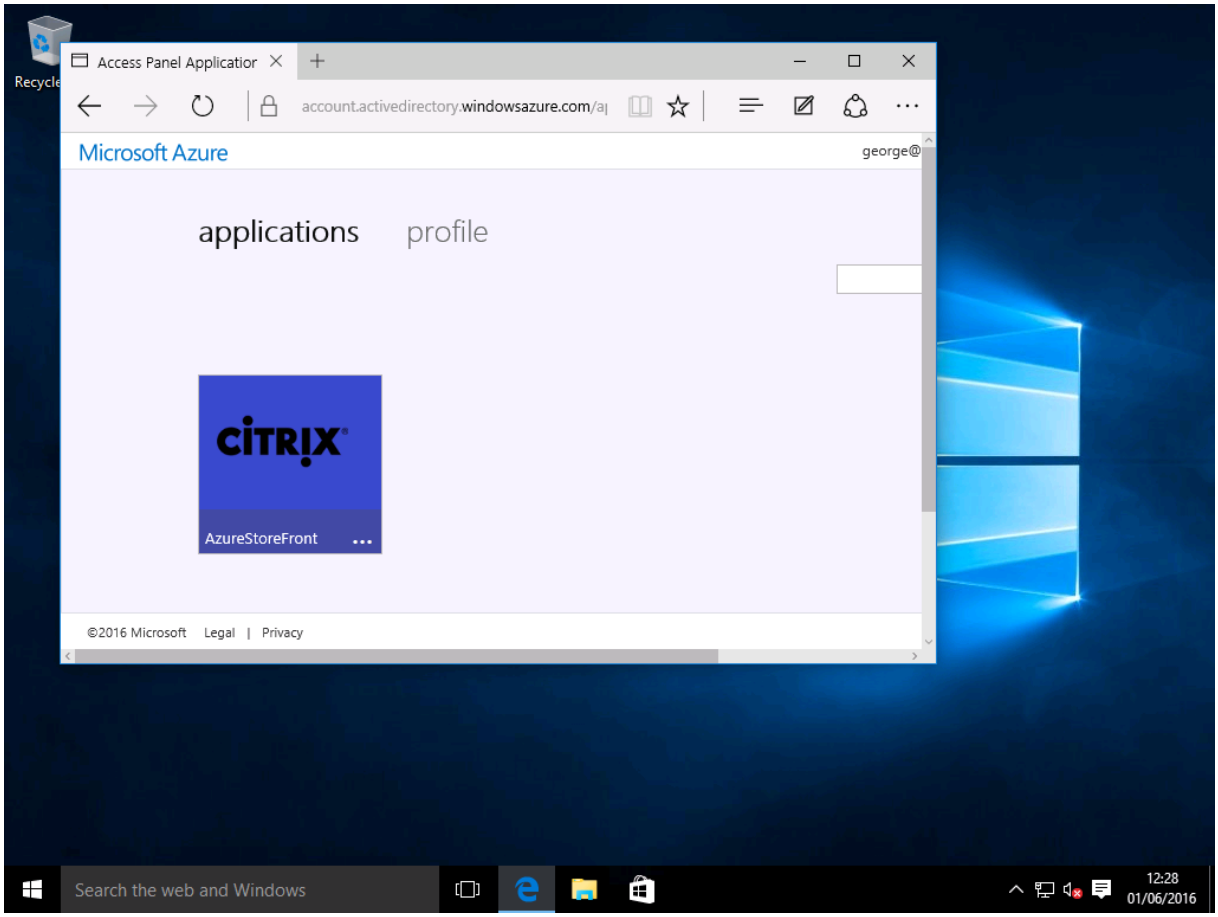


Verificar el sistema de extremo a extremo

Inicie sesión en un escritorio de Windows 10 unido a Azure AD, usando una cuenta registrada en Azure AD. Inicie Microsoft Edge y conéctese a: https://myapps.microsoft.com.

El explorador Web debe mostrar las aplicaciones de Azure AD para el usuario.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Compruebe que hacer clic en el icono que se le redirige a un servidor StoreFront autenticado.

Del mismo modo, compruebe que las conexiones directas a través de la URL de Single Sign-on y una conexión directa con el sitio de NetScaler le redirigen a Microsoft Azure y viceversa.

Finalmente, compruebe que las máquinas que no están unidas a Azure AD también funcionan con las mismas direcciones URL (aunque habrá un único inicio de sesión explícito a Azure AD para la primera conexión).

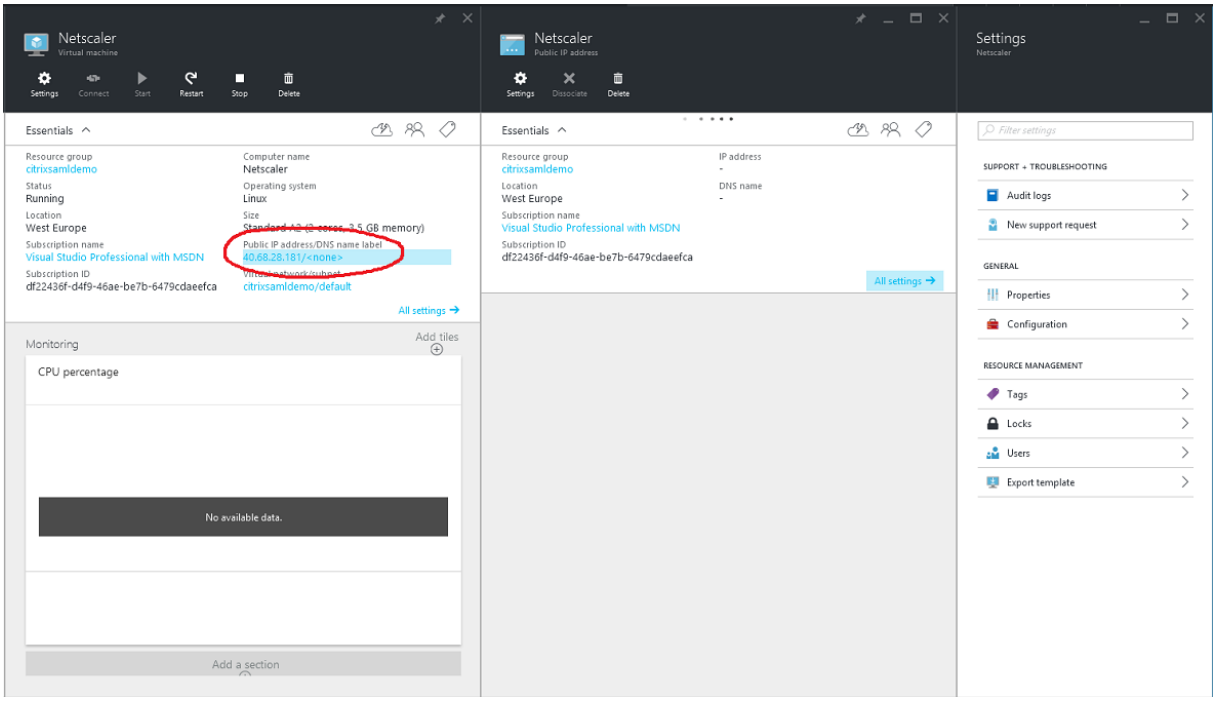
Apéndice

Debe configurar las siguientes opciones estándar cuando configure una máquina virtual en Azure.

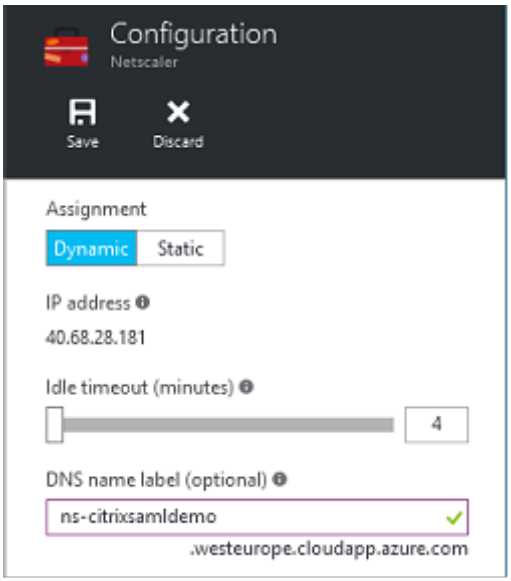
Proporcionar una dirección IP pública y una dirección DNS

Azure da a todas las VM una dirección IP en la subred interna (10.*.*.* en este ejemplo). De forma predeterminada, también se proporciona una dirección IP pública a la que se puede hacer referencia mediante una etiqueta DNS actualizada dinámicamente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Seleccione **Configuration** en **Public IP address/DNS name label**. Elija una dirección DNS pública para la VM. Se puede usar para las referencias de CNAME en otros archivos de zona DNS, asegurándose de que todos los registros DNS quedan apuntando correctamente a la VM incluso aunque la dirección IP se reasigne.



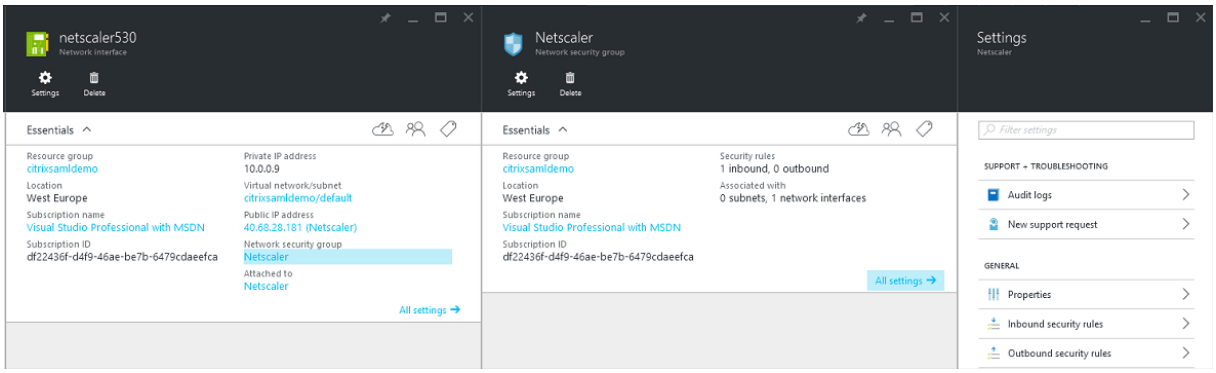
Configurar las reglas de firewall (grupo de seguridad)

Cada VM en una nube tiene un conjunto de reglas de firewall que se aplican automáticamente, lo que se conoce como el grupo de seguridad. El grupo de seguridad controla el tráfico reenviado desde la

© 1999-2019 Citrix Systems, Inc. All rights reserved.

dirección IP privada a la pública. De forma predeterminada, Azure permite el reenvío de RDP a todas las VM. Los servidores NetScaler y ADFS también deben reenviar el tráfico TLS (443).

Abra **Network Interfaces** en una VM, y luego haga clic en la etiqueta **Network Security Group**. Configure **Inbound security rules** para permitir el tráfico de red apropiado.



Información relacionada

- El artículo Servicio de autenticación federada (FAS - Federated Authentication Service) es la referencia principal para la instalación y la configuración de este servicio.
- Las implementaciones más comunes del servicio FAS se resumen en el artículo Información general de las arquitecturas del Servicio de autenticación federada.
- En el artículo Administrar y configurar el Servicio de autenticación federada, se indican otros artículos de procedimientos.

Procedimientos del sistema de autenticación federada: configuración y administración

October 3, 2018

Los siguientes artículos de procedimientos ofrecen instrucciones para la configuración y administración avanzadas del sistema de autenticación federada (FAS):

- Proteger la clave privada
- Configurar la entidad de certificación (CA)
- Seguridad y administración de red
- Solucionar problemas de inicio de sesión en Windows
- Archivos de ayuda de cmdlets del SDK de PowerShell

Información relacionada:

- El artículo Servicio de autenticación federada (FAS o Federated Authentication Service) es la referencia principal para la instalación y la configuración de este servicio.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- En el artículo Introducción a las arquitecturas del Servicio de autenticación federada se ofrece un resumen de las principales arquitecturas de FAS, además de enlaces a otros artículos sobre arquitecturas más complejas.

Configurar el Servicio de autenticación federada para la entidad de certificación

December 4, 2018

En este artículo, se describe la configuración avanzada del servicio de autenticación federada (FAS) de Citrix para que se integre con los servidores de la entidad de certificación (CA) que no admite la consola de administración de FAS. En las instrucciones, se usan las API de PowerShell que suministra el servicio FAS. Debe tener conocimientos básicos de PowerShell para poder ejecutar las instrucciones de este artículo.

Configurar varios servidores de CA para usar en FAS

En esta sección, se describe cómo configurar un servidor FAS para usar varios servidores de CA y emitir certificados. Lo que permite equilibrar la carga y conmutar por error en los servidores de CA.

Paso 1: Calcular cuántos servidores de CA puede ubicar el servicio FAS

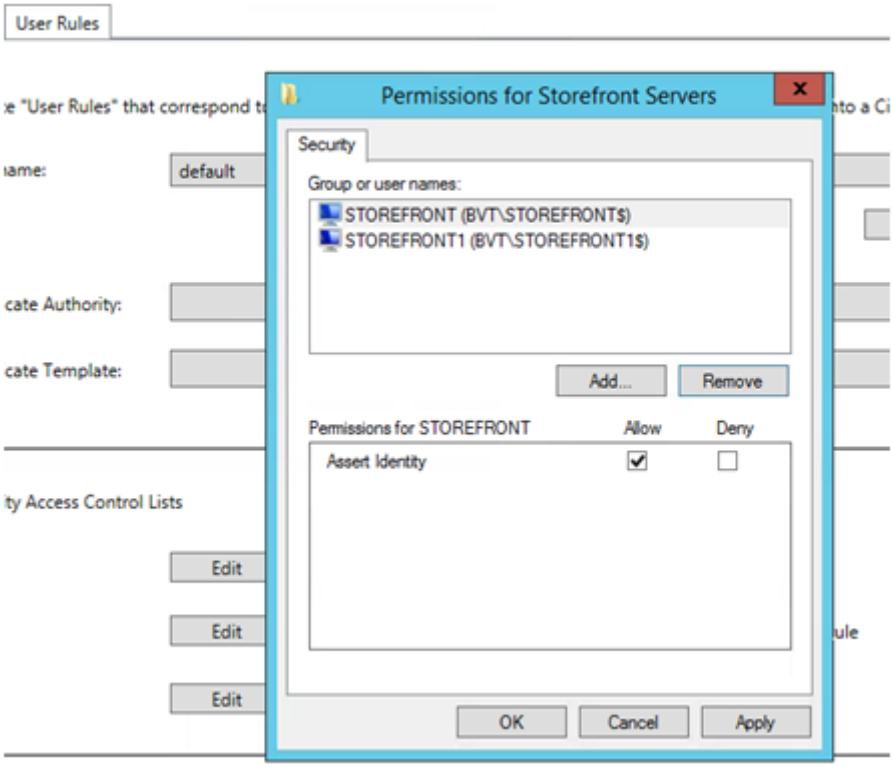
Use el cmdlet Get-FASMsCertificateAuthority para determinar a qué servidores de CA puede conectarse el servicio FAS. En el siguiente ejemplo, se muestra que FAS puede conectarse a tres servidores de CA.

```
PS > Add-PSSnapin Citrix*
PS > Get-FASMsCertificateAuthority

Address                                IsDefault PublishedTemplates
-------                                --------- ------------------
DC1.bvt.local\bvt-DC1-CA                   False {Citrix_SmartcardLogon, Citrix_Regis...
ca1.bvt.local\CA1.bvt.local                False {Citrix_SmartcardLogon, Citrix_Regis...
ca2.bvt.local\ca2.bvt.local                False {Citrix_SmartcardLogon, Citrix_Regis...
```

Paso 2: Modificar la definición de certificado existente

Citrix recomienda crear un rol mediante la consola de administración de FAS, en lugar de utilizar PowerShell para crear el rol. Esto evita la complicación de tener que agregar SDL manualmente más tarde. En el siguiente ejemplo, se crea un rol denominado “default”, con la regla de acceso:

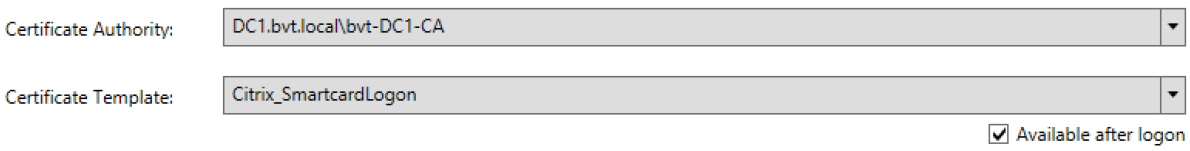
© 1999-2019 Citrix Systems, Inc. All rights reserved.



Para agregar varias entidades de certificación al campo de la entidad de certificación (característica que no se admite en la consola de administración de esta versión), debe configurar la definición de certificado. En primer lugar, necesita el nombre de la definición de certificado. Este nombre no se puede determinar a partir de la consola de administración; use el cmdlet Get-FASCertificateDefinition.

```
PS > Get-FASCertificateDefinition

Name                    : default_Definition
CertificateAuthorities  : {DC1.bvt.local\bvt-DC1-CA}
MsTemplate              : Citrix_SmartcardLogon
AuthorizationCertificate : 86ce221c-7599-43a3-9dbd-8e6a3c2be7b7
PolicyOids              : {}
InSession               : True
```

El equivalente en la interfaz de usuario es:



Una vez obtenido el nombre de la definición de certificado, modifíquela para obtener una lista de CertificateAuthorities, en lugar de una sola:

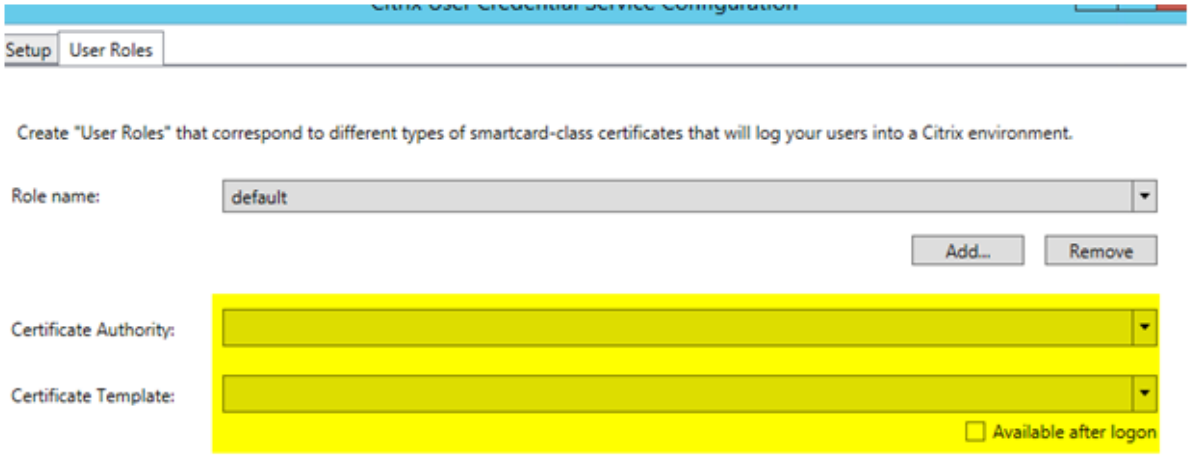
© 1999-2019 Citrix Systems, Inc. All rights reserved.

```
PS > Set-FASCertificateDefinition -Name default_Definition -CertificateAuthorities @("DC1.bvt.
local\bvt-DC1-CA", "ca1.bvt.local\CA1.bvt.local", "ca2.bvt.local\ca2.bvt.local")
```

Ahora, el cmdlet Get-FASCertificateDefinition debe devolver:

```
PS > Get-FASCertificateDefinition
Name                    : default_Definition
CertificateAuthorities  : {DC1.bvt.local\bvt-DC1-CA, ca1.bvt.local\CA1.bvt.local, ca2.bvt.local\ca2.bvt.local}
MsTemplate              : Citrix_SmartcardLogon
AuthorizationCertificate : 86ce221c-7599-43a3-9dbd-8e6a3c2be7b7
PolicyOids              : {}
InSession               : True
```

> **Nota:**
>
> La consola de administración del servicio FAS no funcionará después de realizar esta operación. Verá un campo vacío en “Entidad de certificación” y “Plantilla de certificado” al cargar:



A efectos prácticos, FAS sigue funcionando. Si usa la consola para modificar la regla de acceso, repita el paso 2 para ver todas las entidades de certificación.

Cambios de comportamiento previstos

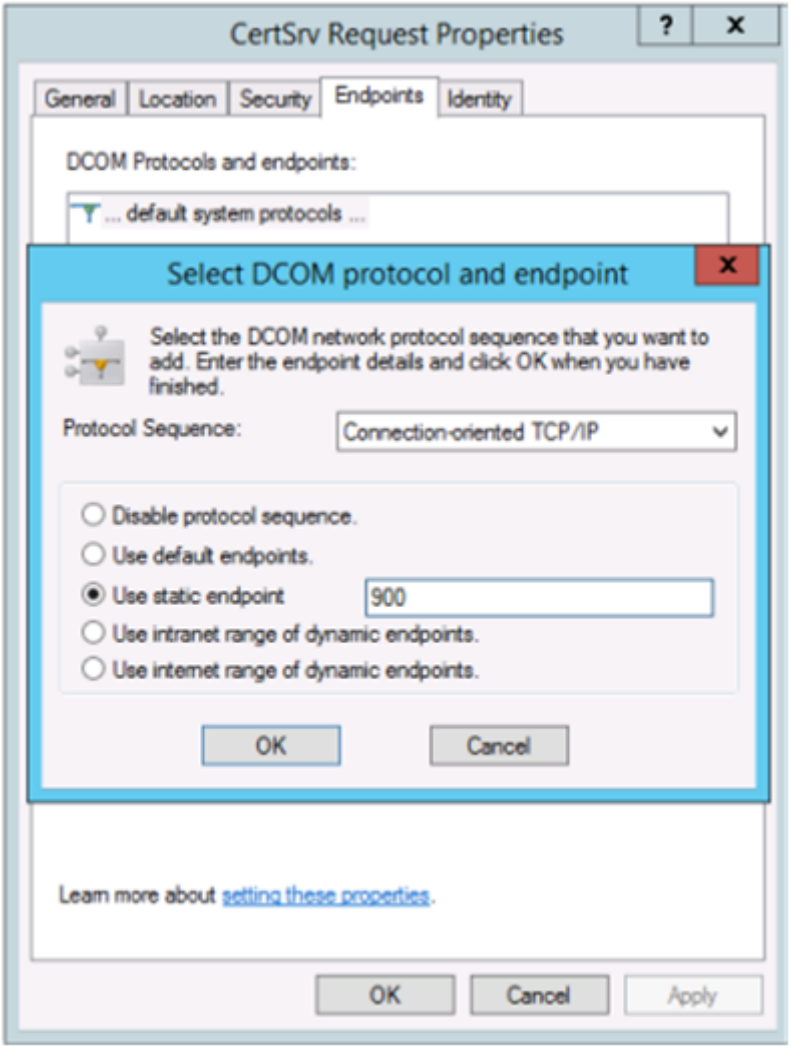
Después de configurar el servidor FAS con varios servidores de CA, la generación de certificados de usuario se distribuye entre todos los servidores de CA configurados. Además, si se produce un error en uno de los servidores de CA configurados, el servidor FAS cambiará a otro servidor disponible de la entidad de certificación.

Configurar CA de Microsoft para el acceso por TCP

De forma predeterminada, la entidad de certificación de Microsoft utiliza DCOM para el acceso. Esto puede provocar complicaciones cuando se implemente la seguridad del firewall, por lo que Microsoft

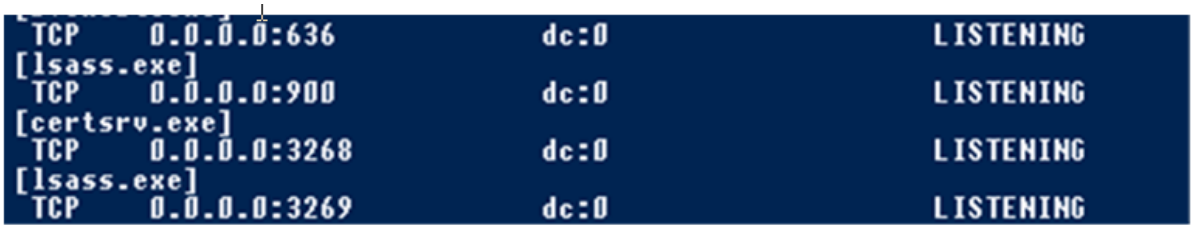
© 1999-2019 Citrix Systems, Inc. All rights reserved.

puede cambiar a un puerto TCP estático. En la entidad de certificación de Microsoft, abra el panel de configuración de DCOM y modifique las propiedades de “CertSrv Request”:



Cambie los “puntos finales” para seleccionar un dispositivo de punto final estático y especifique un número de puerto TCP (900 en la imagen de arriba).

Reinicie la entidad de certificación de Microsoft, y envíe una solicitud de certificado. Si ejecuta `netstat -a -n -b`, debería ver que ahora certsvr escucha en el puerto 900:



No es necesario configurar el servidor del servicio FAS (o cualquier otra máquina que use la entidad de certificación) porque DCOM tiene una fase de negociación que usa el puerto RPC. Cuando un cliente

© 1999-2019 Citrix Systems, Inc. All rights reserved.

quiere usar DCOM, se conecta al servicio de RPC de DCOM que está presente en el certificado de servidor y solicita acceso a un servidor DCOM determinado. Esta acción abre el puerto 900, y el servidor DCOM indica al servidor FAS cómo conectarse.

Generar previamente los certificados de usuario

El tiempo de inicio de sesión mejora significativamente para los usuarios si los certificados de usuario se generan previamente en el servidor FAS. En las siguientes secciones, se describe cómo hacerlo con uno o varios servidores FAS.

Obtener una lista de usuarios de Active Directory

Puede mejorar la generación de certificados si consulta AD y almacena la lista de usuarios en un archivo (por ejemplo, un archivo CSV), como se muestra en el siguiente ejemplo.

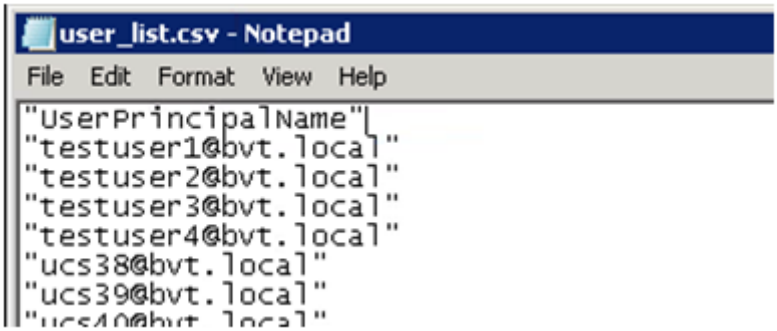
```
Import-Module ActiveDirectory

$searchbase = "cn=users,dc=bvt,dc=local" # AD User Base to Look for Users, leave it blank to search all
$filename = “user_list.csv” # Filename to save

if ($searchbase –ne “”) {
   Get-ADUser -Filter {(UserPrincipalName -ne "null") -and (Enabled -eq "true")} -SearchBase $searchbase -Properties
UserPrincipalName |Select UserPrincipalName | Export-Csv -NoTypeInformation -Encoding utf8 -delimiter ","
$filename
} else {
   Get-ADUser -Filter {(UserPrincipalName -ne "null") -and (Enabled -eq "true")}  -Properties UserPrincipalName
|Select UserPrincipalName | Export-Csv -NoTypeInformation -Encoding utf8 -delimiter "," $filename
}
```

Get-ADUser es un cmdlet estándar para consultar una lista de usuarios. El ejemplo anterior contiene un argumento de filtro para incluir en la lista solo a los usuarios con un UserPrincipalName y un estado de cuenta “enabled” (habilitado).

El argumento SearchBase limita la parte de Active Directory en que buscar usuarios. Puede omitirlo si quiere incluir a todos los usuarios de AD. Nota: Esta consulta puede devolver una gran cantidad de usuarios.

El archivo CSV tiene un aspecto similar a:

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Servidor FAS

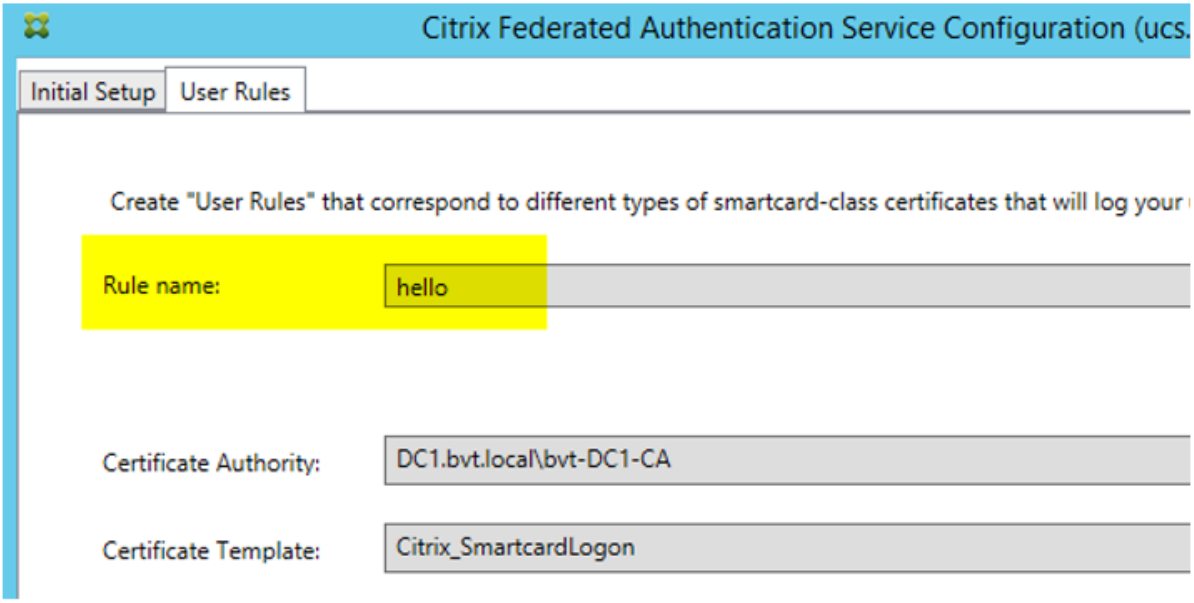
El siguiente script de PowerShell utiliza la lista de usuarios previamente generada y crea a partir de ella una lista de los certificados de usuario.

```
Add-PSSnapin Citrix.A*

$csv = "user_list.csv"
$rule = "default" #rule/role in your admin console
$users = Import-Csv  -encoding utf8 $csv

foreach ( $user in $users )
{
  $server = Get-FASServerForUser -UserPrincipalNames $user.UserPrincipalName
  if ( $server.Server -ne $NULL ) {
     New-FASUserCertificate -Address $server.Server -UserPrincipalName $user.UserPrincipalName -
CertificateDefinition $rule"_Definition" -Rule $rule
  }
  if ( $server.Failover -ne $NULL ) {
     New-FASUserCertificate -Address $server.Failover -UserPrincipalName $user.UserPrincipalName -
CertificateDefinition $rule"_Definition" -Rule $rule
  }
}
```

Si dispone de varios servidores FAS, el certificado de un usuario concreto se generará dos veces: uno en el servidor principal y otro en el servidor de conmutación por error.

El script anterior está orientado a una regla denominada “default”. Si tiene otro nombre de regla (por ejemplo, “hola”), cambie la variable $rule en el script.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Renovar certificados de la entidad de registro

Si utiliza más de un servidor FAS, puede renovar un certificado de autorización de FAS sin que ello afecte a los usuarios con sesión iniciada. Nota: Aunque también puede usar la interfaz gráfica de usuario para desautorizar y reautorizar FAS, usarla tiene como consecuencia que se restablecen las opciones de configuración de FAS.

Lleve a cabo los siguientes pasos:

1. Cree un nuevo certificado de autorización: `New-FasAuthorizationCertificate`
2. Escriba el GUID del nuevo certificado de autorización que devuelve: `Get-FasAuthorizationCertificate`
3. Coloque el servidor FAS en el modo de mantenimiento: `Set-FasServer -Address \<FAS server> -MaintenanceMode $true`
4. Cambie el nuevo certificado de autorización: `Set-FasCertificateDefinition -AuthorizationCertificate \<GUID>`
5. Desactive el modo de mantenimiento del servidor FAS: `Set-FasServer -Address \<FAS server> -MaintenanceMode $false`
6. Elimine el certificado anterior de autorización: `Remove-FasAuthorizationCertificate`

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Información relacionada

- El artículo Servicio de autenticación federada (FAS - Federated Authentication Service) es la referencia principal para la instalación y la configuración de este servicio.
- Las implementaciones más comunes del servicio FAS se resumen en el artículo Introducción a las arquitecturas del Servicio de autenticación federada.
- En el artículo Administrar y configurar el Servicio de autenticación federada se indican otros artículos de procedimientos.

Proteger claves privadas del Servicio de autenticación federada

March 8, 2019

Introducción

Las claves privadas se almacenan por medio de la cuenta de servicio de red y, de forma predeterminada, se marcan como elementos que no se pueden exportar.

Hay dos tipos de claves privadas:

- La clave privada asociada al certificado de la autoridad de registro (RA), procedente de la plantilla de certificado Citrix_RegistrationAuthority.
- La clave privada asociada a los certificados de usuario, procedente de la plantilla de certificado Citrix_SmartcardLogon.

En realidad, existen dos certificados de RA: Citrix_RegistrationAuthority_ManualAuthorization (válido durante 24 horas de forma predeterminada) y Citrix_RegistrationAuthority (válido durante dos años de forma predeterminada).

En el paso 3 de la configuración inicial en la consola de administración del servicio FAS, cuando el administrador hace clic en “Autorizar”, el servidor FAS genera un par de claves y envía una solicitud de firma de certificado (CSR) a la entidad de certificación para el certificado Citrix_RegistrationAuthority_ManualAuthorization. Se trata de un certificado temporal, válido durante 24 horas de forma predeterminada. La entidad de certificación no emite automáticamente el certificado, por lo que un administrador debe autorizar manualmente la emisión en ella. Una vez emitido el certificado al servidor FAS, el servicio FAS utiliza el certificado Citrix_RegistrationAuthority_ManualAuthorization para obtener automáticamente el certificado Citrix_RegistrationAuthority (cuya validez predeterminada es de dos años). El servidor FAS elimina el certificado y la clave de Citrix_RegistrationAuthority_ManualAuthorization tan pronto como obtiene el certificado Citrix_RegistrationAuthority.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

La clave privada asociada al certificado de la autoridad de registro (RA) debe ser especialmente confidencial, porque la directiva de certificados RA permite a quien posea la clave privada emitir solicitudes de certificado para el conjunto de usuarios configurados en la plantilla. Como consecuencia, quien posea esta clave puede conectarse al entorno como ninguno de los usuarios del conjunto.

Puede configurar el servidor FAS para que proteja las claves privadas según los requisitos de seguridad de la empresa. Para ello, elija una de las siguientes opciones:

- El proveedor de servicios de cifrado RSA y AES mejorado de Microsoft o el proveedor de almacenamiento de claves (KSP) de software de Microsoft para las claves privadas del certificado de la autoridad de registro (RA) y de los certificados de usuario.
- El proveedor de almacenamiento de claves de la plataforma Microsoft con un chip del módulo de plataforma segura (TPM) para la clave privada del certificado de RA, y el proveedor de servicios de cifrado RSA y AES mejorado de Microsoft o el proveedor de almacenamiento de claves (KSP) de software de Microsoft para las claves privadas de los certificados de usuario.
- El proveedor de almacenamiento de claves o el servicio de cifrado del distribuidor, ambos con el módulo de seguridad de hardware (HSM), para las claves privadas del certificado de RA y de los certificados de usuario.

Parámetros de configuración de claves privadas

Configure el servicio de autenticación federada (FAS) para usar una de las tres opciones. En un editor de texto, modifique el archivo Citrix.Authentication.FederatedAuthenticationService.exe.config. La ubicación predeterminada del archivo es la carpeta Archivos de programa\Citrix\Federated Authentication Service que se encuentra en el servidor FAS.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="Microsoft Software Key Storage Provider"/ -->

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateNonExportableKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

El servicio FAS lee el archivo de configuración solo cuando se inicia el servicio. Si se cambian los valores, el servicio FAS debe reiniciarse para que se vea la nueva configuración.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Establezca los valores correspondientes en el archivo Citrix.Authentication.FederatedAuthenticationService.exe.co
como se muestra a continuación:

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderLegacyCsp** (cambie entre CAPI y las API de CNG)

Valor	Comentario
true	Usar las API de CAPI
false (opción predeterminada)	Usar las API de CNG

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderName** (nombre del proveedor que se va a usar)

Valor	Comentario
Microsoft Enhanced RSA and AES Cryptographic Provider	Proveedor predeterminado de CAPI
Microsoft Software Key Storage Provider	Proveedor predeterminado de CNG
Microsoft Platform Key Storage Provider	Proveedor predeterminado de TPM. Tenga en cuenta que TPM no se recomienda para las claves de usuario. Use TPM solo para la clave de RA. Si quiere ejecutar el servidor FAS en entornos virtualizados, consulte al distribuidor de TPM y del hipervisor si se admite la virtualización.
HSM_Vendor CSP/Proveedor de almacenamiento de claves	Facilitado por el distribuidor de HSM. El valor difiere de un distribuidor a otro. Si quiere ejecutar el servidor FAS en entornos virtualizados, consulte al distribuidor de HSM si se admite la virtualización.

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderType** (obligatorio solo en caso de API de CAPI)

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Valor	Comentario
24	Predeterminado. Se refiere a Microsoft KeyContainerPermissionAccessEntry.ProviderType Property PROV_RSA_AES 24. Debe ser siempre 24 a menos que esté usando un HSM con CAPI y el proveedor de HSM especifique otra cosa.

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyProtection** (Cuando se necesita que el servicio FAS realice una operación de clave privada, este utiliza el valor especificado aquí) Controla el indicador “exportable” de las claves privadas. Permite el uso del almacenamiento de claves de TPM, si lo admite el hardware.

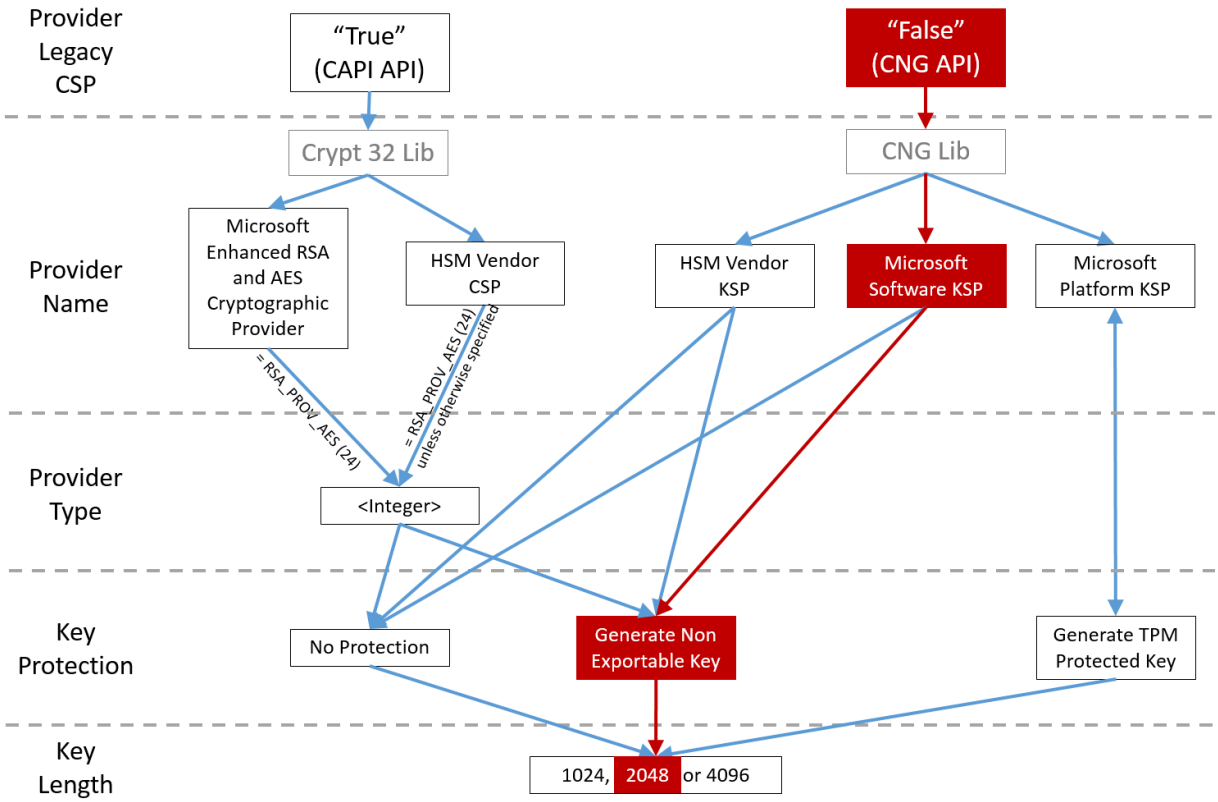
Valor	Comentario
NoProtection	Se puede exportar la clave privada.
GenerateNonExportableKey	Predeterminado. No se puede exportar la clave privada.
GenerateTPMProtectedKey	La clave privada se administrará mediante TPM. La clave privada se almacena mediante el nombre de proveedor que especifique en ProviderName (por ejemplo, el proveedor de almacenamiento de claves de la plataforma Microsoft).

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyLength** (especifique el tamaño de la clave privada en bits)

Valor	Comentario
2048	Valor predeterminado. También se puede usar 1024 o 4096.

A continuación, se muestran los parámetros del archivo de configuración representados gráficamente (las opciones de instalación predeterminadas aparecen en rojo):

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Ejemplos de configuración

Ejemplo 1

En este ejemplo, la clave privada del certificado de RA y las claves privadas de los certificados de usuario se almacenan con el proveedor de almacenamiento de claves de software de Microsoft.

Esta es la configuración predeterminada tras la instalación. No se necesita configurar ninguna clave privada adicional.

Ejemplo 2

En este ejemplo, la clave privada del certificado de RA se almacena en el hardware TPM de la placa base del servidor FAS con el proveedor de almacenamiento de claves de la plataforma Microsoft, mientras que las claves privadas de los certificados de usuario se almacenan con el proveedor de almacenamiento de claves (KSP) de software de Microsoft.

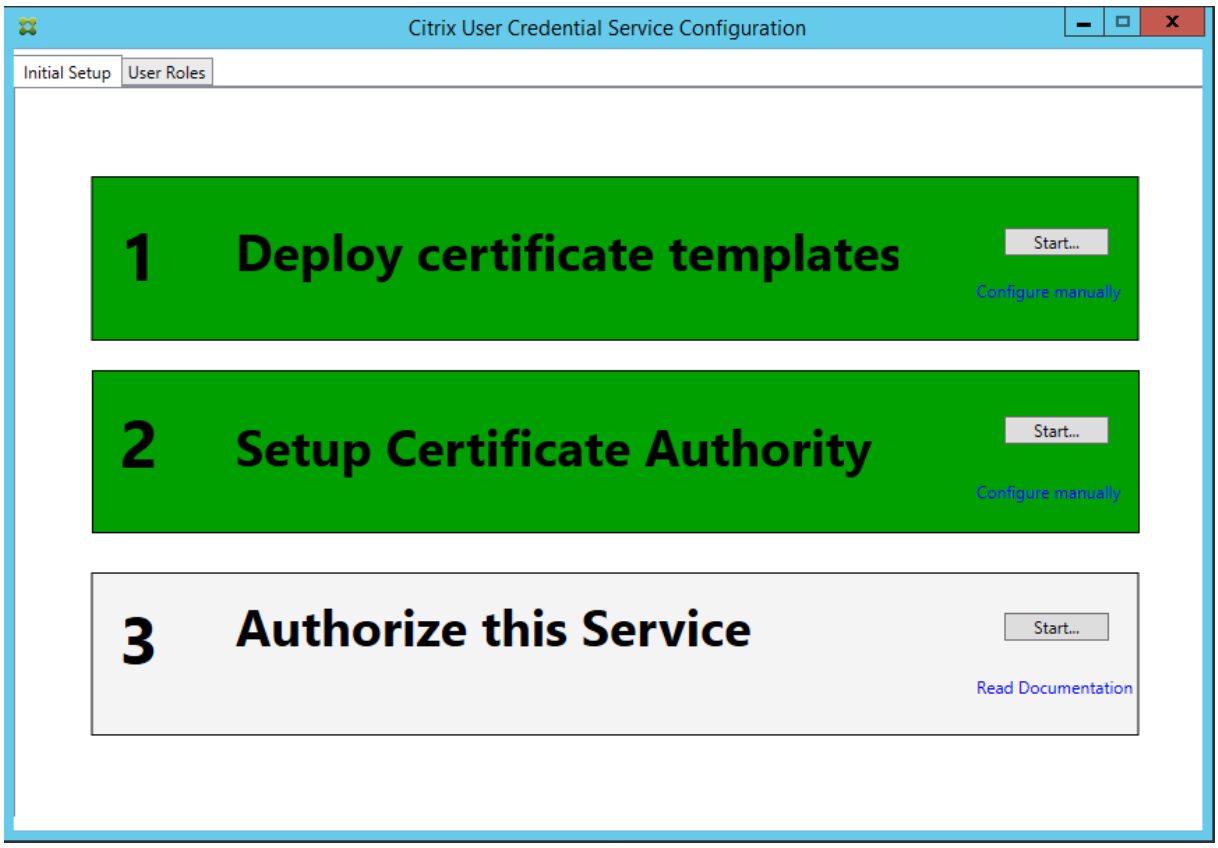
En este caso, se presupone que el TPM de la placa madre del servidor FAS se ha habilitado en BIOS (siguiendo la documentación del fabricante del TPM) y, a continuación, se ha inicializado en Windows; consulte https://technet.microsoft.com/en-gb/library/cc749022(v=ws.10).aspx.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Usar PowerShell (recomendado)

El certificado de RA se puede solicitar sin conexión mediante PowerShell. Se recomienda en empresas que no quieran que su entidad de certificación emita un certificado de RA a través de una solicitud de firma de certificado en línea. Con consola de administración FAS, no se puede solicitar una firma de certificado de RA sin conexión.

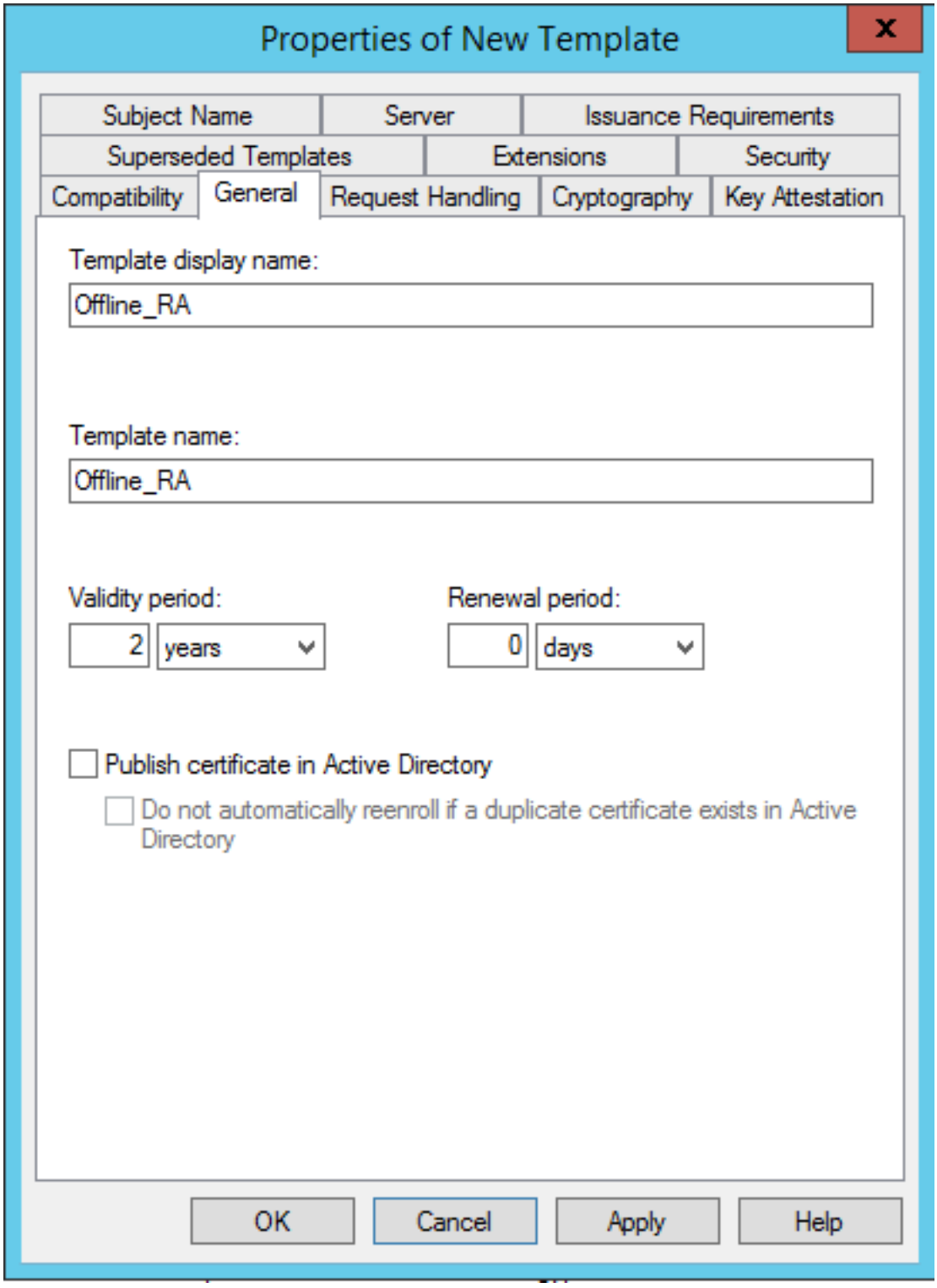
Paso 1: Durante la configuración inicial de FAS con la consola de administración, complete solo los primeros dos pasos, es decir, implemente las plantillas de certificado y configure la entidad de certificación.



Paso 2: En el servidor de la entidad de certificación, agregue el complemento MMC de las plantillas de certificados. Haga clic con el botón secundario en la plantilla **Citrix_RegistrationAuthority_ManualAuthorizatio**n y seleccione **Duplicar plantilla**.

Seleccione la ficha **General**. Cambie el nombre y el período de validez. En este ejemplo, el nombre es Offline_RA y el período de validez es de 2 años:

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Paso 3: En el servidor de la entidad de certificación, agregue el complemento MMC de esta. Haga clic con el botón secundario en **Plantillas de certificado**. Seleccione **Nueva** y, a continuación, haga clic en **Plantilla de certificado que se va a emitir**. Elija la plantilla que acaba de crear.

Paso 4: Cargue los siguientes cmdlets de PowerShell en el servidor FAS:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

```
Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
```

Paso 5: Genere el par de claves RSA en el TPM del servidor FAS y cree la solicitud de firma de certificado con el siguiente cmdlet de PowerShell en el servidor FAS. **Nota:** Algunos TPM limitan la longitud de la clave. La longitud predeterminada de la clave es de 2048 bits. Especifique una longitud de clave que su hardware admita.

```
New-FasAuthorizationCertificateRequest -UseTPM $true -address \<FQDN of
    FAS Server>
```

Por ejemplo:

```
New-FasAuthorizationCertificateRequest -UseTPM $true -address fashsm.
    auth.net
```

Aparecerá lo siguiente:

```
PS C:\Users\Administrator.AUTH> New-UcsAuthorizationCertificateRequest -UseTPM $true -address ucshsm.auth.local

Id                  : 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39
Address             : [Offline CSR]
TrustArea           :
CertificateRequest  : -----BEGIN CERTIFICATE REQUEST-----
                      MIICaDCCAVACAQIwIzEhMB8GCgmSJomT8ixkARkWEUNpdHJpeFRydXNORmFicmljMIIBIjANBgkq
                      hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwAtwoCLXJuJ3yIscT8Y5v/7zuYqBhbHkhZV3wTNfROXW
                      1hCMwi7X4YpTE7CbJtgiFY/9SEBa9StGeTVpeJi66gKoZCdxydc2BwX6JNZrLi9hAflbInFPgrz+
                      vbG3YjKuKtK35JpGqYWjUEDzKiQFaob3Dkh/pwP3V7OcEYthxB8CfbaN9MHOEFbepoSYOCAfunXW
                      snwIbXD9lc/fGyN/3f94P4fbNrjEIOHc+4Oy/WsPgPRgcq9XBwRjzpGjOgOWRoJS9g22OY5PwD77
                      7f7vZvoQkRy5NXXXATJ+xxYEPLp9JuJaE1W%rTJG+%P3SnG/oCCPit7iUIIc9FjGa3qTUQIDAQAB
                      oAAwDQYJKoZIhvcNAQENBQADggEBAIJV8jR9XWHlvztpjxPeJzAVOsrLpOsCfNdvYn9u+I7J8Gsr
                      4tuLjuQ+An4Y2Rw7b6pZxEICV8rqd5Gy+wtPnUZoAf6eLg1Vht2RVfb6d7Ns6+Mc+F5bFegLHs8c
                      Y1ITHOtmcHFKt4Loz5O5E+tQw39MProEj3p7GwF7HrGY+QSbFD38rbL19Z5cfNYYqMbsgyMgdR8F
                      3SmagQjN3C8lyqT8z1iF4132xlmQrP/4XQvr1F+TO15PM5Fxjj6PEKWopWTYZXGzSC1ufxevcO1K
                      +tTH9tQYJM6xw3+6TIcfuWOjrd8KJjTdC5SMu7LJuIajTNZ5Z+1eM61TATO3XG/AB7o=
                      -----END CERTIFICATE REQUEST-----
Status              : WaitingForApproval


PS C:\Users\Administrator.AUTH> _
```

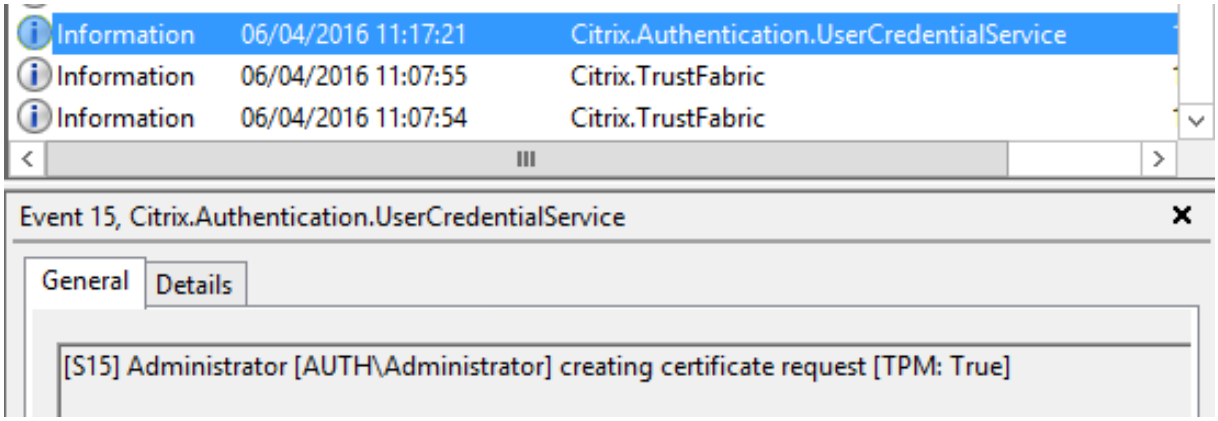
Notas:

- En uno de los siguientes pasos, se necesita el identificador GUID (en este ejemplo, “5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39”).
- Este cmdlet de PowerShell se puede entender como una “invalidación” puntual que se usa para generar la clave privada del certificado de la autoridad de registro.
- Cuando se ejecuta este cmdlet, se comprueban los valores del archivo de configuración, leídos en el inicio del servicio FAS, para determinar la longitud de la clave que se va a usar (la longitud predeterminada es de 2048).
- Como -UseTPM está establecido en $True en esta operación manual de clave privada de certificado de RA que se ha iniciado con PowerShell, el sistema ignora los valores del archivo que no coincidan con la configuración necesaria para usar un TPM.
- Ejecutar este cmdlet no cambia los parámetros del archivo de configuración.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

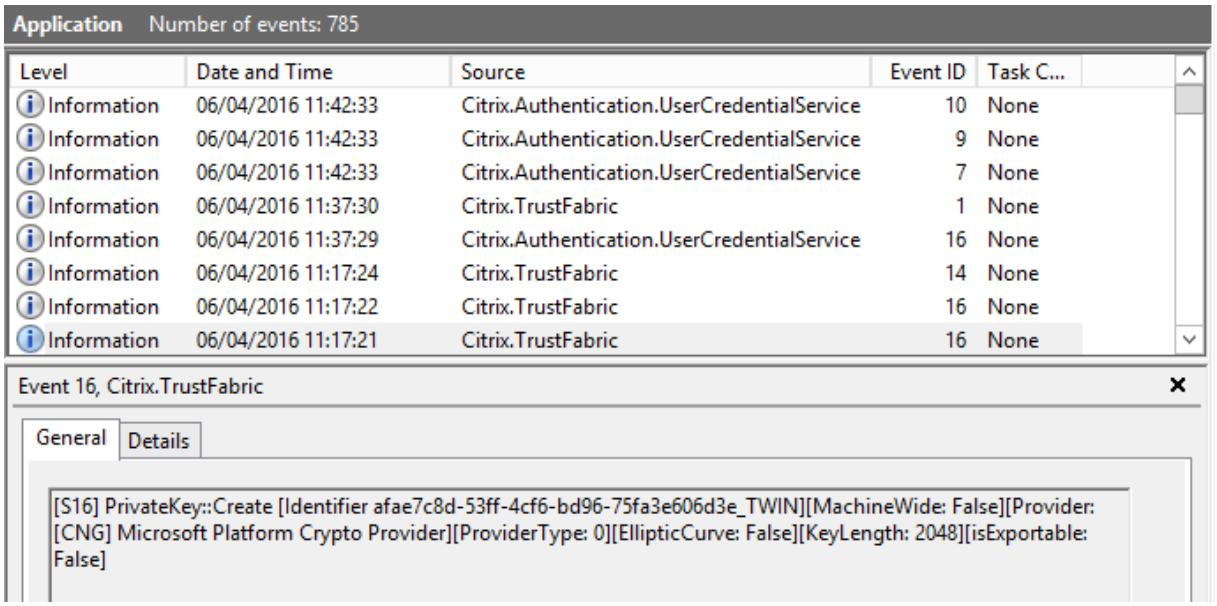
> - En las siguientes operaciones automáticas de clave privada para los certificados de usuario que se inicien con FAS, se utilizarán los valores que se hayan leído del archivo cuando se iniciara el servicio FAS.
> - También se puede establecer el valor de KeyProtection del archivo de configuración en GenerateTPMProtectedKey cuando el servidor FAS emita certificados. De este modo, se generarán claves privadas de certificados de usuario protegidas por el TPM.

Para verificar que se haya utilizado el TPM para generar el par de claves, abra el registro de la aplicación en el visor de eventos de Windows que está presente en el servidor FAS y consulte el momento en que se generó el par de claves.



> **Nota:** "[TPM: True]"

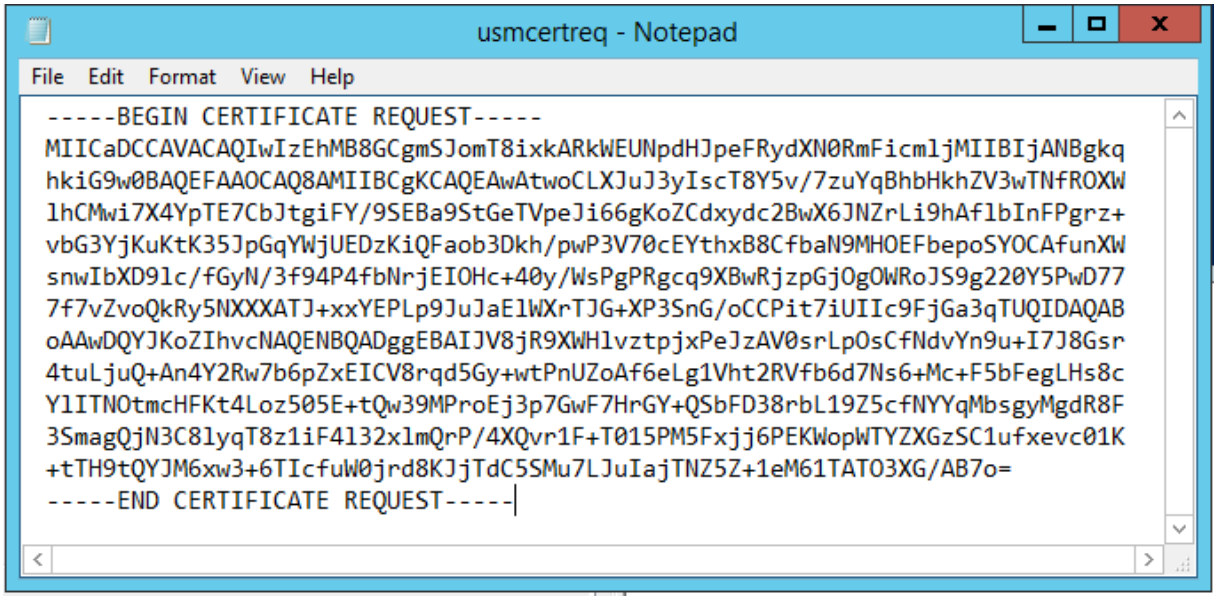
Seguido de:



> **Nota:** "Provider: [CNG] Microsoft Platform Crypto Provider"

Paso 6: Copie la sección de la solicitud de certificado a un editor de texto y guárdela en el disco como un archivo de texto.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Paso 7: Envíe la solicitud de firma de certificado a la entidad de certificación (CA). Para ello, escriba lo siguiente en la instancia de PowerShell presente en el servidor FAS:

```
certreq -submit -attrib "certificatetemplate:\<certificate template
    from step 2>" \<certificate request file from step 6>
```

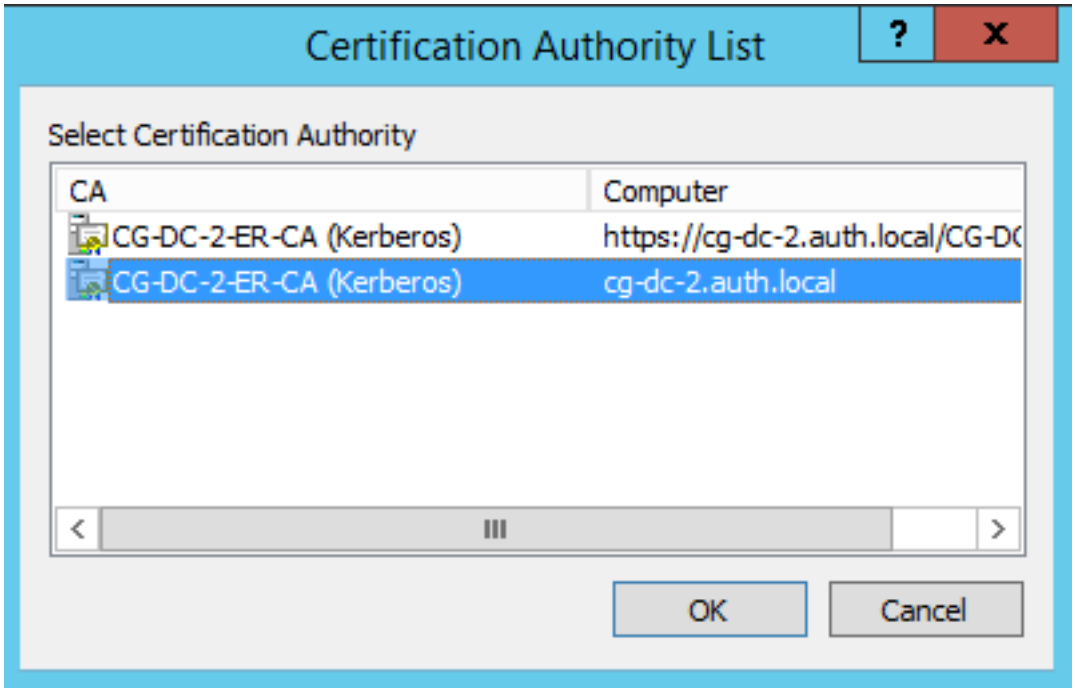
Por ejemplo:

```
certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\
    Administrator.AUTH\Desktop\usmcertreq.txt
```

Aparecerá lo siguiente:

En este punto, es posible que aparezca una ventana con la lista de entidades de certificación. En este ejemplo, la entidad de certificación (CA) tiene habilitadas las inscripciones HTTP (hilera superior) y DCOM (hilera inferior). Seleccione la opción DCOM, si está disponible:

© 1999-2019 Citrix Systems, Inc. All rights reserved.



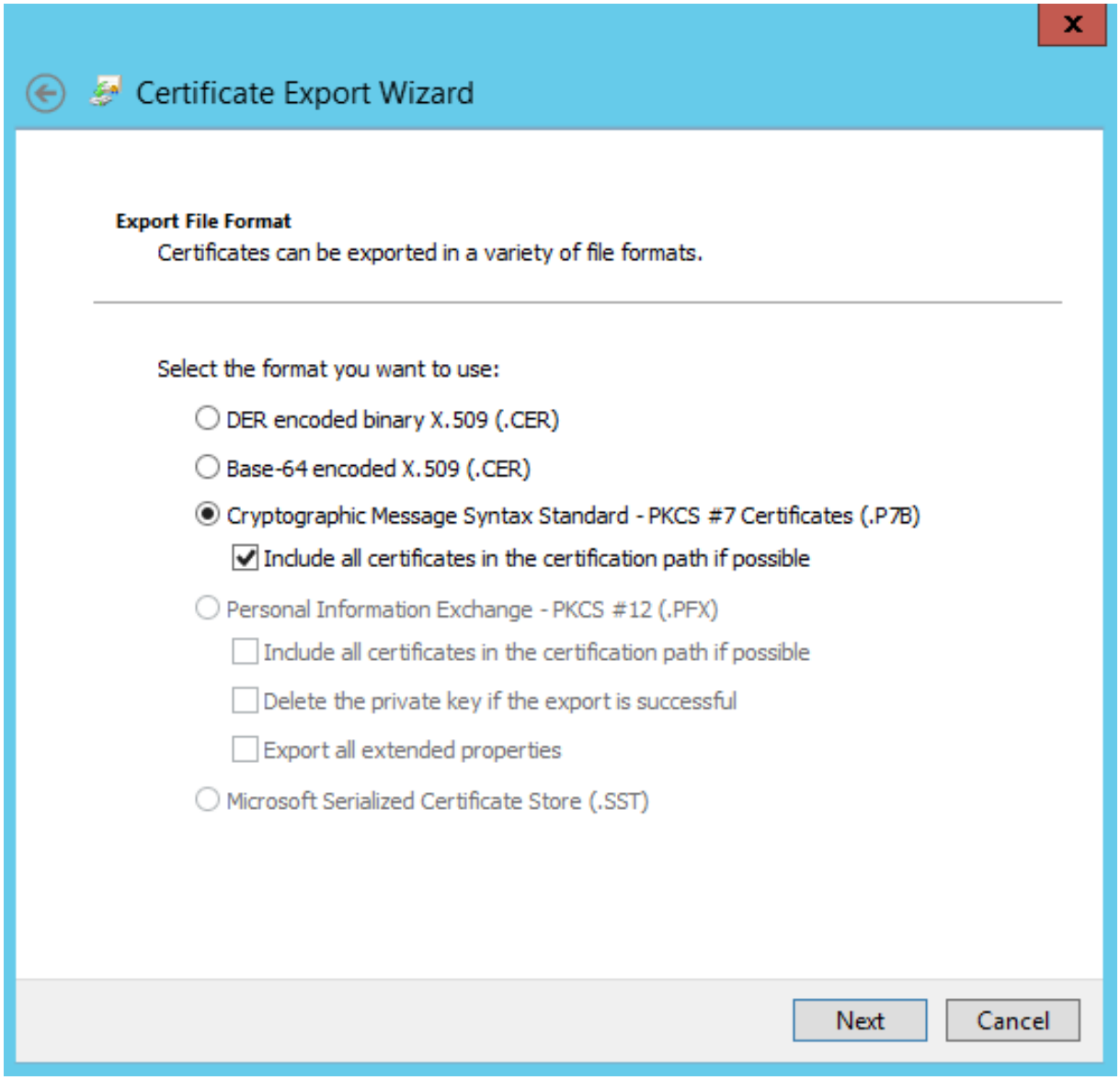
Tras especificar la entidad de certificación (CA), PowerShell pide el ID de la solicitud mediante RequestID:

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Des
ktop\usmcertreq.txt
Active Directory Enrollment Policy
  {4F7616DE-DBDC-4D21-A4FD-2E29502177C2}
  ldap:
RequestId: 106
RequestId: "106"
Certificate request is pending: Taken Under Submission (0)
PS C:\Users\Administrator.AUTH> _
```

Paso 8: En el servidor de la entidad de certificación, en el complemento MMC de esta, haga clic en **Solicitudes pendientes**. Tome nota del identificador de la solicitud. A continuación, haga clic con el botón secundario en la solicitud y elija **Emitir**.

Paso 9: Seleccione el nodo **Certificados emitidos**. Busque el certificado que se acaba de emitir (el ID de solicitud debe coincidir). Haga doble clic para abrir el certificado. Seleccione la ficha **Detalles**. Haga clic en **Copiar a archivo**. Se iniciará el Asistente para exportación de certificados. Haga clic en **Siguiente**. Seleccione las siguientes opciones para el formato de archivo:

© 1999-2019 Citrix Systems, Inc. All rights reserved.



El formato debe ser "**Estándar de sintaxis de cifrado de mensajes: certificados PKCS #7 (.P7B)**" y se debe marcar "**Si es posible, incluir todos los certificados en la ruta de acceso de certificación**".

Paso 10: Copie el archivo del certificado exportado al servidor FAS.

Paso 11: Debe importar el certificado de RA al servidor FAS. Para ello, introduzca este cmdlet de PowerShell en el servidor FAS:

```
Import-FasAuthorizationCertificateResponse -address <FQDN of FAS server> -Id <ID
GUID from step 5> -Pkcs7CertificateFile <Certificate file from step 10>
```

Por ejemplo:

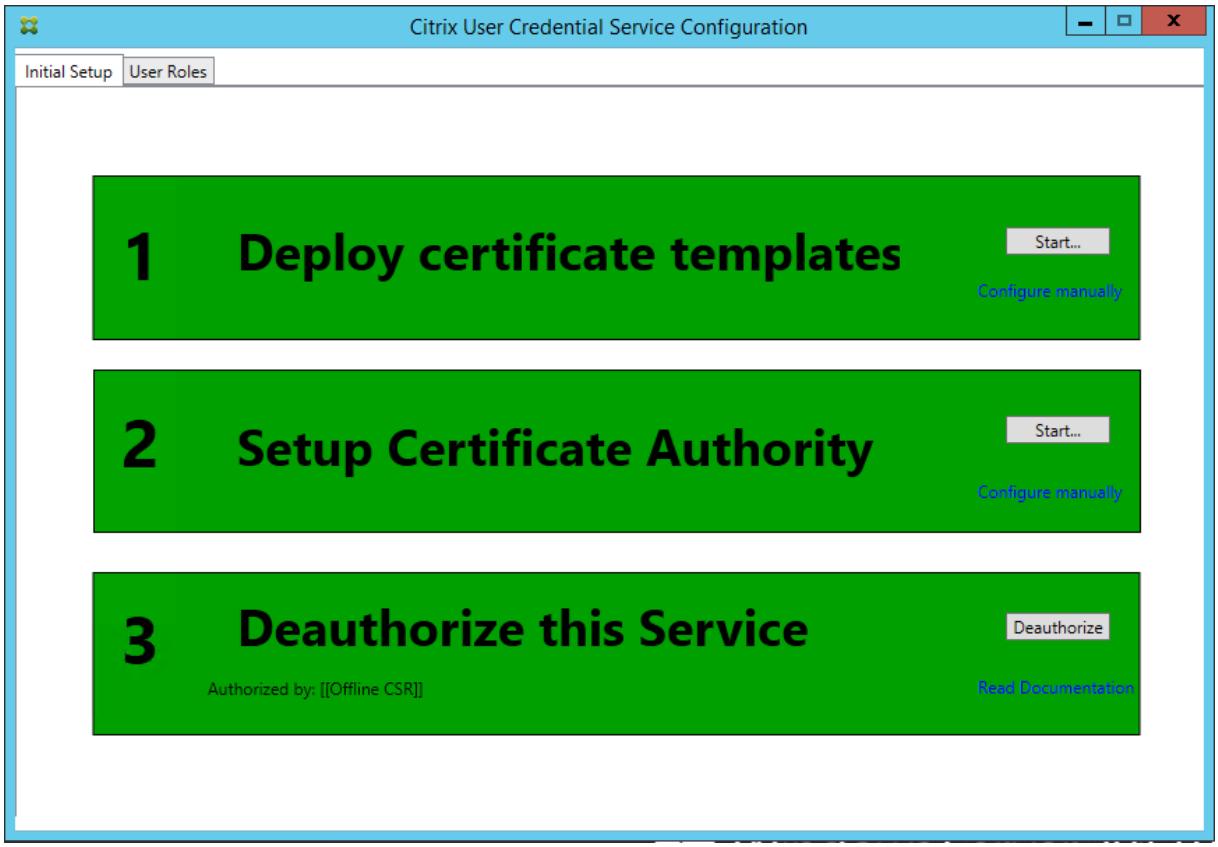
```
Import-FasAuthorizationCertificateResponse -address fashsm.auth.net -Id 5ac3d8bd-
b484-4ebe-abf8-4b2cfd62ca39 -Pkcs7CertificateFile
C:\Users\Administrator.AUTH\Desktop\TPM_FAS_Cert.p7b
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Aparecerá lo siguiente:

```
PS C:\Users\Administrator.AUTH> Import-UcsAuthorizationCertificateResponse -address ucshsm.auth.local -Id 5ac3d8bd-b484-
4ebe-abf8-4b2cfd62ca39 -Pkcs7CertificateFile C:\Users\Administrator.AUTH\Desktop\TPM_UCS_Cert.p7b


Id                  : 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39
Address             : [Offline CSR]
TrustArea           : a5c27fcc-1dd7-4c2b-8963-16ec31102Dfc
CertificateRequest :
Status              : Ok
```

Paso 12: Cierre la consola de administración FAS y reiníciela.



> **Nota:**
>
> El paso “Authorize this Service” pasa a ser verde y cambia a “Deauthorize this Service”. La entrada siguiente es “Authorized by: Offline CSR”.

Paso 13: Seleccione la ficha **User Roles** en la consola de administración FAS y modifique la configuración como se describe en el artículo principal del Servicio de autenticación federada (FAS).

> **Nota:**
>
> Desautorizar el servicio de autenticación federada (FAS) a través de la consola de administración eliminará el rol de usuario.

Uso de la consola de administración FAS

© 1999-2019 Citrix Systems, Inc. All rights reserved.

La consola de administración FAS no puede solicitar firmas de certificado sin conexión, por lo que no es recomendable utilizarla a menos que la empresa permita solicitar firmas de certificado en línea para certificados de RA.

En la configuración inicial de FAS, después de implementar las plantillas de certificado y configurar la entidad de certificación, pero antes de autorizar el servicio (paso 3 en la secuencia de configuración):

Paso 1: Modifique la siguiente línea del archivo de configuración como se muestra a continuación:

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection"
value="GenerateTPMProtectedKey"/>
```

Ahora, el archivo debería aparecer como se muestra a continuación:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="Microsoft Software Key Storage Provider"/ -->

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateTPMProtectedKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

Algunos TPM limitan la longitud de la clave. La longitud predeterminada de la clave es de 2048 bits. Compruebe que el hardware admite la longitud de clave especificada.

Paso 2: Autorice el servicio.

Paso 3: Emita manualmente la solicitud de certificado pendiente desde el servidor de la entidad de certificación. Una vez obtenido el certificado de RA, el paso 3 de la secuencia de configuración que aparece en la consola de administración pasará a ser verde. En este punto, la clave privada del certificado de RA se habrá generado en el TPM. De forma predeterminada, el certificado será válido durante 2 años.

Paso 4: Modifique el archivo de configuración de nuevo a lo siguiente:

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection"
value="GenerateNonExportableKey"/>
```

> **Nota:**
>
> Aunque FAS puede generar certificados de usuario con las claves protegidas de TPM, el hardware

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> de TPM puede ser demasiado lento para implementaciones de gran tamaño.

Paso 5: Reinicie el servicio de autenticación federada de Citrix. Ello obliga al servicio a volver a leer el archivo de configuración y procesar los valores cambiados. Las siguientes operaciones automáticas de clave privada afectarán a las claves de certificado de usuario; las operaciones se almacenarán las claves privadas en el TPM, sino que usarán el proveedor de almacenamiento de claves (KSP) de software de Microsoft.

Paso 6: Seleccione la ficha "User Roles" en la consola de administración FAS y modifique la configuración como se describe en el artículo principal del servicio de autenticación federada (FAS).

> **Nota:**
>
> Desautorizar el servicio de autenticación federada (FAS) a través de la consola de administración eliminará el rol de usuario.

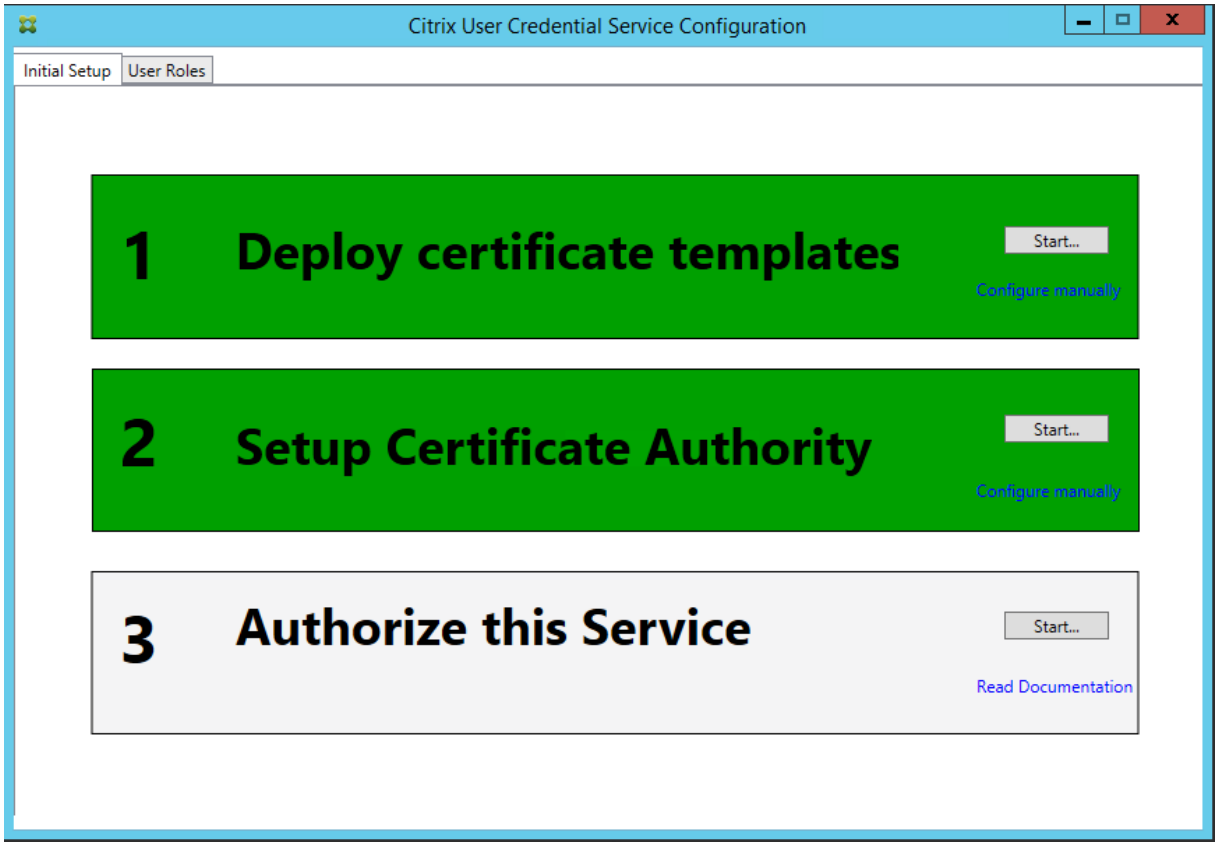
Ejemplo 3

En este ejemplo, la clave privada del certificado de RA y las claves privadas de los certificados de usuario se almacenan en un módulo de seguridad de hardware (HSM). En este ejemplo, se presupone que el lector tiene configurado un módulo HSM. El módulo HSM tendrá un nombre de proveedor; por ejemplo, "HSM_Proveedor de almacenamiento de claves del distribuidor".

Si quiere ejecutar el servidor FAS en entornos virtualizados, consulte al distribuidor de HSM si admite el hipervisor.

Paso 1: Durante la configuración inicial de FAS con la consola de administración, complete solo los primeros dos pasos, es decir, implemente las plantillas de certificado y configure la entidad de certificación.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Paso 2: Consulte la documentación del distribuidor de HSM para determinar el valor de ProviderName que debe tener el módulo HSM. Si el módulo HSM utiliza CAPI, es posible que, en la documentación, el proveedor se conozca como proveedor de servicios de cifrado (CSP). En cambio, si el módulo HSM utiliza CNG, es posible que el proveedor se conozca como proveedor de almacenamiento de claves (KSP).

Paso 3: Modifique el archivo de configuración como se indica a continuación:

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName"
value="HSM_Vendor's Key Storage Provider"/>
```

Ahora, el archivo debería aparecer como se muestra a continuación:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <!-- This option switch between CAPI API  (true) and CNG API (false) Cryptographic Providers  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/>

    <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name.  -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="HSM_Vendor's Key Storage Provider"/>

    <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP).  For example: PROV_RSA_AES is 24  -->
    <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ -->

    <!-- Specify Private Key protection [NoProtection|GenerateNonExportableKey|GenerateTPMProtectedKey] -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateNonExportableKey"/>

    <!-- Specify RSA Key length -->
    <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/>

    <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / -->

    <!-- Logging: Event IDs to not log (comma separated) -->
    <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / -->

    <!-- Logging: Disable Key Management logs -->
    <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ -->
  </appSettings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>
```

En este caso, se presupone que el módulo HSM utiliza CNG, por lo que el valor de ProviderLegacyCsp se establece en false. Si el módulo HSM utiliza CAPI, el valor de ProviderLegacyCsp debe establecerse en true. Consulte la documentación del distribuidor de HSM para determinar si el módulo HSM utiliza CAPI o CNG. Asimismo, consulte la documentación del distribuidor de HSM para saber las longitudes de clave que admite en la generación de claves asimétricas de RSA. En este ejemplo, la longitud de la clave se ha establecido en el valor predeterminado de 2048 bits. Compruebe que el hardware admite la longitud de clave especificada.

Paso 4: Reinicie el servicio de autenticación federada de Citrix para que este lea los nuevos valores del archivo de configuración.

Paso 5: Genere el par de claves RSA en el HSM y cree la solicitud de firma de certificado haciendo clic en **Authorize** en la ficha de configuración inicial de la consola de administración FAS.

Paso 6: Para verificar que el par de claves se ha generado en el HSM, consulte las entradas de la aplicación en el registro de eventos de Windows:

```
[S16] PrivateKey::Create [Identifier e1608812-6693-4c54-a937-91a2e27df75b_TWIN][MachineWide: False][Provider: [CNG] HSM_Vendor's Key Storage Provider][ProviderType: 0][EllipticCurve: False][KeyLength: 2048][isExportable: False]
```

Nota: [Provider: [CNG] HSM_Vendor's Key Storage Provider]

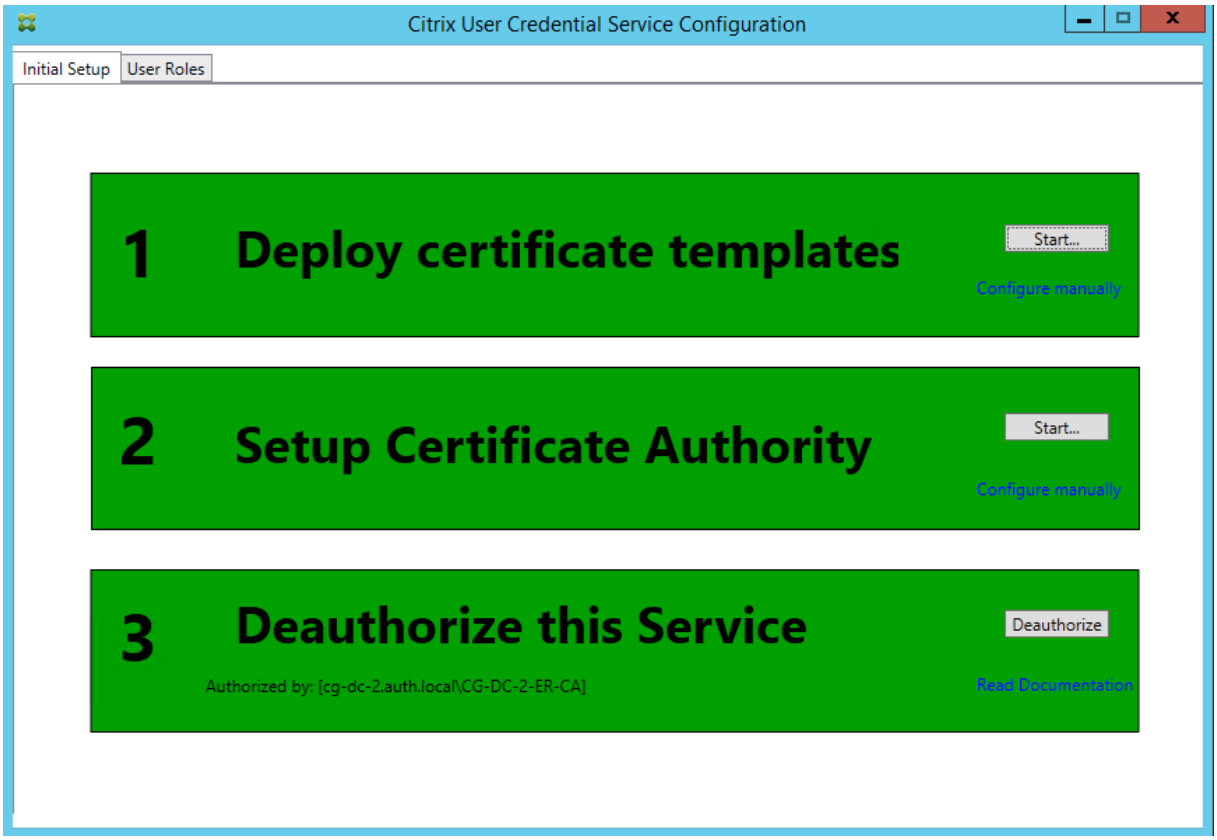
Paso 7: En el servidor de la entidad de certificación, en el complemento MMC de esta, seleccione el nodo **Solicitudes pendientes**:

Request ID	Binary Request	Request Status Code	Request Disposition Message	Request Submission Date	Requester Name	Request Country/Region
107	-----BEGIN NE...	The operation compl...	Taken Under Submission	07/04/2016 14:04	AUTH\UCSHSM$	

Haga clic con el botón secundario en la solicitud y seleccione **Emitir**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> **Nota:**
>
> El paso “Authorize this Service” pasa a ser verde y cambia a “Deauthorize this Service”. La entrada siguiente es “Authorized by: [<nombre de la entidad de certificación>]”.



Paso 8: Seleccione la ficha **User Roles** en la consola de administración FAS y modifique la configuración como se describe en el artículo principal del servicio de autenticación federada (FAS).

> **Nota:**
>
> Desautorizar el servicio de autenticación federada (FAS) a través de la consola de administración eliminará el rol de usuario.

Almacenamiento de certificados del servicio de autenticación federada (FAS)

El servicio de autenticación federada (FAS) no utiliza el almacén de certificados de Microsoft que haya en el servidor FAS para almacenar en él sus certificados. Utiliza una base de datos integrada.

Para determinar el GUID del certificado de RA, introduzca los siguientes cmdlets de PowerShell en el servidor FAS:

```
Add-pssnapin Citrix.a\*
Get-FasAuthorizationCertificate  -address \<FAS server FQDN>
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Por ejemplo, **Get-FasAuthorizationCertificate –address cg-fas-2.auth.net**:

```
PS C:\Users\Administrator.AUTH> Get-UcsAuthorizationCertificate -address cg-ucs-2.auth.local


Id                : a3958424-b8c3-4cac-ba0d-7eb3ce24591c
Address           : cg-dc-2.auth.local\CG-DC-2-ER-CA
TrustArea         : 3df77088-00e0-4dca-a47a-28060dc16986
CertificateRequest :
Status            : MaintenanceDue

Id                : fcb185f9-5069-4e34-8625-a333ac126535
Address           : [Offline CSR]
TrustArea         :
CertificateRequest : -----BEGIN CERTIFICATE REQUEST-----
                     MIICaDCCAVACAQIwIzEhMB8GCgmSJomT8ixkARkWEUNpdHJpeFRydXNORmFicmljMIIBIjANBgkq
                     hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxyNzaiWX8DhUnOZMS2YVSDhr36AV5BGeIYOGVCFKvZPe
                     Rmm/xOVM6cNKsLbew3dYlbo+vdgWg86DFRVxTORhollV86iazDZyOiYGgxe9/s8YZzCspVWN1nB1
                     zXOUJfo1qo9UsmImYr7MR/dhGAtkfsFUoPcd2+zcezmgOfq/4vmCIuerwqzRR5T/p4og7+IjR1se
                     ECz/CbXROOuiDhW+VWbjcsgklcavzvC/jR33F9dZSXNgKRiGHgfd/lBb3elZKA4OOoi90u64Q916
                     3ba9BnihqxIgvwWILOmyUfiJmCgbhLJV4TPBopOdKz/axZEIO5p5XYVjCcpXqhqL7Ppn1wIDAQAB
                     oAAwDQYJKoZIhvcNAQENBQADggEBAJhdvw6yrLGBMtAgo3oPL6o8/at+IqHjHKqgcJNJO/MU7/7X
                     bZB46drLPFzpzF88DkmfoCEgOxlbzFX9waaiFs9CHC/AcEzblN925y1gqljsfC3l5TCKBAeLFoMl
                     PSEkfYMQUOSBYCuLlkFn1LXLSeQ3qJTzSvptYROawFmUMQLffwLSR1vOuS8DJSrpASrwdXJk3TOa
                     Glo/xJo/NRMOwMH+AvGbBsgp3l+jnDjXED5RudqARfgVgcW714JP+XIeFrE1TZmUL2skNIXEPNHC
                     H8eAHdYD26caFigydfefbjx4fbaJDFHJs5+1tnrTZ9knCrawhUiIyOMLGZOOaiER+z8=
                     -----END CERTIFICATE REQUEST-----
Status            : WaitingForApproval
```

Para obtener una lista de certificados de usuario, escriba:

```
Get-FasUserCertificate  -address \<FAS server FQDN>
```

Por ejemplo, **Get-FasUserCertificate –address cg-fas-2.auth.net**

```
PS C:\Users\Administrator.AUTH> Get-UcsUserCertificate -address cg-ucs-2.auth.local


ThumbPrint            : 7BA22879F40EE92125A2F96E7DD2D52C73820459
UserPrincipalName     : walter@adfs.ext
Role                  : default
CertificateDefinition : default_Definition
ExpiryDate            : 05/04/2016 12:02:13
```

> **Nota:**
>
> Al usar un HSM para almacenar las claves privadas, los contenedores de HSM se identifican con un GUID. El GUID para la clave privada en el HSM se puede obtener con:
>
> ```
> Get-FasUserCertificate  -address \<FAS server FQDN> -KeyInfo $true
> ```
>
> Por ejemplo:
>
> ```
> Get-FasUserCertificate  -address [fas3.djwfas.net](http://fas3.
>     djwfas.net/) -KeyInfo $true
> ```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

```
PS C:\Users\administrator> Get-FasUserCertificate -Address fas3.djwfas.net -KeyInfo $true


PrivateKeyIdentifier   : 38405c4d-63af-43e4-9135-2412246b1112
PrivateKeyProvider     : Microsoft Software Key Storage Provider
PrivateKeyIsCng        : True
ThumbPrint             : AD2441F050A02966AA4DB190BA084976528DB667
UserPrincipalName      : joe@djwfas.net
Role                   : default
CertificateDefinition  : default_Definition
SecurityContext        :
ExpiryDate             : 19/01/2018 09:18:48
```

Información relacionada

- El artículo Servicio de autenticación federada (FAS - Federated Authentication Service) es la referencia principal para la instalación y la configuración de este servicio.
- Las implementaciones más comunes del servicio FAS se resumen en el artículo Introducción a las arquitecturas del Servicio de autenticación federada.
- En el artículo Administrar y configurar el Servicio de autenticación federada se indican otros artículos de procedimientos.

Seguridad y configuración de red del Servicio de autenticación federada

March 8, 2019

El Servicio de autenticación federada (FAS) de Citrix está estrechamente integrado con Microsoft Active Directory y con la entidad de certificación (CA) de Microsoft. Es fundamental asegurarse de que el sistema está administrado y protegido correctamente mediante el desarrollo de una directiva de seguridad del mismo modo que lo haría para un controlador de dominio o para otra parte importante de la infraestructura.

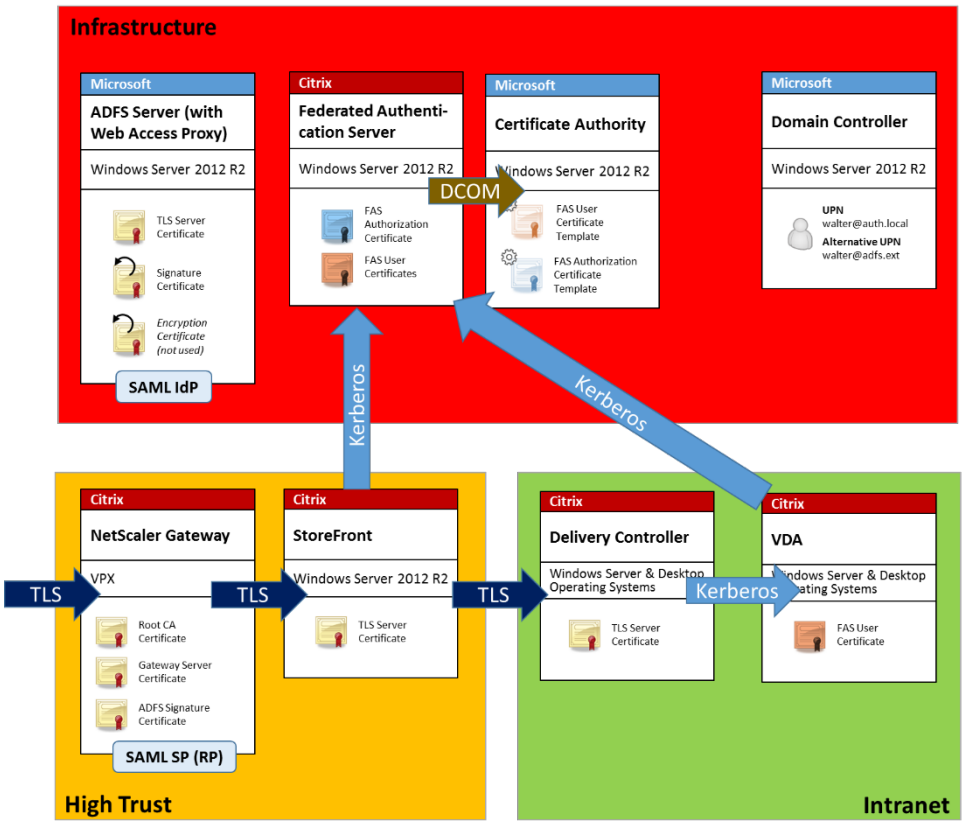
Este documento presenta un resume de las cuestiones de seguridad que se deben tener en cuenta al implementar los servicios FAS. También proporciona una visión general de las características disponibles que pueden ayudarle a proteger su infraestructura.

Arquitectura de red

El diagrama siguiente muestra los componentes principales y los límites de seguridad usados en una implementación de FAS.

El servidor FAS debe tratarse como una parte de la infraestructura fundamental para la seguridad, junto con la entidad de certificación (CA) y el controlador de dominio. En un entorno federado, Citrix NetScaler y Citrix StoreFront son componentes de confianza para realizar la autenticación de usuarios; otros componentes de Citrix Virtual Apps and Desktops no se ven afectados por la introducción de FAS.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Seguridad de red y firewalls

La comunicación entre NetScaler, StoreFront y los componentes de Delivery Controller debe estar protegida con TLS a través del puerto 443. El servidor StoreFront realiza únicamente conexiones salientes y Citrix Gateway debe aceptar solo conexiones a través de Internet que usen HTTPS en el puerto 443.

El servidor StoreFront contacta con el servidor FAS a través del puerto 80 mediante autenticación Kerberos mutua. En la autenticación se utiliza la identidad Kerberos HOST/FQDN del servidor FAS y la identidad Kerberos de la cuenta de máquina del servidor StoreFront. Eso genera un identificador de credenciales de un solo uso, necesario para que Citrix Virtual Delivery Agent (VDA) inicie la sesión del usuario.

Cuando una sesión HDX se conecta al VDA, el VDA también se comunica con el servidor FAS en el puerto 80. En la autenticación, se utiliza la identidad Kerberos HOST/FQDN del servidor FAS y la identidad Kerberos de máquina del VDA. Además, el VDA debe proporcionar el identificador de credenciales para acceder al certificado y la clave privada.

La entidad de certificación (CA) de Microsoft acepta la comunicación con DCOM autenticado con Kerberos, que se puede configurar para usar un puerto TCP fijo. La CA también requiere que el servidor FAS proporcione un paquete CMC firmado por un certificado de agente de inscripción de confianza.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Servidor	Puertos de firewall
Servicio de autenticación federada	[entrada] Kerberos por HTTP desde StoreFront y los VDA, [salida] DCOM hacia la entidad de certificación (CA) de Microsoft
NetScaler	[entrada] HTTPS desde las máquinas cliente, [entrada o salida] HTTPS hacia o desde el servidor StoreFront, [salida]HDX hacia VDA
StoreFront	[entrada] HTTPS desde NetScaler, [salida] HTTPS a Delivery Controller, [salida] Kerberos HTTP hacia FAS
Delivery Controller	[entrada] HTTPS desde el servidor StoreFront, [entrada o salida] Kerberos a través de HTTP desde los VDA
VDA	[entrada o salida] Kerberos por HTTP desde Delivery Controller, [entrada] HDX desde Citrix Gateway, [salida] Kerberos HTTP hacia FAS
Entidad de certificación de Microsoft	[entrada] DCOM y firmado desde FAS

Responsabilidades de administración

La administración del entorno se puede dividir en los siguientes grupos:

Nombre	Responsabilidad
Administrador de la organización	Instalar y proteger las plantillas de certificado en el bosque
Administrador del dominio	Configurar parámetros de directivas de grupo
Administrador de CA	Configurar la entidad de certificación
Administrador de FAS	Instalar y configurar el servidor FAS
Administrador de StoreFront y NetScaler	Configurar la autenticación de usuarios
Administrador de Citrix Virtual Desktops	Configurar los VDA y los Controllers

Cada administrador controla diferentes aspectos del modelo de seguridad global, lo que permite aplicar un enfoque de defensa en profundidad para proteger el sistema.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configuración de directivas de grupo

Las máquinas FAS de confianza se identifican en una tabla de búsqueda por "número de índice -> FQDN" configurada mediante Directiva de grupo. Al contactar con un servidor FAS, los clientes verifican la identidad Kerberos `HOST\<fqdn>` del servidor FAS. Todos los servidores que tienen acceso al servidor FAS deben tener configuraciones idénticas de FQDN con el mismo índice; de lo contrario, StoreFront y los VDA pueden contactar con servidores FAS distintos.

Para evitar errores de configuración, Citrix recomienda aplicar una única directiva a todas las máquinas del entorno. Ponga cuidado a la hora de modificar la lista de servidores de FAS, especialmente al quitar o reordenar las entradas.

El control de este objeto de directiva de grupo debe estar limitado a los administradores de FAS (y/o los administradores de dominio) encargados de instalar y retirar servidores FAS. Ponga cuidado para no reutilizar un nombre de dominio completo (FQDN) al poco tiempo de retirar un servidor FAS.

Plantillas de certificado

Si no quiere utilizar la plantilla de certificado Citrix_SmartcardLogon suministrada con FAS, puede modificar una copia de ella. Se admiten las siguientes modificaciones.

Cambiar el nombre de una plantilla de certificado

Si quiere cambiar el nombre de Citrix_SmartcardLogon para que coincida con la nomenclatura de nombramiento de plantillas que estipula la organización, debe:

- Crear una copia de la plantilla de certificado y cambiarle el nombre para que coincida con la nomenclatura de la denominación de la organización.
- Use comandos de PowerShell FAS para administrar FAS, en lugar de la interfaz del usuario administrador. (La interfaz del usuario administrador se diseñó para usarla únicamente con los nombres de plantilla predeterminados de Citrix.)
  - Utilice el complemento Plantillas de certificados de MMC de Microsoft o el comando Publish-FasMsTemplate para publicar la plantilla, y
  - Utilice el comando New-FasCertificateDefinition para configurar FAS con el nombre de su plantilla.

Modificar propiedades generales

Puede modificar el período de validez de la plantilla de certificado.

No modifique el período de renovación. FAS ignora esta configuración en la plantilla de certificado. FAS renovará automáticamente el certificado a mitad de su período de validez.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Modificar propiedades de gestión de peticiones

No modifique estas propiedades. FAS ignora esta configuración en la plantilla de certificado. FAS siempre desmarca **Permitir que la clave privada se pueda exportar** y **Renovar con la misma clave**.

Modificar propiedades de criptografía

No modifique estas propiedades. FAS ignora esta configuración en la plantilla de certificado.

Consulte Protección de claves privadas para el Servicio de autenticación federada para conocer los parámetros equivalentes que ofrece FAS.

Modificar propiedades de atestación de clave

No modifique estas propiedades. FAS no admite la atestación de la clave.

Modificar propiedades de plantillas reemplazadas

No modifique estas propiedades. FAS no admite la sustitución de plantillas.

Modificar propiedades de extensiones

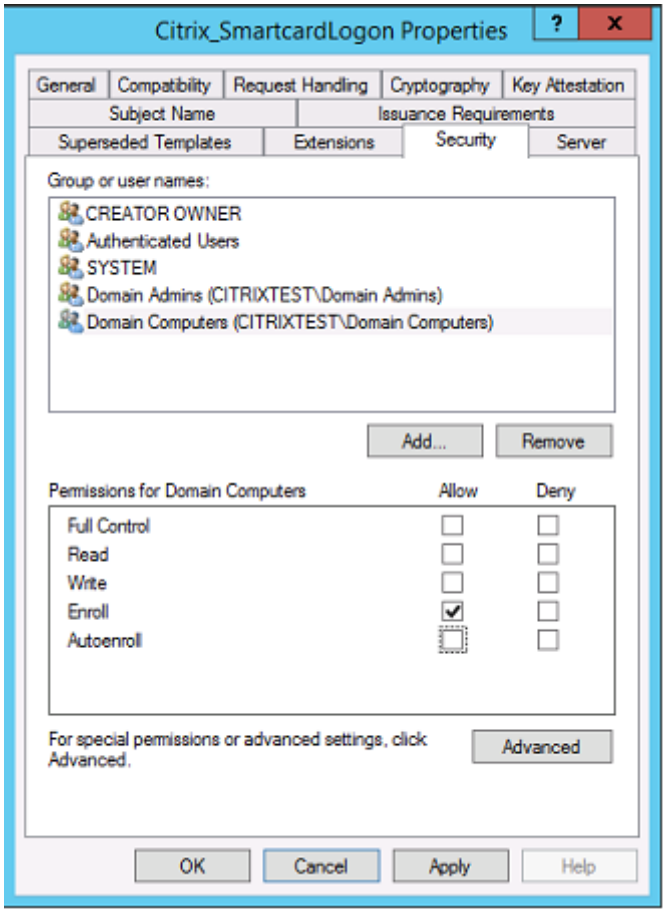
Puede modificar estas opciones de configuración para que coincidan con la directiva de la organización.

Nota: Una configuración inadecuada de las extensiones puede causar problemas de seguridad o resultar en certificados inutilizables.

Modificar propiedades de seguridad

Citrix recomienda modificar estas opciones de configuración para conceder el permiso de **inscripción** solo a las cuentas de máquina de los servidores FAS. En cuanto a otros servicios, conceda también el permiso de **control total** al sistema. No se requiere ningún otro permiso. Puede que le interese conceder otros permisos; por ejemplo, para permitir que los administradores de FAS vean una plantilla modificada para solucionar problemas.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Modificar propiedades de nombre del sujeto

Si fuera necesario, puede modificar estas opciones de configuración para que coincidan con la directiva de la organización.

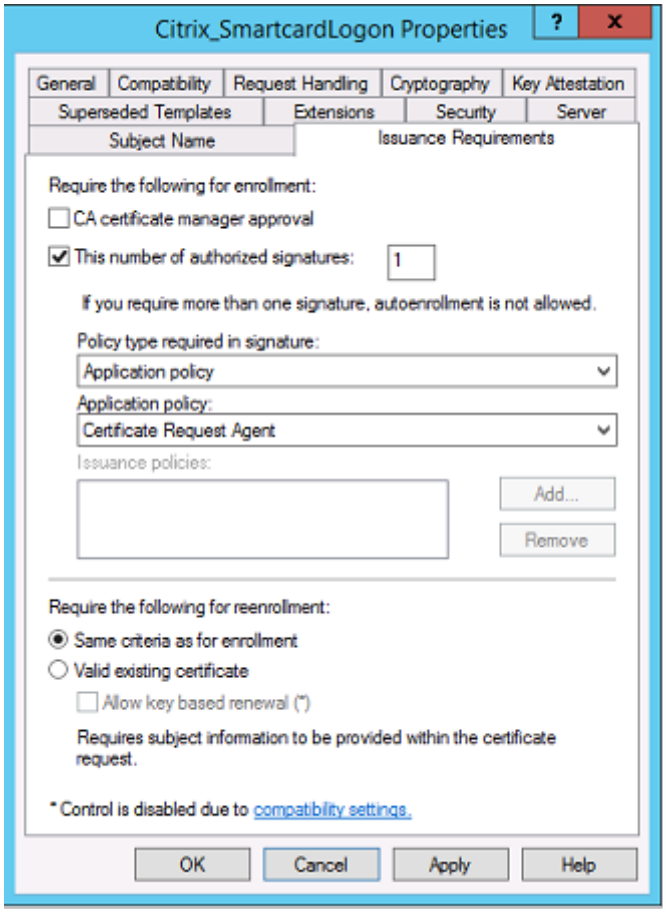
Modificar propiedades de servidor

Aunque Citrix no lo recomienda, puede modificar estas opciones de configuración para que coincidan con la directiva de la organización si fuera necesario.

Modificar propiedades de requisitos de emisión

No modifique estos parámetros. Estos parámetros deben ser como se muestra a continuación:

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Modificar propiedades de compatibilidad

Puede modificar estos parámetros. El valor debe ser al menos **Windows Server 2003 CAs** (versión 2 del esquema). Sin embargo, FAS solo admite entidades emisoras de certificados Windows Server 2008 y posterior. Además, como se ha explicado anteriormente, FAS pasa por alto la configuración adicional disponible si se selecciona **Windows Server 2008 CAs** (versión 3 del esquema) o **Windows Server 2012 CAs** (versión 4 del esquema).

Administrar la entidad de certificación

El administrador de la entidad de certificación (CA) es responsable de la configuración del servidor CA y de la clave privada de emisión de certificados que se usa.

Publicar plantillas

Para que una entidad de certificación emita certificados basados en una plantilla proporcionada por el administrador de la empresa, el administrador de CA debe elegir publicar esa plantilla.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

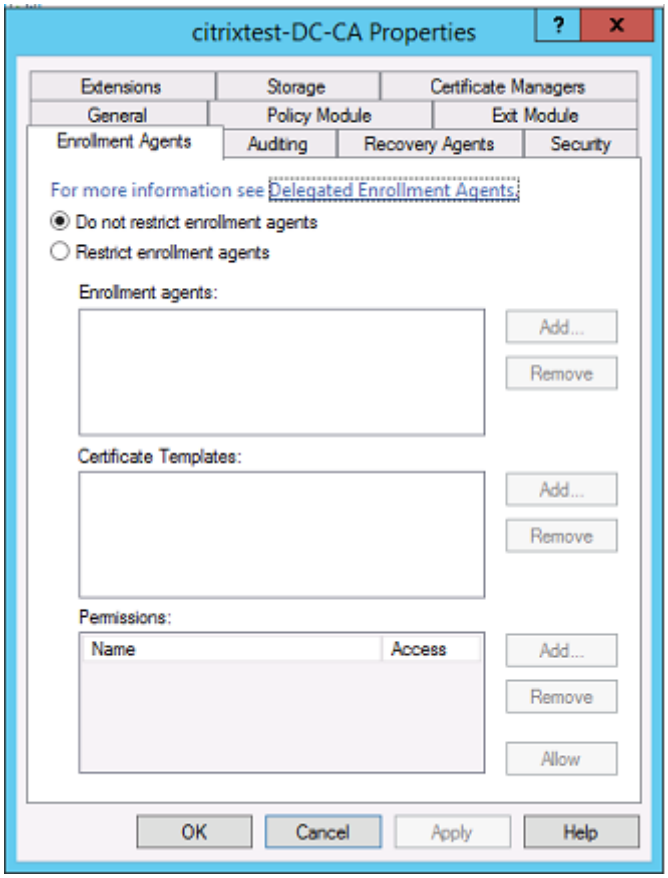
Una sencilla medida de seguridad consiste en publicar solo las plantillas de RA cuando se están instalando los servidores FAS, o insistir en un proceso de emisión que tenga lugar completamente fuera de línea. En ambos casos, el administrador de la CA debe mantener el control total de la autorización de las solicitudes de certificados de RA, y tener una directiva para autorizar los servidores FAS.

Parámetros de firewall

Por lo general, el administrador de la entidad de certificación (CA) también tiene el control de los parámetros de firewall de red de la CA, lo que permite controlar las conexiones entrantes. El administrador de la CA puede configurar reglas de firewall y DCOM TCP para que solo los servidores FAS puedan solicitar certificados.

Inscripción restringida

De forma predeterminada, cualquier titular de un certificado RA puede emitir certificados a cualquier usuario, usando cualquier plantilla de certificado que permita el acceso. Debe restringirse a un grupo de usuarios sin privilegios con la ayuda de la propiedad “Restringir agentes de inscripción” de la CA.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

Módulos de directiva y auditoría

Para implementaciones avanzadas, se pueden usar módulos de seguridad personalizados con los que se puede hacer un seguimiento y vetar la emisión de certificados.

Administrar FAS

FAS tiene varias características de seguridad.

Restringir StoreFront, usuarios y VDA mediante una lista de control de acceso

En el centro del modelo de seguridad de FAS está el control del acceso a la funcionalidad para las cuentas de Kerberos:

Vector de acceso	Descripción
[Proveedor de identidades] de StoreFront	Estas cuentas de Kerberos son de confianza para declarar que un usuario se ha autenticado correctamente. Si una de estas cuentas está en situación de riesgo, se pueden crear y usar certificados para los usuarios permitidos por la configuración de FAS.
[Entidad de confianza] de los VDA	Estas son las máquinas a las que se permite acceder a los certificados y las claves privadas. Se necesita también un identificador de credencial obtenido por el IdP, de modo que una cuenta de VDA de este grupo que esté en situación de riesgo tendrá un ámbito muy limitado para atacar el sistema.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Vector de acceso	Descripción
Usuarios	Esto controla qué usuarios pueden ser objeto de aserciones de proveedor de identidades (IdP). Tenga en cuenta que esto se solapa con las opciones de configuración de Agente de inscripción restringido (Restricted Enrollment Agent) en la CA. En general, se recomienda incluir solo cuentas sin privilegios en esta lista. Esto evita que una cuenta de StoreFront que esté en situación de riesgo pueda aumentar sus privilegios a un nivel administrativo superior. En concreto, las cuentas de administrador de dominio no deben permitirse en esta lista de control de acceso.

Configurar reglas

Las reglas son útiles cuando hay varias implementaciones de Citrix Virtual Apps o Citrix Virtual Desktops independientes que usan la misma infraestructura de servidor FAS. Cada regla tiene un conjunto de opciones de configuración aparte; en concreto, las listas de control de acceso se pueden configurar de forma independiente.

Configurar la entidad de certificación (CA) y las plantillas

Se pueden configurar plantillas de certificados y entidades de certificación diferentes para distintos derechos de acceso. En configuraciones avanzadas, se puede elegir usar certificados más o menos potentes en función del entorno. Por ejemplo, los usuarios identificados como “externos” pueden tener un certificado con menos privilegios que los usuarios “internos”.

Certificados de sesión y de autenticación

El administrador de FAS puede controlar si el certificado usado para autenticar está disponible para su uso también dentro de la sesión del usuario. Por ejemplo, puede tener solo certificados de “firma” disponibles durante la sesión, y usar el certificado más potente de “inicio de sesión” solo para iniciar sesión.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Protección de la clave privada y longitud de la clave

El administrador de FAS puede configurar FAS para almacenar las claves privadas en un módulo de seguridad de hardware (HSM) o en un módulo de plataforma de confianza (TPM). Citrix recomienda que se almacene, por lo menos, la clave privada del certificado de RA en un módulo TPM para protegerla; esta opción se ofrece como parte del proceso de solicitud de certificado "sin conexión".

Del mismo modo, las claves privadas de certificado de usuario se pueden guardar en un módulo TPM o HSM. Todas las claves deben generarse como "no-exportables" y deben tener una longitud mínima de 2048 bits.

Registros de eventos

El servidor FAS proporciona registros de eventos detallados sobre configuración y tiempo de ejecución, que se pueden utilizar para la auditoría y la detección de intrusiones.

Acceso administrativo y herramientas de administración

El servicio FAS incluye herramientas y características de administración remota (autenticación Kerberos mutua). Los miembros del grupo "Administradores locales" tienen control total sobre la configuración de FAS. Esta lista se debe mantener con cuidado.

Administradores de VDA, Citrix Virtual Apps y Citrix Virtual Desktops

En general, usar FAS no cambia el modelo de seguridad de los administradores de VDA ni Delivery Controller, ya que el "identificador de credencial" de FAS simplemente reemplaza la "contraseña de Active Directory". Los grupos de administración de Controller y VDA deben contener solo usuarios de confianza. Deben mantenerse registros de eventos y auditoría.

Seguridad general de los servidores Windows

Todos los servidores deben contar con las revisiones disponibles y tener instalado un software de firewall y antivirus estándar. Los servidores de la infraestructura de importancia crítica para la seguridad deben ubicarse en un lugar protegido físicamente, y hay que poner especial cuidado en las opciones de cifrado de los discos y el mantenimiento de las máquinas virtuales.

Los registros de eventos y auditoría deben almacenarse de forma segura en una máquina remota.

El acceso RDP debe limitarse solo a administradores autorizados. Cuando sea posible, las cuentas de usuario deben requerir el inicio de sesión con tarjeta inteligente, especialmente para las cuentas de administradores de dominio y de CA.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Información relacionada

- El artículo Servicio de autenticación federada (FAS - Federated Authentication Service) es la referencia principal para la instalación y la configuración de este servicio.
- Las arquitecturas de FAS se resumen en el artículo Introducción a las arquitecturas del Servicio de autenticación federada.
- En el artículo Administrar y configurar el Servicio de autenticación federada se indican otros artículos de procedimientos.

Soluciones a problemas de inicio de sesión en Windows relacionados con el Servicio de autenticación federada

December 4, 2018

En este artículo, se describen los registros y los mensajes de error que Windows muestra cuando un usuario inicia sesión con certificados y/o tarjetas inteligentes. Estos registros ofrecen información que se puede utilizar para solucionar fallos de autenticación.

Certificados e infraestructura de clave pública

Active Directory de Windows mantiene varios almacenes de certificados que administran certificados para los usuarios que inician sesión.

- **Almacén de certificados NTAuth:** Para autenticarse en Windows, la entidad de certificación (CA) que acaba de emitir los certificados de usuario (es decir, no se admiten entidades de certificación en cadena) debe colocarse en el almacén NTAuth. Para ver los certificados, desde el programa CertUtil, escriba: certutil –viewstore –enterprise NTAuth.
- **Almacén de certificados raíz e intermedios:** Por lo general, los sistemas de inicios de sesión con certificados pueden proporcionar solo un certificado, de modo que, si se utilizan certificados en cadena, el almacén de certificados intermedios de todas las máquinas debe incluir esos certificados. El certificado raíz debe estar en el almacén raíz de confianza y el penúltimo certificado debe estar en el almacén NTAuth.
- **Extensiones del certificado de inicio de sesión y directivas de grupo**. Windows se puede configurar para aplicar la verificación de EKU y otras directivas de certificados. Consulte la documentación de Microsoft: https://technet.microsoft.com/en-us/library/ff404287%28v=ws.10%29.aspx.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Directiva de Registro	Descripción
AllowCertificatesWithNoEKU	Cuando está inhabilitada, los certificados deben incluir la propiedad Uso mejorado de clave (EKU) para el inicio de sesión con tarjeta inteligente.
AllowSignatureOnlyKeys	De forma predeterminada, Windows filtra y excluye las claves privadas de los certificados que no permiten el descifrado RSA. Esta opción anula ese filtro.
AllowTimeInvalidCertificates	De forma predeterminada, Windows filtra y excluye los certificados caducados. Esta opción anula ese filtro.
EnumerateECCCerts	Habilita la autenticación de curva elíptica.
X509HintsNeeded	Si un certificado no contiene un nombre principal de usuario (UPN) único o contiene uno que puede ser ambiguo, esta opción permite a los usuarios especificar manualmente su cuenta de inicio de sesión en Windows.
UseCachedCRLOnlyAnd, IgnoreRevocationUnknownErrors	Inhabilita la comprobación de revocación (normalmente establecida en el controlador de dominio).

- **Certificados de controlador de dominio:** Para la autenticación de conexiones Kerberos, todos los servidores deben tener los certificados “Domain Controller” (Controlador de dominio) que corresponden. Se pueden solicitar desde el menú de complemento MMC “Local Computer Certificate Personal Store” (Almacén personal de certificados del equipo local).

Nombre UPN y asignación de certificados

Se recomienda que los certificados de usuario contengan un nombre principal de usuario (UPN) único en la extensión Nombre alternativo del firmante.

Nombres UPN en Active Directory

De forma predeterminada, en Active Directory todos los usuarios tienen un UPN implícito que se forma siguiendo el formato <samUsername>@<domainNetBios> y <samUsername>@<domainFQDN>,

© 1999-2019 Citrix Systems, Inc. All rights reserved.

es decir, <nombre de usuario SAM>@<NetBIOS del dominio> y <nombre de usuario SAM>@<FQDN de dominio>. Los dominios y los nombres FQDN disponibles se incluyen en la entrada RootDSE del bosque. Tenga en cuenta que un solo dominio puede tener varias direcciones FQDN registradas en el RootDSE.

Además, todo usuario en Active Directory tiene un nombre UPN explícito y altUserPrincipalNames. Son las entradas de LDAP que especifican el nombre UPN para el usuario.

Cuando se buscan usuarios por nombre UPN, Windows examina primero el dominio actual (basado en la identidad del proceso que busca el nombre UPN) para buscar nombres UPN explícitos y luego busca nombres UPN alternativos. Si no hay coincidencias, busca el nombre UPN implícito, lo que puede resultar en varios dominios en el bosque.

Servicio de asignaciones de certificado

Si un certificado no incluye un nombre UPN explícito, Active Directory tiene la opción de almacenar un certificado público exacto para cada uso en un atributo "x509certificate". Para resolver un certificado así para un usuario, el sistema puede consultar ese atributo directamente (de forma predeterminada, en un único dominio).

Se ofrece una opción para que el usuario especifique una cuenta de usuario que acelere la búsqueda, lo que también permite que esta funcionalidad se utilice en un entorno de varios dominios.

Si hay varios dominios en el bosque y el usuario no especifica explícitamente un dominio, RootDSE de Active Directory especifica la ubicación del servicio de asignaciones de certificado. Por regla general, este servicio se encuentra en una máquina del catálogo global y tiene una vista en caché de todos los atributos "x509certificate" del bosque. Ese equipo resulta eficaz para buscar cuentas de usuario en cualquier dominio basándose solamente en el certificado.

Controlar la selección del controlador de dominio para iniciar sesión

Cuando un entorno contiene varios controladores de dominio, es muy útil ver y precisar el controlador de dominio concreto (restringir los demás) que debe utilizarse para la autenticación, de modo que los registros se puedan habilitar y recuperar.

Controlar la selección del controlador de dominio

Para forzar Windows a usar un controlador de dominio Windows concreto para el inicio de sesión, puede establecer explícitamente la lista de los controladores de dominio que una máquina Windows puede utilizar. Para ello, debe configurar el archivo lmhosts: \Windows\System32\drivers\etc\lmhosts.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Por regla general, hay un archivo de muestra denominado “lmhosts.sam” en esa ubicación. Solo necesita incluir una línea:

1.2.3.4 cnetbiosname #PRE #DOM:mydomain

Donde “1.2.3.4” es la dirección IP del controlador de dominio llamado “dcnetbiosname” en el dominio “mydomain”.

Después de reiniciarse, la máquina Windows usará esa información para iniciar sesión en “mydomain”. Tenga en cuenta que esta configuración debe revertirse cuando la depuración se complete.

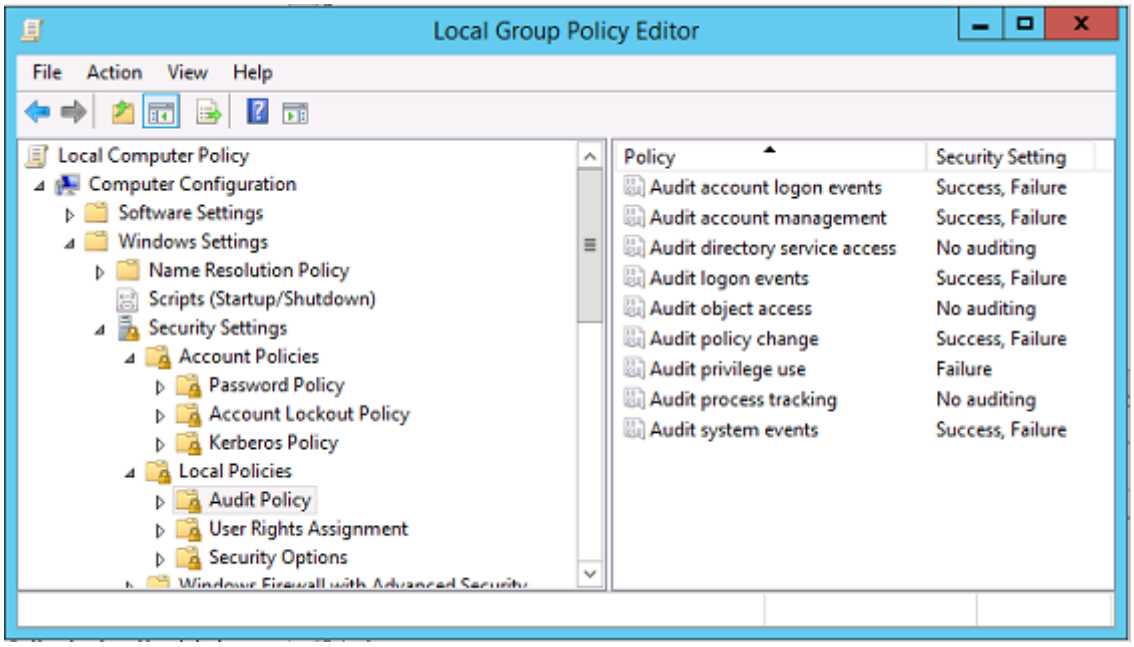
Identificar el controlador de dominio en uso

Durante el inicio de sesión, Windows aplica una variable de entorno MSDOS con el controlador de dominio que inició la sesión del usuario. Para verlo, inicie el símbolo del sistema con el comando: **echo %LOGONSERVER%**.

Los registros relacionados con la autenticación se almacenan en el equipo que devuelva este comando.

Habilitar eventos de auditoría de cuentas

De forma predeterminada, los controladores de dominio de Windows no habilitan los registros de auditoría completa de la cuenta. La captura de registros se puede controlar mediante directivas de auditoría, ubicadas en la configuración de seguridad del Editor de directivas de grupo. Una vez habilitadas, el controlador de dominio genera más información de registro de sucesos que se guarda en el archivo del registro de seguridad.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

Registros de validación de certificados

Comprobar la validez del certificado

Si un certificado de tarjeta inteligente se exporta como certificado DER (sin clave privada requerida), se puede validar con el comando: certutil –verify user.cer

Habilitar la captura de registros de CAPI

En el controlador de dominio y la máquina de usuarios, abra el visor de eventos y habilite la captura de registros de Microsoft/Windows/CAPI2/Operational Logs.

Puede gestionar la captura de registros CAPI con las claves de Registro en: CurrentControlSet\Services\crypt32.

Valor	Descripción
DiagLevel (DWORD)	Nivel de detalle (de 0 a 5)
DiagMatchAnyMask (QUADWORD)	Filtro de eventos (use 0xffffff para todo)
DiagProcessName (MULTI_SZ)	Filtrar por nombre del proceso (por ejemplo, LSASS.exe)

Registros de CAPI

Mensaje	Descripción
Compilar cadena	LSA llamado CertGetCertificateChain (incluye resultado)
Comprobar revocación	LSA llamado CertVerifyRevocation (incluye resultado)
Objetos X509	En el modo detallado, los certificados y las listas de revocación de certificados (CRL) se vuelcan en AppData\LocalLow\Microsoft\X509Objects
Comprobar directiva de cadena	LSA llamado CertVerifyChainPolicy (incluye parámetros)

Mensajes de error

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Código de error	Descripción
Certificate not trusted (El certificado no es de confianza)	El certificado de tarjeta inteligente no se ha podido crear con certificados provenientes de los almacenes de certificados intermedios y certificados raíz de confianza alojados en el equipo.
Certificate revocation check error (Error en la comprobación de revocaciones de certificados)	La lista de revocación de certificados de la tarjeta inteligente no se ha podido descargar desde la dirección que especifica el punto de distribución de la CRL del certificado. Si la comprobación de revocación de certificados es obligatoria, este error impide el inicio de sesión. Consulte la sección Certificados e infraestructura de clave pública.
Certificate Usage errors (Errores de uso de certificados)	El certificado no es adecuado para el inicio de sesión. Por ejemplo, puede tratarse de un certificado de servidor o un certificado de firma.

Registros Kerberos

Para habilitar captura de registros Kerberos, en el controlador de dominio y la máquina del usuario final, cree los siguientes valores de Registro:

Subárbol de Registro	Nombre del valor	Valor [DWORD]
CurrentControlSet\Control\Lsa	LogLevel	0x1
CurrentControlSet\Control\Lsa\Kerberos\Parameters	LogToFile	0xffffffff
CurrentControlSet\Services\Kdc	KdcDebugLevel	0x1
CurrentControlSet\Services\Kdc	KdcExtraLogLevel	0x1f

El registro Kerberos se guarda en el registro de eventos del sistema.

- Los mensajes del tipo “El certificado no es de confianza” deberían ser fáciles de diagnosticar.
- Hay dos códigos de error que son informativos y se pueden ignorar sin consecuencias negativas:
  - KDC_ERR_PREAUTH_REQUIRED (utilizado para la compatibilidad con versiones anteriores de controladores de dominio)

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Error desconocido 0x4b

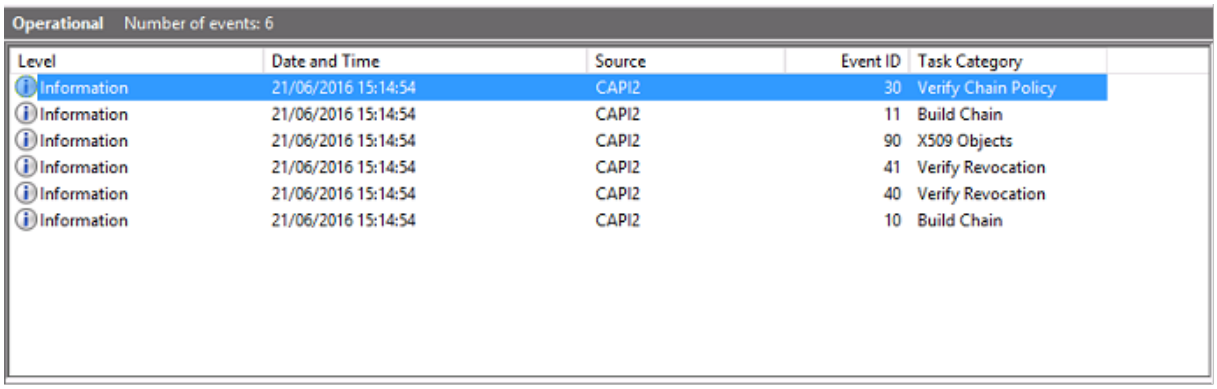
Mensajes del registro de sucesos

En esta sección, se describen entradas de registro previstas en el controlador de dominio y en la estación de trabajo cuando el usuario inicia sesión con un certificado.

- Registro de CAPI2 del controlador de dominio
- Registros de seguridad del controlador de dominio
- Registro de seguridad del VDA
- Registro de CAPI del VDA
- Registro del sistema del VDA

Registro de CAPI2 del controlador de dominio

Durante el inicio de sesión, el controlador de dominio valida el certificado del autor de llamada, con lo que genera la siguiente secuencia de entradas de registro.



El último mensaje del registro de eventos muestra Isass.exe en el controlador de dominio creando una cadena basada en el certificado proporcionado por el agente VDA y comprobando la validez de ese certificado (incluida la revocación). El resultado se devuelve como “ERROR_SUCCESS”.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

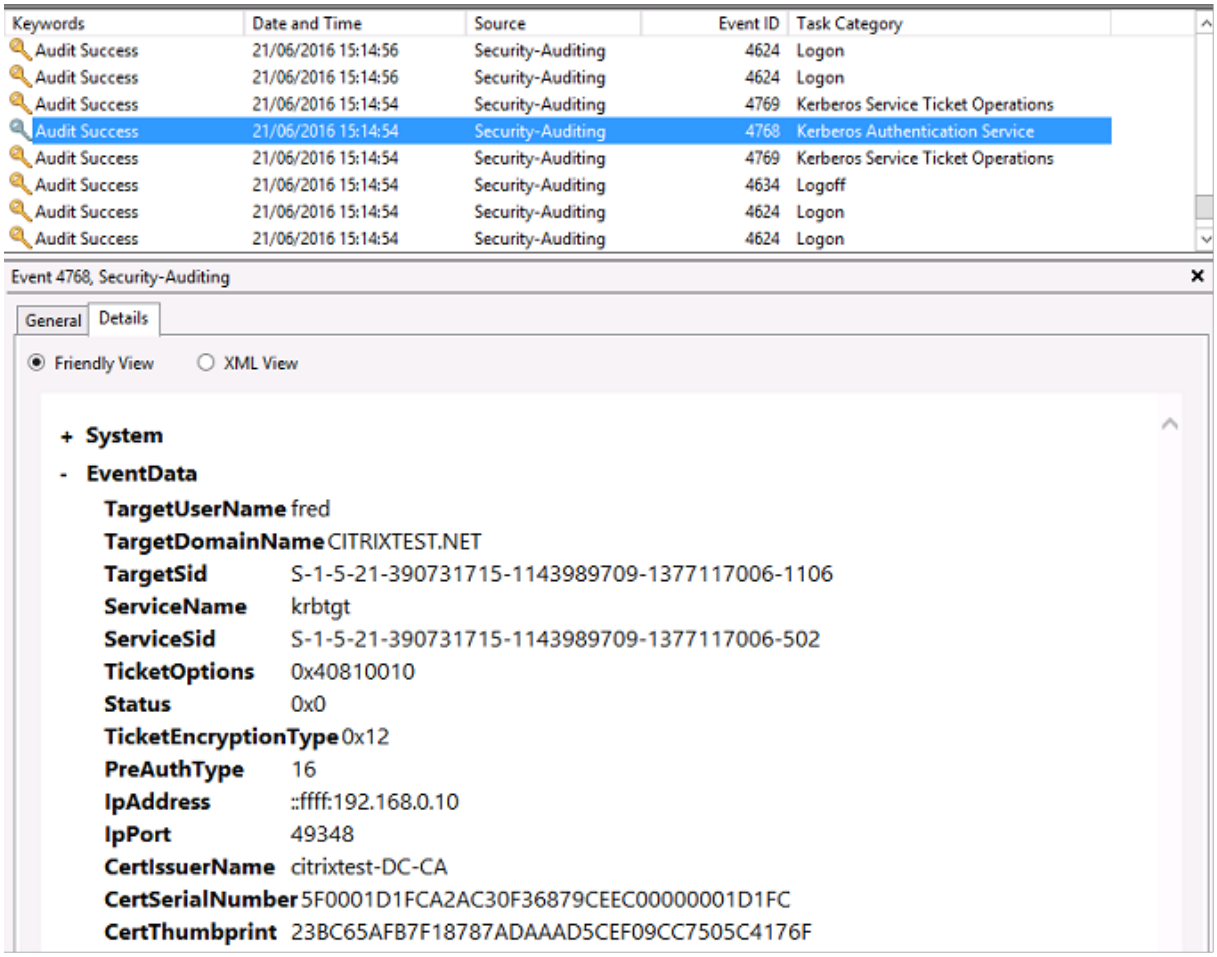
- **CertVerifyCertificateChainPolicy**
  - **Policy**
    - [**type**] CERT_CHAIN_POLICY_NT_AUTH
    - [**constant**] 6
  - **Certificate**
    - [**fileRef**] 23BC65AFB7F18787ADAAAD5CEF09CC7505C4176F.cer
    - [**subjectName**] fred
  - **CertificateChain**
    - [**chainRef**] {FF03F79B-52F8-4C93-877A-5DFFE40B9574}
  - **Flags**
    - [**value**] 0
  - **Status**
    - [**chainIndex**] -1
    - [**elementIndex**] -1
  - **EventAuxInfo**
    - [**ProcessName**] lsass.exe
  - **CorrelationAuxInfo**
    - [**TaskId**] {F5E7FD3F-628F-4C76-9B1C-49FED786318F}
    - [**SeqNumber**] 1
  - **Result**
    - [**value**] 0

Registro de seguridad del controlador de dominio

El controlador de dominio muestra una secuencia de eventos de inicio de sesión (la clave es 4768), donde el certificado se usa para emitir el vale de concesión de vales Kerberos (krbtgt).

Los mensajes anteriores a este muestran la cuenta de máquina del servidor que se autentica en el controlador de dominio. Los mensajes siguientes muestran la cuenta de usuario que pertenece al nuevo vale krbtgt que se usa para autenticarse en el controlador de dominio.

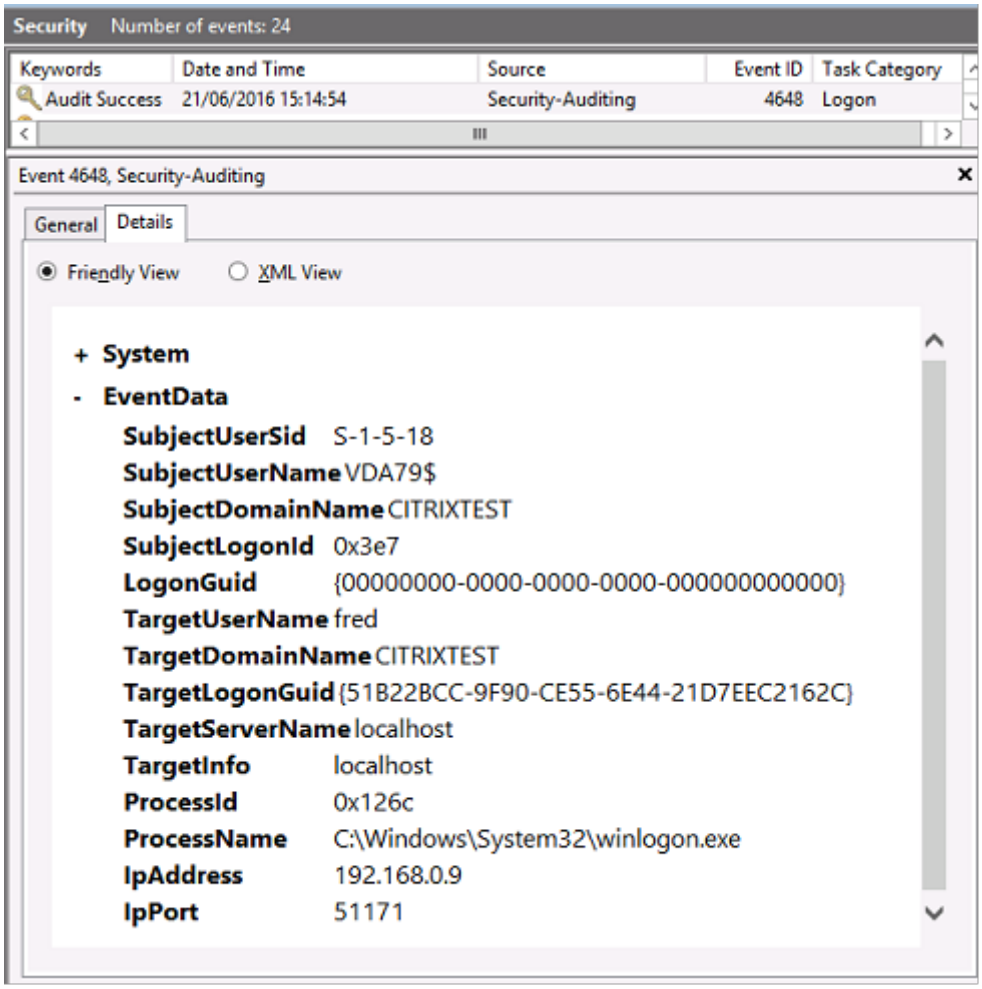
© 1999-2019 Citrix Systems, Inc. All rights reserved.



Registro de seguridad del VDA

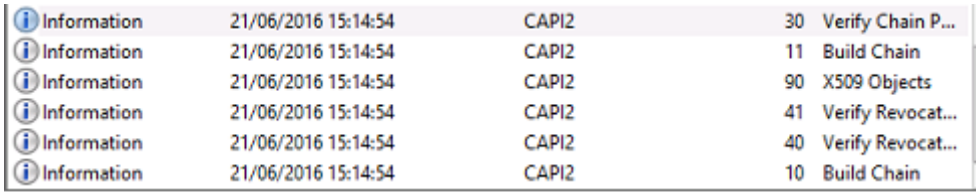
El registro de auditoría de seguridad del VDA que corresponde al evento de inicio de sesión es la entrada cuyo ID de evento es 4648, originado de winlogon.exe.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

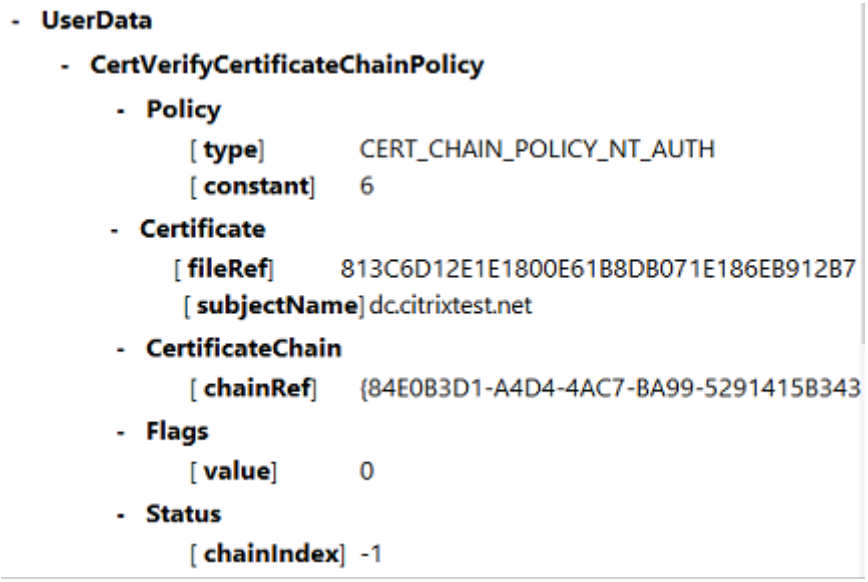


Registro de CAPI del VDA

En este ejemplo, el registro de CAPI del VDA muestra una sola secuencia de compilación de cadena y comprobación desde lsass.exe, que valida el certificado del controlador de dominio (dc.citrixtest.net).

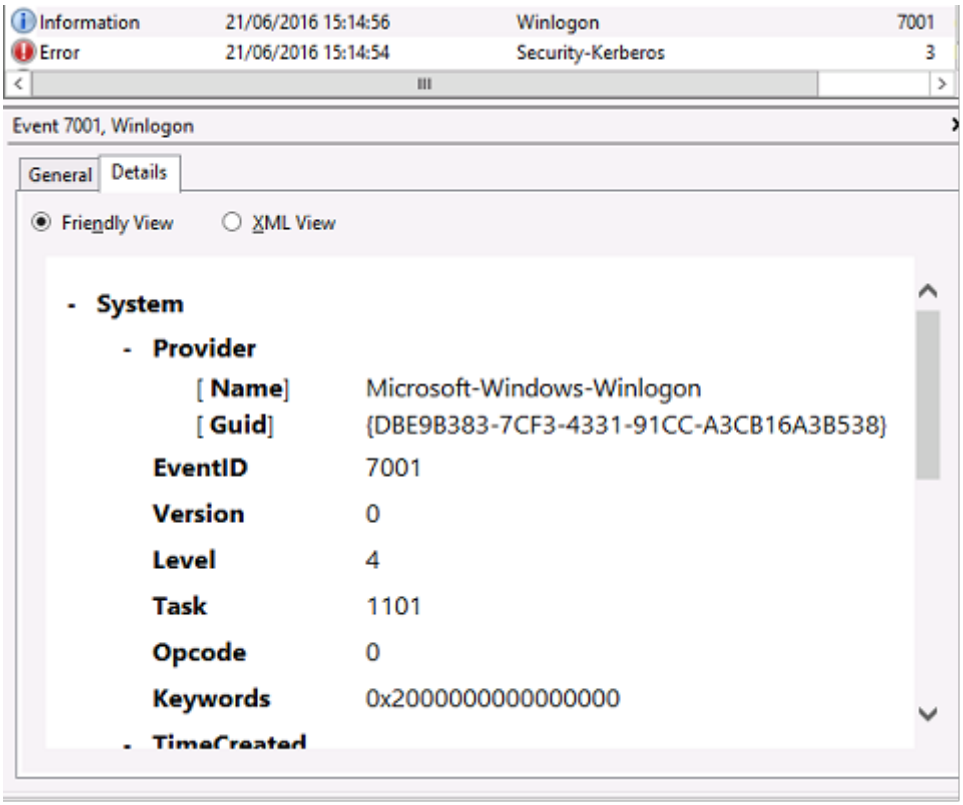


© 1999-2019 Citrix Systems, Inc. All rights reserved.



Registro del sistema del VDA

Si la captura de registros Kerberos está habilitada, el registro del sistema muestra el error KDC_ERR_PREAUTH_REQUIRED (que se puede ignorar) y una entrada de Winlogon con el mensaje de que el inicio de sesión con Kerberos se realizó correctamente.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

Mensajes de error del usuario final

En esta sección, se ofrece una lista de los mensajes de error comunes que ve un usuario en la página de inicio de sesión de Windows.

Mensaje de error mostrado	Descripción y referencia
Nombre de usuario o contraseña no válidos.	El equipo cree que usted tiene un certificado y una clave privada válidos, pero el controlador de dominio Kerberos ha rechazado la conexión. Consulte la sección *Registros Kerberos* de este artículo.
El sistema no pudo iniciar sesión. No se pudieron comprobar las credenciales. / La solicitud no se admite.	No se puede contactar con el controlador de dominio, o bien, el controlador de dominio no tiene instalados los certificados correspondientes. Vuelva a inscribir los certificados “Domain Controller” y “Domain Controller Authentication” en el controlador de dominio, como se describe en CTX206156. Suele valer la pena intentarlo incluso cuando los certificados existentes parezcan válidos.
El sistema no pudo iniciar sesión. No se puede determinar el estado de revocación del certificado de la tarjeta inteligente usado para la autenticación.	Los certificados intermedios y de raíz no están instalados en el equipo local. Consulte CTX206156 para obtener instrucciones sobre la instalación de certificados de tarjeta inteligente en equipos sin dominio. Asimismo, consulte Certificados e infraestructura de clave pública.
No puede iniciar sesión porque el inicio de sesión con tarjeta inteligente no se admite en su cuenta.	No se ha configurado completamente ninguna cuenta de usuario de grupo de trabajo para el inicio de sesión con tarjeta inteligente.
La clave solicitada no existe.	Un certificado hace referencia a una clave privada a la que no se puede acceder. Puede ocurrir cuando la tarjeta inteligente PIV no se ha configurado completamente y falta el archivo CHUID o CCC.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Mensaje de error mostrado	Descripción y referencia
Ha ocurrido un error al intentar usar la tarjeta inteligente.	El middleware de la tarjeta inteligente no se ha instalado correctamente. Consulte CTX206156 para obtener las instrucciones de instalación de tarjetas inteligentes.
“Inserte una tarjeta inteligente.	No se ha detectado el lector o la tarjeta inteligente. Si la tarjeta inteligente está insertada, este mensaje indica un problema de hardware o middleware. Consulte CTX206156 para obtener las instrucciones de instalación de tarjetas inteligentes.
El PIN no es correcto.	La tarjeta inteligente ha rechazado el PIN especificado por el usuario.
No se ha encontrado ningún certificado de tarjeta inteligente válido.	Es posible que las extensiones del certificado no estén configuradas correctamente o puede que la clave RSA sea demasiado corta (<2048 bits). Consulte CTX206901 para obtener información acerca de la generación de certificados de tarjeta inteligente válidos.
La tarjeta inteligente está bloqueada.	Se ha bloqueado una tarjeta inteligente (por ejemplo, el usuario ha introducido un PIN incorrecto varias veces). Un administrador puede tener acceso al código PUK (el código para desbloquear el PIN) de la tarjeta inteligente, por lo que puede restablecer el PIN de usuario mediante una herramienta suministrada por el proveedor de la tarjeta inteligente. Si el código PUK no está disponible (o está bloqueado), la tarjeta inteligente debe restablecerse a los parámetros de fábrica.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Mensaje de error mostrado	Descripción y referencia
Solicitud incorrecta.	La clave privada de la tarjeta inteligente no admite el cifrado que requiere el controlador de dominio. Por ejemplo, puede que el controlador de dominio haya solicitado “un descifrado de clave privada”, pero la tarjeta inteligente solo respalda la firma. Normalmente, esto indica que las extensiones del certificado no están configuradas correctamente o la clave RSA es demasiado corta (<2048 bits). Consulte CTX206901 para obtener información acerca de la generación de certificados de tarjeta inteligente válidos.

Información relacionada

- Configurar un dominio para el inicio de sesión con tarjeta inteligente: http://support.citrix.com/article/CTX206156
- Directivas de inicio de sesión con tarjeta inteligente: https://technet.microsoft.com/en-us/library/ff404287%28v=ws.10%29.aspx
- Habilitar la captura de registros de CAPI: http://social.technet.microsoft.com/wiki/contents/articles/242.troubleshooting-pki-problems-on-windows.aspx
- Habilitar la captura de registros de Kerberos: https://support.microsoft.com/en-us/kb/262177
- Instrucciones para habilitar el inicio de sesión mediante tarjeta inteligente con entidades de certificación de terceros: https://support.microsoft.com/en-us/kb/281245

Cmdlets de PowerShell para el Servicio de autenticación federada (FAS)

October 3, 2018

Aunque la consola de administración del Servicio de autenticación federada es adecuada para implementaciones simples, la interfaz de PowerShell ofrece opciones más avanzadas. Si va a usar opciones que no están disponibles en la consola, Citrix recomienda utilizar solo PowerShell para la configuración.

El siguiente comando agrega los cmdlets de PowerShell para FAS:

```
1 Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

En una ventana de PowerShell, use Get-Help <*nombre del cmdlet*> para ver la ayuda del cmdlet.

Para obtener más información sobre los cmdlets de FAS PowerShell SDK, consulte https://developer-docs.citrix.com/.

Dispositivos

March 8, 2019

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:

- Citrix Ready Workspace Hub
- Dispositivo USB genérico
- Dispositivos móviles y de pantalla táctil
- Dispositivos en serie
- Teclados especiales
- Dispositivos TWAIN
- Cámaras Web

Dispositivo USB optimizado y genérico

Un dispositivo USB optimizado es aquel para el cual la aplicación Citrix Workspace tiene respaldo específico. Por ejemplo, la capacidad de redirigir cámaras web utilizando el canal virtual multimedia HDX. Un dispositivo genérico es un dispositivo USB para el que no hay respaldo específico en la aplicación Citrix Workspace.

De forma predeterminada, la redirección de USB genérico no puede redirigir dispositivos USB con respaldo optimizado 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Cuando se dan estas condiciones, el dispositivo de almacenamiento masivo se redirige utilizando 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 sólo 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

Citrix Ready Workspace Hub

March 14, 2019

Citrix Ready Workspace Hub combina entornos digitales y físicos para entregar aplicaciones y datos dentro de un espacio inteligente y seguro. El sistema completo conecta dispositivos (o *cosas*), como aplicaciones móviles y sensores, para crear un entorno inteligente que responda adecuadamente.

Citrix Ready Workspace Hub se basa en la plataforma Raspberry Pi 3 y se convierte en un servicio sólido que se entrega a través de Citrix Cloud. Los usuarios de Citrix Ready Workspace Hub pueden autenticar sus dispositivos móviles a través de la aplicación Citrix Workspace para ejecutar aplicaciones o escritorios publicados. Por ejemplo, Citrix Virtual Apps and Desktops, Citrix Content Collaboration y Microsoft Outlook. A continuación, el dispositivo móvil se conecta a Citrix Ready Workspace Hub y transmite el escritorio o la aplicación hacia una pantalla más grande.

Citrix Ready Workspace Hub habilita Citrix Casting, que ofrece dos casos de uso que mejoran la productividad y la colaboración de los usuarios.

- Roaming de la sesión: Una sesión de Citrix puede moverse y pasar desde el dispositivo móvil (dispositivo Android) al Workspace Hub.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Transmisión de pantalla: El usuario redirige su pantalla desde una sesión remota desde un dispositivo Android o Windows a un concentrador desocupado.

Citrix Casting utiliza la detección de balizas o un escáner de código QR para conectarse. Con la detección de balizas, si hay varios Citrix Ready Workspace Hub disponibles, el usuario debe seleccionar el concentrador apropiado. Como alternativa, un escáner de códigos QR ofrece seguridad para impedir la transmisión involuntaria a la pantalla incorrecta.

Además, los administradores pueden configurar su entorno con varios monitores de pantalla utilizando un adaptador de pantalla secundaria (Secondary Display Adapter o SDA). Al hacerlo se permite al usuario extender el escritorio o la aplicación en cualquiera de los casos de uso.

Requisitos del sistema

Red

- El dispositivo móvil debe estar en la misma red (Wi-Fi o una red de área local) que el Workspace Hub.
- No bloquee el puerto 55555 entre el dispositivo móvil y Workspace Hub.
- Para Citrix Casting, no bloquee el puerto 1494.
- El puerto 55556 es el puerto predeterminado para las conexiones SSL entre los dispositivos móviles y Citrix Ready Workspace Hub. Puede configurar otro puerto SSL en la página de parámetros de Pi. Si el puerto SSL está bloqueado, los usuarios no pueden establecer conexiones SSL con el concentrador.

Citrix Virtual Desktops

Citrix Ready Workspace Hub se admite en Citrix XenDesktop 7.6 y versiones posteriores.

- Para el roaming de la sesión, compruebe que Citrix Ready Workspace Hub pueda acceder a los servidores Virtual Delivery Agent (VDA).
- Para el roaming de la sesión y la transmisión de pantalla, compruebe que la directiva **Usar códec de vídeo para compresión** en Citrix Studio esté establecida en **Para la pantalla entera**. De lo contrario, podría causar problemas de rendimiento.

Hardware

- Citrix Ready Workspace Hub
- Dos monitores (solo para configuraciones de monitor doble)
- Dispositivo móvil que ejecuta la aplicación Citrix Workspace
- Cable HDMI y fuente de alimentación

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Cable MicroUSB a USB A (si se usa un adaptador de pantalla secundaria o [SDA])
- Hardware opcional (teclado USB, mouse USB o auriculares)
- SDA de Raspberry Pi Zero

Desde octubre de 2018, admitimos dispositivos que se ejecuten en los siguientes sistemas operativos y versiones de Citrix Receiver o de la aplicación Citrix Workspace:

- Android: Citrix Receiver 3.13.5 y versiones posteriores; aplicación Citrix Workspace 1808 para Android y versiones posteriores
- iOS: aplicación Citrix Workspace 1810.1 para iOS
- Mac: aplicación Citrix Workspace 1808 para Mac (Solo las funciones Vista previa y Transmisión de pantalla)
- Windows: aplicación Citrix Workspace 1809 para Windows (solo Transmisión de pantalla)

Actualizar HDX Ready Pi

Para actualizar un dispositivo HDX Ready Pi existente a un Citrix Ready Workspace Hub, consulte los siguientes procedimientos.

- **Viewsonic:** https://www.stratodesk.com/t25-upgrade
- **NComputing**: https://www.ncomputing.com/hub

Configuración inicial con administración interna centralizada

Para crear una consola de administración de Stratodesk, vaya al sitio Web de Stratodesk y cree una cuenta.
https://www.stratodesk.com/kb/Main_Page

Instalación inicial con Citrix Endpoint Management

Para usar Citrix Endpoint Management como la solución de administración para Citrix Ready Workspace Hub, debe configurar ese Workspace Hub para que haga referencia a la URL de administración central. Siga los pasos documentados en Citrix Endpoint Management Server.

> **Nota**
>
> Si el dispositivo ya hace referencia a una consola de administración de NoTouch, puede que deba restablecerlo a los valores predeterminados de fábrica.

Configuración sin administración centralizada

1. Inicie el dispositivo Citrix Ready Workspace Hub.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

2. Vaya a **Inicio > Configuración**. La contraseña predeterminada es “admin”.
3. Vaya a **Conexiones > Agregar**.
4. Modifique la nueva conexión y elija **Citrix/Workspace Hub** en “Modo de conexión”. Haga clic en **Guardar**.
5. En la parte superior de la pantalla, haga clic en el botón **Workspace Hub**.
6. Escriba la URL correspondiente a la pantalla de inicio (agregue `http://` o `https://` a la URL). Por lo general, el enlace apunta a una URL de StoreFront o Citrix Gateway. Sin embargo, puede establecer cualquier URL que quiera iniciar en el concentrador.
7. Haga clic en **Guardar.**
8. Reinicie el dispositivo Citrix Ready Workspace Hub.

Configurar Citrix Virtual Apps and Desktops

Realice algunos cambios en su configuración de Citrix Virtual Apps and Desktops para tener la mejor experiencia con Citrix Ready Workspace Hub.

Skype Empresarial

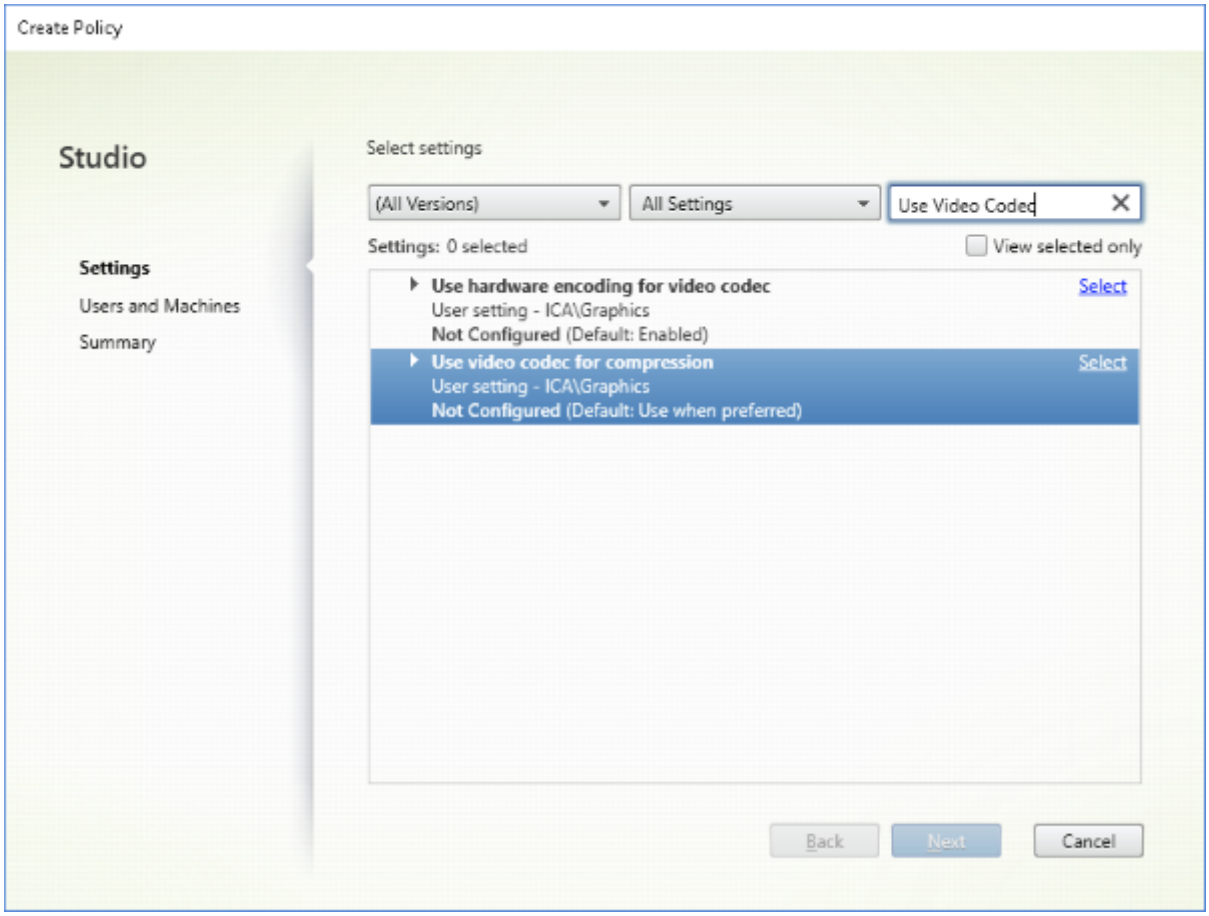
Para usar Skype Empresarial, instale el HDX RealTime Optimization Pack 2.4 o una versión posterior en el VDA. **Desactive** la **generación por hardware** (Use Hardware Rendering) si usa Optimization Pack (consulte la sección “Directiva de rendimiento” para obtener más información).

> **Nota**
>
> Actualmente, los monitores dobles no se admiten la versión 2.4.

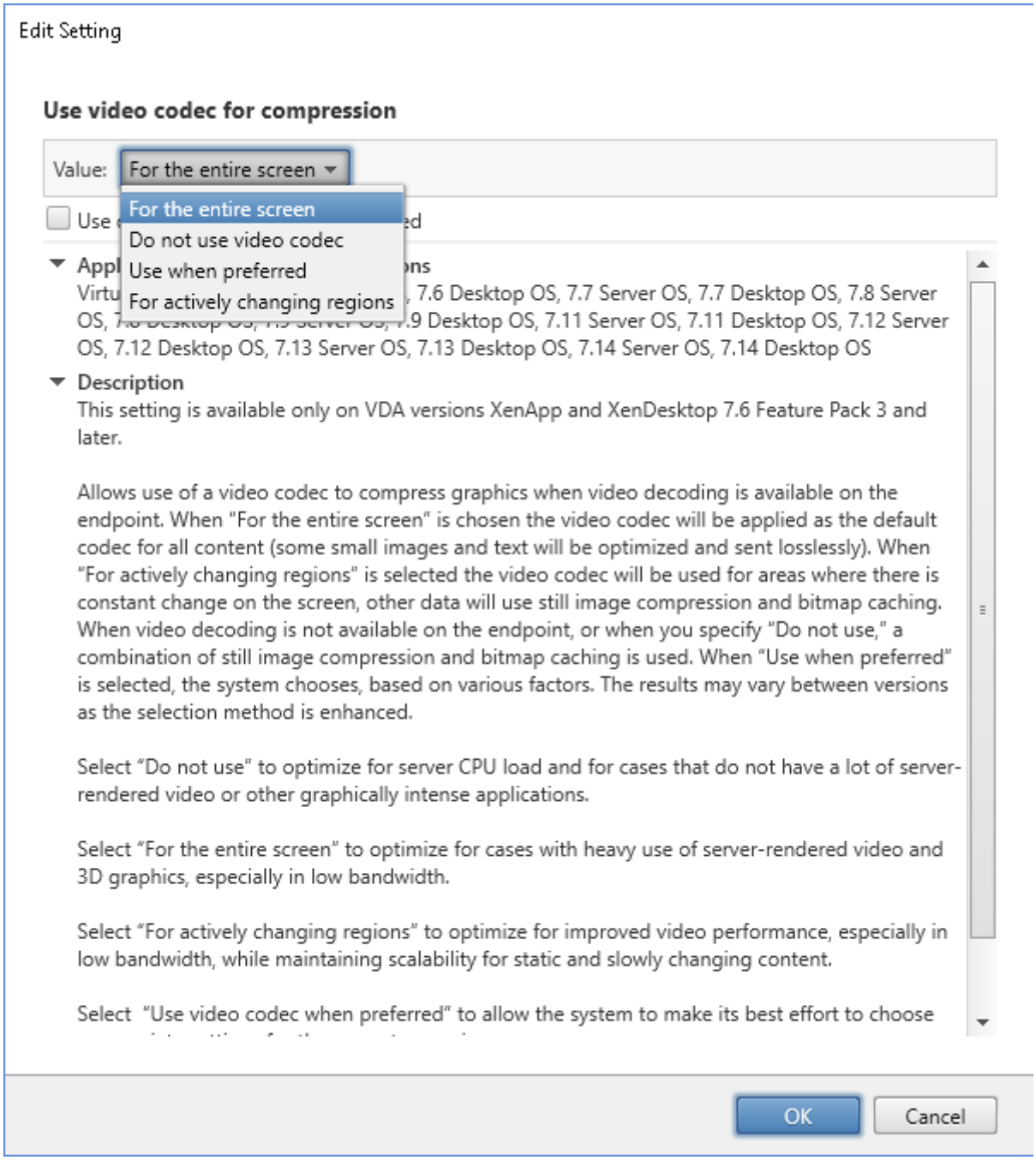
Directiva de rendimiento

Para obtener la mejor experiencia en Citrix Ready Workspace Hub (y SDA), habilite la codificación H.264 para el modo de pantalla completa. Para ello, cree una directiva y habilite el códec de vídeo para la compresión H.264 (H.264) para el modo de pantalla completa.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



© 1999-2019 Citrix Systems, Inc. All rights reserved.



Para confirmar que la compresión H.264 está habilitada para el modo de pantalla completa con el fin de que el adaptador SDA pueda funcionar, consulte uno de los siguientes procedimientos.

- Revise la directiva de Citrix desde el Delivery Controller.
- En una sesión VDA, utilice el monitor HDX 3.x. Consulte el artículo del Knowledge Center CTX135817.
- En una sesión de VDA, coloque la línea siguiente en la terminal: `wmic /namespace:\root\citrix\hdx path citrix_virtualchannel_thinwire get /value`

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Luego puede comprobar si el modo gráfico está configurado correctamente para el modo de pantalla completa H.264:

1. **Component_VideoCodecUse = FullScreen**
2. **Component_Encoder = DeepCompressionV2Encoder**
3. **IsActive = Active**

Si el modo gráfico está configurado para la pantalla selectiva H.264, confirme que:

1. **Component_VideoCodecUse = Para áreas en cambio constante**
2. **Component_Encoder = CompatibilityEncoder**
3. **IsActive = Active**

Para obtener una resolución de pantalla mejor, habilite el atributo **ClearType** en Windows VDA. Consulte Vista general de Microsoft Cleartype y Cómo activar o desactivar ClearType en Windows 10 para más información.

Configuración de monitor doble

Para admitir monitores dobles, se requiere un adaptador de pantalla secundaria (SDA). Puede adquirir un adaptador SDA en ViewSonic o NComputing. Para obtener más información, consulte https://www.stratodesk.com/kb/Multimonitor.

Configuración de hardware

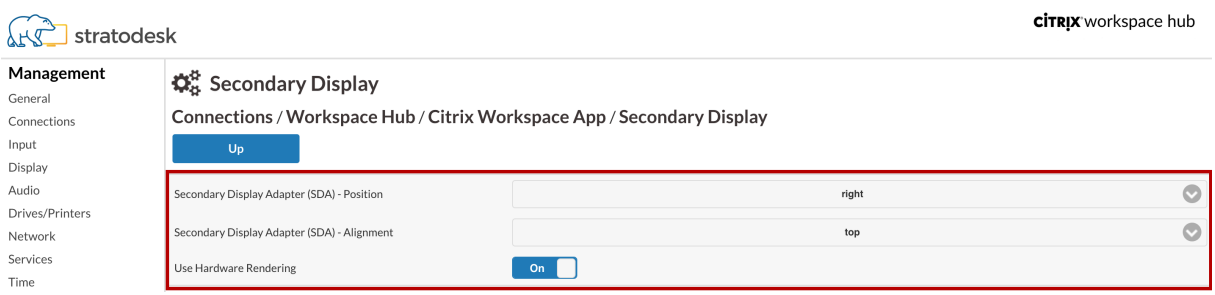
Hay dos puertos micro USB en el SDA. Uno está etiquetado como “Corriente” y el otro está etiquetado como “USB”. Conecte un adaptador estándar de alimentación por USB de Raspberry Pi en el puerto de alimentación, luego utilice un cable micro USB estándar que vaya desde el puerto USB del SDA hasta Citrix Ready Workspace Hub.

Configuración del software

Consulte la sección anterior Configurar Citrix Virtual Apps and Desktops. Siga la directiva de rendimiento para configurar la generación H.264 en ambas pantallas.

Cuando mueva una sesión por roaming al Citrix Ready Workspace Hub, los monitores dobles se pueden iniciar automáticamente. Para cambiar la configuración del diseño y la distribución, desde la consola de administración de Stratodesk, vaya a la ruta de configuración **Conexiones > Workspace Hub > Aplicación Citrix Workspace > Pantalla secundaria**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Citrix Ready Workspace Hub en la aplicación Citrix Workspace

Puede habilitar la aplicación Citrix Workspace para usarla con Citrix Ready Workspace Hub. Este software de uso sencillo proporciona un acceso seguro y transparente a las aplicaciones y escritorios específicos a los que los usuarios tienen acceso. Workspace Hub le permite iniciar los recursos del espacio de trabajo desde varias plataformas y clientes. Para obtener más información sobre cómo configurar los dispositivos para su uso con Workspace Hub, consulte la documentación de las plataformas Android, iOS, Windows y Mac.

Inicie sesión en Workspace Hub con itinerancia de sesiones o proyección de pantalla. La itinerancia de sesiones le permite iniciar sesión en Workspace Hub introduciendo el perímetro de autenticación por proximidad o escaneando el código QR. Sin embargo, la proyección de pantalla requiere iniciar sesión en el dispositivo y luego activar el código QR para transferir la sesión.

Roaming de sesión con autenticación por proximidad

La autenticación por proximidad puede autenticar a los usuarios e iniciar una sesión automáticamente sin que los usuarios toquen el dispositivo. La proximidad se basa en la tecnología Bluetooth para localizar dispositivos móviles. Una vez que se completa la configuración y se inicia la aplicación Citrix Workspace, la sesión se moverá por al Citrix Ready Workspace Hub cuando el dispositivo entre en el perímetro de autenticación por proximidad del concentrador. Esta función solo está disponible para dispositivos Android.

Roaming de sesión con autenticación por código QR

Escanee el código QR en la pantalla del concentrador para transferir la sesión. Cuando la sesión se mueve a un Workspace Hub, el concentrador tiene el control total de todos los periféricos disponibles en la sesión.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Transmitir pantalla con autenticación por código QR

Para proyectar una sesión en un concentrador, debe iniciar la sesión en un dispositivo primero, y luego escanear el código QR en el concentrador. Tras empezar a transmitir la pantalla de la sesión al concentrador, puede usar el teclado y ratón en el dispositivo móvil para controlar la sesión en el concentrador.

Para obtener más información sobre la itinerancia de sesiones y la proyección de pantalla al concentrador, consulte la documentación de ayuda para dispositivos iOS y Android.

Sesión de larga duración

Durante una sesión larga, puede dejar el dispositivo Android con la pantalla bloqueada. Para que la sesión no se interrumpa, tenga en cuenta los siguientes consejos:

- La optimización de la batería puede interferir con su sesión. Para evitar los efectos de la optimización de batería, agregue la aplicación Citrix Workspace a las listas para ignorar la optimización de batería en Android.
  - En Google Pixel, vaya a **Ajustes > Batería > Optimización de batería > Todas las aplicaciones > Citrix Receiver > No optimizar**.
  - En la mayor parte de los dispositivos **Samsung, vaya a Ajustes > Batería > Uso de batería > Optimizar uso de batería > Todas las aplicaciones > Citrix Receiver > No optimizar**.
  - Si está utilizando una aplicación de optimización de batería de terceros, elimine la aplicación Citrix Workspace para Linux de su lista de optimización.
- Citrix recomienda llevar la interfaz principal de la aplicación Citrix Workspace al primer plano antes de bloquear la pantalla. Así, el sistema operativo del dispositivo móvil no finalizará la sesión de la aplicación Citrix Workspace.

Registro estándar

Esta función le permite registrar la ejecución de los procesos que tienen lugar en Citrix Ready Workspace Hub y proporcionar un cambio dinámico del nivel de depuración para los diferentes módulos.

Compatibilidad con Citrix Virtual Apps

Al iniciar aplicaciones desde el Workspace Hub mediante la aplicación Citrix Workspace, es posible que la sesión se abra detrás de la pantalla de inicio. Hay dos maneras de traer la sesión iniciada al primer plano.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

1. En el icono de menú situado en la parte inferior izquierda de la pantalla de inicio, haga clic en **Citrix Virtual Apps > Mostrar todas las aplicaciones virtuales de Citrix** para ver las sesiones iniciadas en modo de ventana.
2. Seleccione **Citrix Virtual Apps > ApplicationName** para mostrar una sesión concreta en primer plano.

Navegación automática de la pantalla de inicio

En la versión 1812 de Citrix Ready Workspace Hub, Citrix ha introducido la navegación automática de la pantalla de inicio como función experimental. Configure varias direcciones URL para la pantalla de inicio en el Workspace Hub. Haga clic en las flechas de la parte inferior de la página para navegar ágilmente entre los recursos.

Configuración

A partir de ahora, el demonio ctxlogd y la utilidad setlog se incluyen en el paquete del concentrador. De forma predeterminada, el demonio ctxlogd se inicia cuando inicia el concentrador.

demonio ctxlogd

Todos los demás servicios que se rastrean dependen del demonio ctxlogd. Para detener el demonio ctxlogd, si no desea mantener el concentrador rastreado, puede finalizar el proceso relacionado con ctxlogd. El archivo de registros wsh.log se encuentra en `/opt/Citrix/WorkspaceHub/Logs`.

utilidad setlog

La utilidad setlog, en `/opt/Citrix/WorkspaceHub/lib/wshlog`, le permite cambiar dinámicamente el nivel de depuración para diferentes módulos. Solo los usuarios root tienen permiso para ejecutarlo. Puede agregar `sudo` al encabezado del comando para ejecutar el comando utilizando el usuario pi.

Por ejemplo:

1. Para verificar el nivel de registro actual para todos los módulos:

   ```
   sudo /opt/Citrix/WorkspaceHub/lib/wshlog/setlog levels
   ```

2. Para establecer el nivel de registro como detallado para el módulo controlService:

   ```
   sudo /opt/Citrix/WorkspaceHub/lib/wshlog/setlog level WSH_CONTROLSERVICE
    verbose
   ```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Puede obtener más información de uso en el manual de ayuda `sudo /opt/Citrix/WorkspaceHub/lib/wshlog/ setlog --help`.

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 mejorar la calidad y el rendimiento de sus productos.

Citrix Ready Workspace Hub utiliza Google Analytics, como se documenta en Cómo utiliza Google los datos cuando usted usa los sitios o aplicaciones de nuestros socios para el análisis de datos. Puede desactivar el CEIP si no desea enviar sus datos a Google Analytics.

Conmutador CEIP

De forma predeterminada, usted participa automáticamente en el programa CEIP. Puede desactivar el CEIP a través de la interfaz de usuario de Stratodesk.

Datos del CEIP recopilados desde el Workspace Hub

La siguiente tabla enumera los tipos de información anónima que se recopila. Los datos no contienen detalles que lo identifiquen a usted como cliente.

Punto de datos	Nombre de la clave	Descripción
Función de navegación automática habilitada/inhabilitada	auto_navigation	Indica si la función Navegación automática está habilitada o no. 1: habilitada. 0: inhabilitada
Versión de SO	os_release	Información de versión del sistema operativo de PI, como 4.9.35-v7
Versión de SO	os_version	Información de versión del sistema operativo de PI, como 2017-07-05-raspbian-Jessie
Versión de Workspace Hub	wsh_version	Información de versión de Workspace Hub, como 1.0.72
Función SSL habilitada o no	ssl_mode	Indica si la función SSL está habilitada o no. 1: habilitada. 0: inhabilitada

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Punto de datos	Nombre de la clave	Descripción
Con o sin monitor doble	monitor_mode	Indica si se usa o no el monitor doble. 1: monitor doble. 0: monitor único
Resolución del monitor	monitor_resolution_p3	Resolución de pantalla para el monitor que conecta con p3.
Resolución del monitor	monitor_resolution_p0	Resolución de pantalla para el monitor que conecta con p0.
Tiempo de duración de sesión (solo para la itinerancia de sesión)	tiempo de sesión	El tiempo de duración de una sesión

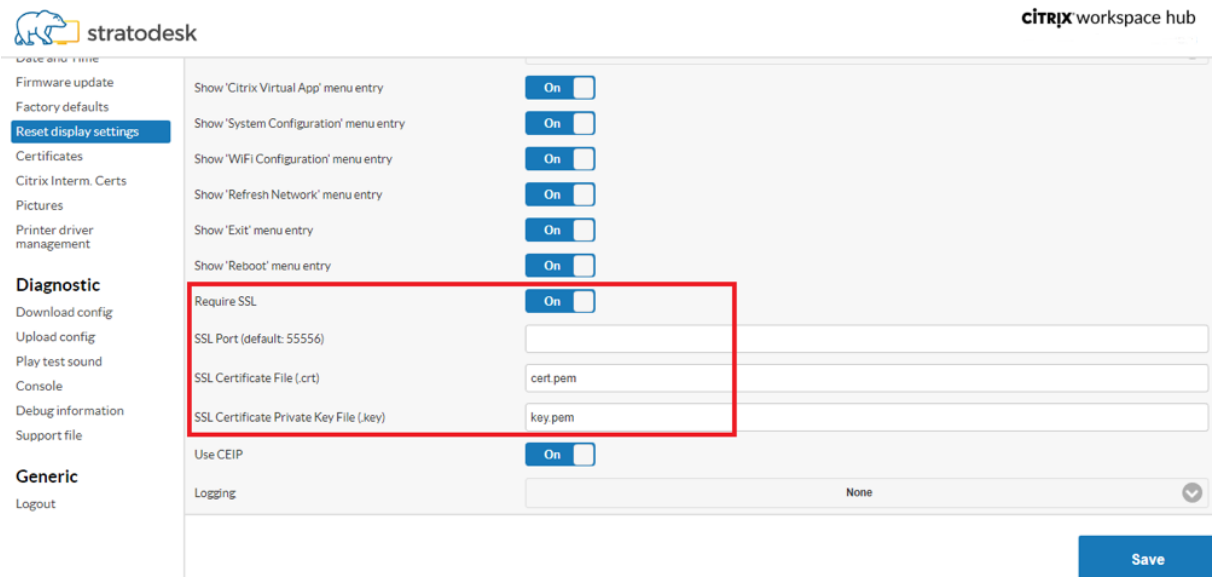
Conexión de seguridad

Se admiten las conexiones SSL/TLS entre dispositivos móviles y Citrix Ready Workspace Hub, y se habilitan por motivos de seguridad. El puerto SSL/TLS se puede configurar. Debe comprobar, sin embargo, que el certificado SSL/TLS esté cargado y su ruta configurada correctamente en el concentrador. Los certificados autofirmados deben instalarse en dispositivos Android antes de que los usuarios comiencen a trabajar con el concentrador.

Para configurar SSL/TLS:

1. Para obtener información sobre cómo agregar certificados y claves privadas a Citrix Ready Workspace Hub, consulte https://www.stratodesk.com/kb/Certificates#Method_2:_Distribute_certificates_automatically
2. Actualice los nombres del archivo de certificado (cert.pem) y del archivo de clave privada (clave.pem). A continuación, haga clic en **Guardar**. Ambas opciones se encuentran en **Conexiones > Workspace Hub > Workspace Hub**.
3. Reinicie Citrix Workspace Hub para que los cambios surtan efecto.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



También puede inhabilitar el parámetro SSL cambiando la opción **Requerir SSL** a **No**.

Accesos directos

- Control + Alt +S: Lee información relevante cuando se solucionan problemas.
- Control + Alt + C: Abre el menú de configuración.
- Cuando se utiliza Citrix Casting, deslizar dos dedos hacia abajo en el teléfono desconecta la sesión, independientemente del estado de la sesión o de cómo se realizó la transmisión de pantalla a Workspace Hub.

Limitaciones conocidas

- Las tiendas de la Interfaz Web no admiten el roaming de la sesión. Por eso, no marque la casilla **Agregar tipo de cuenta como Interfaz Web**.
- Si sale de la sesión de Windows en Citrix Ready Workspace Hub haciendo clic en **Cerrar sesión** o **Desconectar** en Windows mientras transmite la pantalla, la sesión puede tardar unos 20 segundos en salir del concentrador.
- Los monitores dobles admiten la itinerancia de sesiones. No se admite la transmisión de la sesión.
- Para poder utilizar Optimization Pack, **Use Hardware Rendering** debe estar **desactivado**. Esta función solo funciona en la pantalla principal. La ventana en la pantalla secundaria es gris.
- Dispositivos mouse inalámbricos - Puede notar un retraso si utiliza un mouse inalámbrico. Notifique este error en el foro de debates de Citrix Workspace Hub. Incluya la marca y modelo del mouse.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Citrix Casting funciona solo cuando el dispositivo móvil está conectado a la misma red que Workspace Hub.
- Red inalámbrica 5G: Workspace Hub se basa en la plataforma Raspberry Pi 3, que actualmente no admite la red inalámbrica 5G. Sin embargo, puede admitir 5G con una llave de hardware USB inalámbrica (opción no recomendada).
- El certificado raíz de CA debe estar firmado con SHA256. La aplicación Citrix Workspace para Linux no acepta certificados firmados con SHA1. https://support.citrix.com/article/CTX200114
- No se admite el protocolo Enlightened Data Transport (EDT) con Citrix Ready Workspace Hub.

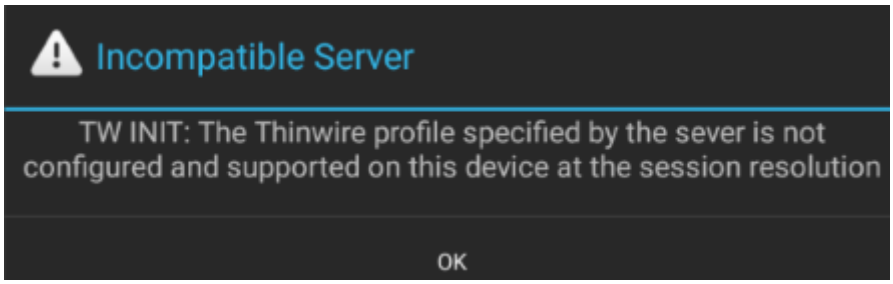
Solucionar problemas

Fallo en la transmisión de pantalla

La función de transmisión de pantalla que ofrece Citrix Ready Workspace Hub admite tanto el modo gráfico H.264 a pantalla completa como H.264 selectivo. Sin embargo, para un rendimiento óptimo, se recomienda utilizar H.264 para la pantalla completa. Si tiene un fallo en la transmisión de la pantalla, compruebe que el modo gráfico esté configurado correctamente.

Mensaje de "servidor incompatible"

En la aplicación Citrix Workspace para Android, un fallo en la transmisión de la sesión genera el siguiente mensaje:



Este error ocurre si un modo gráfico está configurado como H.264 selectivo en el VDA. La transmisión de pantalla ofrece un mejor rendimiento con el modo gráfico H.264 a pantalla completa. Vuelva a configurar el modo gráfico a "Para la pantalla entera" en **Configuración del sistema > Conexiones > Workspace Hub**, o actualice el agente VDA a 7.19 o versiones posteriores.

Problemas relacionados con SSL

De manera predeterminada, SSL está habilitada en Citrix Ready Workspace Hub. Compruebe que el certificado SSL esté cargado y que su ruta esté configurada correctamente en el concentrador. Los

© 1999-2019 Citrix Systems, Inc. All rights reserved.

problemas de configuración de SSL pueden provocar un error al iniciar Citrix Casting. Si la sesión deja de responder, recibirá un mensaje de alerta.

Problema de usuario	Sugerencia
El proceso `WorkspaceHubControlService` no se inicia correctamente.	En el terminal, escriba el comando: `ps -ef|grep ControlService`. Si no se encuentra ningún proceso, verifique con TI que los puertos 55555 y 55556 no están bloqueados en la red.
SSL está habilitado sin certificados instalados en el concentrador o está configurado con un certificado con ruta incorrecta.	Verifique que los certificados y los archivos de claves estén instalados en Citrix Ready Workspace Hub. Para ello, vaya a `/opt/Citrix/WorkspaceHub/keystore/certs` y confirme que los certificados están instalados. Si usa la imagen de Stratodesk, siga la ruta al elemento de configuración ssl_enabled en **Configuración del sistema > Conexiones > Citrix Workspace Hub > Workspace Hub**. Si usa la imagen de Citrix, consulte el archivo **ssl.config** en `/opt/Citrix/WorkspaceHub/config/`.
SSL está habilitado en Citrix Ready Workspace Hub, pero el certificado no está instalado en el cliente Android.	Instale los archivos de claves en el cliente Android.
Ya hay un proceso DisplayConnector en ejecución.	Un proceso anterior DisplayConnector no finalizó correctamente. Finalice el proceso y trate de transmitir de nuevo la pantalla.

Fallo en el roaming de la sesión

Este problema puede ocurrir después de configurar un nuevo Citrix Ready Workspace Hub. El roaming de la sesión puede fallar cuando las configuraciones de Workspace Hub no cumplen con la sesión de VDA.

Para solucionar este problema:

1. Inicie la sesión VDA utilizando la aplicación Citrix Workspace para Linux instalada en el concentrador.
2. Compruebe que SSL esté configurado correctamente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Problemas resueltos

Para obtener una lista completa de problemas solucionados con la versión 1812, consulte la sección Problemas solucionados en Citrix Virtual Apps and Desktops.

Problemas conocidos

Para obtener más información sobre los problemas conocidos de Citrix Ready Workspace Hub, consulte la sección Problemas conocidos en CVAD.

Información de asistencia

Puede acudir al proveedor aprobado donde adquirió el dispositivo Citrix Ready Workspace Hub para obtener ayuda. Esos proveedores son NComputing, Stratodesk, y ViewSonic.

Dispositivos USB genéricos

December 4, 2018

La tecnología HDX ofrece **compatibilidad optimizada** con los dispositivos USB más comunes. Estos dispositivos son:

- Monitores
- Mouse
- Teclados
- Teléfonos VoIP
- Auriculares con micro
- Cámaras Web
- Escáneres
- Cámaras
- Impresoras
- Unidades
- Lectores de tarjetas inteligentes
- Tabletas de dibujo
- Paneles táctiles de firma electrónica

El respaldo optimizado (o compatibilidad optimizada) ofrece una experiencia de usuario mejorada, con mejor rendimiento y eficiencia del ancho de banda en una conexión por red WAN. El respaldo optimizado suele ser la mejor opción, sobre todo en entornos de alta latencia o cuando se requiera confidencialidad.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

La tecnología HDX ofrece la **redirección de USB genérico** para dispositivos específicos sin respaldo optimizado o cuando ese respaldo no es adecuado. Para obtener más información sobre la redirección de USB genérico, consulte Redirigir USB genérico.

Para obtener más información sobre dispositivos USB y la aplicación Citrix Workspace para Windows, consulte Configurar la redirección de dispositivos USB compuestos y [Configurar el respaldo para USB].(/es-es/citrix-workspace-app-for-windows/configure/config-xdesktop/config-usb-support.html)

Dispositivos móviles y de pantalla táctil

December 4, 2018

Modo tableta para dispositivos de pantalla táctil mediante Windows Continuum

Continuum es una característica de Windows 10 que se adapta al uso que se le da al dispositivo cliente. Esta versión de Continuum, incluido el cambio dinámico entre los diferentes modos, está disponible a partir de en la versión 7.16 de VDA y Citrix Receiver para Windows 4.10.

El VDA presente en Windows 10 detecta la presencia de un teclado o mouse en un cliente táctil y coloca al cliente en el modo escritorio. Si el teclado o el mouse no están presentes, el VDA de Windows 10 coloca al cliente en el modo móvil o tableta. Esta detección ocurre en la conexión y la reconexión. También ocurre al conectar o desconectar el teclado o el mouse.

Esta función está activada de forma predeterminada. Para inhabilitar esta versión de la funcionalidad, modifique las configuraciones de directiva Alternar del modo tableta en el artículo de configuraciones de la directiva ICA.

Para la versión de la funcionalidad que se incluye en XenApp 7.14 y 7.15 LTSR y XenDesktop 7.14 y 7.15 LTSR, use los parámetros de Registro para inhabilitar la función. Para obtener más información, consulte Modo tableta para dispositivos de pantalla táctil.

El **modo tableta** ofrece una interfaz de usuario que se adapta mejor a las pantallas táctiles:

- Botones ligeramente más grandes.
- La pantalla de Inicio y cualquier aplicación que abra se inicia en modo de pantalla completa.
- La barra de tareas contiene el botón Atrás.
- Se han quitado iconos de la barra de tareas.

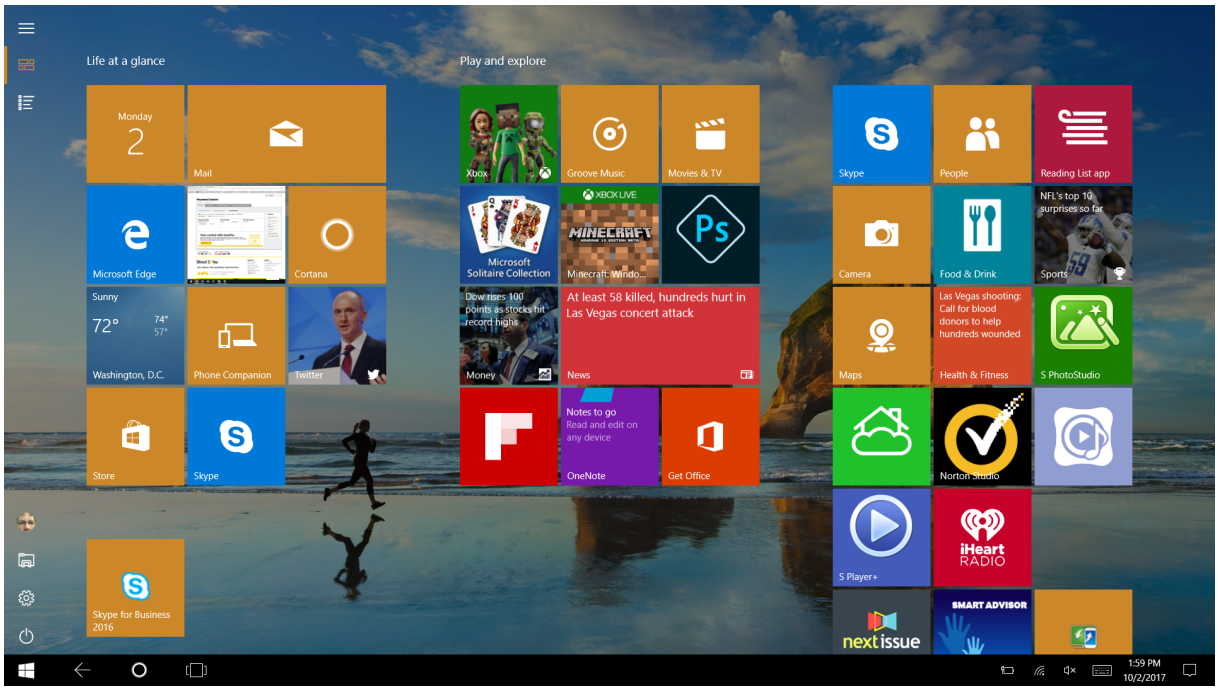
Puede utilizar el Explorador de archivos.

El **modo escritorio** ofrece la interfaz de usuario tradicional, donde se interactúa de la misma manera que con el PC, el teclado y el mouse.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

El modo tableta requiere al menos la versión 7.2 de XenServer. XenServer 7.2 se integra con el VDA de Citrix Virtual Desktops, con lo que el hipervisor cambia para permitir la configuración de firmware virtual para dispositivos 2 en 1. Windows 10 carga el controlador GPIO en la máquina virtual de destino basándose en esta BIOS actualizada. Se utiliza para alternar entre los modos escritorio y tableta dentro de la máquina virtual. Para obtener más información, consulte las notas de la versión.

La aplicación Citrix Workspace para HTML5 (la versión ligera) no admite las características de Windows Continuum.



Ejecute el comando CLI de XenServer para permitir que se pueda cambiar entre el ordenador 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).

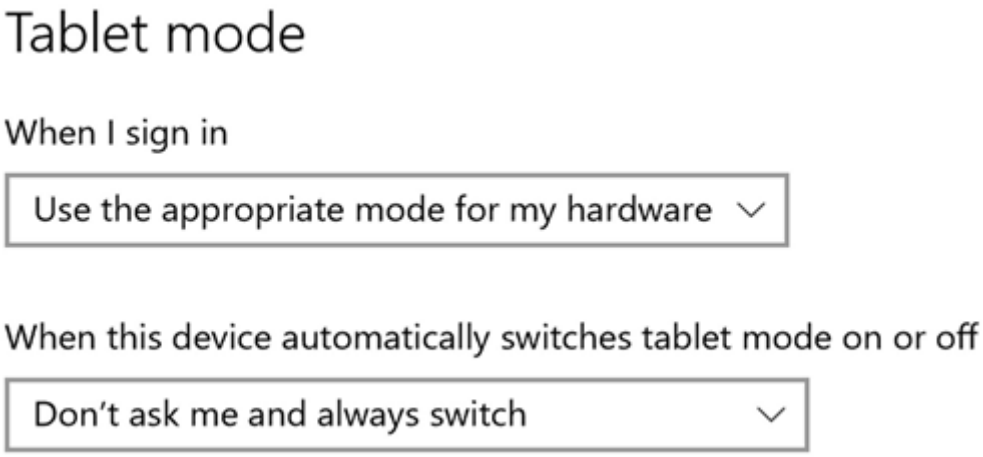
Antes de iniciar una sesión:

Antes de iniciar una sesión, se recomienda que vaya a **Configuración > Sistema > Modo tableta** en el VDA y establezca las siguientes opciones en los menús de lista desplegable:

- Usar el modo adecuado para mi hardware
- No preguntarme y cambiar siempre

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Si no configura estas opciones antes de iniciar la sesión, configúrelas después de iniciar la sesión y reinicie el VDA.



Puertos serie

March 14, 2019

La mayoría de los PC nuevos no tienen puertos serie integrados (COM). Es fácil agregar puertos usando convertidores USB. Las aplicaciones adecuadas para los puertos serie suelen ser sensores, controladores, lectores antiguos de cheques, paneles táctiles, etc. Algunos dispositivos USB de puerto COM virtual utilizan controladores específicos del fabricante en lugar de los controladores que ofrece Windows (usbser.sys). Estos controladores permiten forzar el puerto COM virtual del dispositivo USB para que no cambie incluso aunque se conecte a otras ranuras USB. Se puede hacer desde **Administrador de dispositivos > Puertos (COM y LPT) > Propiedades** o desde la aplicación que controla el dispositivo.

La asignación de puertos COM del cliente permite utilizar los dispositivos conectados a los puertos COM del dispositivo de usuario durante las sesiones virtuales. Estas asignaciones se pueden utilizar de la misma forma que cualquier otra asignación de red.

Un controlador del sistema operativo asigna un nombre de enlace simbólico a cada puerto COM, como COM1 y COM2. Las aplicaciones usan ese enlace para acceder al puerto.

> **Importante**
>
> - El hecho de que un dispositivo se pueda conectar al dispositivo de punto final directamente por USB no significa que ese dispositivo se puede redirigir utilizando 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 proto-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

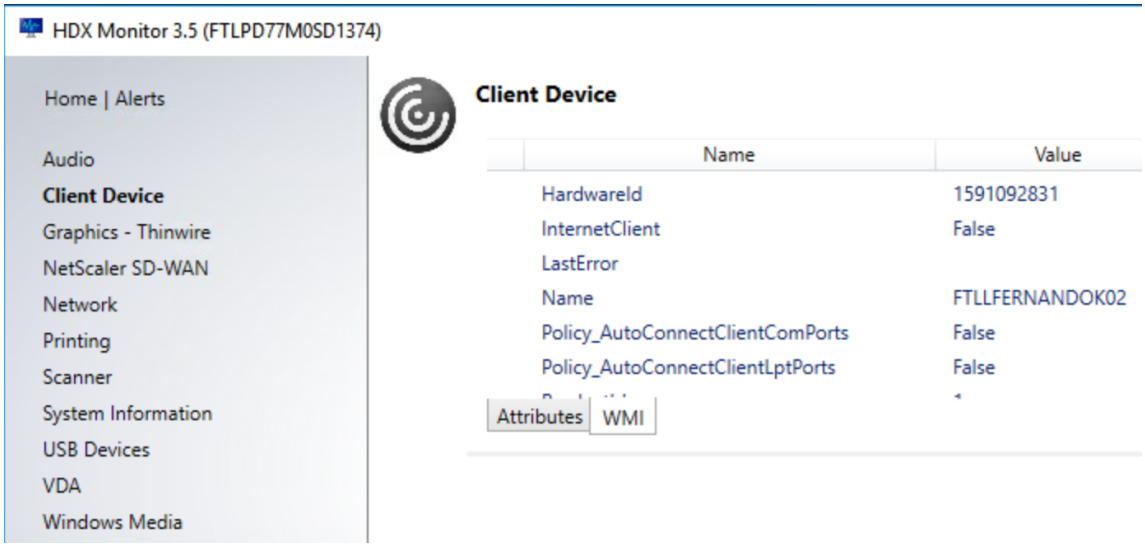
> colos frecuentes para COM virtual son: CDC ACM o MCT. Cuando se conecta a través de un puerto RS-485, es posible que las aplicaciones no funcionen en absoluto. Debe obtener un convertidor de RS-485 a RS232 para usar RS-485 como puerto COM.
> - Algunas aplicaciones reconocen el dispositivo (por ejemplo, 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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.

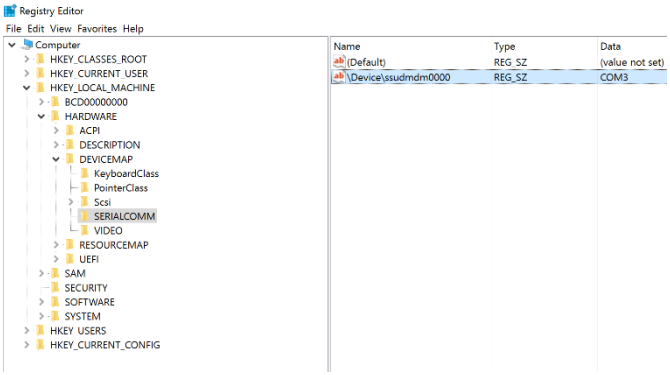
```
C:\Windows\system32>net use
New connections will be remembered.


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).

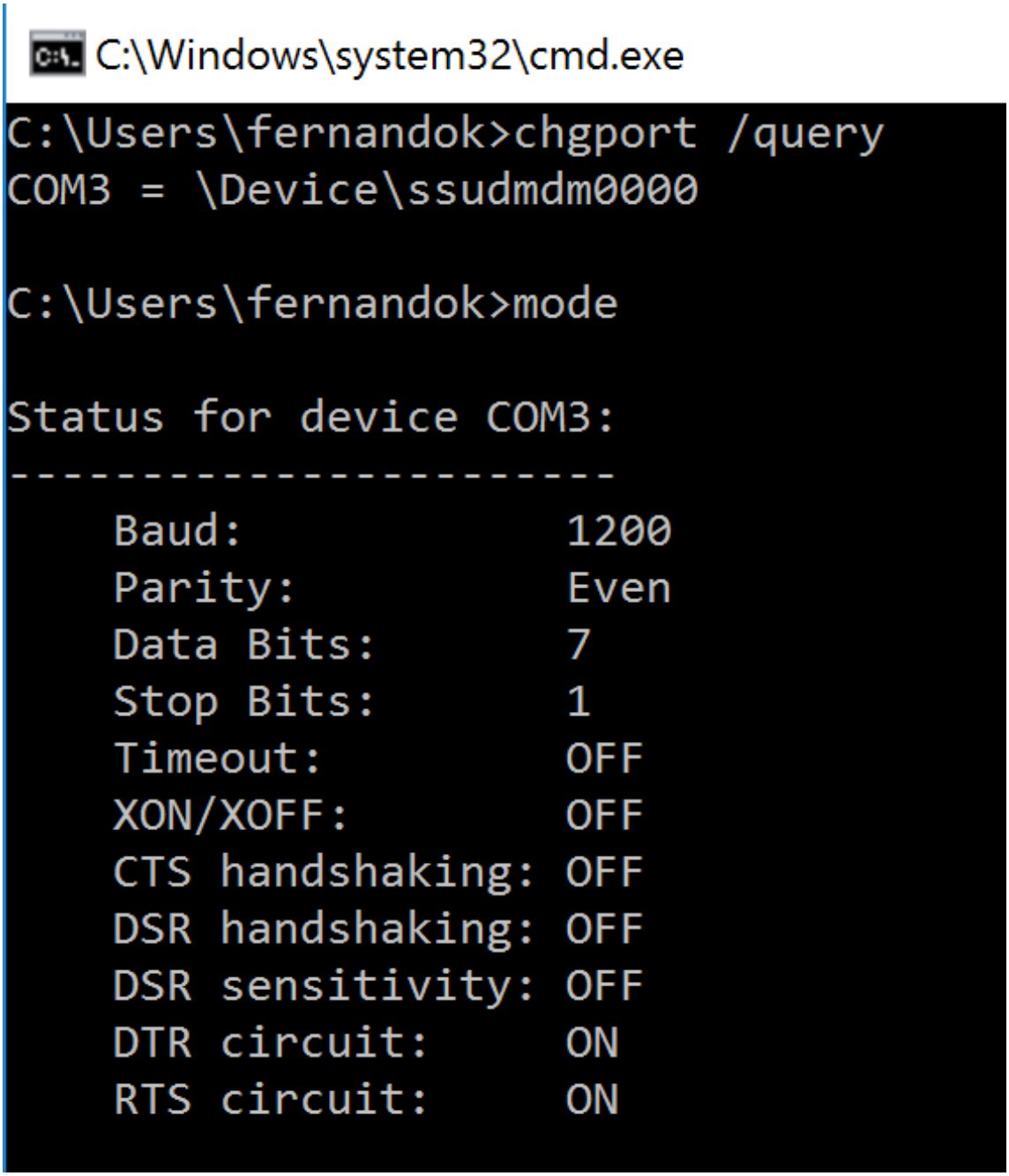
Solucionar problemas

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:



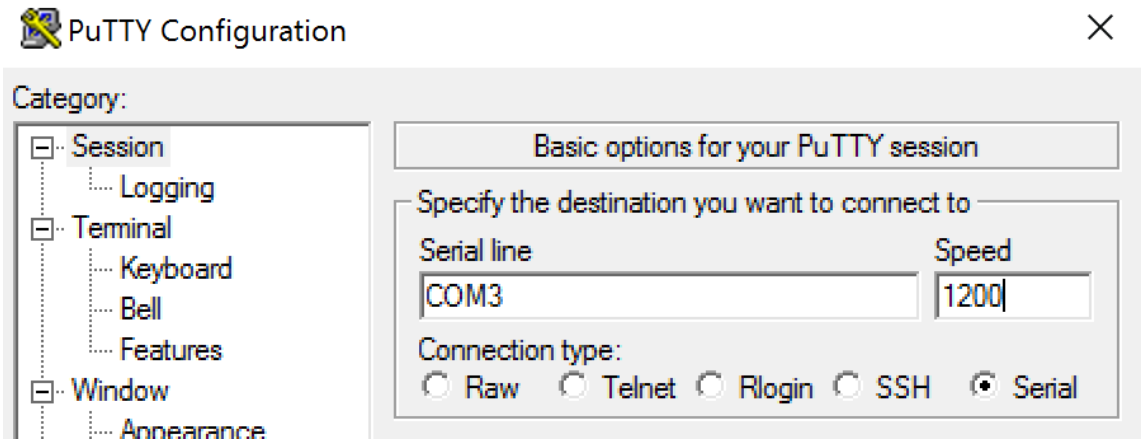
© 1999-2019 Citrix Systems, Inc. All rights reserved.

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



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 (usando 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 usando 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:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- 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 Citrix se envían al VDA y se almacenan en: **HKLN\SOFTWARE\Policies\Citrix <ID de la sesión de usuario>**
- 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, .exe. Los errores aparecen como ”Acceso denegado” o similar.

Teclados especiales

January 29, 2019

Teclados Bloomberg

> **Advertencia**
>
> Si se modifica el Registro de forma incorrecta, se pueden generar problemas graves que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Citrix Virtual Apps and Desktops admite el teclado Starboard modelo 4 de Bloomberg (y el modelo anterior 3). Este teclado permite a los clientes del sector financiero utilizar funciones especiales en el teclado para poder acceder a datos del mercado financiero y realizar transacciones rápidamente.

Este teclado es compatible con los cuadros de conmutadores KVM y puede funcionar en dos modos:

- PC (un cable USB sin KVM)
- Modo KVM (dos cables USB con uno enrutado a través de KVM)

> **Importante**
>
> Se recomienda usar el teclado Bloomberg con una sola sesión. Es decir, no se recomienda utilizar este teclado con varias sesiones simultáneas (de un cliente a varias sesiones).

El teclado Bloomberg 4 es un dispositivo USB compuesto que consta de cuatro dispositivos USB en una carcasa física:

- Teclado.
- Lector de huellas dactilares.
- Dispositivo de sonido con teclas para aumentar y disminuir el volumen o silenciar el altavoz y el micrófono. Este dispositivo incluye altavoz, micrófono y conector integrado para el micrófono y los auriculares.
- Concentrador USB para conectar todos estos dispositivos al sistema.

Requisitos:

- La sesión a la que se conecta la aplicación Citrix Workspace para Windows debe admitir dispositivos USB.
- La aplicación Citrix Workspace 1808 para Windows o Citrix Receiver para Windows 4.8, como mínimo, para admitir los modelos 3 y 4 del teclado Bloomberg.
- La aplicación Citrix Workspace 1808 para Windows o Citrix Receiver para Windows 4.12, como mínimo, para usar el modo KVM (dos cables USB con uno enrutado a través de KVM) para el modelo 4.

Para obtener información sobre cómo configurar los teclados Bloomberg en la aplicación Citrix Workspace para Windows, consulte Configurar teclados Bloomberg.

Habilitar el respaldo para teclados Bloomberg:

De forma predeterminada, el respaldo para el teclado mejorado de Bloomberg está inhabilitado. Para habilitar este respaldo, modifique esta entrada de Registro en la máquina cliente antes de iniciar una conexión.

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB

Nombre: **EnableBloombergHID** (dword)

Valor: 0 (Inhabilitar) 1 (Habilitar)

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Comprobar el respaldo:

Para determinar si el respaldo para 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 respaldo para el teclado Bloomberg está habilitado, Desktop Viewer muestra tres dispositivos debajo del icono USB:

- Escáner de huellas dactilares de Bloomberg
- Características 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 respaldo para el teclado Bloomberg está habilitado, los tres dispositivos aparecen en el menú Dispositivos.

La marca de verificación situada junto a cada uno de estos dispositivos indica que están conectados remotamente a la sesión.

Dispositivos TWAIN

October 3, 2018

Requisitos

- El escáner debe ser compatible con TWAIN.
- Instale los controladores TWAIN en el dispositivo local. No son necesarios en el servidor.
- Conecte el escáner localmente (por ejemplo, por USB).
- Compruebe que el escáner esté utilizando el controlador TWAIN local, no el servicio Adquisición de imágenes de Windows.
- Compruebe que no se aplica ninguna directiva (por ejemplo, que limite el ancho de banda en la sesión ICA) a la cuenta de usuario que se utiliza para la prueba. Por ejemplo, la directiva Límite de ancho de banda de redirección de dispositivos USB del cliente.

Para obtener información acerca de las configuraciones de directiva, consulte Configuraciones de directiva de Dispositivos TWAIN.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Cámaras web

March 8, 2019

Streaming por cámara web de alta definición

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. Usted elige la cámara web desde la aplicación. Si la cámara web y la aplicación admiten la generación de alta definición, la aplicación usa la resolución de alta definición. Damos respaldo a resoluciones de cámara web hasta 1920 x 1080.

Esta función requiere Citrix Receiver para Windows, versión mínima 4.10.

Para obtener más información sobre el streaming de cámaras web de alta definición, consulte HDX y los requisitos de las conferencias de vídeo para la compresión de vídeo de cámaras web.

> **ADVERTENCIA**
>
> Si se modifica el Registro de forma incorrecta, se pueden generar problemas graves que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Use el Editor del Registro bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Puede usar una clave de Registro para inhabilitar la función. Se usa la resolución predeterminada de 352 x 288:

HKEY_LOCAL_MACHINE\Software\Citrix\HDXRealTime

Nombre: Disable_HighDefWebcam

Tipo: REG_DWORD

Datos: 1 = Desactiva la distribución por streaming de la cámara web de alta definición

Puede usar claves de Registro en el cliente para configurar una resolución específica. Compruebe que la cámara admite la resolución especificada:

HKEY_CURRENT_USER\Software\Citrix\HDXRealTime

Nombre: DefaultWidth

Tipo: REG_DWORD

Datos (decimales): Anchura deseada (por ejemplo, 1280)

Nombre: DefaultHeight

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Tipo: REG_DWORD

Datos (decimales): Altura deseada (por ejemplo, 720)

Gráficos

December 4, 2018

> **Nota:**
>
> Puede obtener información sobre los cambios en los nombres de producto aquí.

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 y 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 y 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 y 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 sistemas operativos de escritorio Windows

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Con HDX 3D Pro, puede entregar aplicaciones de uso intensivo de gráficos como parte de escritorios o aplicaciones alojadas en máquinas con SO de escritorio. 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 sistemas operativos de servidor Windows

HDX 3D Pro permite que las aplicaciones con muchos gráficos que se ejecutan en sesiones de sistema operativo de servidor 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

Framehawk es una tecnología de pantallas remotas para usuarios móviles con conexiones inalámbricas de banda ancha (redes de telefonía móvil WiFi, 4G o LTE). Framehawk resuelve obstáculos como interferencias espectrales y propagaciones multitrayecto para ofrecer una experiencia de usuario fluida e interactiva a los usuarios de aplicaciones y escritorios virtuales.

Marca de agua de sesión basada en texto

Las marcas de agua de la sesión basadas en texto ayudan a disuadir del robo de datos y rastrear los datos robados. Esta información rastreable aparece en el escritorio de la sesión como un elemento de disuasión para quienes usan fotografías y capturas de pantalla para robar datos. Puede especificar una marca de agua que sea una capa de texto 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.

Información relacionada

- HDX 3D Pro
- Aceleración de GPU para sistemas operativos de escritorio Windows
- Aceleración de GPU para sistemas operativos de servidor Windows
- Framehawk

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Thinwire
- Marca de agua de sesión basada en texto

HDX 3D Pro

November 29, 2018

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.

Cuando instala un VDA en un SO de escritorio, el VDA evalúa los criterios y establece automáticamente el modo correspondiente. Si hay disponible una GPU compatible, el VDA se configura para usar la GPU y HDX 3D Pro para la codificación y la representación de gráficos. De lo contrario, el subsistema de gráficos implementa Citrix Virtual Displays en el modo estándar de VDA. Para los clientes con varios monitores, damos respaldo a una combinación simultánea de unidades GPU compatibles en el VDA y Citrix Virtual Displays.

Para conocer las configuraciones de la directiva de HDX 3D Pro, consulte “Optimizar para cargas de trabajo de gráficos 3D” y “Mostrar indicador de calidad sin pérdida” en Configuraciones de directiva de Gráficos.

Todas las aplicaciones Citrix Workspace respaldadas 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 respaldadas 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 ordenador (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:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- En conexiones de red de área extensa (WAN). Entrega una experiencia de usuario interactiva en conexiones WAN con anchos de banda bajos, incluso hasta 1,5 Mbps.
- En conexiones de red de área local (LAN). Entrega una experiencia de usuario equivalente a la de un escritorio local en las conexiones LAN.

  Puede reemplazar estaciones de trabajo complejas y costosas por dispositivos de usuario más simples, al mover el procesamiento de gráficos al centro de datos para una administración centralizada.

HDX 3D Pro ofrece la aceleración GPU para las máquinas con sistema operativo de escritorio de Windows o servidor de Windows. Para obtener más información, consulte Aceleración de GPU para sistemas operativos de escritorio Windows y Aceleración de GPU para sistemas operativos de servidor Windows.

HDX 3D Pro es compatible con máquinas sin sistema operativo, además de las tecnologías de virtualización de GPU y GPU PassThrough que ofrecen los siguientes hipervisores:

- Citrix XenServer
  - GPU PassThrough con NVIDIA GRID e Intel GVT-d
  - Virtualización de GPU con NVIDIA GRID e Intel GVT-g
- Microsoft Hyper-V
  - GPU PassThrough (asignación de dispositivos diferenciados) con NVIDIA GRID y AMD
- VMware vSphere
  - GPU PassThrough (vDGA) con NVIDIA GRID, Intel e IOMMU de AMD
  - Virtualización de GPU con NVIDIA GRID y MxGPU de AMD
- Serie NV de Microsoft Azure
- Instancias de Amazon AWS EC2 G3

Para conocer las versiones de XenServer respaldadas, consulte Citrix XenServer Hardware Compatibility List.

La herramienta HDX Monitor permite validar la operación y la configuración de las tecnologías de visualización HDX, así como diagnosticar y solucionar problemas relacionados con HDX. Para descargar la herramienta y obtener más información acerca de ella, consulte https://taas.citrix.com/hdx/download/.

Aceleración de GPU para sistemas operativos de servidor Windows

October 3, 2018

HDX 3D Pro permite que las aplicaciones con muchos gráficos que se ejecutan en sesiones de sistema operativo de servidor Windows se representen en la unidad de procesamiento de gráficos (GPU) del

© 1999-2019 Citrix Systems, Inc. All rights reserved.

servidor. Al trasladar la representación de los gráficos de OpenGL, DirectX, Direct3D y Windows Presentation Foundation (WPF) a la unidad de procesamiento de gráficos (GPU) del servidor, la CPU del servidor no se 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.

Como Windows Server es un sistema operativo multiusuario, una GPU a la que se accede mediante Citrix Virtual Apps se puede compartir entre varios usuarios sin necesidad de virtualización de GPU (vGPU).

Para las instrucciones que impliquen modificar el Registro, tenga cuidado: si lo modifica de forma incorrecta, pueden producirse problemas graves que pueden requerir la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Compartir GPU

El uso compartido de GPU permite la generación por hardware de GPU de aplicaciones OpenGL y DirectX en las sesiones de escritorio remoto, y tiene las características siguientes:

- 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 pueden instalar varias GPU en un hipervisor y asignar VM a cada una de estas GPU individualmente, ya sea mediante la instalación de una tarjeta gráfica con más de una GPU, o bien, mediante la instalación de varias tarjetas gráficas con una o más GPU cada una. No se recomienda combinar tarjetas gráficas heterogéneas en un servidor.

Las máquinas virtuales requieren acceso de PassThrough directo a una GPU, que está disponible con Citrix XenServer, VMware vSphere vDGA e Intel GVT-d. Cuando se usa HDX 3D Pro junto con la función GPU Passthrough, cada GPU en el servidor da respaldo a una máquina virtual con varios usuarios.

El uso compartido de GPU no depende de ninguna tarjeta gráfica específica.

- Al ejecutar en un hipervisor, seleccione una plataforma de hardware y tarjetas gráficas que sean compatibles con la implementación de la función GPU Passthrough del hipervisor. La lista de hardware que ha aprobado la certificación con XenServer GPU PassThrough se encuentra disponible en Dispositivos de GPU PassThrough.
- 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 usando el Administrador de dispositivos.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 vuelve extremadamente sobrecargado, esto puede provocar inestabilidad o incluso el bloqueo del controlador de la tarjeta gráfica. Limite el número de usuarios simultáneos para evitar esos problemas.

Para confirmar que está teniendo lugar la aceleración por GPU, use una herramienta de terceros, como GPU-Z. GPU-Z está disponible en http://www.techpowerup.com/gpuz/.

- Acceso a un codificador de vídeo de alto rendimiento para las GPU de NVIDIA y los procesadores gráficos de Intel Iris Pro. Esta funcionalidad se controla mediante una configuración de directiva (habilitada de forma predeterminada) y permite el uso de codificación por hardware para la codificación H.264 (si está disponible). Si no está disponible, el VDA recurre a la codificación basada en CPU con el códec de vídeo del software. Para obtener más información, consulte Configuraciones de directiva de gráficos.

Presentación de DirectX, Direct3D y WPF

La presentación de DirectX, Direct3D y WPF está solo disponible en servidores con una GPU que admita una interfaz de control de presentación (DDI), versión 9ex, 10 u 11.

- En Windows Server 2008 R2, DirectX y Direct3D no requieren ninguna configuración especial para usar una única GPU.
- En Windows Server 2016 y Windows Server 2012, las sesiones de Servicios de Escritorio remoto (RDS) en el servidor host de sesión de Escritorio remoto usan el Controlador de representación básica de Microsoft como el adaptador predeterminado. Para usar la GPU en sesiones de RDS en Windows Server 2012, habilite la configuración Usar el adaptador de gráficos de hardware predeterminado para todas las sesiones de Servicios de Escritorio remoto en la directiva de grupo Directiva de equipo local > Configuración del equipo > Plantillas administrativas > Componentes de Windows > Servicios de Escritorio remoto > Host de sesión de Escritorio remoto > Entorno de sesión remota.
- Para habilitar las aplicaciones WPF para que representen gráficos mediante la GPU del servidor, cree los siguientes parámetros en el Registro de Windows del servidor que ejecuta sesiones de SO de servidor Windows:
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Multiple Monitor Hook] “EnableWPFHook”=dword:00000001
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\ Multiple Monitor Hook] “EnableWPFHook”=dword:00000001

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Aceleración de GPU para aplicaciones OpenCL o CUDA

La aceleración de GPU para aplicaciones OpenCL y CUDA que se ejecutan en una sesión de usuario está inhabilitada de forma predeterminada.

Para usar las funcionalidades POC de aceleración de CUDA, habilite los siguientes parámetros de Registro:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] “CUDA”=dword:000000
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] “CUDA”=dword:00000001

Para usar las funcionalidades POC de aceleración de OpenCL, habilite los siguientes parámetros de Registro:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] “OpenCL”=dword:0000
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] “OpenCL”=dword:00000001

Aceleración de GPU para sistemas operativos de escritorio Windows

March 8, 2019

Con HDX 3D Pro, puede entregar aplicaciones de uso intensivo de gráficos como parte de escritorios o aplicaciones que se alojan en máquinas de SO de escritorio. 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. El verdadero uso compartido de GPU de hardware proporciona escritorios adecuados para los usuarios con requisitos de diseño complejos y exigentes. La virtualización de GPU para las tarjetas NVIDIA GRID (consulte NVIDIA GRID), utiliza los mismos controladores de gráficos NVIDIA que se implementan en sistemas operativos no virtualizados. La virtualización de GPU también se admite en las CPU Intel de 5.ª y 6.ª generación con gráficos Intel Iris Pro con Intel GVT-g. Para obtener más información sobre estas familias de procesadores Intel, consulte 5th Generation Intel Core Processors y 6th Generation Intel Core i5 Processors.También se admite la virtualización de GPU para las tarjetas de servidor FirePro de serie S de AMD, consulte AMD Professional Graphics virtualization solution.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

HDX 3D Pro ofrece las siguientes características:

- 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 o H.265 se puede usar con tarjetas de NVIDIA que admiten NVENC.
- Opción de compresión sin pérdida para casos especiales. HDX 3D Pro también ofrece un códec sin pérdida basado en CPU para dar respaldo a las aplicaciones que necesitan gráficos de calidad perfecta, como las que crean imágenes que se utilizarán con fines médicos. La compresión sin pérdida solo se recomienda para casos de uso especializados, ya que consume muchos más recursos de red y de procesamiento.

  Cuando se utiliza la compresión sin pérdida:

  - El indicador de compresión sin pérdida es un icono de la bandeja del sistema que notifica al usuario cuando la pantalla muestra fotogramas con o sin pérdida. Lo que ayuda cuando la 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 deseleccionar la compresión sin pérdida en cualquier momento de la sesión, haga clic con el botón derecho en el icono 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 el códec de compresión sin pérdida en cada conexión, seleccione "Siempre sin pérdida" en la 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 HKLM\SOFTWARE\Citrix\HDX3D\LLIndicator.
  - 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 claves deben estar separadas por comas (,). El orden de las claves no importa.
  - A, C, S, W y K son claves 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

  - Por ejemplo:
    * Para F10, defina K = 0x79.
    * Para Ctrl + F10, defina C = 1, K = 0x79.
    * Para Alt + A, defina A = 1, K = a; o bien A = 1, K = A; o bien, K = A, A = 1.
    * Para Ctrl + Alt + 5, defina C = 1, A = 1, K = 5; o bien, A = 1, K = 5, C = 1.
    * Para Ctrl + Mayús + F5, defina A = 1, S = 1, K = 0x74.

> **Precaución:**
>
> Si modifica el Registro de forma incorrecta, podrían generarse problemas graves que pueden provocar la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

- Respaldo para varios monitores de alta resolución. Para máquinas de SO de escritorio, HDX 3D Pro respalda el uso de dispositivos de usuario con hasta cuatro monitores. Los usuarios pueden organizar sus monitores con la configuración que deseen y pueden mezclar monitores con resoluciones y orientaciones diferentes. La cantidad de monitores se ve limitada solamente por la capacidad de la GPU del equipo host, el dispositivo de usuario y el ancho de banda disponible. HDX 3D Pro admite todas las resoluciones de monitor. Sólo la capacidad de la GPU en el equipo host limita el uso de ciertas resoluciones.

  HDX 3D Pro también ofrece respaldo limitado para acceso con monitor doble a escritorios Windows XP. Para obtener más información acerca de este tema, consulte Agentes VDA en máquinas con Windows XP o Windows Vista.

- Resolución dinámica. Puede cambiar el tamaño de la ventana de la aplicación o del escritorio virtual a cualquier resolución.**Nota:** El único método admitido para cambiar la resolución es cambiar el tamaño de la ventana de la sesión de VDA. El cambio de resolución desde dentro de la sesión de VDA (mediante el Panel de control > Apariencia y personalización > Pantalla > Resolución de pantalla) no está respaldado.

- Respaldo para la arquitectura de NVIDIA GRID. HDX 3D Pro admite tarjetas NVIDIA GRID (consulte NVIDIA GRID) para GPU PassThrough y uso compartido de GPU. La vGPU de NVIDIA GRID permite que múltiples máquinas virtuales tengan acceso directo y simultáneo a una única GPU física, usando los mismos controladores de gráficos de NVIDIA que se implementan en sistemas operativos no virtualizados.

- Respaldo para VMware vSphere y VMware ESX mediante vDGA. Puede utilizar HDX 3D Pro con vDGA para cargas de trabajo de RDS y VDI.

- Respaldo para VMware vSphere/ESX mediante NVIDIA GRID vGPU y MxGPU de AMD.

- Respaldo para Microsoft Hyper-V mediante la asignación de dispositivos diferenciados de Windows Server 2016.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Respaldo de gráficos para centros de datos con la familia de procesadores Intel Xeon E3. HDX 3D Pro admite varios monitores (hasta 3), poner en blanco la consola, una resolución personalizada y una alta velocidad de fotogramas con la familia de procesadores Intel respaldada.Para obtener más información, consulte http://www.citrix.com/intel y http://www.intel.com/content/www/us/en/servers/data-center-graphics.html.
- Respaldo para RapidFire de AMD en las tarjetas de servidor FirePro de serie S de AMD. HDX 3D Pro admite varios monitores (6 como máximo), consola vacía, resolución personalizada y alta velocidad de fotogramas. Nota: El respaldo HDX 3D Pro para MxGPU de AMD (virtualización de GPU) funciona solo con vGPU de VMWare vSphere. XenServer y Hyper-V son compatibles con GPU PassThrough. Para obtener más información, consulte AMD Virtualization Solution.
- Acceso a un codificador de vídeo de alto rendimiento para las GPU de NVIDIA y los procesadores gráficos de Intel Iris Pro. Esta funcionalidad se controla mediante una configuración de directiva (habilitada de forma predeterminada) y permite el uso de codificación por hardware para la codificación H.264 (si está disponible).Si no está disponible, el VDA volverá a la codificación basada en CPU con el códec de vídeo del software. Para obtener más información, consulte Configuraciones de directiva de gráficos.

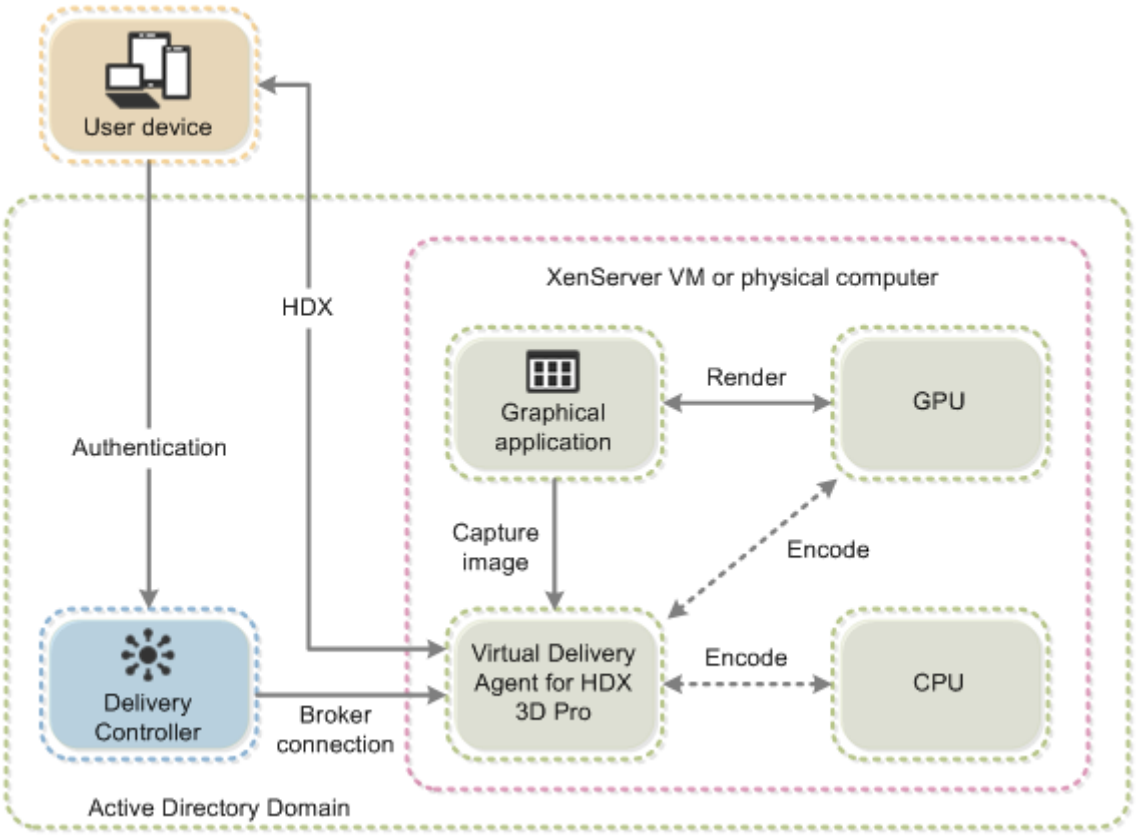
Como se muestra en la siguiente imagen:

- Cuando un usuario inicia sesión en la aplicación Citrix Workspace y accede al escritorio o a la aplicación virtual, el Controller autentica al usuario y se comunica con el VDA para que HDX 3D Pro actúe como intermediario en 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 aplicación o escritorio y las interacciones del usuario con las mismas se transmiten entre el equipo host y el dispositivo de usuario a través de una conexión HDX directa entre la aplicación Citrix Workspace y el VDA para HDX 3D Pro.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Instalar y actualizar controladores NVIDIA

La API de NVIDIA GRID proporciona acceso directo al búfer de trama de la GPU, lo que proporciona la velocidad de fotogramas más alta para una experiencia de usuario fluida e interactiva. Si instala controladores NVIDIA antes de instalar un agente VDA con HDX 3D Pro, NVIDIA GRID se habilita de manera predeterminada.

Para habilitar NVIDIA GRID en una VM, inhabilite el Adaptador de pantalla básico de Microsoft desde el Administrador de dispositivos. Ejecute el siguiente comando y luego reinicie el VDA: **NVFBCEnable.exe -enable -noreset**

Si instala controladores NVIDIA después de instalar un agente VDA con HDX 3D Pro, NVIDIA GRID se inhabilita. Habilite NVIDIA GRID mediante la herramienta NVFBCEnable suministrada por NVIDIA.

Para inhabilitar NVIDIA GRID, ejecute el siguiente comando y luego reinicie el VDA: **NVFBCEnable.exe -disable -noreset**

Instalar controladores de gráficos Intel

Puede instalar los controladores de gráficos Intel antes de instalar el VDA. El siguiente paso solo es necesario si instala los controladores Intel después de instalar un agente VDA con HDX 3D Pro o si el

© 1999-2019 Citrix Systems, Inc. All rights reserved.

controlador Intel se ha actualizado.

Para habilitar los controladores Intel requeridos para el respaldo de varios monitores, ejecute el siguiente comando mediante GfxDisplayTool.exe y luego reinicie el VDA: **GfxDisplayTool.exe -vd enable**

GfxDisplayTool.exe se incluye con el instalador del VDA. GfxDisplayTool.exe se encuentra en C:\Archivos de programa\Citrix\ICAServices.

> **Nota:**
>
> La desinstalación de controles Intel o NVIDIA dentro de sesiones ICA no recibe respaldo.

Optimizar la experiencia del usuario de HDX 3D Pro

Para utilizar HDX 3D Pro con varios monitores, asegúrese de que el equipo host está configurado para, al menos, el número de monitores conectados a los dispositivos de usuario. Los monitores conectados al equipo host pueden ser físicos o virtuales.

No conecte un monitor (ya sea físico o virtual) a un equipo host mientras un usuario está conectado a la aplicación o escritorio virtual que proporciona la aplicación gráfica. Si lo hace, puede provocar inestabilidad durante toda la sesión del usuario.

Indique a los usuarios que no se admiten cambios en la resolución del escritorio (por ellos o una aplicación) mientras haya sesiones de aplicaciones gráficas en curso. Después de cerrar la sesión de la aplicación, el usuario puede cambiar la resolución de la ventana de Desktop Viewer en la aplicación Citrix Workspace: Preferencias de Desktop Viewer.

Cuando varios usuarios comparten una conexión con ancho de banda limitado (como los usuarios en una sucursal), Citrix recomienda utilizar la directiva Límite de ancho de banda global de la sesión para limitar el ancho de banda disponible para cada usuario. Esto 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 en todo momento.

Para los usuarios de ratones 3D, Citrix recomienda aumentar la prioridad del canal virtual Redirección USB genérica a 0. Para obtener información sobre cómo cambiar la prioridad del canal virtual, consulte CTX128190.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Framehawk

January 29, 2019

Framehawk es una tecnología especializada en pantallas remotas para usuarios móviles con conexiones inalámbricas de banda ancha (redes de telefonía móvil Wi-Fi, 4G o LTE) que pueden sufrir un descarte de paquetes elevado. Framehawk resuelve obstáculos como interferencias espectrales y propagaciones multitrayecto. Framehawk ofrece una experiencia fluida e interactiva a los usuarios de aplicaciones y escritorios virtuales que operen desde dispositivos móviles, como tabletas y portátiles, con iOS o Windows. Para maximizar la escalabilidad de servidores pero minimizar el consumo del ancho de banda de la red, recomendamos usar Framehawk solo para el caso de uso específico descrito. Para todos los demás casos de uso, recomendamos el transporte adaptable, que incorpora muchos conceptos de Framehawk para maximizar el rendimiento de los datos.

Se pueden utilizar las plantillas de directiva de Citrix para implementar Framehawk en un conjunto de usuarios para determinadas circunstancias de acceso que se adecúen a su empresa. Framehawk está orientado a casos de uso de dispositivos móviles con una pantalla, como equipos portátiles y tabletas. Use Framehawk cuando el valor empresarial del rendimiento interactivo en tiempo real justifica el coste adicional en recursos de servidor y requisitos de una conexión de banda ancha.

Cómo mantiene Framehawk una experiencia de usuario fluida

Piense en Framehawk como toda la complejidad del ojo humano que se implementa como un software que observa lo que hay en el búfer de fotogramas y distingue los diferentes tipos de contenido en la pantalla. ¿Qué es importante para el usuario? Cuando se trata de zonas de la pantalla que cambian rápidamente (vídeos o gráficos en movimiento), no detectamos si se pierden algunos píxeles por el camino. Esas áreas se sobrescriben rápidamente con nuevos datos.

Pero, cuando se trata de zonas estáticas de la pantalla, nos volvemos muy exigentes. Por ejemplo, los iconos en el área de notificaciones o de la barra de herramientas, texto que vemos tras desplazarnos hasta el punto desde el que queremos comenzar al leer Esperamos que cada píxel de esas zonas esté perfectamente definido. A diferencia de los protocolos, cuyo objetivo es la precisión técnica desde una perspectiva de **unos y ceros**, el propósito de Framehawk es ser relevante para el ser humano que está utilizando la tecnología.

Framehawk incluye un amplificador de señales de calidad de servicio de siguiente generación y un mapa de calor basado en tiempo para conseguir una identificación de cargas de trabajo más eficiente y precisa. Utiliza transformaciones autónomas de recuperación automática, además de compresión de datos, y evita la retransmisión de datos para mantener la respuesta de clics, la linealidad y una cadencia coherente. En una conexión de red con pérdida de datos, Framehawk oculta la pérdida gracias a la interpolación, y el usuario sigue percibiendo una buena calidad de imagen y disfrutando de una experiencia más fluida. Además, los algoritmos de Framehawk diferencian de forma inteligente entre

© 1999-2019 Citrix Systems, Inc. All rights reserved.

los diferentes tipos de pérdidas de paquetes. Por ejemplo, pérdidas aleatorias (en las que envía más datos para compensar) frente a la pérdida por congestión (no envía más datos porque el canal ya está obstruido).

El motor de intenciones Framehawk Intent Engine en la aplicación Citrix Workspace distingue entre: el desplazamiento hacia arriba o hacia abajo, el zoom para acercar o alejar la imagen, el movimiento a la izquierda o a la derecha, la lectura, la escritura y otras acciones comunes. Además, gestiona la comunicación de retorno al Virtual Delivery Agent (VDA) mediante un diccionario compartido. Si el usuario lee, la calidad visual del texto debe ser excelente. Si el usuario se desplaza, el desplazamiento debe ser rápido y fluido. Por si fuera poco, tiene que poder interrumpirse sin complicaciones, de modo que el usuario siempre tenga el control de la interacción con la aplicación o el escritorio.

Al medir la cadencia de una conexión de red (similar a la tensión de una cadena de bicicleta en un sistema de **marchas**), la lógica de Framehawk puede reaccionar más rápidamente, lo que proporciona una experiencia de alta calidad en conexiones con altos niveles de latencia. Este sistema único y patentado de mediciones ofrece una respuesta constante y actualizada de parte de las condiciones de red, lo que permite a Framehawk reaccionar de inmediato a cambios de ancho de banda, latencia y pérdidas de datos.

Consideraciones de diseño al usar Thinwire y Framehawk

Framehawk usa una capa de transporte de datos generada sobre UDP (User Datagram Protocol). El protocolo UDP es solo una pequeña pieza de la estrategia de Framehawk para superar el problema de la pérdida de paquetes (como se puede constatar al comparar el rendimiento de Framehawk con otros protocolos basados en UDP). UDP ofrece una base importante para las técnicas centradas en el usuario que distinguen Framehawk.

¿Qué ancho de banda necesita Framehawk?

El ancho de banda de la red inalámbrica depende de varios factores, como la cantidad de usuarios que comparten la conexión, la calidad de esa conexión y las aplicaciones que se usan. Para un rendimiento óptimo, Citrix sugiere una base de 4 o 5 Mbps más aproximadamente 150 Kbps por usuario simultáneo.

Generalmente, recomendamos un ancho de banda formado por una base de 1,5 Mbps y 150 Kbps por usuario para Thinwire. Para obtener más información, consulte el blog sobre ancho de banda de Citrix Virtual Apps and Desktops. Sin embargo, verá que, con una pérdida de paquetes del 3%, Thinwire por TCP necesita mucho más ancho de banda que Framehawk para mantener una experiencia de usuario óptima.

Thinwire sigue siendo el canal principal de presentación para la comunicación remota en el protocolo ICA. Framehawk está inhabilitado de forma predeterminada. Citrix recomienda habilitarlo de forma selectiva para casos de acceso a redes inalámbricas de banda ancha en su empresa. Recuerde que Framehawk requiere considerablemente más recursos de servidor (memoria y CPU) que Thinwire.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Requisitos y consideraciones

Framehawk requiere, como mínimo, VDA 7.6.300 y Administración de directivas de grupo 7.6.300.

El dispositivo de punto final debe tener, como mínimo, la aplicación Citrix Workspace para Windows 1808 o Citrix Receiver para Windows 4.3.100, la aplicación Citrix Workspace para iOS 1808 o Citrix Receiver para iOS 6.0.1.

De manera predeterminada, Framehawk usa un intervalo de puertos UDP bidireccional (de 3224 a 3324) para intercambiar datos del canal de presentación Framehawk con la aplicación Citrix Workspace; el intervalo puede personalizarse en una configuración de directiva llamada **Intervalo de puertos del canal de presentación Framehawk**. Cada conexión simultánea entre el cliente y el escritorio virtual requiere de un puerto único. Para entornos de SO multiusuario (como los servidores Citrix Virtual Apps), es necesario definir los puertos suficientes para admitir la cantidad máxima de sesiones de usuario simultáneas. Para SO de un solo usuario (como escritorios VDI), basta con definir un único puerto UDP. Framehawk intenta utilizar el primer puerto definido, hasta llegar al último puerto especificado en el intervalo. Este mecanismo se aplica a conexiones que pasan por Citrix Gateway y conexiones internas directamente al servidor StoreFront.

Para obtener acceso remoto, se debe implementar un Citrix Gateway. De forma predeterminada, Citrix Gateway utiliza el puerto UDP 443 para la comunicación cifrada entre la aplicación Citrix Workspace del cliente y Citrix Gateway. Este puerto debe estar abierto en los firewall externos para permitir la comunicación segura en ambas direcciones. Este protocolo se denomina Datagram Transport Layer Security (DTLS).

> **Nota:**
>
> Las conexiones de Framehawk/DTLS no se admiten en dispositivos FIPS.

El tráfico cifrado de Framehawk se admite en NetScaler Gateway a partir de la versión 11.0.62 y en NetScaler Unified Gateway a partir de la versión 11.0.64.34.

Se admite la alta disponibilidad de NetScaler a partir de XenApp y XenDesktop 7.12.

Tenga en cuenta las siguientes recomendaciones antes de implementar Framehawk:

- Póngase en contacto con el administrador de seguridad para confirmar que los puertos UDP definidos para Framehawk están abiertos en el firewall. El proceso de instalación no configura automáticamente el firewall.
- A menudo, Citrix Gateway se instala en la zona desmilitarizada, rodeado de firewalls externos e internos. Compruebe que el puerto UDP 443 está abierto en el firewall externo. Verifique asimismo que los puertos UDP del 3224 al 3324 están abiertos en el firewall interno si el entorno usa los intervalos predeterminados de puertos.

Configuración

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> **Precaución:**
>
> Citrix recomienda habilitar Framehawk solamente para usuarios que tendrán probablemente grandes pérdidas de paquetes. También se recomienda no habilitar Framehawk como una directiva universal para todos los objetos del sitio.

Framehawk está inhabilitado de forma predeterminada. Cuando está habilitado, el servidor intenta usar Framehawk para los gráficos y la entrada de los usuarios. Si no se cumplen los requisitos previos por cualquier motivo, se establece la conexión en el modo predeterminado (Thinwire).

Las siguientes configuraciones de directiva afectan Framehawk:

- Canal de presentación Framehawk: Habilita o inhabilita la funcionalidad.
- Intervalo de puertos del canal de presentación Framehawk: Especifica el intervalo de puertos UDP (del número de puerto más bajo al más alto) que el VDA utiliza para intercambiar datos del canal de presentación Framehawk con el dispositivo del usuario. El agente VDA intenta utilizar todos los puertos, comenzando por el de número más bajo y subiendo en cada intento subsiguiente. El puerto gestiona el tráfico de entrada y salida.

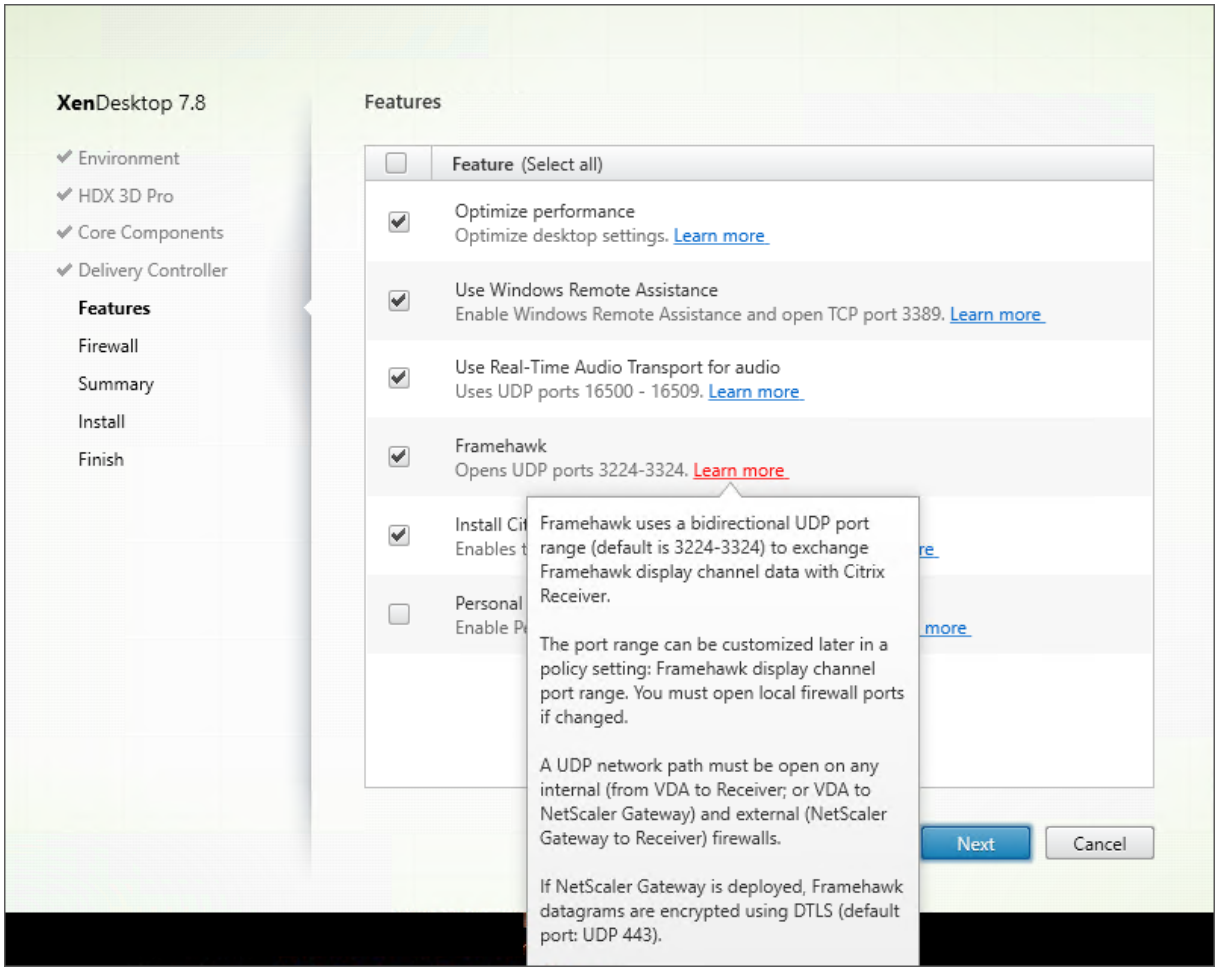
Abrir puertos para el canal de presentación Framehawk

A partir de XenApp y XenDesktop 7.8, dispone de una opción para volver a configurar el firewall durante el paso **Características** de la instalación del VDA. Si se marca, esta casilla abre los puertos UDP del 3224 al 3324 en el Firewall de Windows. Tenga en cuenta que es necesario configurar manualmente el firewall en algunas circunstancias:

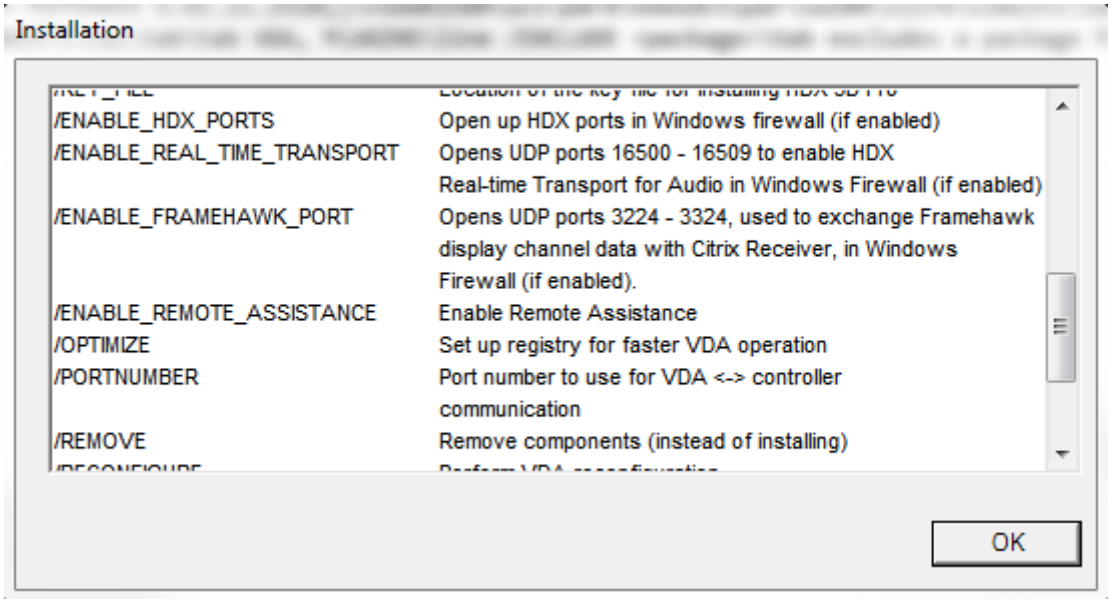
- Para los firewalls de red.
  O bien:
- Si se personaliza el intervalo predeterminado de puertos.

Para abrir esos puertos UDP, marque la casilla **Framehawk**:

© 1999-2019 Citrix Systems, Inc. All rights reserved.



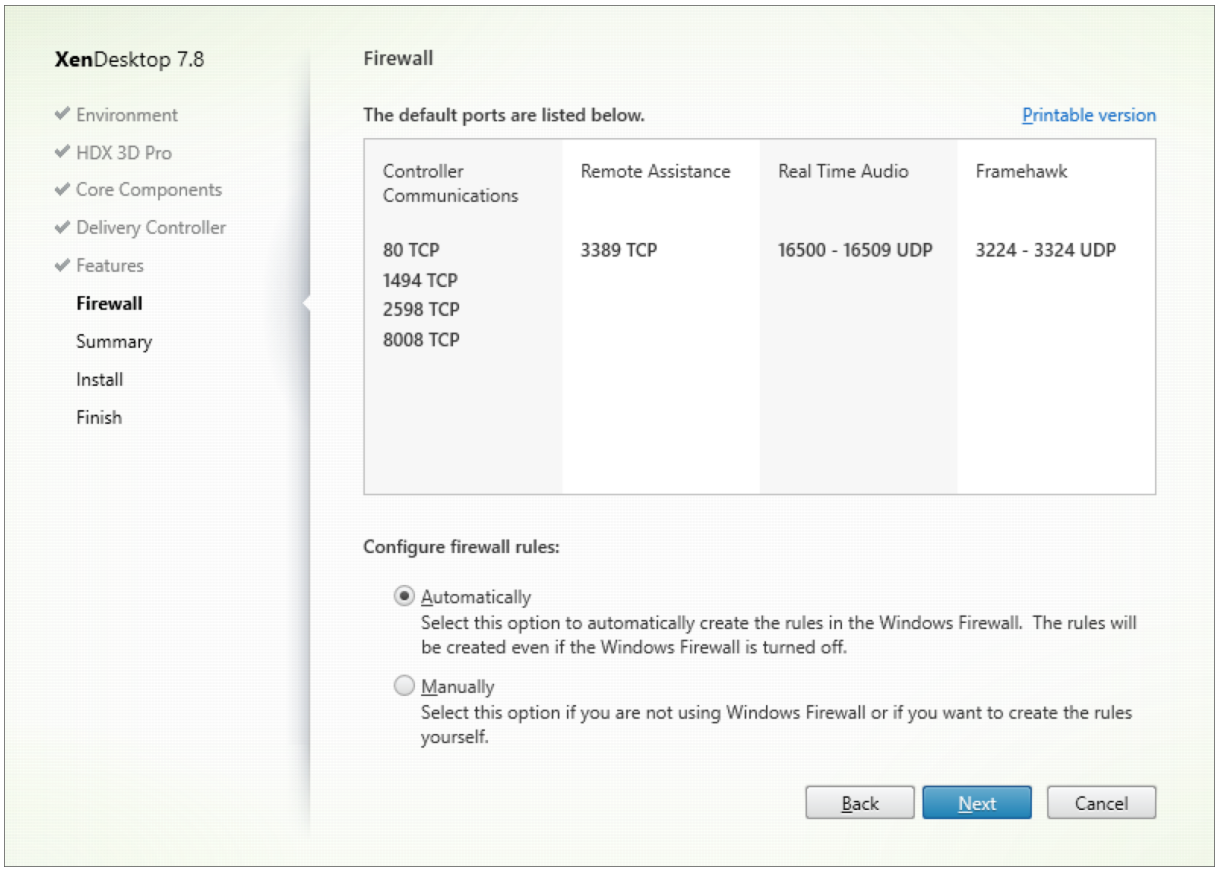
También puede utilizar la línea de comandos para abrir los puertos UDP para Framehawk mediante **/ENABLE_FRAMEHAWK_PORT**:



© 1999-2019 Citrix Systems, Inc. All rights reserved.

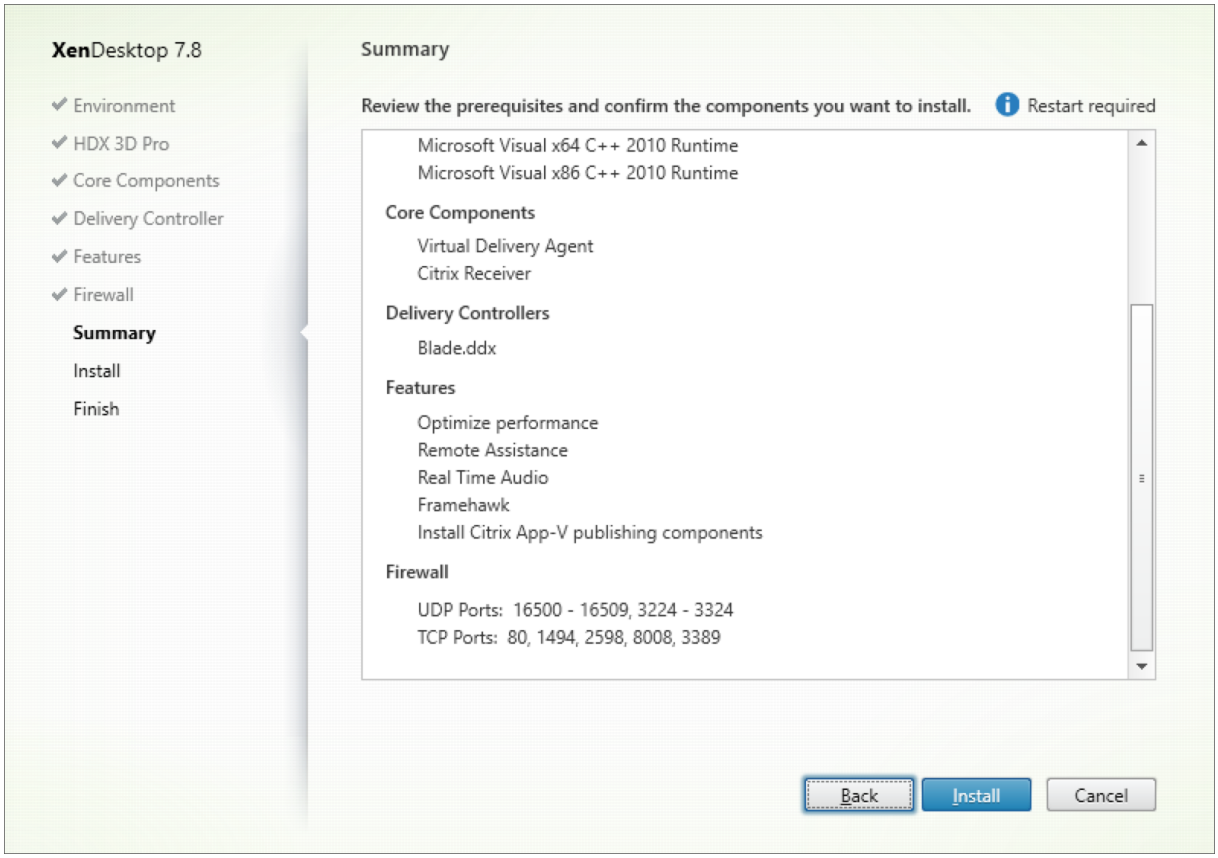
Comprobar las asignaciones de puertos UDP a Framehawk

Durante la instalación, puede comprobar los puertos UDP asignados Framehawk en la pantalla **Firewall**:



En la pantalla **Resumen**, se indica si la función Framehawk está habilitada:

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Respaldo de Citrix Gateway para Framehawk

El tráfico cifrado de Framehawk se admite a partir de Citrix Gateway 1808 o a partir de NetScaler Gateway 11.0.62.10 y en Citrix Unified Gateway 1808 o NetScaler Unified Gateway a partir de la versión 11.0.64.34.

- Citrix Gateway remite a la arquitectura de implementación en que se puede acceder al servidor virtual de VPN de Gateway directamente desde el dispositivo del usuario final. Es decir, el servidor virtual de la red VPN tiene una dirección IP pública asignada y el usuario se conecta directamente a esa dirección IP.
- Citrix Gateway con Unified Gateway remite a la implementación en que el servidor de VPN de Gateway está enlazado como destino al servidor virtual de conmutación de contenido (CS). En esta implementación, el servidor virtual de CS tiene la dirección IP pública y el servidor virtual de VPN de Gateway tiene una IP ficticia.

Para habilitar el respaldo a Framehawk en Citrix Gateway, el parámetro del protocolo DTLS debe estar habilitado en el servidor virtual de VPN de Gateway. Una vez habilitado el parámetro y actualizados los componentes de Citrix Virtual Apps o Citrix Virtual Desktops, el audio, el vídeo y el tráfico interactivo de Framehawk se cifran entre el servidor virtual de VPN de Gateway y el dispositivo del usuario.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Citrix Gateway, Unified Gateway y Citrix Gateway con Global Server Load Balancing (Equilibrio de carga del servidor global) son compatibles con Framehawk.

Los siguientes casos no son compatibles con Framehawk:

- HDX Insight
- Citrix Gateway en modo IPv6
- Doble salto de Citrix Gateway
- Citrix Gateway con configuración en clústeres

Caso	Respaldo para Framehawk
Citrix Gateway	Sí
Citrix Gateway + Global Server Load Balancing	Sí
Citrix Gateway con Unified Gateway	Sí. **Nota:** Se da respaldo a Unified Gateway 11.0.64.34 y versiones posteriores.
HDX Insight	No
Citrix Gateway en modo IPv6	No
Doble salto de Citrix Gateway	No
Varios Secure Ticket Authority en Citrix Gateway	Sí
Citrix Gateway con alta disponibilidad	Sí
Citrix Gateway con configuración en clústeres	No

Configurar Citrix Gateway para que respalde Framehawk

Para habilitar el respaldo a Framehawk en Citrix Gateway, el parámetro del protocolo DTLS debe estar habilitado en el nivel del *servidor virtual* de VPN de Gateway. Una vez habilitado el parámetro y actualizados los componentes de Citrix Virtual Apps o Citrix Virtual Desktops, el audio, el vídeo y el tráfico interactivo de Framehawk se cifran entre el servidor virtual de VPN de Gateway y el dispositivo del usuario.

Se necesita esta configuración para habilitar el cifrado de UDP en Citrix Gateway para el acceso remoto.

Al configurar Citrix Gateway para que respalde Framehawk:

- Compruebe que el puerto UDP 443 está abierto en los firewalls externos
- Compruebe que el puerto de CGP (predeterminado: 2598) está abierto en los firewalls externos
- Habilite el protocolo DTLS en la configuración del servidor virtual de VPN

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Desenlace y vuelva a enlazar el par de claves de certificado SSL. Este paso no es necesario si se usa Citrix Gateway 1808 o versiones posteriores, o NetScaler 11.0.64.34 o versiones posteriores.

Para configurar Citrix Gateway para que admita Framehawk:

1. Implemente y configure Citrix Gateway para comunicarse con StoreFront y autenticar a los usuarios de Citrix Virtual Apps and Desktops.
2. En la ficha de configuración de Citrix Gateway, expanda Citrix Gateway y seleccione **Virtual Servers**.
3. Elija **Edit** para ver los parámetros básicos del servidor virtual de la red VPN. Compruebe el estado del parámetro de DTLS.
4. Elija **More** para ver más opciones de configuración:
5. Elija **DTLS** para ofrecer seguridad en las comunicaciones de protocolos de datagramas como Framehawk. Haga clic en **Aceptar**. El área de configuración básica del servidor virtual de la red VPN muestra que el indicador de DTLS está establecido en **True**.
6. Vuelva a abrir la pantalla de vinculación del certificado de servidor, y haga clic en **+** para enlazar el par de claves de certificado.
7. Elija el par de claves de certificado de antes y haga clic en **Select**.
8. Guarde los cambios en la vinculación del certificado de servidor.
9. Después de guardar, aparecerá el par de claves de certificado. Haga clic en **Bind**.
10. Omita el mensaje de advertencia **No usable ciphers configured on the SSL vserver/service** (No se han configurado cifrados que se puedan utilizar en el servicio o servidor virtual SSL), si aparece.

Pasos para versiones anteriores de NetScaler Gateway

Si usa una versión de NetScaler Gateway anterior a 11.0.64.34:

1. Vuelva a abrir la pantalla de vinculación del certificado de servidor, y haga clic en + para enlazar el par de claves de certificado.
2. Elija el par de claves de certificado de antes y haga clic en **Select**.
3. Guarde los cambios en la vinculación del certificado de servidor.
4. Después de guardar, aparecerá el par de claves de certificado. Haga clic en **Bind**.
5. Omita el mensaje de advertencia **No usable ciphers configured on the SSL vserver/service** (No se han configurado cifrados que se puedan utilizar en el servicio o servidor virtual SSL), si aparece.

Si quiere configurar Unified Gateway para admitir Framehawk:

1. Compruebe que Unified Gateway esté instalado y correctamente configurado. Para obtener más información, consulte la información acerca de Unified Gateway en el sitio de documentación de productos Citrix.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

2. Habilite el parámetro DTLS en el servidor virtual de VPN que está vinculado al *servidor virtual* de CS como *servidor virtual de destino*.

Limitaciones

Si hay entradas DNS obsoletas del servidor virtual de Citrix Gateway en el dispositivo cliente, es posible que el transporte adaptable y Framehawk recurran al transporte TCP en lugar del transporte UDP. Si se recurre al transporte TCP, vacíe la memoria caché DNS en el cliente y vuelva a establecer la sesión mediante el transporte UDP.

Framehawk no admite cursores de mouse de 32 bits, como el de aplicaciones del tipo PTC Creo.

Framehawk está pensado para dispositivos móviles (como portátiles y tabletas) que usan un solo monitor. Por eso, Framehawk recurre a Thinwire en una configuración de dos o más monitores.

Respaldar otros productos de VPN

Citrix Gateway es el único producto SSL VPN que respalda el cifrado de UDP que requiere Framehawk. La directiva de Framehawk puede no aplicarse si se usa otra solución SSL VPN o una versión incorrecta de Citrix Gateway. Los productos tradicionales IPSec VPN respaldarán Framehawk sin modificaciones.

Supervisar Framehawk

Puede supervisar el uso y el rendimiento de Framehawk desde Citrix Director. La vista de detalles del canal virtual HDX ofrece información útil para la supervisión y la solución de problemas relacionados con Framehawk en cualquier sesión. Para ver las métricas relacionadas con Framehawk, seleccione **Gráficos - Framehawk**.

Si se establece la conexión de Framehawk, verá **Provider = VD3D** y **Connected = True** en la página de detalles. Es normal que el estado del canal virtual sea inactivo, porque se supervisa el canal de señalización, que solo se usa durante el proceso inicial de enlace. En esa página, también se ofrecen otros datos estadísticos útiles sobre la conexión.

Si se producen problemas, consulte el blog para solucionar problemas de Framehawk.

Thinwire

January 29, 2019

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Introducción

Thinwire es la tecnología predeterminada de Citrix para pantallas remotas que se utiliza en Citrix Virtual Apps y Desktops.

Las tecnologías de pantallas remotas permiten que los gráficos generados en una máquina se transmitan (normalmente a través de una red) a otra máquina para que se vean desde allí.

Una buena solución de pantallas remotas debe ofrecer una experiencia de usuario altamente interactiva que sea similar a la de un equipo local. Thinwire lo consigue porque utiliza un abanico de técnicas complejas y eficientes para la compresión y el análisis de imágenes. Thinwire maximiza la escalabilidad de los servidores y consume menos ancho de banda que otras tecnologías de pantallas remotas.

Gracias a este equilibrio, Thinwire cubre la mayoría de los casos de uso generales que pueda haber en una empresa, y se usa como la tecnología predeterminada para pantallas remotas en Citrix Virtual Apps and Desktops.

Thinwire o Framehawk

Thinwire debería utilizarse para entregar cargas de trabajo típicas (por ejemplo, escritorios, aplicaciones de productividad de oficina o de explorador Web). Thinwire también se recomienda para entornos de varios monitores, de alta resolución o con casos de configuración elevada de ppp, así como para cargas de trabajo con una mezcla de contenido de vídeo y no vídeo.

En cambio, Framehawk debería utilizarse para trabajadores móviles con conexiones inalámbricas de banda ancha cuando la pérdida de paquetes puede ser grande de forma intermitente.

HDX 3D Pro

En su configuración predeterminada, Thinwire puede entregar 3D o gráficos de interacción alta. Sin embargo, se recomienda habilitar el modo HDX 3D Pro desde la directiva **Optimizar para cargas de trabajo de gráficos 3D** de Citrix para casos en que hay unidades GPU. El modo HDX 3D Pro utiliza la GPU para la aceleración de hardware y configura Thinwire con los parámetros óptimos para los gráficos. Lo que ofrece una experiencia más fluida para gráficos 3D profesionales. Para obtener más información, consulte HDX 3D Pro y Aceleración de GPU para sistemas operativos de escritorio Windows.

Requisitos y consideraciones

- Thinwire se ha optimizado para sistemas operativos modernos, como Windows Server 2012 R2, Windows Server 2016, Windows 7 y Windows 10. Para Windows Server 2008 R2, se recomienda

© 1999-2019 Citrix Systems, Inc. All rights reserved.

el modo de gráficos antiguo. Utilice las plantillas de directivas de Citrix integradas, así como las plantillas "Alta escalabilidad de servidores para sistemas operativos antiguos" y "Optimización de redes WAN para sistemas operativos antiguos" para entregar las combinaciones de configuraciones de directiva que Citrix recomienda para estos casos de uso.

> **Nota:**
>
> No se admite el modo de gráficos antiguo en esta versión. Este modo se incluye para la compatibilidad con versiones anteriores cuando se usa XenApp 7.15 LTSR y XenDesktop 7.15 LTSR, así como las versiones anteriores de VDA con Windows 7 y Windows 2008 R2.

- El parámetro de directiva que controla el comportamiento de Thinwire, **Usar códec de vídeo para compresión**, está disponible en las versiones de VDA de Citrix Virtual Apps and Desktops 7 1808 y versiones posteriores, así como XenApp y XenDesktop 7.6 FP3 y versiones posteriores. La opción **Usar códec de vídeo si se prefiere** es la configuración predeterminada en las versiones de VDA de Citrix Virtual Apps and Desktops 7 1808 o versiones posteriores, así como XenApp y XenDesktop 7.9 o versiones posteriores.
- Todas las aplicaciones Citrix Workspace admiten Thinwire. Sin embargo, algunas aplicaciones Citrix Workspace pueden admitir funciones de Thinwire que otras no admiten (por ejemplo, gráficos de 8 o 16 bits para reducir el uso del ancho de banda). La aplicación Citrix Workspace negocia automáticamente si admitir o no esas funciones.
- Thinwire usará más recursos de servidor (CPU, memoria) cuando haya varios monitores y una alta resolución de pantalla. Es posible ajustar la cantidad de recursos que utiliza Thinwire. Sin embargo, puede que eso provoque un aumento del uso de ancho de banda.
- En situaciones de poco ancho de banda y latencia alta, considere la posibilidad de habilitar gráficos de 8 o 16 bits para mejorar la interactividad, aunque ello afectará a la calidad visual, sobre todo en una profundidad de color de 8 bits.

Configuración

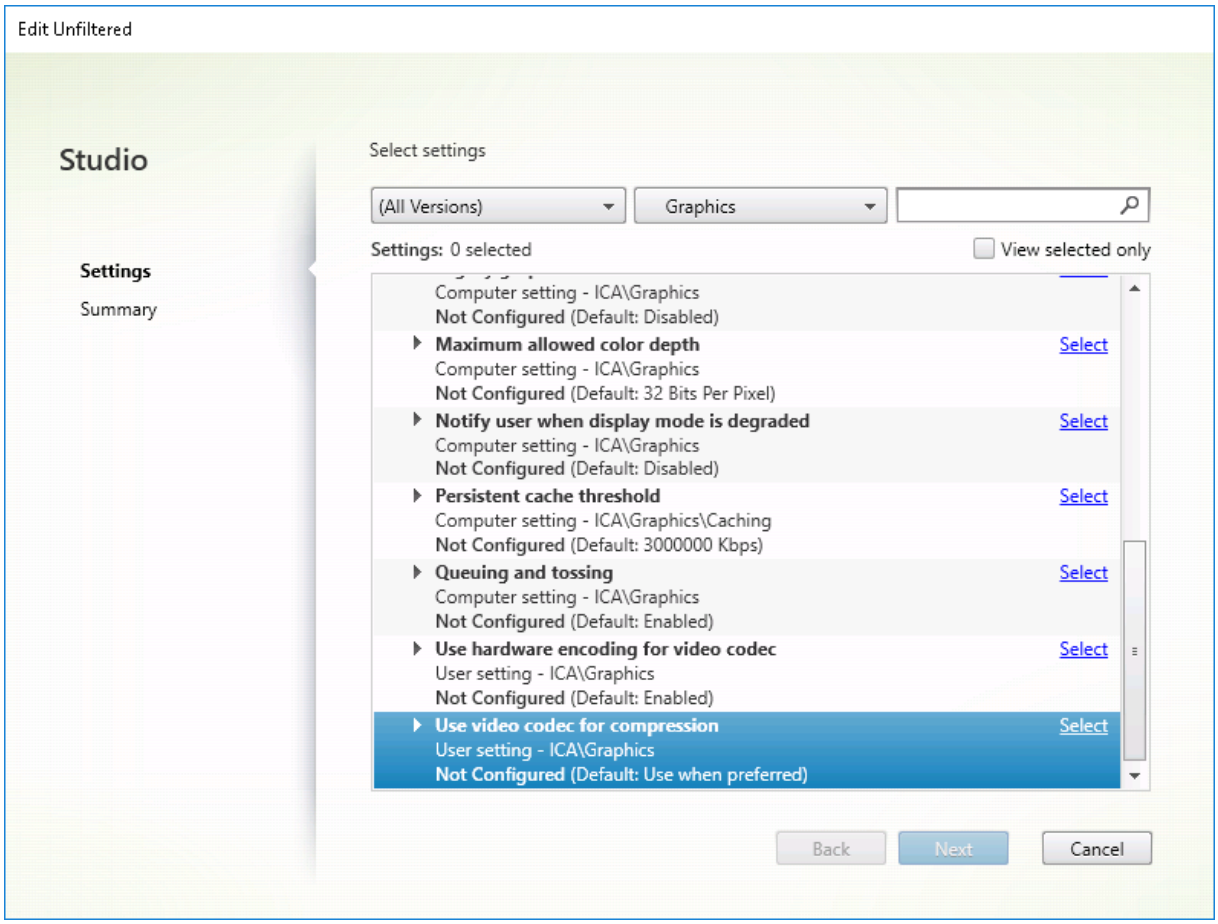
Thinwire es la tecnología predeterminada de pantallas remotas.

La siguiente configuración de directiva de Gráficos establece las opciones predeterminadas y ofrece alternativas a diferentes casos de uso:

- Usar códec de vídeo para compresión
  - **Usar códec de vídeo si se prefiere**. Esta es la opción predeterminada. No se requiere ninguna configuración adicional. Si mantiene esta configuración como predeterminada, Thinwire se seleccionará para todas las conexiones de Citrix, y se optimizará para la escalabilidad, el ancho de banda y una calidad de imagen superior para cargas de trabajo típicas de escritorio.
- Las demás opciones de esta configuración de directiva seguirán utilizando Thinwire combinado con otras tecnologías para diferentes casos de uso. Por ejemplo:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Para áreas en cambio constante**. En Thinwire, la tecnología de pantalla adaptable identifica las imágenes en movimiento (vídeo, 3D en movimiento) y usa H.264 o H.265 solo en aquella parte de la pantalla donde se mueva la imagen.
- **Para la pantalla entera**. Entrega Thinwire con H.264 o H.265 en pantalla completa para mejorar la experiencia del usuario y optimizar el ancho de banda, sobre todo cuando haya un uso intensivo de gráficos 3D.



Varias configuraciones de directiva más, incluidas las siguientes configuraciones de directiva de Presentación visual, se pueden usar para optimizar el rendimiento de la tecnología de pantallas remotas Thinwire las admite todas:

- Profundidad de color preferida para gráficos simples
- Velocidad de fotogramas de destino
- Calidad visual

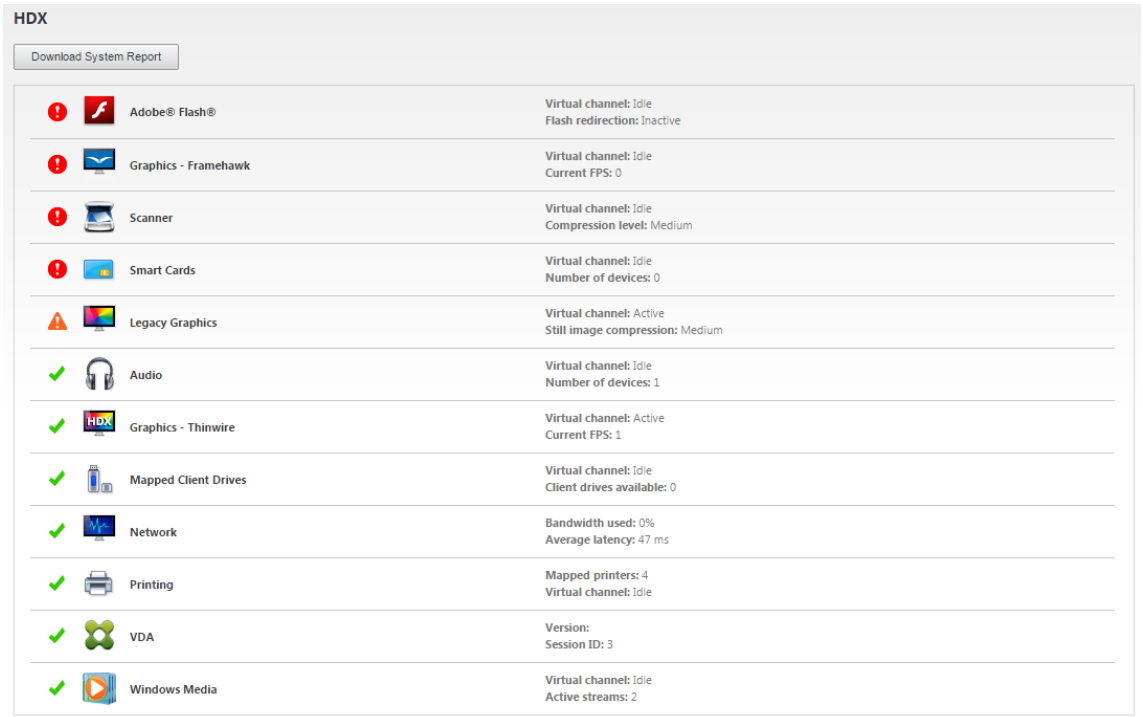
Para conocer las combinaciones de configuraciones de directiva que Citrix recomienda para diferentes casos de uso en empresas, use las plantillas de directivas de Citrix integradas. Las plantillas **Alta escalabilidad de servidores** y **Experiencia de usuario de muy alta definición** usan Thinwire con las mejores combinaciones de configuraciones de directiva para las prioridades de la empresa y las expectativas de los usuarios.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Supervisar Thinwire

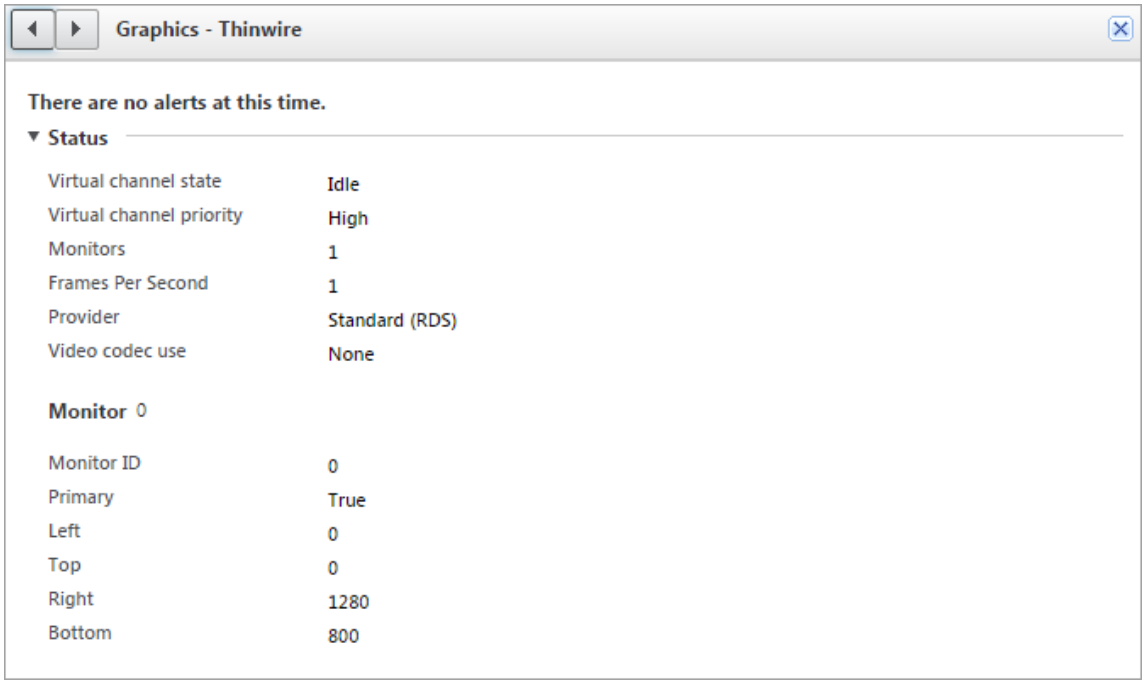
Puede supervisar el uso y el rendimiento de Thinwire desde Citrix Director. La vista de detalles del canal virtual HDX ofrece información útil para la supervisión y la solución de problemas relacionados con Thinwire en cualquier sesión. Para ver las métricas relacionadas con Thinwire:

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**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Métodos de codificación

En XenApp y XenDesktop 7.16 y sus versiones anteriores, Thinwire ofrecía tres modos de codificación de mapas de bits, utilizados en la comunicación remota de gráficos para el VDA del sistema operativo de servidor y de escritorio:

- Pantalla completa H.264
- Thinwire Plus
- Thinwire Plus con H.264 selectivo

En la comunicación remota GDI antigua, se utilizaba el controlador remoto de XPDM, no un codificador Thinwire de mapa de bits.

En una sesión de escritorio estándar, la mayoría de las imágenes son gráficos simples o regiones de texto. Cuando se utiliza uno de los tres modos de codificación de mapas de bits mencionados, Thinwire selecciona estas áreas para la codificación sin pérdida mediante el códec 2DRLE. En el lado del cliente de la aplicación Citrix Workspace, esos elementos se decodifican utilizando el decodificador 2DRLE del lado de la aplicación Citrix Workspace para mostrarlos en la sesión.

Códec de compresión sin pérdida (MDRLE)

En XenApp y XenDesktop 7.17, hemos agregado un codificador MDRLE, con una razón de compresión más alta y menor consumo de ancho de banda que el códec 2DRLE en sesiones de escritorio estándar.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Por lo general, un menor consumo de ancho de banda implica una interactividad de sesión mejorada (especialmente en enlaces compartidos o restringidos) y costes reducidos. Por ejemplo, el consumo de ancho de banda previsto cuando se utiliza el códec MDRLE es, aproximadamente, entre un 10 y un 15 % más pequeño que con XenApp y XenDesktop 7.15 LTSR para cargas de trabajo estándar de Office.

No se requiere ninguna configuración para el códec MDRLE. Si la aplicación Citrix Workspace admite la decodificación MDRLE, el VDA utiliza su propia codificación de MDRLE y la decodificación MDRLE de la aplicación Citrix Workspace. En cambio, si la aplicación Citrix Workspace no admite la decodificación MDRLE, el VDA recurre automáticamente a la codificación 2DRLE.

Requisitos de MDRLE

- Agentes VDA de Citrix Virtual Apps and Desktops 7 1808 (versión mínima)
- XenApp y XenDesktop: VDA 7.17 (versión mínima)
- Aplicación Citrix Workspace para Windows 1808 (versión mínima)
- Citrix Receiver para Windows 4.11 (versión mínima)

Modo progresivo

La interactividad de la sesión puede degradarse en enlaces de latencia baja o poco ancho de banda. Por ejemplo, en enlaces con menos de 2 Mbps de ancho de banda o una latencia de más de 200 ms, el desplazamiento por una página Web puede ralentizarse, dejar de responder o aparecer entrecortado. Las operaciones de teclado y mouse pueden retrasarse con respecto a las actualizaciones de gráficos. Con la versión 7.17, se podían usar las directivas para reducir el consumo del ancho de banda configurando la calidad visual de la sesión en “Baja” o estableciendo una profundidad de color menor (gráficos de 16 u 8 bits). Sin embargo, se tenía que saber que un usuario tenía poca conectividad. HDX Thinwire no podía ajustar dinámicamente la calidad de la imagen estática en función de las condiciones de red.
En la versión 7.18, HDX Thinwire cambia de forma predeterminada a un modo de actualización progresiva cuando el ancho de banda disponible baja de 2 Mbps o la latencia de red excede los 200 ms. En este modo:

- Todas las imágenes estáticas se comprimen mucho.
- La calidad del texto se reduce.

Las imágenes transitorias (vídeo) se siguen gestionando con la pantalla adaptable o H.264 selectivo.

Cómo se usa el modo progresivo

De forma predeterminada, el modo progresivo está en espera en las configuraciones de la directiva Calidad visual: Alta, Media (predeterminado) y Baja.

El modo progresivo se desactiva (no se usa) cuando:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Calidad visual = Siempre sin pérdida o Gradual sin pérdida
- Preferencia de profundidad de color para gráficos sencillos = 8 bits
- Usar códec de vídeo para compresión = Para la pantalla entera (cuando quiere H.264 a pantalla completa)

Si el modo progresivo está en espera, se habilita de forma predeterminada cuando se da una de las siguientes condiciones:

- El ancho de banda disponible baja a menos de 2 Mbps
- La latencia de red aumenta por encima de 200 ms

Después de un cambio de modo, transcurre un mínimo de 10 segundos en ese modo, aunque las condiciones adversas de la red fueran temporales.

Cambiar el comportamiento del modo progresivo

Puede cambiar el estado del modo progresivo con la siguiente clave de Registro:

[REG_DWORD] HKEY_LOCAL_MACHINE\Software\Citrix\Graphics\ProgressiveDisplay

Valores:

0 = Siempre desactivado (no usar en ninguna circunstancia)

1 = Automático (alternar según las condiciones de la red, este es el valor predeterminado)

2 = Siempre activado

Cuando está en el modo automático (1), puede usar la siguiente clave de Registro para cambiar los umbrales en los que se alterna al modo progresivo:

[REG_DWORD] HKEY_LOCAL_MACHINE\Software\Citrix\Graphics\ProgressiveDisplayBandwidthThreshold

Valor: <umbral en Kbps> (predeterminado = 2048)
Ejemplo: 4096 = Activa el modo progresivo si el ancho de banda baja de 4 Mbps

[REG_DWORD] HKEY_LOCAL_MACHINE\Software\Citrix\Graphics\ProgressiveDisplayLatencyThreshold

Valor: <umbral en ms> (predeterminado = 200)
Ejemplo: 100 = Activa el modo progresivo si la latencia de la red baja de 100 ms.

Marca de agua de sesión basada en texto

March 8, 2019

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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 característica 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 característica 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 de servidor 7.17
SO de escritorio 7.17

Limitaciones:

- No se admiten las marcas de agua de la sesión en las sesiones donde se utilizan: el acceso a aplicaciones locales, la redirección de Flash, 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 características deben estar inhabilitadas.
- La marca de agua de la sesión no se respalda y 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Usar codificación por hardware para códec de vídeo en **Habilitado**
Usar códec de vídeo para compresión en **Usar códec de vídeo si se prefiere**

Para asegurarse de que la marca de agua aparezca, establezca **Usar codificación por hardware para códec de vídeo** en **Inhabilitado** o establezca **Usar códec de vídeo para compresión** en **Para áreas en cambio constante** o **No usar códec de vídeo**.

- La marca de agua de la sesión solo admite el modo gráfico de Thinwire, no Framehawk ni la redirección de composición del escritorio (DCR).
- Si usa la Grabación de sesiones, la sesión grabada no incluirá la marca de agua.
- Si usa la Asistencia remota de Windows, la marca de agua no aparece.
- Si un usuario presiona la tecla **Imprimir pantalla**, la pantalla capturada en el lado del VDA no incluirá las marcas de agua. Le recomendamos que tome las medidas oportunas para evitar que se copie la imagen capturada.

Contenido multimedia

January 29, 2019

> **Nota:**
>
> Puede obtener información sobre los cambios en los nombres de producto aquí.

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 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, el respaldo a 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 y NVIDIA NVENC proporcionan la codificación H.264 acelerada por hardware.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

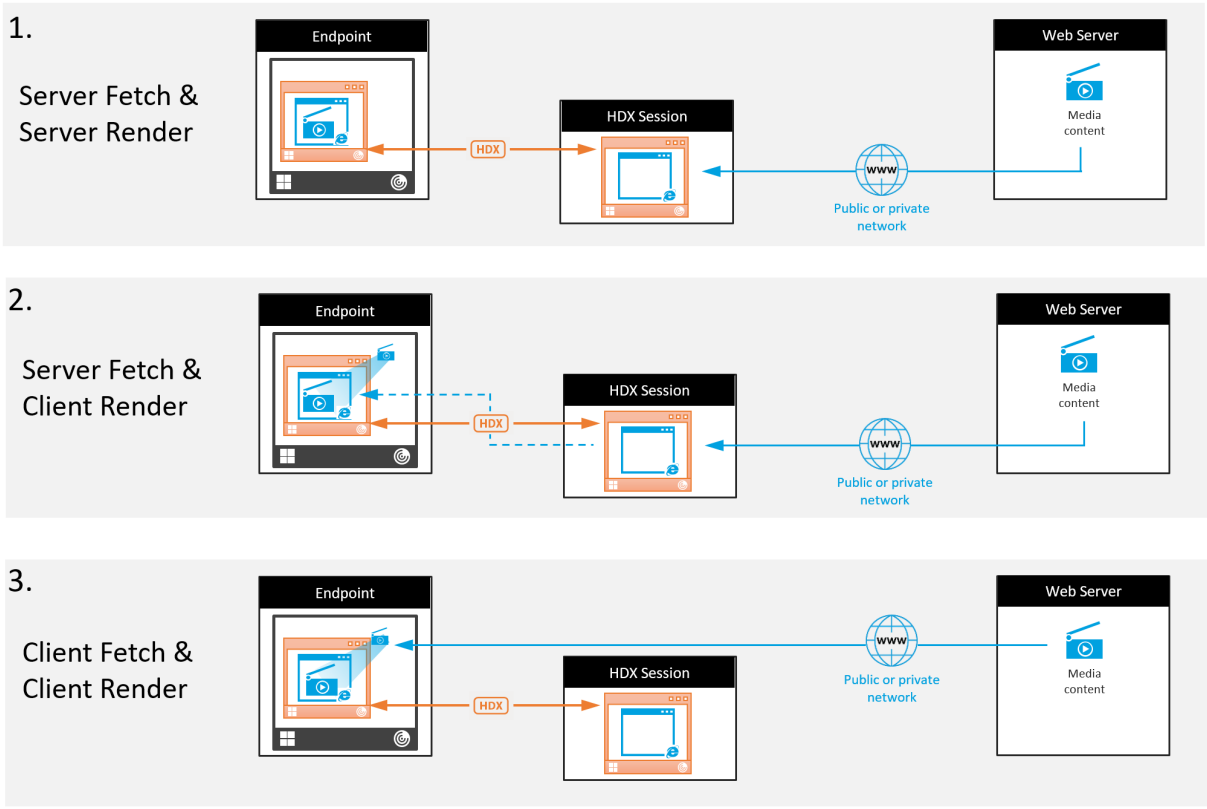
Puesto que la mayoría de los servidores no ofrecen la aceleración de hardware para la compresión de vídeo, la escalabilidad de servidor se ve afectada negativamente si todo el procesamiento de vídeo se realiza en el servidor de la CPU. Para mantener una alta escalabilidad de servidor, muchos formatos multimedia pueden redirigirse al dispositivo del usuario para generarse localmente. 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.

La redirección de Flash redirige el contenido de vídeo Adobe Flash a un Reproductor de Flash que se ejecuta localmente en el dispositivo de usuario.
El vídeo HTML5 ha empezado a utilizarse frecuentemente, por lo que Citrix ha introducido una tecnología de redirección para este tipo de contenido.
Asimismo, 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 respaldo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 la carga que representan la decodificación y la presentación se transmite a los dispositivos cliente, con lo que se ahorran ciclos de CPU en el servidor.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 escritorio (Windows, Mac OS X y Linux) ofrecen entornos multimedia que permiten un desarrollo más rápido de aplicaciones multimedia. En esta tabla se muestran algunos de los entornos multimedia más comunes. En cada entorno se divide el procesamiento multimedia en varias etapas y se usa una arquitectura adaptada.

Framework	Platform (Plataforma)
DirectShow	Windows (98 y versiones posteriores)
Media Foundation	Windows (Vista y versiones posteriores)
Gstreamer	Linux
QuickTime	Mac OS X

Respaldo para doble salto con tecnologías de redirección multimedia

Redirección de Flash de HDX	No
Redirección de Windows Media	Sí
Redirección de vídeos HTML5	Sí
Redirección de sonido	No

Funciones de audio

March 8, 2019

Puede configurar y agregar las siguientes configuraciones de directiva de Citrix a una directiva que

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 Sonido, Configuraciones de directiva de Ancho de banda y Configuraciones de directiva de Conexiones de multisecuencia.

> **Importante**
>
> Se recomienda entregar audio por el protocolo UDP (User Datagram Protocol) en lugar de TCP, aunque 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 usar el transporte TCP. TCP respalda el cifrado TLS de punto a punto desde el VDA a la aplicación Citrix Workspace.

Calidad de sonido

En general, un sonido de mayor calidad consume más ancho de banda y utiliza más recursos de CPU del servidor, al enviar más datos de sonido a los dispositivos de los usuarios. La compresión de sonido permite llegar a un equilibrio entre calidad de sonido 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 sonido.

De forma predeterminada, la directiva “Calidad de sonido” está establecida en “Alta: sonido de alta definición” cuando se utiliza el transporte TCP. En cambio, la directiva “Calidad de sonido” se establece en “Medio: optimizado para voz” cuando se utiliza el transporte UDP (opción recomendada). La configuración “Alta: sonido de alta definición” ofrece sonido estéreo de alta fidelidad, pero consume más ancho de banda que cualquier otro parámetro de calidad. No use este nivel de calidad de sonido 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 sonido que no son adecuados para las comunicaciones en tiempo real. Se recomienda la configuración de directiva “Medio: optimizado para voz” para sonido 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 sonido 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 Sonido. Recuerde que debe habilitar “Parámetros de sonido del cliente” en el dispositivo del usuario.

Redirección de sonido del cliente

Para permitir que los usuarios reciban audio desde una aplicación en un servidor mediante los altavoces u otros dispositivos de sonido en sus dispositivos de usuario, deje la configuración **Redirección de sonido del cliente** en su opción predeterminada (**Permitida**).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

La asignación de sonido del cliente genera una carga adicional para los servidores y para la red. Cuando la Redirección de sonido del cliente está Prohibida, toda la función de sonido de HDX queda inhabilitada.

Para obtener más información acerca de la configuración, consulte Configuraciones de directiva de Sonido. Recuerde que debe habilitar "Parámetros de sonido 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 la configuración "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 Sonido. Recuerde que debe habilitar "Parámetros de sonido del cliente" en el dispositivo del usuario.

Sonido Plug and Play

La configuración de directiva Sonido Plug and Play controla si se permite o se impide el uso de varios dispositivos de sonido para grabar y reproducir sonido. Esta configuración está **Habilitada** de forma predeterminada. Sonido Plug and Play permite que se reconozcan los dispositivos de sonido, incluso aunque no se conecten hasta que la sesión del usuario se haya iniciado.

Esta configuración solo se aplica a máquinas de SO de servidor Windows.

Para obtener más información acerca de la configuración, consulte Configuraciones de directiva de Sonido.

Límite de ancho de banda de redirección de sonido y Porcentaje límite de ancho de banda de redirección de sonido

La configuración de directiva Límite de ancho de banda de redirección de sonido especifica el ancho de banda máximo (en kilobits por segundo) que se puede usar para la reproducción y grabación de sonido en una sesión.

La configuración Porcentaje límite de ancho de banda de redirección de sonido especifica el ancho de banda máximo que se puede usar para la redirección de sonido, expresado como un porcentaje del ancho de banda total disponible.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 sonido del cliente" en el dispositivo del usuario.

Transporte de sonido en tiempo real sobre UDP e Intervalo de puertos UDP de sonido

De manera predeterminada, la opción "Transporte de sonido 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 sonido en tiempo real por UDP. En caso de una congestión de red o pérdida de paquetes, se recomienda configurar UDP/RTP para el sonido para garantizar la mejor experiencia de usuario Para el audio en tiempo real típico de aplicaciones softphone, el sonido UDP se prefiere a 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 sonido" especifica el intervalo de números de puerto que Virtual Delivery Agent (VDA) utiliza para intercambiar datos de paquetes de audio con el dispositivo de usuario.

De manera predeterminada, el intervalo es de 16500 a 16509.

Para obtener más información sobre el Transporte de sonido en tiempo real sobre UDP, consulte Configuraciones de directiva de Sonido. Para obtener más información sobre el Intervalo de puertos UDP de sonido, consulte Configuraciones de directiva de Conexiones de multisecuencia. Recuerde que debe habilitar "Parámetros de sonido del cliente" en el dispositivo del usuario.

Configuraciones de directiva de sonido 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**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **No configurada**. De forma predeterminada, la redirección de sonido está habilitada con alta calidad de sonido, o con los parámetros de sonido personalizados configurados previamente.
- **Habilitada**. Habilita la redirección de sonido usando las opciones seleccionadas.
- **Inhabilitada**. Inhabilita la redirección de sonido.

4. Si ha seleccionado **Habilitada**, elija una calidad de sonido. Para el sonido UDP, use solo la calidad de sonido **media** (la predeterminada).
5. Para el sonido 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 sonido 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 sonido 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. Haga las siguientes entradas en la sección [Application].

```
; This text enables Real-Time Transport

EnableRtpAudio=true

; This text allows Real-Time Transport Through gateway

EnableUDPThroughGateway=true

; This text sets audio quality to Medium

AudioBandwidthLimit=1-

; UDP Port range

RtpAudioLowestPort=16500

RtpAudioHighestPort=16509
```

Si el sonido UDP se habilita mediante la edición de default.ica, el sonido UDP estará habilitado para todos los usuarios que utilicen esa tienda.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 sonido y vídeo.

HDX ofrece una opción de eliminación del eco (habilitada de forma predeterminada), que permite minimizarlo. La eficacia de la eliminación del eco depende de la distancia entre los altavoces y el micrófono. Los dispositivos no deben estar demasiado cerca ni demasiado lejos el uno del otro.

La eliminación de eco se puede inhabilitar mediante un parámetro de Registro.

> **Advertencia**
>
> Si se edita el Registro de forma incorrecta, se pueden generar problemas graves que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

1. En el Editor del Registro, vaya a una de estas ubicaciones:
   - Equipos de 32 bits: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanc
   - Equipos de 64 bits: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ClientAudio\EchoCancellation
2. Cambie la Información del valor a FALSE.

Softphone

Una aplicación softphone es un software que actúa como una interfaz de teléfono. Se utiliza un software softphone para realizar llamadas por Internet desde un equipo o una tableta, por ejemplo. Con softphone, puede marcar números de teléfono y llevar a cabo otras funciones relacionadas con el teléfono a través de una pantalla.

Citrix Virtual Apps and Desktops admiten varias alternativas para la entrega de aplicaciones softphone.

- **Modo de control**. La aplicación softphone alojada controla un teléfono físico configurado. En este modo, no hay tráfico de audio que pase por el servidor Citrix Virtual Apps and Desktops.
- **Respaldo optimizado HDX RealTime para softphone**. 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:
  - HDX RealTime Optimization Pack, que optimiza la entrega de Skype Empresarial y Lync de Microsoft.
  - Virtualization Experience Media Engine (VXME) de Cisco para Jabber.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

  - Avaya Communicator para entornos VDI para one-X Communicator y one-X Agent.
- **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 sonido pasa al dispositivo del usuario. Para obtener más información, consulte Acceso a aplicaciones locales y redirección de URL.
- **Respaldo optimizado HDX RealTime para softphone.** VoIP por ICA.

Respaldo para softphone genérico

El respaldo para softphone genérico 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.

El respaldo para softphone genérico es una característica 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 sonido desde y hacia los auriculares, el micrófono y el altavoz o el teléfono del usuario?

Citrix Virtual Apps and Desktops contienen numerosas tecnologías para respaldar la entrega de softphone genérico:

- Códec optimizado para voz si quiere codificar rápidamente sonido en tiempo real y quiere un uso eficiente del ancho de banda.
- Pila de sonido para latencia baja.
- Búfer de vibración en el servidor para suavizar el sonido 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 características:

- Búfer de vibración en el cliente. Suaviza el sonido incluso cuando fluctúa la latencia de red.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Eliminación de eco. Permite mayor variación en la distancia entre el micrófono y los altavoces para usuarios que no disponen de auriculares con micrófono.
- Sonido Plug and Play. Los dispositivos de sonido no necesitan estar conectados antes de iniciar una sesión. Se pueden conectar en cualquier momento.
- Enrutamiento de dispositivos de sonido. Los usuarios pueden dirigir tonos a los altavoces, mientras que la voz va a sus auriculares.
- ICA de multisecuencia: Permite el enrutamiento flexible basado 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 sonido en tiempo real por RTP.

Para ver un resumen de las características de la aplicación Citrix Workspace, consulte Matriz de características de Citrix Receiver.

Recomendaciones de configuración del sistema

Hardware y software del cliente:
Para una calidad de audio óptima, 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 respaldo para 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.

Sonido UDP:
El sonido 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 sonido 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 respaldo para IPv6, puede inhabilitar IPv6 en esos dispositivos.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configure esta funcionalidad para admitir la calidad de servicio.

Parámetros para usar conexiones WAN:
Puede chatear por voz en conexiones de red de área local (LAN) y red de área extensa (WAN). En una conexión WAN, la calidad del sonido 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 sonido 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 Virtual Delivery Agent (VDA) en el centro de datos, le recomendamos usar el parámetro de códec optimizado para voz, también conocido como calidad de sonido 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 sonido desde y hacia el dispositivo de usuario:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **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 Citrix Virtual Apps and Desktops.

Citrix Audio Virtual Channel

Citrix Audio Virtual Channel (CTXCAM) bidireccional permite la entrega de sonido de forma eficiente en la red. HDX RealTime genérico toma el sonido 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 sonido 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 código optimizado para voz (calidad media). Sus características 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 sonido. La opción predeterminada es el códec de sonido 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 (sonido 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 sonido. La excepción principal es cuando se usa un dispositivo de sonido 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.

Redirección de contenido de explorador Web

January 29, 2019

Redirigir el contenido del explorador Web impide que las páginas Web incluidas en la lista blanca se generen en el lado del agente VDA. Esta función utiliza la aplicación Citrix Workspace para crear una

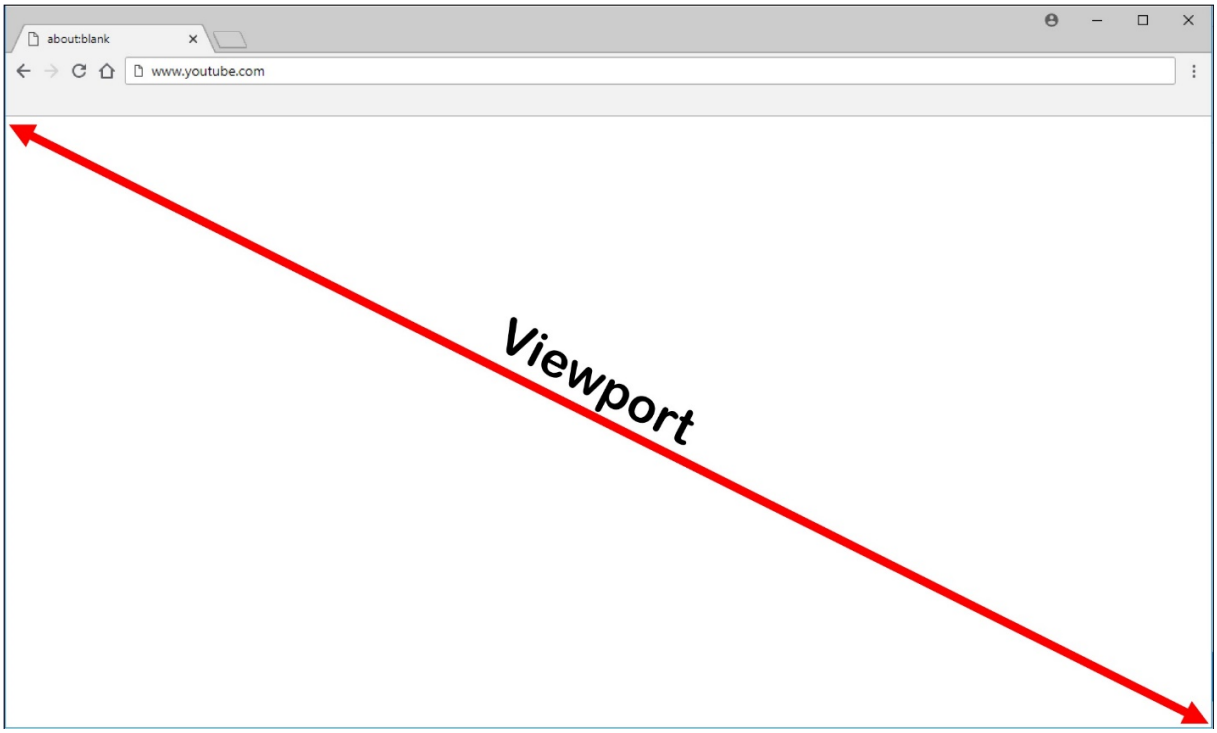
© 1999-2019 Citrix Systems, Inc. All rights reserved.

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) utilizando una lista negra.

Este motor Web de distribución superpuesta se ejecuta en el dispositivo de punto final, en lugar de ejecutarse en el VDA, y utiliza la CPU, la GPU, la memoria RAM y la red del dispositivo de punto final.

Solo se redirige la ventanilla del explorador Web. La ventanilla es el área rectangular del explorador Web donde aparece el contenido. La ventanilla no incluye elementos como la barra de direcciones, la barra de favoritos ni la barra de estado. Esos elementos están en la interfaz de usuario, que todavía se ejecutan en el explorador en el VDA.

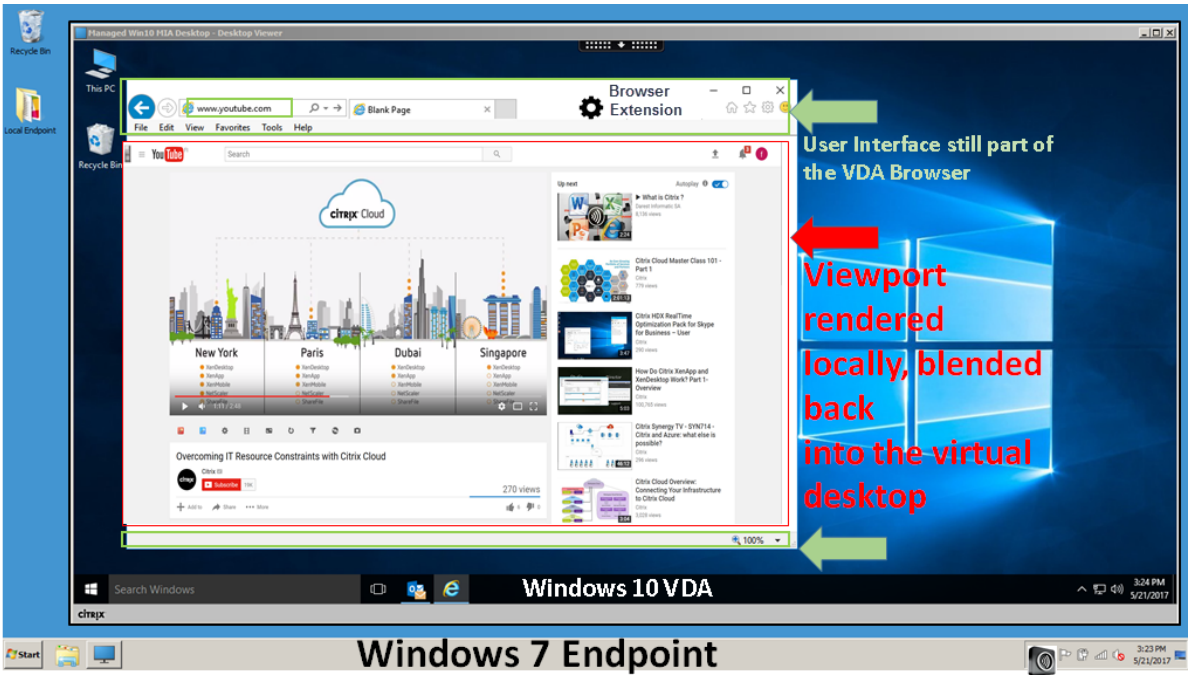


1. Configure una directiva de Studio que especifique una lista de control de acceso que contenga las URL incluidas en la lista blanca para permitir redirecciones o la lista negra para inhabilitar la redirección de URL específicas. Para que el explorador Web presente en el VDA detecte que la URL a la que se dirige el usuario está incluida en la lista blanca o en la lista negra, la extensión del explorador Web busca la URL en esas listas. La extensión del explorador web (BHO) para Internet Explorer 11 está incluida en los medios de instalación y se instala automáticamente. Para Chrome, la extensión del explorador está disponible en Chrome Web Store y puede implementarla utilizando las directivas de grupo y los archivos ADMX. Las extensiones de Chrome se instalan basándose en el usuario. No es necesario actualizar una imagen maestra para agregar

© 1999-2019 Citrix Systems, Inc. All rights reserved.

o eliminar una extensión.

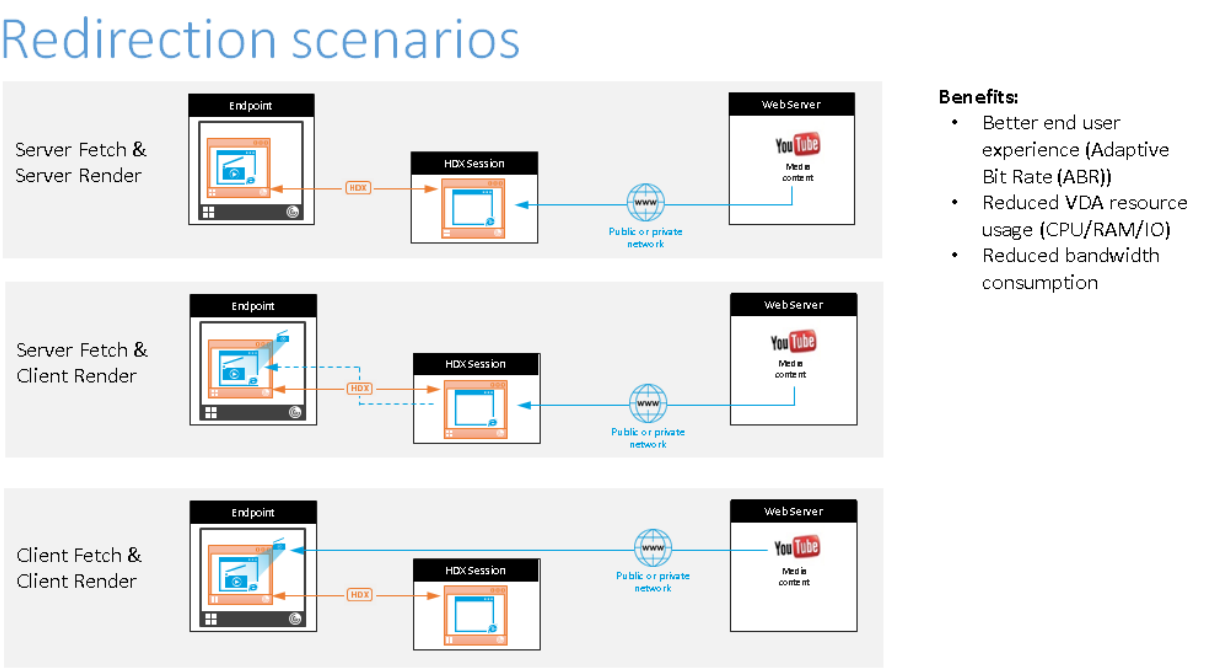
2. Si se encuentra una coincidencia en la lista blanca (por ejemplo `https://www.mycompany.com/`), y no hay ninguna coincidencia en la lista negra (por ejemplo `https://www.mycompany.com/engineering`), un canal virtual (CTXCSB) indica a la aplicación Citrix Workspace que se requiere una redirección y 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.



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 blanca o la redirección ha fallado. Se recurre a la generación de la página Web en el VDA y se usa Thinwire para generar remotamente los gráficos. Se usan directivas para controlar el comportamiento cuando se recurre al mecanismo alternativo. Alto consumo de CPU, memoria RAM y ancho de banda en el VDA.
- **Obtención en el servidor y generación en el cliente:** La aplicación Citrix Workspace se comunica con el servidor Web y obtiene el contenido desde este a través del VDA mediante un canal virtual (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.
- **Obtención en el cliente y generación en el cliente:** Como la aplicación Citrix Workspace se comunica directamente con el servidor Web, requiere acceso a Internet. En este caso, no se consume la red, la CPU ni la memoria RAM del sitio de XenApp y XenDesktop.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



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 utilizando la directiva existente **Prevención de respaldo de Windows Media**. Establezca esta directiva en **Reproducir todo el contenido solo en el cliente** o **Reproducir solo el contenido accesible por el cliente en el cliente**. Estas configuraciones bloquean la reproducción de elementos de vídeo en el servidor si hay fallos en la redirección de cliente. Esta directiva tiene efecto solo cuando la redirección de contenido del explorador Web está habilitada y la directiva **Lista de control de acceso** contiene la URL alternativa. La URL no puede constar en la directiva de la lista negra.

Requisitos del sistema:

Dispositivos de punto final de Windows:

- Windows 7, 8.x, o 10
- Aplicación Citrix Workspace 1808 o versiones posteriores
- Citrix Receiver para Windows 4.10 o versiones posteriores

Dispositivos de punto final de Linux:

- Aplicación Citrix Workspace 1808 para Linux o versiones posteriores
- Citrix Receiver para Linux 13.9 o versiones posteriores
- Los terminales de clientes ligeros deben incluir WebKitGTK+

Citrix Virtual Apps and Desktops 7 1808; XenApp y XenDesktop 7.18, 7.17, 7.16:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Sistema operativo del VDA: Windows 10 (versión mínima 1607), Windows Server 2012 R2, Windows Server 2016
- Explorador en el VDA:
  - Google Chrome v66 o versiones posteriores (Chrome requiere la aplicación Citrix Workspace 1809 para Windows en el dispositivo de punto final del usuario, Citrix Virtual Apps and Desktops 7 1808 VDA y la extensión de redirección de contenido de explorador)
  - Internet Explorer 11 con estas opciones configuradas:
    * Desmarque **Modo protegido mejorado** en: **Opciones de Internet** > **Avanzado > Seguridad**.
    * Marque **Habilitar extensiones de explorador de terceros** en: **Opciones de Internet > Avanzado > Exploración**

Solucionar problemas:

Para obtener información sobre la resolución de problemas, consulte https://support.citrix.com/article/CTX230052

Extensión de Chrome de redirección de contenido de explorador Web

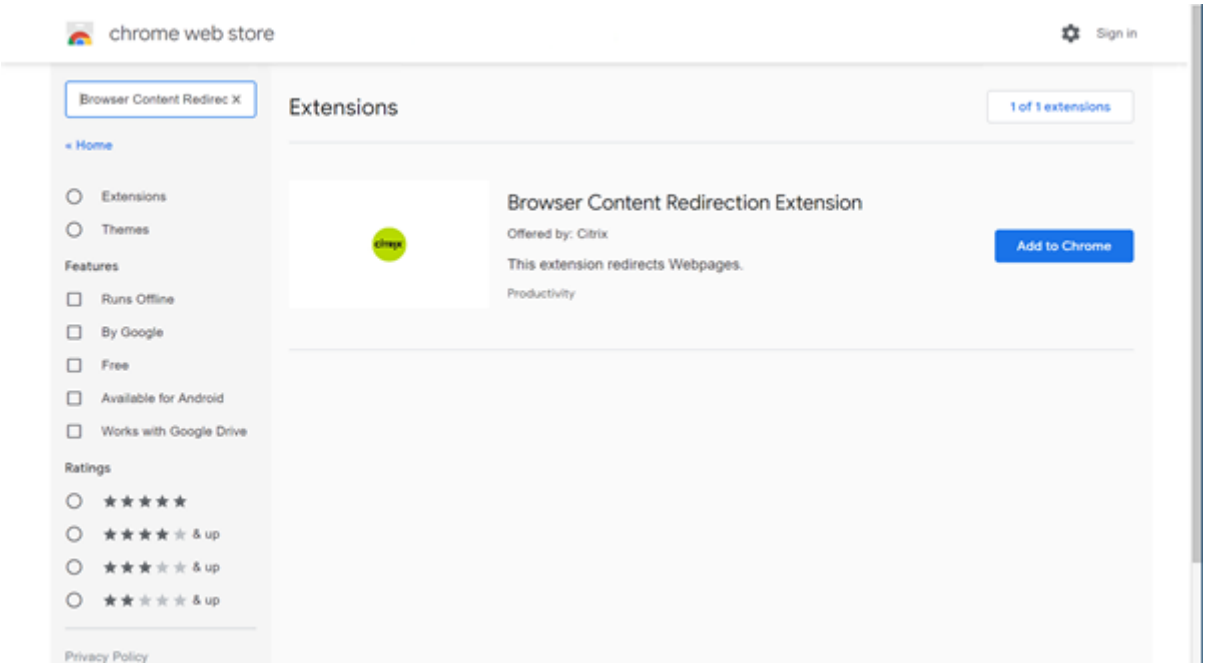
Para usar la redirección de contenido de explorador con Chrome, agregue la extensión de redirección de contenido de explorador desde Chrome Web Store. Haga clic en **Añadir a Chrome** en el entorno de Citrix Virtual Apps and Desktops 7 1808.

> **Importante**
>
> La extensión **no** se requiere en la máquina cliente del usuario - solo en el VDA.

Requisitos del sistema

- Chrome v66 o versiones posteriores
- Extensión de redirección de contenido de explorador Web
- Citrix Virtual Apps and Desktops 7 1808 o versiones posteriores
- Aplicación Citrix Workspace para Windows 1809 o versiones posteriores

© 1999-2019 Citrix Systems, Inc. All rights reserved.

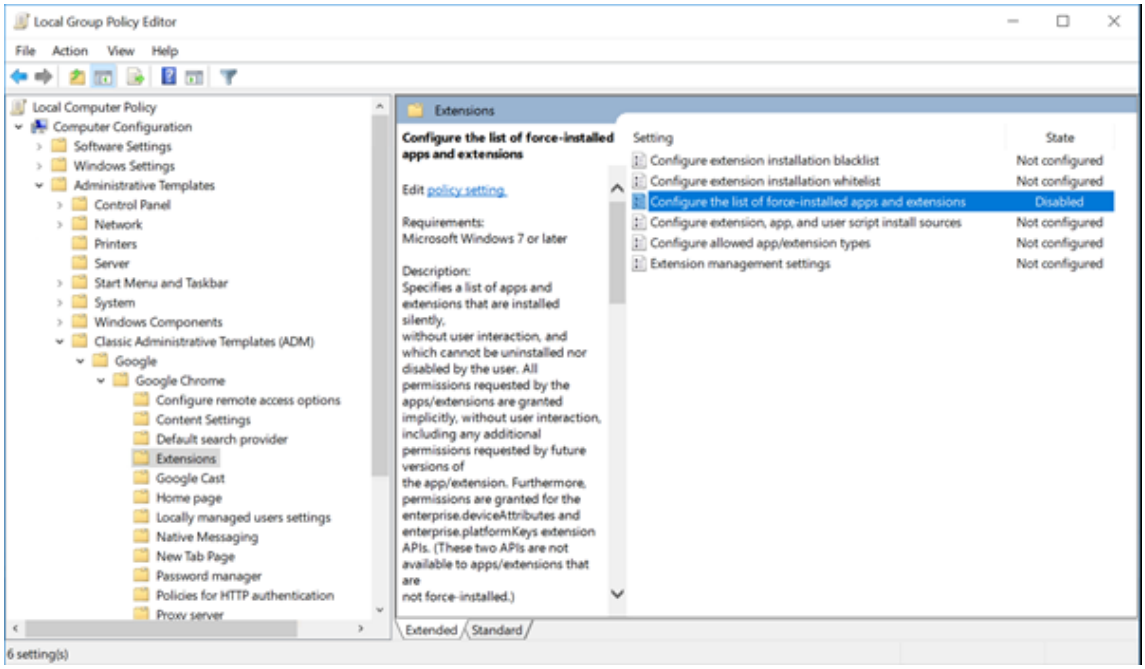


Este método funciona para usuarios individuales. Para implementar la extensión a un gran grupo de usuarios en su organización, implemente la extensión utilizando la directiva de grupo.

Implementar la extensión utilizando la directiva de grupo

1. Importe los archivos ADMX de Google Chrome a su entorno. Para obtener información sobre cómo descargar plantillas de directivas, e instalar y configurar las plantillas en su editor de directivas de grupo, consulte https://support.google.com/chrome/a/answer/187202?hl=en.
2. Abra su Consola de administración de directivas de grupo y vaya a **Configuración de usuario\Plantillas administrativas\Plantillas administrativas clásicas (ADM)\Google\Google Chrome\Extensiones**. Habilite el parámetro **Configurar la lista de aplicaciones y extensiones con instalación forzada**.

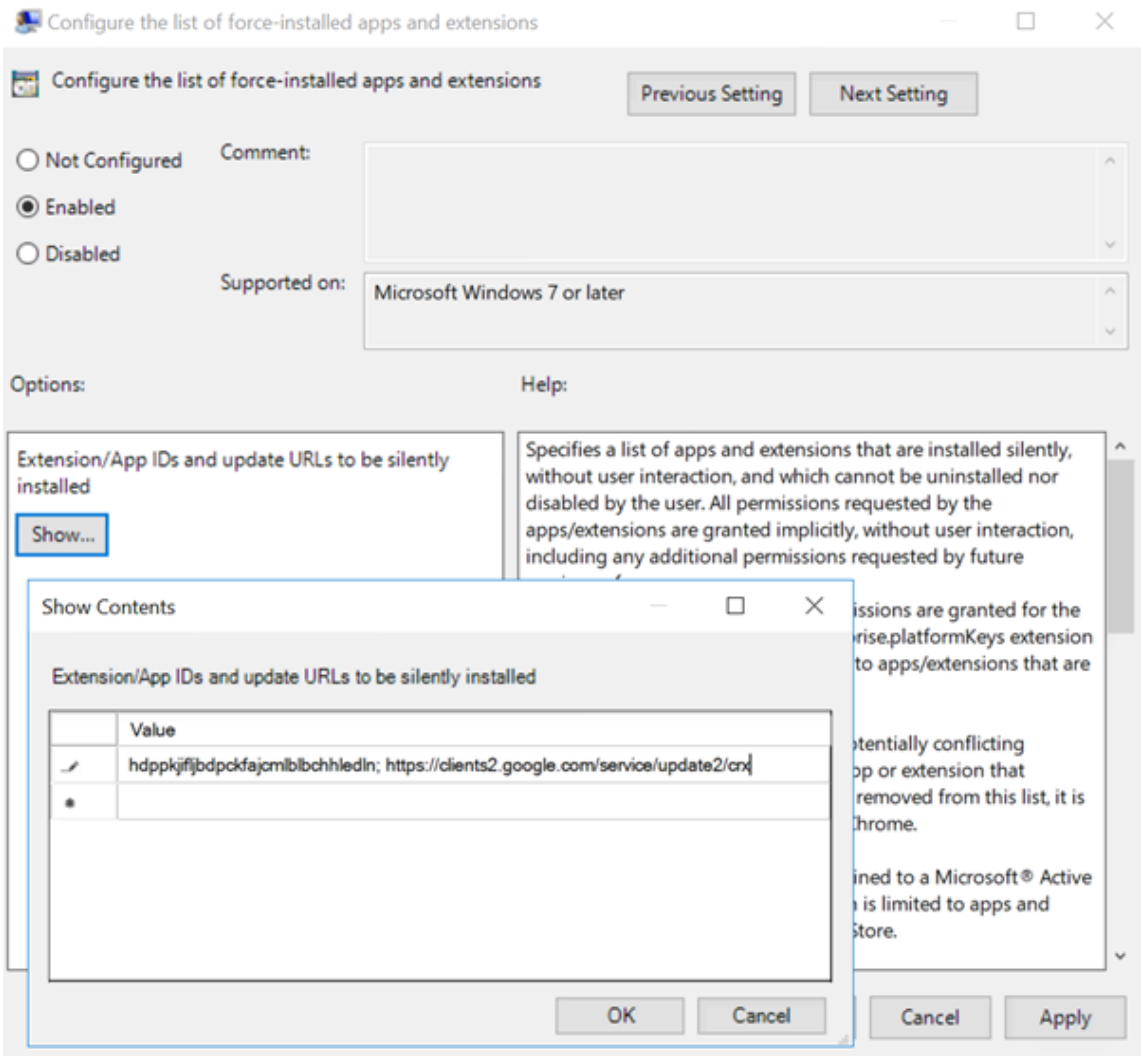
© 1999-2019 Citrix Systems, Inc. All rights reserved.



3. Haga clic en **Mostrar** y escriba la siguiente cadena, que corresponde a la ID de extensión. Actualice la URL de la extensión de redirección de contenido de explorador Web.

   ```
   hdppkjifljbdpckfajcmlblbchhledln; https://clients2.google.com/service/update2/crx
   ```

© 1999-2019 Citrix Systems, Inc. All rights reserved.



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 eliminarla.

   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.

Optimización del lado del cliente para Citrix Receiver para Windows 4.10

HdxBrowser.exe es el explorador Web superpuesto presente en el dispositivo de punto final que es responsable de la representación de Internet Explorer 11 en el lado del cliente. Para habilitar

© 1999-2019 Citrix Systems, Inc. All rights reserved.

HdxBrowser.exe y utilizar los recursos de la GPU en el cliente, establezca estas claves de Registro en el dispositivo de punto final Windows.

> **Advertencia**
>
> Si se modifica el Registro de forma incorrecta, se pueden generar problemas graves que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

\HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_GPU_RENDERI
(crear si no está presente)

Y

\HKEY_CURRENT_USER)\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_GPU_RENDERIN
(crear si no está presente)

Nombre del valor: HdxBrowser.exe
Datos del valor: 00000001
Tipo: DWORD

Redirección de Flash

October 3, 2018

> **Importante**
>
> El 25 de julio de 2017, Adobe anunció el ciclo Fin de vida (EOL) para Flash. Adobe planea dejar de actualizar y distribuir el reproductor de Flash (Flash Player) al final del año 2020.
>
> Microsoft ha anunciado que va a ir retirando progresivamente el respaldo para Flash en Internet Explorer antes de la fecha anunciada por Adobe. Va a quitar Flash de Windows antes de finales del año 2020. Cuando eso ocurra, los usuarios ya no podrán habilitar ni ejecutar Flash en Internet Explorer.
>
> Citrix se ha sumado a esta directriz de Microsoft y seguirá ofreciendo mantenimiento y respaldo a la redirección de Flash de HDX hasta el final del año 2020. No hemos decidimos aún de qué versiones de Citrix Virtual Apps and Desktops excluir el código de redirección de Flash, pero recomendamos que cambie a la redirección de vídeo HTML5 siempre que sea posible. La redirección de vídeo HTML5 es idónea para controlar el contenido multimedia. Por ejemplo, para vídeos de comunicaciones corporativas, tutoriales o cuando una tercera parte aloja el contenido.
>
> Para obtener más información sobre la redirección de vídeo HTML5, consulte Redirección multi-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> media HTML5.

La redirección de Flash descarga el procesamiento de la mayoría del contenido Adobe Flash (incluidas animaciones, vídeos y aplicaciones) a los dispositivos Windows y Linux x86 de 32 bits de los usuarios conectados por LAN o WAN. La redirección de Flash reduce la carga del servidor y de la red, y da como resultado una mayor escalabilidad, al mismo tiempo que garantiza una experiencia de usuario de alta definición. Configurar la redirección de Flash requiere a su vez configurar parámetros tanto en el lado del cliente como en el lado del servidor.

> **Advertencia**
>
> La redirección de Flash requiere una interacción considerable entre los componentes del servidor y del dispositivo de usuario. Esta función solo debe utilizarse en entornos donde no se requiera una separación de seguridad entre el dispositivo de usuario y el servidor. Además, configure los dispositivos de usuario para usar esta función solo con servidores de confianza. Puesto que la redirección de Flash requiere que el reproductor de Adobe Flash esté instalado en el dispositivo de usuario, esta funcionalidad solo debe habilitarse si el propio reproductor de Flash es seguro.

La redirección de Flash está respaldada tanto en los clientes como en los servidores. Si el cliente respalda la redirección de Flash de segunda generación, el contenido Flash se genera en el cliente. Las funciones de redirección de Flash incluyen respaldo para las conexiones de usuario a través de una WAN, respaldo inteligente y una lista de compatibilidad de URL (más adelante, dispone de más información).

La redirección de Flash usa el registro de eventos de Windows en el servidor para registrar sucesos de Flash. El registro de eventos indica si se está usando la redirección de Flash y ofrece información sobre los problemas que se produzcan. A continuación se enumeran las acciones más comunes a todos los eventos registrados por la redirección de Flash:

- Redirección de Flash registra eventos en el registro Aplicación.
- En los sistemas con Windows 10, Windows 8 o Windows 7, aparece un registro específico de la redirección de Flash en el nodo Registros de aplicaciones y servicios.
- El valor de Origen es Flash.
- El valor de Categoría es Ninguno.

Para obtener información actualizada sobre la compatibilidad de HDX Flash, consulte CTX136588.

Configurar la redirección de Flash en el servidor

Para configurar la redirección de Flash en el servidor, utilice las siguientes configuraciones de directiva de Citrix. Para obtener información más detallada, consulte Configuraciones de directiva de Redirección de Flash.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- De manera predeterminada, la redirección de Flash está habilitada. Para anular este comportamiento predeterminado cuando se trata de páginas Web e instancias Flash específicas, use la configuración Lista de compatibilidad de URL de Flash.
- **Respaldo inteligente de Flash**. Detecta las instancias de "películas" Flash pequeñas (por ejemplo, las que se usan con frecuencia para anuncios publicitarios) y las genera en el servidor, en lugar de redirigirlas al dispositivo del usuario. Esta optimización no provoca interrupciones ni errores durante la carga de la página Web o la aplicación de Flash. De forma predeterminada, el respaldo inteligente de Flash está habilitado. Para redirigir todas las instancias del contenido Flash para generarse en el dispositivo del usuario, inhabilite esta configuración de directiva. Algunos contenidos Flash pueden no redirigirse correctamente.
- **Lista de URL para obtener contenido Flash del lado del servidor.** Esta configuración especifica sitios Web cuyo contenido Flash se puede descargar en el servidor y transferir luego al dispositivo del usuario para generarlo allí. (De manera predeterminada, la redirección de Flash descarga el contenido Flash directamente en el dispositivo de usuario con obtención de contenido del lado del cliente.) Esta configuración funciona con (y requiere) la configuración "Habilitar obtención de contenido del lado del servidor" en el dispositivo de usuario. Esta configuración está destinada principalmente para sitios de la intranet y aplicaciones Flash internas. Consulte los siguientes apartados para obtener información más detallada. También funciona con la mayoría de los sitios de Internet, y se puede usar cuando el dispositivo de usuario no tiene acceso directo a Internet. Por ejemplo, cuando el servidor Citrix Virtual Apps and Desktops proporciona esa conexión.
  La obtención de contenido del lado del servidor no respalda las aplicaciones Flash que usan los protocolos de mensajería en tiempo real (RTMP). En su lugar, se utiliza la generación del lado del servidor, que admite HTTP y HTTPS.
- **Lista de compatibilidad de URL de Flash**. Especifica dónde se genera el contenido Flash de los sitios Web de la lista: en el dispositivo del usuario, en el servidor o se bloquea.
- **Lista de colores de fondo de Flash**. Permite hacer una correspondencia entre los colores de las páginas Web y las instancias de Flash, lo que mejora la apariencia de la página Web cuando se usa la redirección de Flash.

Configurar la redirección de Flash en el dispositivo del usuario

Instale la aplicación Citrix Workspace y Adobe Flash Player en el dispositivo del usuario. No se necesita ninguna otra configuración en el dispositivo del usuario.

Puede cambiar los parámetros predeterminados usando objetos de directiva de grupo de Active Directory. Importe y agregue la plantilla administrativa HDX MediaStream Flash Redirection - Client (HdxFlashClient.adm), que está disponible en las siguientes carpetas:

- En equipos de 32 bits: %Archivos de programa%\Citrix\ICA Client\Configuration\idioma
- En equipos de 64 bits: %Archivos de programa (x86)%\Citrix\ICA Client\Configuration\idioma

© 1999-2019 Citrix Systems, Inc. All rights reserved.

La configuración de directiva aparece en Plantillas administrativas > Plantillas administrativas clásicas (ADM) > HDX MediaStream Flash Redirection - Client. Consulte la documentación de Microsoft Active Directory para obtener más información acerca de los objetos de directiva de grupo y las plantillas.

Cambiar cuándo se usa la redirección de Flash:

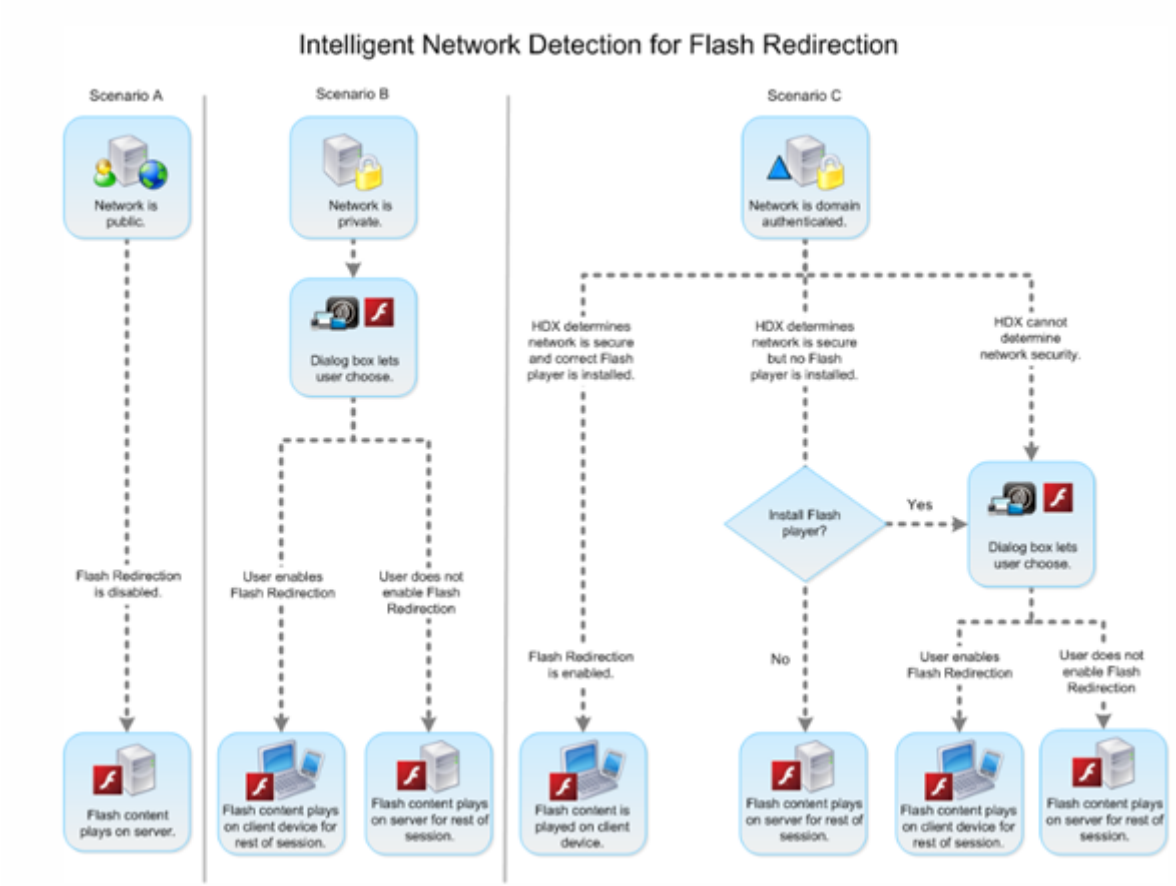
Junto con los parámetros del lado del servidor, la configuración de directiva "Habilitar la redirección de HDX MediaStream para Flash en el dispositivo de usuario" decide si el contenido de Adobe Flash se redirige al dispositivo del usuario para generarse localmente. De manera predeterminada, la redirección de Flash está habilitada y usa la detección inteligente de red para determinar cuándo es mejor reproducir el contenido Flash en el dispositivo del usuario.

Si no hay ninguna configuración definida y se usa Desktop Lock, la redirección de Flash está habilitada en el dispositivo del usuario de manera predeterminada.

Para cambiar cuándo se usa la redirección de Flash o para inhabilitar la redirección de Flash en el dispositivo del usuario:

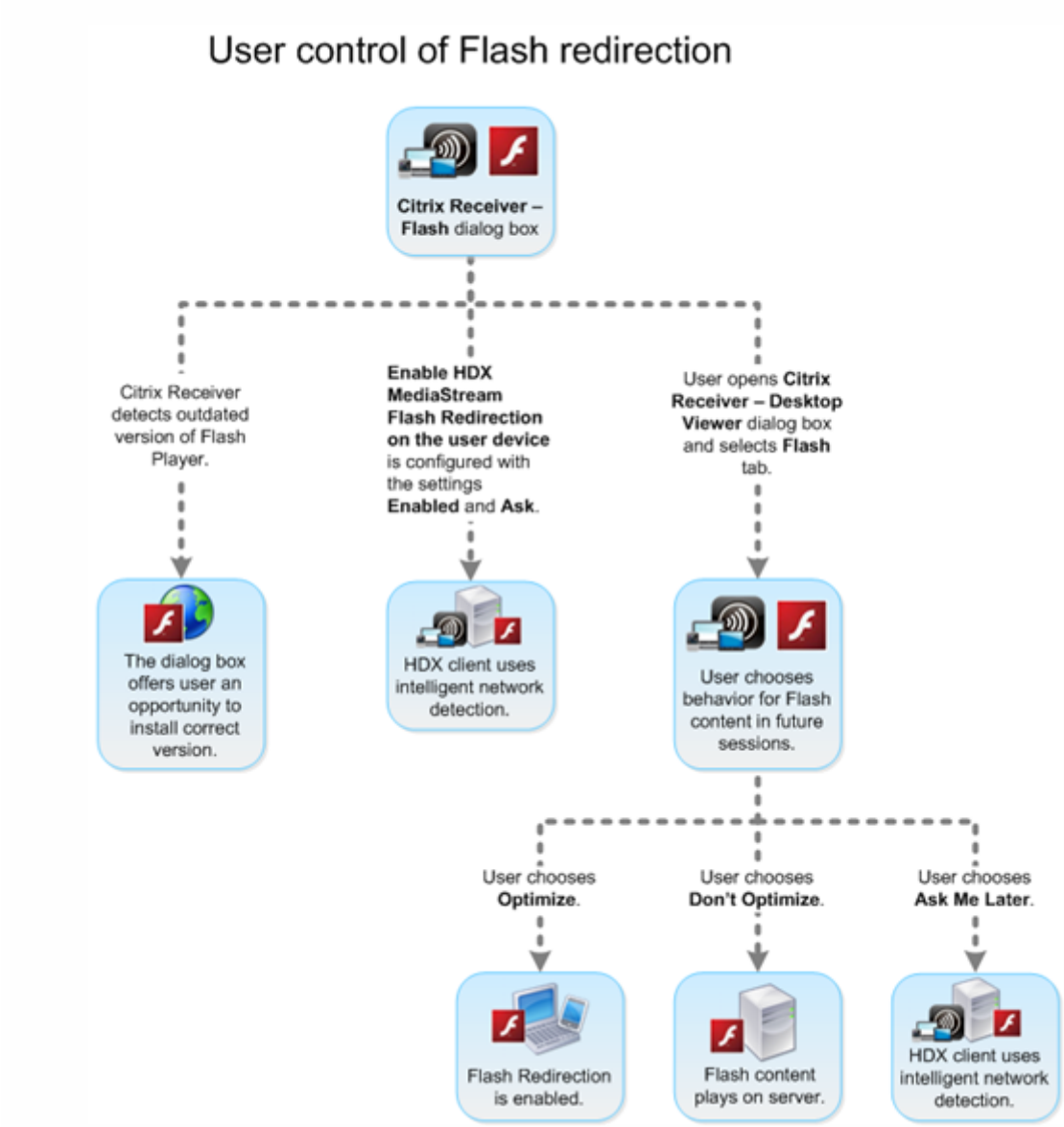
1. En la lista "Configuración", seleccione "Habilitar la redirección de HDX MediaStream para Flash en el dispositivo de usuario" y después elija "configuración de directiva".
2. Seleccione No configurada, Habilitada (opción predeterminada) o Inhabilitada.
3. Si ha seleccionado "Habilitada", elija una opción en la lista "Usar la redirección de HDX MediaStream para Flash":
    - Seleccione "Con segunda generación solamente" para usar la redirección de Flash más reciente cuando la configuración requerida esté presente, y volver a la generación en el lado del servidor cuando no lo esté.
    - Para usar siempre la redirección de Flash, seleccione "Siempre". El contenido Flash se genera en el dispositivo del usuario.
    - Para no usar nunca la redirección de Flash, seleccione "Nunca". El contenido Flash se genera en el servidor.
    - Para usar la detección inteligente de red, evaluar el nivel de seguridad de la red en el lado del cliente y, así, determinar cuándo es adecuado usar la redirección de Flash, seleccione "Preguntar" (opción predeterminada). Si la seguridad de la red no se puede determinar, se pregunta al usuario si usar la redirección de Flash. Si el nivel de seguridad de la red no se puede determinar, se pregunta al usuario si quiere usar la redirección de Flash.
      En la siguiente imagen se muestra cómo se controla la redirección de Flash en diversos tipos de red.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Los usuarios pueden anular la detección de red inteligente desde el cuadro de diálogo de la aplicación Citrix Workspace > Preferencias de Desktop Viewer. Para ello, deben seleccionar “Optimizar” o “No optimizar” en la ficha “Flash”. Las opciones disponibles varían según cómo esté configurada la redirección de Flash en el dispositivo de usuario, como se muestra en la siguiente imagen.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Sincronizar las cookies HTTP del lado del cliente con las del lado del servidor:

La sincronización de las cookies HTTP del cliente con las del servidor está inhabilitada de manera predeterminada. Habilite la sincronización para descargar las cookies HTTP del servidor. Tras la descarga, estas cookies HTTP se usan para obtener contenido en el cliente, y están disponibles según sea necesario para los sitios con contenido Flash.

Las cookies del lado del cliente no se reemplazan durante la sincronización. Permanecen disponibles incluso aunque la directiva de sincronización se desactive más tarde.

1. En la lista Configuración, seleccione Habilitar la sincronización de las cookies HTTP del lado del cliente con el lado del servidor y haga clic en configuración de directiva.
2. Seleccione No configurado, Habilitado o Inhabilitado (opción predeterminada).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Habilitar la obtención de contenido en el lado del servidor:

De manera predeterminada, la redirección de Flash descarga contenido de Adobe Flash directamente en el dispositivo de usuario, donde se reproduce. Al habilitar la obtención de contenido en el servidor, el contenido Flash se descarga en el servidor y después se envía al dispositivo de usuario. A menos que exista una directiva que lo anule (como por ejemplo, un sitio bloqueado con la directiva Lista de compatibilidad de URL de Flash), el contenido de Flash se reproduce en el dispositivo del usuario.

La obtención de contenido del lado del servidor se utiliza con frecuencia cuando el dispositivo de usuario se conecta a sitios internos mediante NetScaler Gateway y cuando el dispositivo de usuario no tiene acceso directo a Internet.

La obtención de contenido del lado del servidor no respalda las aplicaciones Flash que usan los protocolos de mensajería en tiempo real (RTMP). En su lugar, para esos sitios se usa la generación en el lado del servidor.

La redirección de Flash admite tres opciones para habilitar la obtención de contenido del lado del servidor. Dos de estas opciones incluyen la capacidad de almacenar en caché contenido del lado del servidor en el dispositivo del usuario. Al hacerlo, se mejora el rendimiento porque el contenido que se reutiliza ya está disponible en el dispositivo del usuario para generarse. El contenido de la memoria caché se almacena de forma separada de otro contenido HTTP almacenado en caché en el dispositivo de usuario.

Se recurre automáticamente a la obtención de contenido del lado del servidor cuando cualquiera de las opciones de habilitación anteriores está seleccionada y falla la obtención de archivos SWF en el lado del cliente.

La habilitación de la obtención de contenido en el lado del servidor requiere una configuración de parámetros tanto en el dispositivo cliente como en el servidor.

1. En la lista “Configuración”, seleccione “Habilitar obtención de contenido del lado del servidor” y seleccione “configuración de directiva”.
2. Seleccione No configurado, Habilitado o Inhabilitado (opción predeterminada). Si habilita esta configuración, elija una opción de la lista Estado de la obtención de contenido del lado del servidor:

Opción	Descripción
Inhabilitada	Inhabilita la obtención de contenido del lado del servidor, anulando el parámetro Lista de URL para obtener contenido Flash del lado del servidor en el servidor. También se inhabilita la opción de respaldo de obtención de contenido del lado del servidor.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Opción	Descripción
Habilitada	Habilita la obtención de contenido del lado del servidor para las páginas Web y las aplicaciones Flash identificadas en la Lista de URL para obtener contenido Flash del lado del servidor. El respaldo de obtención de contenido del lado del servidor está disponible, pero el contenido Flash no se guarda en caché.
Habilitada (caché persistente)	Habilita la obtención de contenido del lado del servidor para las páginas Web y las aplicaciones Flash identificadas en la “Lista de URL para obtener contenido Flash del lado del servidor”. Está disponible el respaldo de obtención de contenido del lado del servidor. El contenido obtenido mediante la obtención de contenido del lado del servidor se almacena en caché en el dispositivo de usuario y se guarda para las distintas sesiones.
Habilitada (caché temporal)	Habilita la obtención de contenido del lado del servidor para las páginas Web y las aplicaciones Flash identificadas en la “Lista de URL para obtener contenido Flash del lado del servidor”. Está disponible el respaldo de obtención de contenido del lado del servidor. El contenido obtenido mediante la obtención de contenido del lado del servidor se almacena en caché en el dispositivo del usuario y se elimina al final de cada sesión.

3. En el servidor, habilite la configuración de directiva Lista de URL para obtener contenido Flash del lado del servidor y rellénela con direcciones URL de destino.

Redirigir los dispositivos de usuario a otros servidores para la obtención de contenido del lado del cliente:

Para redirigir un intento de obtener contenido Flash, use el parámetro “Reglas de reescritura de URL para la obtención de contenido del lado del cliente”, que es una función de la redirección de Flash de segunda generación. Al configurar esta función, debe proporcionar dos patrones de URL. Cuando

© 1999-2019 Citrix Systems, Inc. All rights reserved.

el dispositivo de usuario intenta obtener contenido desde un sitio Web que coincide con el primer patrón (el patrón de coincidencia de URL), se redirige al sitio Web especificado por el segundo patrón (el formato de URL reescrito).

Puede usar este parámetro como compensación para redes de entrega de contenido. Algunos sitios Web que entregan contenido Flash usan la redirección de redes de entrega de contenido para permitir al usuario obtener el contenido a partir del grupo más cercano de servidores que entregan el mismo contenido. Al utilizar la obtención de contenido para la redirección de Flash del lado del cliente, se solicita el contenido Flash desde el dispositivo del usuario. El servidor solicita el resto de la página Web en la que reside el contenido Flash. Si la red de entrega de contenido está en uso, la solicitud del servidor se redirige al servidor más cercano. La solicitud del dispositivo del usuario sigue a la misma ubicación. Esta ubicación puede no ser la más cercana al dispositivo del usuario. Según la distancia, puede haber cierta demora entre la carga de la página Web y la reproducción del contenido Flash.

1. En la lista "Configuración", seleccione "Reglas de reescritura de URL para la obtención de contenido del lado del cliente" y haga clic en "configuración de directiva".
2. Seleccione No configurada, Habilitada o Inhabilitada. La opción predeterminada es "No configurada". Si elige "Inhabilitada", se ignorarán las reglas de reescritura de URL configuradas en el paso siguiente.
3. Si habilita la configuración, seleccione "Mostrar". Mediante la sintaxis de expresiones regulares de Perl, escriba el patrón de coincidencia de direcciones URL en la casilla Nombre de valor y el formato de URL reescrita en la casilla Valor.

Comprobar la versión mínima para la redirección de Flash

> **Advertencia**
>
> Si se edita el Registro de forma incorrecta, se pueden generar problemas graves que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Puede agregar parámetros de Registro que especifiquen la versión mínima necesaria para la redirección de Flash en dispositivos cliente que acceden a agentes VDA mediante la aplicación Citrix Workspace para Windows o la aplicación Citrix Workspace para Linux. Esta característica de seguridad garantiza que no se utilice una versión obsoleta de Flash.

ServerFlashPlayerVersionMinimum es un valor de cadena que especifica la versión mínima de Flash Player que debe estar presente en el servidor ICA (VDA).

ClientFlashPlayerVersionMinimum es un valor de cadena que especifica la versión mínima de Flash Player que debe estar presente en el cliente ICA (aplicación Citrix Workspace).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Estas cadenas de texto para la versión se pueden indicar como “10”, “10.2” o “10.2.140”. Solo se comparan los números de las versiones principales, secundarias y de compilación. El número de revisión se ignora. Por ejemplo, en caso de una cadena de versión especificada como “10” y solo con el número de versión principal indicado, se asume que los números de compilación y versión secundaria son cero.

FlashPlayerVersionComparisonMask es un valor DWORD que, cuando se establece en cero, inhabilita la comparación de la versión de Flash Player del cliente ICA con la versión de Flash Player del servidor ICA. La máscara de comparación tiene otros valores, pero no los use, porque el significado de una máscara que no sea cero puede cambiar. Se recomienda establecer la máscara de comparación en cero solo para clientes pertinentes. No se recomienda establecer la máscara de comparación para cualquier cliente. Si no se indica ninguna máscara de comparación, la redirección de Flash requiere que el cliente ICA disponga de Flash Player con un número de versión mayor o igual que la versión de Flash Player presente en el servidor ICA. Para ello, compara solo el número de versión principal de Flash Player.

Para que se realice la redirección, además de la comprobación con la máscara de comparación, las comprobaciones de versiones mínimas del cliente y del servidor también deben realizarse correctamente.

La subclave ClientID0x51 especifica la aplicación Citrix Workspace para Linux. La subclave ClientID0x1 especifica la aplicación Citrix Workspace para Windows. El nombre de esta subclave se forma añadiendo el ID del producto del cliente en formato hexadecimal (sin los ceros a la izquierda) a la cadena de texto “ClientID”.

Ejemplo de configuración para el Registro de un VDA de 32 bits:

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer] Configuración independiente del cliente

“ClientFlashPlayerVersionMinimum”=”13.0” Versión mínima requerida para el cliente ICA “ServerFlashPlayerVersionMinimum”=”13.0” Versión mínima requerida para el servidor ICA [HKEY_LOCAL_MACHINE\SOFT
Configuración del cliente ICA en Windows

“ClientFlashPlayerVersionMinimum”=”16.0.0” Este parámetro indica la versión mínima de Flash Player necesaria para el cliente Windows [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Se
Configuración del cliente ICA en Linux

“FlashPlayerVersionComparisonMask”=dword:00000000 Este parámetro inhabilita la comparación de versiones para el cliente Linux (no se comprueba si el cliente tiene una versión más reciente de Flash Player que el servidor) “ClientFlashPlayerVersionMinimum”=”11.2.0” Este parámetro indica la versión mínima de Flash Player necesaria para el cliente Linux.

Ejemplo de configuración para el Registro de un VDA de 64 bits:
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer]

© 1999-2019 Citrix Systems, Inc. All rights reserved.

“ClientFlashPlayerVersionMinimum”=”13.0” “ServerFlashPlayerVersionMinimum”=”13.0”[HKEY_LOCAL_MACHINE

“ClientFlashPlayerVersionMinimum”=”16.0.0”[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMe

“FlashPlayerVersionComparisonMask”=dword:00000000 “ClientFlashPlayerVersionMinimum”=”11.2.0”

Redirección multimedia HTML5

December 14, 2018

La redirección multimedia HTML5 amplía las funciones de redirección multimedia de HDX MediaStream para incluir audio y vídeo de HTML5. Debido al aumento de la distribución en línea de contenido multimedia, sobre todo para dispositivos móviles, la industria de exploración ha desarrollado métodos más eficientes para presentar audio y vídeo.

Flash ha sido el estándar, pero requiere un complemento, no funciona en todos los dispositivos y resulta en un mayor uso de batería en los dispositivos móviles. Empresas como YouTube, NetFlix y versiones más recientes de los exploradores de Mozilla, Google y Microsoft están migrando a HTML5, con lo que HTML5 se convierte en el nuevo estándar.

El contenido multimedia basado en HTML5 presenta muchas ventajas frente los plug-ins propietario, incluidos:

- Estándares independientes de empresas (W3C)
- Flujo de trabajo simplificado para la administración de los derechos digitales (DRM)
- Mejor rendimiento sin los problemas de seguridad que implican los complementos

Descargas progresivas HTTP

La descarga progresiva HTTP es un método de semidistribución por streaming basado en HTTP que admite HTML5. En una descarga progresiva, el explorador Web reproduce un solo archivo (codificado con una sola calidad) mientras ese archivo se descarga desde un servidor Web HTTP. El vídeo se almacena en el disco tal cual se recibe, y se reproduce desde ese disco. Si vuelve a reproducir el vídeo, el explorador Web puede cargar el vídeo desde la memoria caché.

Para ver un ejemplo de descarga progresiva, consulte la página para pruebas de redirección de vídeo HTML5. Utilice las herramientas de desarrollo que facilita su explorador Web para inspeccionar los elementos de vídeo en la página Web y buscar los orígenes (un formato de contenedor mp4) en la etiquetas de vídeos HTML5:

Comparación entre HTML5 y Flash

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Función	HTML5	Flash
Requiere un reproductor propietario	No	Sí
Se ejecuta en dispositivos móviles	Sí	Algunos
Velocidad de ejecución en distintas plataformas	Alto	Lenta
Respaldado en 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 vídeo en el sitio Web. HdxVideo.js se comunica con WebSocketService mediante Secure WebSockets (SSL/TLS).
- **Certificados SSL de WebSocket**
  - Para la CA (raíz): **Citrix XenApp/XenDesktop HDX In-Product CA** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX In-Product CA)
    Ubicación: Certificados (Equipo local) > Entidades de certificación raíz de confianza > Certificados.
  - Para la entidad final (hoja): **Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX Service)
    Ubicación: Certificados (Equipo local) > Personal > Certificados.
- **WebSocketService.exe:** Se ejecuta en el sistema local y realiza la terminación SSL y la asignación de sesiones de usuario. TLS Secure WebSocket escucha en 127.0.0.1 en el puerto 9001.
- **WebSocketAgent.exe:** Se ejecuta en la sesión del usuario y genera el vídeo según las instrucciones de los comandos de WebSocketService.

Cómo habilito la redirección de vídeo HTML5

En esta versión, esta funcionalidad está disponible solo para las páginas Web controladas. Requiere que se añada HdxVideo.js de JavaScript (incluido en los medios de instalación de Citrix Virtual Apps

© 1999-2019 Citrix Systems, Inc. All rights reserved.

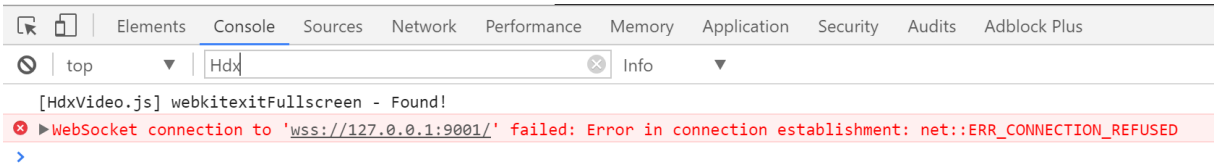
and Desktops) a las páginas Web donde está disponible el contenido multimedia HTML5. Por ejemplo, vídeos en un sitio de formación interna.

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 reciben respaldo.

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:



Conferencias de vídeo de HDX y compresión de vídeo de cámara Web de HDX

March 14, 2019

> **Advertencia**
>
> Si se edita el Registro de forma incorrecta, se pueden generar problemas graves que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Las aplicaciones que se ejecutan en la sesión virtual pueden utilizar cámaras Web. Para ello, se debe definir la compresión de vídeo de la cámara Web de HDX o la redirección USB genérica 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 la cámara Web de HDX si es posible. Para evitar que los usuarios cambien la compresión de vídeo de cámara Web de HDX, inhabilite la redirección de dispositivos USB desde las configuraciones de directiva de ICA > Dispositivos USB. Los usuarios de la aplicación Citrix Workspace pueden anular este comportamiento predeterminado. Para ello, deben seleccionar el parámetro **No usar mi micrófono ni mi cámara Web** en **Micro y cámara Web** de Desktop Viewer.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Compresión de vídeo de cámara Web de HDX

La compresión de vídeo de la cámara Web de HDX también se llama modo de cámara Web **optimizado**. Este tipo de compresión de vídeo de la cámara Web utiliza la tecnología de framework multimedia que forma parte del sistema operativo cliente para interceptar el vídeo de los dispositivos de captura, transcodificarlo y comprimirlo. Los fabricantes de los dispositivos de captura suministran controladores que complementan la arquitectura de streaming del kernel del sistema operativo.

El cliente gestiona la comunicación con la cámara Web. El cliente envía el vídeo solo al servidor que puede mostrarlo correctamente. El servidor no trata directamente con la cámara Web, pero está integrado, con lo que el usuario recibe la misma experiencia en el escritorio que un tratamiento directo. La aplicación Workspace comprime el vídeo para ahorrar ancho de banda y proporcionar una mejor capacidad de recuperación en conexiones WAN.

La compresión de vídeo de cámara Web de HDX requiere que las siguientes configuraciones de directiva estén habilitadas (están todas habilitadas de forma predeterminada).

- Conferencia multimedia
- Redirección de Windows Media

Si una cámara Web es compatible con la codificación por hardware, la compresión de vídeo de HDX utiliza la codificación por hardware de manera predeterminada. La codificación por hardware puede consumir más ancho de banda que la codificación por software. Para forzar la compresión de software, agregue el siguiente valor de clave DWORD a la clave de Registro:

HKEY_CURRENT_USER\Software\Citrix\HdxRealTime: DeepCompress_ForceSWEncode=1

Requisitos para la compresión de vídeo de cámara Web de HDX

Clientes respaldados: La aplicación Citrix Workspace para Windows, la aplicación Citrix Workspace para Mac, la aplicación Citrix Workspace para Chrome y la aplicación Citrix Workspace para Linux.

Aplicaciones de conferencias de vídeo respaldadas (32 y 64 bits):

- Adobe Connect
- Cisco Webex y Webex Teams
- GoToMeeting
- Google Hangouts y Hangouts Meet
- IBM Sametime
- Microsoft Skype Empresarial 2015
- Microsoft Lync 2010 y 2013
- Microsoft Skype 7 o posterior
- Aplicaciones de vídeo basadas en Media Foundation en Windows 8.x o posterior, Windows Server 2012 R2 y posterior

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para usar Skype en un cliente Windows, modifique el Registro en el cliente y en el servidor:

- Clave del Registro de cliente HKEY_CURRENT_USER\Software\Citrix\HdxRealTime

  Nombre: DefaultHeight

  Tipo: REG_DWORD

  Datos: 240

  Nombre: DefaultWidth, Tipo: REG_DWORD

  Datos: 320

- Clave del Registro de servidor HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Vd3d\Compatibility

  Nombre: skype.exe

  Tipo: REG_DWORD

  Datos: Establecido en 0

Otros requisitos del dispositivo de usuario:

- Hardware adecuado para reproducir sonido.
- Cámara Web compatible con DirectShow (use la configuración predeterminada de la cámara Web). Las cámaras Web que pueden codificar hardware reducen el uso de la CPU en el lado del cliente.
- Para la compresión de vídeo de cámara Web de HDX, instale los controladores de cámara Web en el cliente, obtenidos del fabricante de la cámara, si es posible.

Streaming por cámara Web de alta definición

La aplicación presente en el servidor selecciona el formato de cámara web y la resolución en función de los tipos de formato compatibles. Cuando se inicia una sesión, el cliente envía la información de la cámara web al servidor. Usted elige la cámara Web desde la aplicación. Si la cámara Web y la aplicación admiten la generación de alta definición, la aplicación usa la resolución de alta definición. Damos respaldo a resoluciones de cámara Web hasta 1920 x 1080.

Esta característica requiere la aplicación Citrix Workspace para Windows (versión mínima 1808) o Citrix Receiver para Windows (versión mínima 4.10).

Puede usar una clave de Registro para inhabilitar la función. Se usa la resolución predeterminada de 352 x 288:

HKEY_LOCAL_MACHINE\Software\Citrix\HDXRealTime

Nombre: Enable_HighDefWebcam

Tipo: REG_DWORD

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Datos: 0 = Desactiva la distribución por streaming de la cámara Web de alta definición

Puede usar claves de Registro en el cliente para configurar una resolución específica. Compruebe que la cámara admite la resolución especificada:

HKEY_CURRENT_USER\Software\Citrix\HDXRealTime

Nombre: DefaultWidth

Tipo: REG_DWORD

Datos (decimales): Anchura deseada (por ejemplo, 1280)

Nombre: DefaultHeight

Tipo: REG_DWORD

Datos (decimales): Altura deseada (por ejemplo, 720)

Redirección de USB genérico de HDX Plug-n-Play

La redirección USB genérica de HDX Plug-n-Play (isócrona) también se denomina modo de cámara Web **genérico**. La ventaja de la redirección USB genérica de HDX Plug-n-Play es que no es necesario instalar controladores en el cliente ligero o el dispositivo de punto final. La pila USB está virtualizada, de modo que todo lo que conecte al cliente local se envía a la máquina virtual remota. El escritorio remoto actúa como si lo hubiera conectado al entorno nativo. El escritorio Windows se ocupa de toda la interacción con el hardware, y se ejecuta siguiendo la lógica Plug-n-Play para buscar los controladores correctos. La mayoría de las cámaras Web funcionan si los controladores existen y pueden funcionar sobre ICA. El modo genérico de cámara Web consume mucho más ancho de banda (muchos megabits por segundo) porque se envían vídeos sin comprimir con el protocolo USB a través de la red.

Redirección de Windows Media

December 14, 2018

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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

con Citrix Diagnosis Facility (CDF) desde HostMMTransport.dll. Para obtener más información, consulte Citrix Scout.

La Redirección de Windows Media intercepta la canalización multimedia en el 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 la canalización 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 la canalización multimedia que existe en el servidor host. Los clientes Linux usan marcos multimedia similares de código abierto para reconstruir la canalización 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

November 29, 2018

> **Nota:**
>
> Puede obtener información sobre los cambios en los nombres de producto aquí.

La redirección de contenido permite controlar si los usuarios acceden a la información desde aplicaciones publicadas en servidores o desde aplicaciones que se ejecutan localmente en dispositivos de usuario.

Redirección de carpetas del cliente

La redirección de carpetas del cliente cambia el modo en que los archivos del lado del cliente son accesibles desde la sesión en el host. Cuando se habilita solo la asignación de unidades del cliente

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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. Para la mayoría de los casos, existen mejores formas de redirigir el contenido. Este tipo de redirección solo se admite en agentes VDA de SO de servidor (no en agentes VDA de SO de escritorio).

Acceso a aplicaciones locales y redirección de URL

La función "Acceso a aplicaciones locales" integra perfectamente las aplicaciones Windows instaladas localmente en un entorno de escritorio alojado sin cambiar de un equipo a otro.

La tecnología HDX ofrece la **redirección de USB genérico** para dispositivos específicos sin respaldo optimizado o cuando ese respaldo no es adecuado.

Redirección de carpetas del cliente

January 29, 2019

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 usuario, solo se redirige la parte del volumen local que especifique el usuario.

Solo las carpetas especificadas por el usuario aparecerán como enlaces UNC dentro de las sesiones, en lugar de aparecer todo el sistema de archivos del 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 está respaldada en máquinas con SO de escritorio Windows.

La redirección de carpetas del cliente para una unidad USB externa no se guardará 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> **Advertencia**
>
> Si se modifica el Registro de forma incorrecta, se pueden generar problemas graves que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

1. En el servidor:
   a) Cree una clave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection.
   b) Cree un valor REG_DWORD.
      - Nombre: CFROnlyModeAvailable
      - Tipo: REG_DWORD
      - Datos: Establézcalo en 1.
2. En el dispositivo de usuario:
   a) Compruebe que está instalada la versión más reciente de la aplicación Citrix Workspace.
   b) En el directorio de instalación de la aplicación Citrix Workspace, inicie CtxCFRUI.exe.
   c) Seleccione el botón de opción Personalizada y agregue, modifique o quite carpetas.
   d) Desconecte y vuelva a conectar sus sesiones para que la configuración tenga efecto.

Redirección del host al cliente

March 8, 2019

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.

La **redirección del host al cliente** es un tipo de redirección de contenido. Solo se admite en agentes VDA de SO de servidor (no en agentes VDA de SO de escritorio).

- Cuando la redirección del host al cliente está habilitada, las direcciones URL se interceptan en el servidor VDA y se envían al dispositivo de usuario. El explorador Web o el reproductor multimedia presentes en el dispositivo de usuario abren esas direcciones URL.
- Si habilita la redirección del host al cliente y el dispositivo de usuario no puede conectarse a una URL, esa URL se la redirige de vuelta al VDA de servidor.
- Cuando la redirección del host al cliente está inhabilitada, los usuarios pueden abrir las URL con exploradores Web o reproductores multimedia que residan en el VDA de servidor.
- Cuando la redirección del host al cliente está habilitada, los usuarios no pueden inhabilitarla.

Anteriormente, la redirección del host al cliente recibía el nombre de **redirección del servidor al**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

cliente.

Cuándo usar la redirección del host al cliente

Puede plantearse usar la redirección del host al cliente en casos determinados y poco frecuentes por motivos de rendimiento, compatibilidad o cumplimiento de normativas. Para la mayoría de los casos, existen mejores formas de redirigir el contenido.

Rendimiento:

Puede utilizar la redirección del host al cliente para obtener un mayor rendimiento. Así, siempre se usa la aplicación instalada en el dispositivo de usuario, en lugar de usar la aplicación del VDA.

Tenga en cuenta que la redirección del host al cliente mejora el rendimiento solo cuando se dan condiciones específicas, porque el VDA ya optimiza Adobe Flash y otros tipos de contenido multimedia. Antes de optar por ello, considere la posibilidad de usar otros métodos (como las directivas, indicadas en las tablas de este artículo), en lugar de la redirección del host al cliente. Las directivas permiten una mayor flexibilidad y normalmente ofrecen una mejor experiencia de usuario, especialmente para aquellos dispositivos de usuario que no sean muy potentes.

Compatibilidad:

Puede usar la redirección del host al cliente para obtener una mayor compatibilidad en los siguientes casos:

- Usa tipos de contenido que no son HTML o multimedia (por ejemplo, direcciones URL personalizadas).
- Usa un formato antiguo (por ejemplo, Real Media) que el reproductor multimedia del VDA no admite con la redirección multimedia.
- Solo una cantidad pequeña de usuarios utiliza la aplicación del tipo de contenido y ellos ya tienen la aplicación instalada en sus dispositivos respectivos.
- El VDA no puede acceder a determinados sitios Web (por ejemplo, sitios Web internos de otra empresa).

Conformidad:

Puede usar la redirección del host al cliente para obtener un mayor cumplimiento en los siguientes casos:

- El contrato de licencia de la aplicación o del contenido no permite publicar mediante el VDA.
- La directiva de la empresa no permite que un documento se cargue en el VDA.

Algunas situaciones son más propias de entornos complejos y de casos en que el dispositivo de usuario y el VDA pertenecen a empresas diferentes.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Consideraciones de dispositivo del usuario

Los entornos pueden abarcar varios tipos de dispositivos de usuario.

Dispositivo de usuario	Situación o entorno	Método de redirección de contenido
Tableta	-	Cualquier método (consulte la siguiente tabla)
Equipo portátil	-	Cualquier método (consulte la siguiente tabla)
Equipo de escritorio	Los usuarios usan una amplia gama de aplicaciones instaladas en el dispositivo del usuario	Cualquier método (consulte la siguiente tabla)
Equipo de escritorio	Los usuarios solo usan algunas aplicaciones conocidas que están instaladas en el dispositivo del usuario	Acceso a aplicaciones locales
Equipo de escritorio	Los usuarios no utilizan las aplicaciones instaladas en el dispositivo del usuario	Redirección multimedia, redirección de Flash
Dispositivo de escritorio	El proveedor admite la redirección multimedia, la redirección de Flash o ambas	Redirección multimedia, redirección de Flash
Cliente ligero	El proveedor admite la redirección multimedia, la redirección de Flash y la redirección del host al cliente	Cualquier método (consulte la siguiente tabla)
Cliente cero	El proveedor admite la redirección multimedia, la redirección de Flash o ambas	Redirección multimedia, redirección de Flash

A continuación, dispone de ejemplos para guiarle a la hora de escoger el método adecuado para la redirección de contenido.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Enlace de direcciones URL	Situación o entorno	Método de redirección de contenido
Una página Web o documento	El VDA no puede acceder a la URL	Redirección del host al cliente
Una página Web	La página Web contiene Adobe Flash	Redirección de Flash
Un archivo multimedia o transmisión por streaming	El VDA tiene un reproductor multimedia compatible	Redirección multimedia
Un archivo multimedia o transmisión por streaming	El VDA no tiene ningún reproductor multimedia compatible	Redirección del host al cliente
Un documento	El VDA no tiene ninguna aplicación para ese tipo de documento	Redirección del host al cliente
Un documento	No descargue el documento en el dispositivo del usuario	Sin redirección
Un documento	No descargue el documento en el VDA	Redirección del host al cliente
Un tipo de URL personalizada	El VDA no tiene ninguna aplicación para ese tipo de URL personalizada	Redirección del host al cliente

Estas aplicaciones Citrix Workspace admiten la redirección del host al cliente:

- 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

Para usar la redirección del host al cliente, el dispositivo del usuario debe contar con un explorador Web, un reproductor multimedia u otra aplicación adecuada para el contenido. Si el usuario usa uno de los siguientes dispositivos, confirme que el dispositivo tiene las aplicaciones adecuadas y una administración de energía conveniente.

- Dispositivo de escritorio
- Cliente ligero
- Cliente con requisitos mínimos (o cliente Zero)

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Los dispositivos de usuario que están habilitados para el acceso a aplicaciones locales usan otro mecanismo para la redirección de contenido y no necesitan la redirección de contenido del host al cliente.

Puede usar directivas de Citrix para impedir la redirección de contenido del host al cliente en caso de dispositivos no adecuados.

Cómo es la redirección del host al cliente para los usuarios

La redirección del host al cliente se usa cuando las direcciones URL:

- Están incrustadas como hipervínculos en una aplicación (por ejemplo, en un documento o mensaje de correo electrónico).
- Se han seleccionado desde menús o diálogos de una aplicación de VDA, siempre que la aplicación use la API ShellExecuteEx de Windows.
- Se han introducido en el diálogo Ejecutar de Windows.

La redirección del host al cliente no se usa para direcciones URL en un explorador Web. Es decir, en una página Web o escrita en la barra de direcciones del explorador Web.

> **Nota**
>
> Si los usuarios cambian su explorador Web predeterminado en el VDA, ese cambio puede interferir con la redirección del host al cliente de las aplicaciones. Un ejemplo de cambio de explorador Web predeterminado es usar "Establecer programas predeterminados".

Cuando la redirección de contenido del host al cliente está habilitada, la aplicación que se utiliza para abrir la URL usa la configuración del dispositivo de usuario para el tipo de URL y el tipo de contenido. Por ejemplo:

- Una URL de HTTP con un tipo de contenido HTML se abre en el explorador Web predeterminado.
- Una URL de HTTP con un tipo de contenido PDF puede abrirse en el explorador Web predeterminado o en otra aplicación.

Esta configuración del dispositivo del usuario no se controla desde la redirección de contenido del host al cliente. Si no controla la configuración del dispositivo del usuario, considere la posibilidad de usar la redirección de Flash y la redirección multimedia en lugar de la redirección de contenido del host al cliente.

Los siguientes tipos de URL se abren localmente en los dispositivos de usuario cuando está habilitada la redirección del host al cliente:

- HTTP
- HTTPS
- RTSP
- RTSPU

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- PNM
- MMS

Para eliminar y agregar tipos de URL, puede cambiar la lista de tipos de URL que se usa en la redirección del host al cliente. Los tipos de URL incluyen tipos personalizados.

Habilitar la redirección del host al cliente

Habilitar la redirección del host al cliente es un proceso que se inicia con la activación de una directiva Citrix.

La configuración de directiva "Redirección del host al cliente" se encuentra en la sección Configuraciones de directiva de Redirección de archivos. De forma predeterminada, esta configuración está inhabilitada.

Además, es posible que deba establecer claves de Registro y directivas de grupo para los agentes VDA de servidor, según el sistema operativo de los VDA.

- Si el VDA de servidor es Windows Server 2008 R2 SP1, no se necesita configurar claves de Registro ni ninguna directiva de grupo.
- En cambio, si el VDA de servidor es Windows Server 2012, Windows Server 2012 R2 o Windows Server 2016, deberá establecer claves de Registro y una directiva de grupo.

> **Advertencia**
>
> Utilizar el Editor del Registro de forma incorrecta puede provocar problemas graves que podrían conllevar la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Cambios en el Registro

1. Copie el texto ubicado entre "**Reg file start**" y "**Reg file end**" indicado en el ejemplo, y péguelo en el Bloc de notas.
2. Guarde el archivo de la aplicación Bloc de notas con "Guardar como", con el tipo **Todos los archivos** y el nombre **ServerFTA.reg**.
3. Distribuya el archivo **ServerFTA.reg** a los servidores mediante la directiva de grupo de Active Directory.

```
1  --  Reg file start --
2
3      Windows Registry Editor Version 5.00
4      [HKEY_CLASSES_ROOT\ServerFTAHTML\shell\open\command]
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

```
5
6       @=""C:\Program Files (x86)\Citrix\system32\iexplore.exe" %1"
7       [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA]
8
9       @="ServerFTA"
10      [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA\Capabilities]
11
12      "ApplicationDescription"="Server FTA URL."
13
14      "ApplicationIcon"="C:\Program Files (x86)\Citrix\system32\iexplore.
            exe,0"
15
16      "ApplicationName"="ServerFTA"
17      [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA\Capabilities\
            URLAssociations]
18
19      "http"="ServerFTAHTML"
20
21      "https"="ServerFTAHTML"
22      [HKEY_LOCAL_MACHINE\SOFTWARE\RegisteredApplications]
23
24      "Citrix.ServerFTA"="SOFTWARE\Citrix\ServerFTA\Capabilities"
25
26      -- Reg file end --
```

Cambios en la directiva de grupo

Cree un archivo XML. Copie el texto ubicado entre "xml file start" y "xml file end", péguelo en el archivo XML y, a continuación, guarde el archivo como **ServerFTAdefaultPolicy.xml**.

```
1  -- xml file start --
2
3  <?xml version="1.0" encoding="UTF-8"?>
4
5  <DefaultAssociations>
6
7  <Association Identifier="http" ProgId="ServerFTAHTML" ApplicationName="
       ServerFTA" />
8
9  <Association Identifier="https" ProgId="ServerFTAHTML" ApplicationName=
       "ServerFTA" />
10
11 </DefaultAssociations>
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

```
12
13 -- xml file end --
```

En la Consola de administración de directivas de grupo actual, vaya a: **Configuración del equipo** > **Plantillas administrativas** > **Componentes de Windows** > **Explorador de archivos** > **Definir un archivo de configuración de asociaciones predeterminadas,** y proporcione el archivo ServerFTAdefaultPolicy.xml que ha creado.

Cambiar la lista de tipos de URL para la redirección del host al cliente

Si quiere cambiar la lista de los tipos de URL para la redirección del host al cliente, defina la siguiente clave de Registro en el VDA de servidor.

Clave: HKLM\Software\Wow6432Node\Citrix\SFTA

Para eliminar tipos de URL de la lista, establezca DisableServerFTA y NoRedirectClasses:

Nombre: DisableServerFTA
Tipo: REG_DWORD
Datos: 1

Nombre: NoRedirectClasses
Tipo: REG_MULTI_SZ
Datos: Especifique una 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 agregar tipos de URL a la lista, establezca ExtraURLProtocols:

Nombre: ExtraURLProtocols
Tipo: REG_MULTI_SZ
Datos: Especifique cualquier combinación de tipos de URL. Todos los tipos de URL deben contener el sufijo “://”; separe los valores con punto y coma. Por ejemplo:

tipopersonalizado1://;tipopersonalizado2://

Cómo habilitar la 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 la siguiente clave de Registro en el VDA de servidor.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Clave: HKLM\Software\Wow6432Node\Citrix\SFTA

Nombre: ValidSites
Tipo: REG_MULTI_SZ
Datos: Especifique cualquier combinación de nombres de dominio completos (FQDN). Si especifica varios nombres de dominio completos, debe ser en líneas independientes. Un nombre de dominio completo puede incluir un 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.ejemplo.com

*.ejemplo.com

Acceso a aplicaciones locales y redirección de URL

March 8, 2019

Introducción

La función Acceso a aplicaciones locales integra perfectamente las aplicaciones Windows instaladas localmente en un entorno de escritorio alojado sin cambiar de un equipo 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.
- Elimine la latencia del doble salto cuando las aplicaciones están alojadas aparte del escritorio virtual, colocando 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, tales como 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

disponible en más de una URL. Inicia un explorador local (basado en la lista negra de URL de su explorador) seleccionando enlaces incrustados en un explorador en una sesión de escritorio. Si navega a una URL que no está en la lista negra, 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 vínculos incrustados solo con http, los vínculos se abren directamente con la aplicación cliente. No se admiten ni la lista negra ni la lista blanca de URL.

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 blanca de URL y la lista negra de URL en el Virtual Delivery Agent. Estas listas contienen claves de Registro de cadena múltiple que especifican la configuración de directiva Redirección de URL; para obtener más información, consulte la configuración de la directiva 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 fue aprovisionado desde un centro de datos en el Reino Unido y el cliente se conecta desde India, el usuario espera ver in.msn.com, pero en su lugar 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. Aunque existe una función para redirección de Flash, esta función se complementa redirigiendo sitios que contienen otros tipos de contenido multimedia, tales 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,

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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

La función Acceso a aplicaciones locales recibe respaldo en los sistemas operativos válidos para los VDA de SO de servidor Windows y los VDA de SO de escritorio Windows. Acceso a aplicaciones locales requiere la aplicación Citrix Workspace para Windows 4.1 (versión mínima). Se admiten los siguientes exploradores Web:

- Internet Explorer 11 Puede usar Internet Explorer 8, 9 o 10, pero Microsoft respalda (y Citrix recomienda usar) la versión 11.
- Firefox 3.5 a 21.0
- Chrome 10

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.
  - En caso de usarse varios monitores, si uno de ellos está maximizado, ese monitor se convierte en el escritorio predeterminado de todas las aplicaciones que se inician en esa sesión, incluso aunque el resto de las aplicaciones normalmente se inicien 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 respaldan las aplicaciones de pantalla completa. Estas aplicaciones pueden ser aquellas que se abren en el modo de pantalla completa, como las presentaciones con dia-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

positivas 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 barras de tareas no se respalda en caso de aplicaciones alojadas en el cliente o aplicaciones del VDA que combinan 32 bits y 64 bits, como la agrupación de aplicaciones locales de 32 bits con aplicaciones de VDA de 64 bits y viceversa.
  - 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 reciben respaldo.
- 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 usando).
- 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 a 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.

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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

  - Las aplicaciones de la Tienda Windows instaladas en el cliente no se enumeran 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 blanca y la lista negra de URL para la redirección de URL. Para obtener más información, consulte las configuraciones de directiva Acceso a aplicaciones locales.

Habilitar el acceso a aplicaciones locales y la redirección de URL durante la instalación de la aplicación Citrix Workspace:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para habilitar el acceso a aplicaciones locales y la redirección de URL para todas las aplicaciones locales:

1. Establezca la configuración de directiva **Permitir acceso a aplicaciones locales** como **Habilitada**. 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 inhabilitada, no funcionan en el VDA ni los accesos directos de Acceso a aplicaciones locales ni las aplicaciones publicadas del administrador.) Esta configuración de directiva se aplica a toda la máquina y a la directiva Redirección de URL.
2. Habilite el Acceso a aplicaciones locales y la Redirección de URL durante la instalación de la aplicación Citrix Workspace para todos los usuarios de una máquina. Esta acción registra también los complementos del explorador Web necesarios para la redirección de URL. En el símbolo del sistema, ejecute el comando apropiado para instalar la aplicación Citrix Workspace con la opción siguiente:

   CitrixReceiver.exe /ALLOW_CLIENTHOSTEDAPPSURL=1

   CitrixReceiverWeb.exe /ALLOW_CLIENTHOSTEDAPPSURL=1

Habilitar la plantilla de Acceso a aplicaciones locales desde el Editor de directivas de grupo:

1. Ejecute **gpedit.msc**.
2. Seleccione **Configuración del equipo**. Haga clic con el botón secundario en **Plantillas administrativas** y seleccione **Agregar o quitar plantillas > Agregar**.
3. Agregue la plantilla receiver.adm ubicada en la carpeta Configuration de la aplicación Citrix Workspace (por regla general, en C:\Archivos de programa (x86)\Citrix\Online Plugin\Configuration). (Una vez agregada la plantilla receiver.adm al nodo Configuración del equipo, también estará disponible en el nodo Configuración de usuario.)
4. Expanda **Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Componentes de Citrix > Citrix Workspace > Experiencia de usuario**.
5. Seleccione **Configuración del acceso a aplicaciones locales**.
6. 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* en este artículo.

Proporcionar acceso solo a las aplicaciones publicadas:

1. En el servidor donde está instalado Delivery Controller, ejecute **regedit.msc**.
   a) Vaya a HKLM\Software\Wow6432Node\Citrix\DesktopStudio.
   b) Agregue la entrada REG_DWORD ClientHostedAppsEnabled con el valor 1. (Un valor 0 inhabilita el acceso a aplicaciones locales.)
2. Reinicie el servidor Delivery Controller y, a continuación, reinicie Studio.
3. Publique aplicaciones de acceso local.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

a) Seleccione los **Grupos de entrega** en el panel de navegación de Studio y, a continuación, seleccione la ficha Aplicaciones.
b) Seleccione **Crear aplicación de acceso local** en el panel Acciones.
c) Seleccione el Grupo de entrega de escritorios.
d) Escriba la ruta completa al archivo ejecutable de la aplicación en la máquina local del usuario.
e) Indique si el acceso directo a la aplicación local en el escritorio virtual estará visible en el menú Inicio, en el escritorio, o en ambos.
f) Acepte los valores predeterminados en la página **Nombre** y revise los parámetros.

4. Habilite el Acceso a aplicaciones locales y la Redirección de URL durante la instalación de la aplicación Citrix Workspace para todos los usuarios de una máquina. Esta acción registra también los complementos del explorador Web necesarios para la redirección de URL. Desde el símbolo del sistema, ejecute el comando para instalar la aplicación Citrix Workspace con la opción siguiente:
   CitrixReceiver.exe /ALLOW_CLIENTHOSTEDAPPSURL=1
   CitrixReceiverWeb.exe /ALLOW_CLIENTHOSTEDAPPSURL=1
5. Establezca la configuración de directiva **Permitir acceso a aplicaciones locales** como **Habilitada**. 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 inhabilitada, no funcionan en el VDA ni los accesos directos de aplicaciones publicadas por el administrador ni los de acceso a aplicaciones locales.)

Registro de 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*>

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Donde <*explorador*> puede ser IE, FF, Chrome o All.

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 de servidor Windows.

C:\Archivos de programa (x86)\Citrix\System32\VDARedirector.exe /regAll

Interceptación de URL entre exploradores Web:

- De manera predeterminada, Internet Explorer redirige la dirección URL que se haya introducido. Si la URL no está en la lista negra, 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 negra.

Para que la redirección de URL funcione correctamente, habilite el complemento cuando lo solicite el explorador Web. Si se inhabilitan los complementos que usan las opciones de Internet o los que pide el sistema, la redirección de URL no funciona correctamente.

- Los complementos de Firefox siempre redirigen las direcciones URL.

Cuando se instala un complemento, Firefox pide confirmación para permitir o impedir la instalación del complemento en una página de nueva pestaña. Permita el complemento para poder usar esta función.

- El complemento de Chrome siempre redirige la URL final de navegación y no las direcciones URL introducidas.

Las extensiones han sido instaladas externamente. Si inhabilita 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:

1. En el escritorio alojado, ejecute **regedit.msc**.
2. Vaya a HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Client Hosted Apps\Policies\Session State.Para un sistema de 64 bits, vaya a HKEY_LOCAL_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies\Session State.
3. Agregue la entrada Terminate de REG_DWORD y alguno de estos valores:
    - 1 - Las aplicaciones locales siguen ejecutándose cuando un usuario cierra sesión o se desconecta del escritorio virtual. Tras la reconexión, las aplicaciones locales vuelven a integrarse si están disponibles en el escritorio virtual.
    - 3 - Las aplicaciones locales se cierran cuando el usuario cierra la sesión o se desconecta del escritorio virtual.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Consideraciones sobre unidades del cliente y redirección de USB genérico

March 14, 2019

La tecnología HDX ofrece **compatibilidad optimizada** con los dispositivos USB más comunes. El respaldo optimizado (o compatibilidad optimizada) ofrece una experiencia de usuario mejorada, con mejor rendimiento y eficiencia del ancho de banda en una conexión por red WAN. El respaldo optimizado 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 compatibilidad optimizada o cuando esa compatibilidad no es adecuada, por ejemplo:

- El dispositivo USB tiene otras funciones avanzadas que no forman parte del respaldo optimizado, como mouse o cámaras Web con botones adicionales.
- Los usuarios necesitan funciones que no forman parte del respaldo optimizado, como grabar un CD.
- 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 respaldo optimizado 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.

> **Nota**
>
> - La redirección de USB genérico puede utilizarse junto con la compatibilidad optimizada. Si habilita la redirección USB genérica, configure las directivas de dispositivos USB de Citrix tanto para la redirección USB genérica como para el respaldo optimizado.
> - La configuración de directiva Reglas de optimización de dispositivos USB del cliente de Citrix es una configuración específica para la redirección USB genérica, para un determinado de dispositivo USB. No se aplica al respaldo optimizado que se describe aquí.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Consideraciones de rendimiento para dispositivos USB

Con la redirección USB genérica, 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 el respaldo optimizado, 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 la 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. Esto se aplica cuando se utiliza el respaldo optimizado o la redirección de USB genérico.

> **Importante**
>
> En caso de dispositivos y datos confidenciales, proteja siempre la conexión HDX mediante TLS o IPSec.
>
> Habilite el respaldo solo para los dispositivos USB que necesite. Configure la redirección de USB genérico y la compatibilidad optimizada 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 características de USB introducidas en USB 3.0 tales como la velocidad extra.

Estas aplicaciones Citrix Workspace admiten la redirección USB genérica:

- Aplicación Citrix Workspace para Windows; consulte Configurar la entrega de aplicaciones
- Aplicación Citrix Workspace para Mac; consulte Aplicación Citrix Workspace para Mac.
- Aplicación Citrix Workspace para Linux; consulte Optimizar
- Aplicación Citrix Workspace para Chrome OS; consulte Aplicación Citrix Workspace para Chrome

Para ver las versiones de la aplicación Citrix Workspace, consulte Tabla de funciones de la aplicación Citrix Workspace.

Si usa versiones anteriores de la aplicación Citrix Workspace, consulte la documentación de la aplicación Citrix Workspace para ver si se admite la redirección USB genérica. 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 escritorio 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 de servidor hasta la versión actual con las siguientes restricciones:

- El VDA debe estar ejecutándose en Windows Server 2012 R2 o Windows Server 2016.
- Solo se admiten los casos de salto único. La redirección de USB genérico de doble salto no se admite en sesiones de aplicaciones alojadas en escritorios.
- 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), incluido el respaldo completo a la virtualización.

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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 USB genérica 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, la aplicación Citrix Workspace para Windows se configura con parámetros de Registro que pueden gestionarse desde una plantilla administrativa. 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 funciones y funcionalidad 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. Estas medidas se aplican 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).

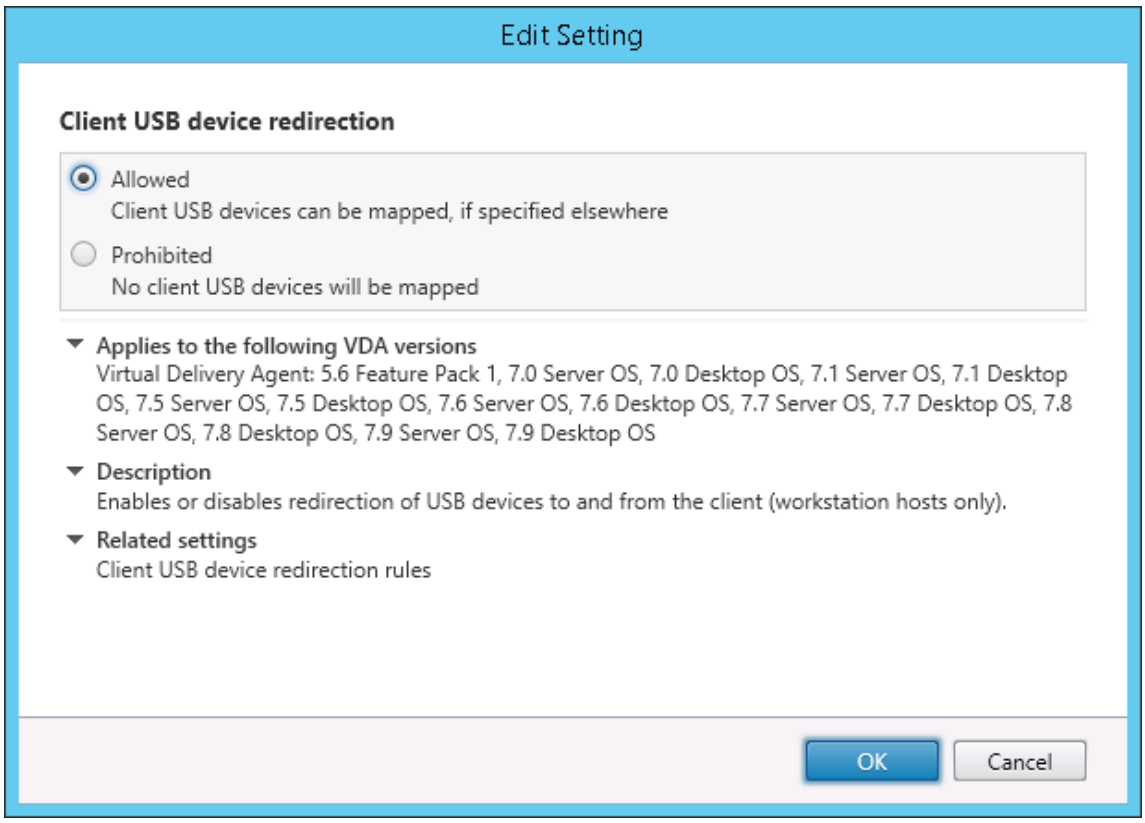
Habilitar la redirección de USB genérico

Para habilitar la redirección USB genérica 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**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

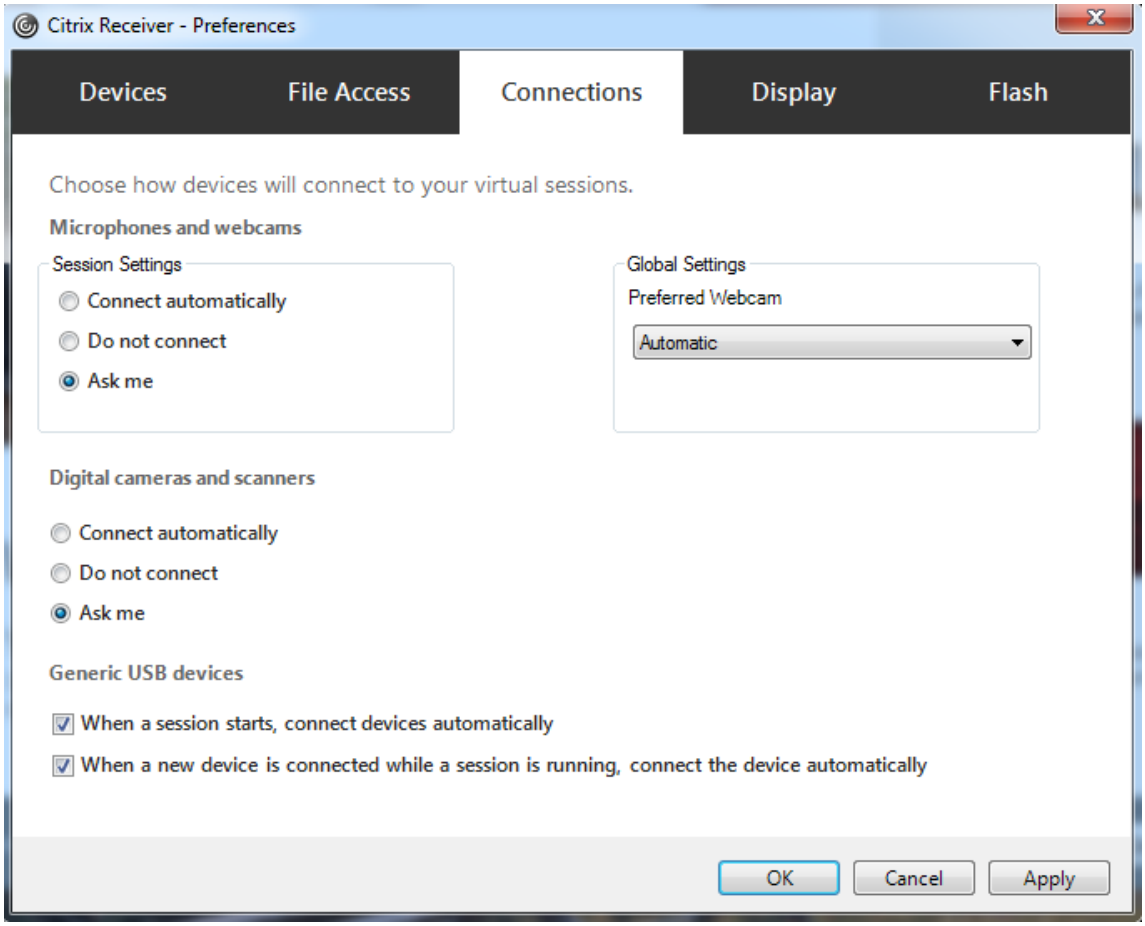


2. (Optativo.) Para actualizar la lista de dispositivos USB disponibles para la redirección, agregue la configuración Reglas de redirección de dispositivos USB del cliente a una directiva y especifique las reglas de la directiva USB.

   En la aplicación Citrix Workspace:

3. Especifique que los dispositivos se conecten automáticamente, sin redirección manual. Puede hacerlo mediante una plantilla administrativa, o bien en la aplicación Citrix Workspace para Windows > Preferencias > Conexiones.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Si especificó reglas de directiva USB para el VDA en el paso anterior, especifique las mismas reglas de directiva para la aplicación Citrix Workspace.

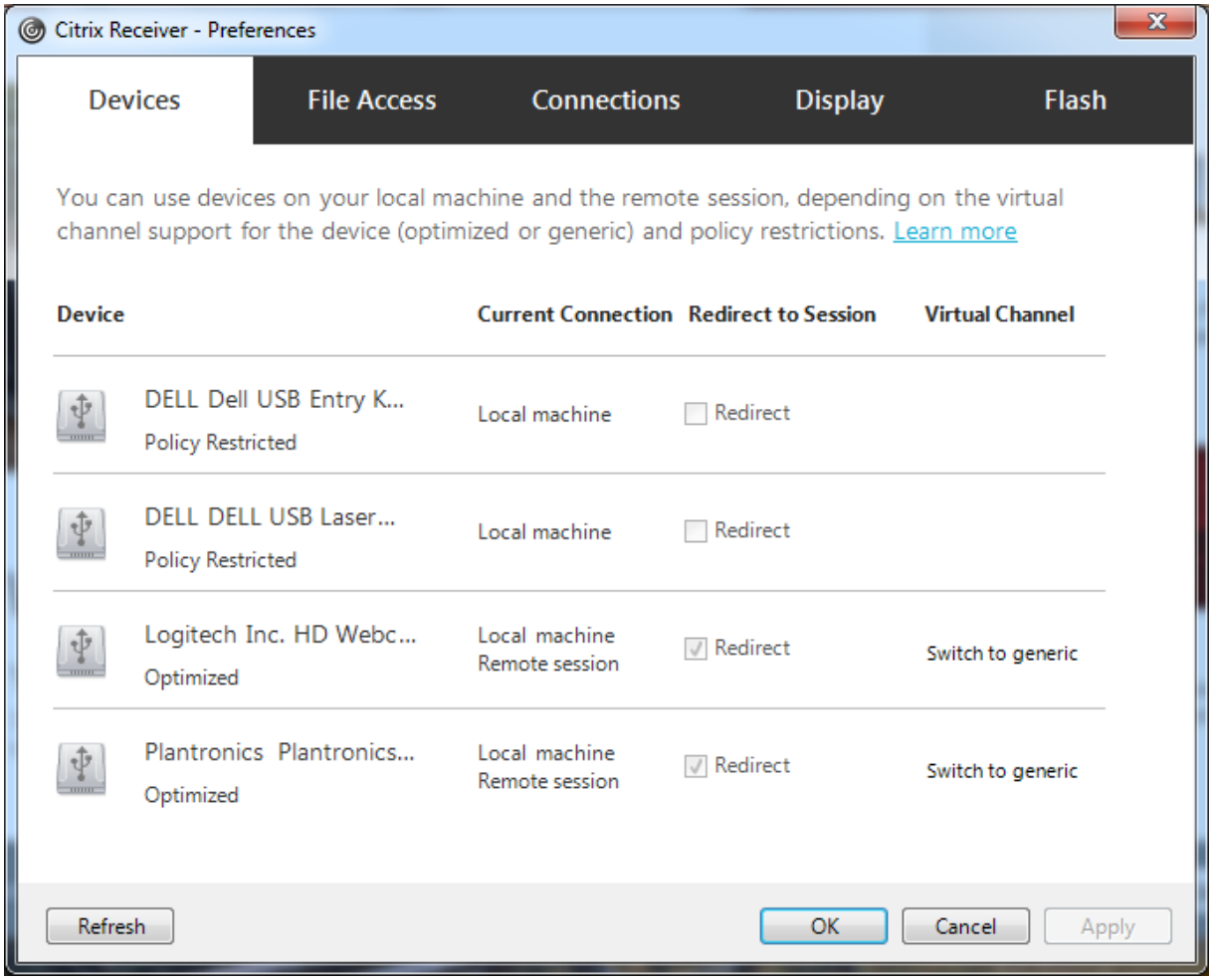
Para los clientes ligeros, consulte al fabricante para obtener detalles sobre el respaldo de USB y cualquier configuración requerida.

Configurar los tipos de dispositivos USB disponibles para la redirección de USB genérico

Los dispositivos USB se redirigen automáticamente cuando el respaldo de USB está habilitado 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 se trabaja en modo Desktop Appliance y 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. Los usuarios pueden obtener más ayuda sobre la forma de hacerlo en el artículo Mostrar los dispositivos en Desktop Viewer en la ayuda de la aplicación Citrix Workspace para Windows.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Para usar la redirección de USB genérico en lugar de la compatibilidad optimizada, puede:

- En la aplicación Citrix Workspace, seleccione manualmente el dispositivo USB con que se va a usar la redirección USB genérica, 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 USB genérica 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 USB genérica, debe conocer al menos la clase y la subclase del dispositivo USB.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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, también 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 características 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 USB genérica especificando reglas de redirección de dispositivos USB tanto para el VDA como para la aplicación Citrix Workspace. De esta manera, se anularán las reglas predeterminadas de la directiva USB.

Para el VDA:

- Modifique las reglas de invalidación del administrador para las máquinas con sistema operativo de servidor mediante las reglas de directiva de grupo. La Consola de administración de directivas de grupo se incluye en los medios de instalación:
  - Para x64: dvd root \os\lang\x64\Citrix Policy\ CitrixGroupPolicyManagement_x64.msi
  - Para x86: dvd root \os\lang\x86\Citrix Policy\ CitrixGroupPolicyManagement_x86.msi

En la aplicación Citrix Workspace para Windows:

- Modifique el Registro en el dispositivo del usuario. En los medios de instalación, se incluye una plantilla administrativa (archivo ADM) que permite cambiar el dispositivo cliente mediante la Directiva de grupo de Active Directory:
  dvd root \os\lang\Support\Configuration\icaclient_usb.adm.

> **Advertencia**
>
> Si se modifica el Registro de forma incorrecta, se pueden generar problemas graves que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Las reglas predeterminadas del producto se almacenan en HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRu
No modifique las reglas predeterminadas del producto. En su lugar, úselas como una guía para la creación de reglas de suplantación del administrador, según se explica a continuación en este artículo. Las suplantaciones del objeto de directiva de grupo (GPO) se evalúan antes que las reglas predeterminadas del producto.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Las reglas de suplantación del administrador se almacenan en HKLM\SOFTWARE\Policies\Citrix\PortICA\GenericUS
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**
>
> Si utiliza el archivo de plantilla ADM, debe crear reglas en una única línea, como una lista separada por punto y coma.

Ejemplos:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Este ejemplo muestra una regla de directiva 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 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 respaldo optimizado para dispositivos de almacenamiento USB. Este respaldo 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 USB genérica o ambos. Se controlan con directivas de Citrix. Las principales diferencias son:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Función	Asignación de unidades del cliente	Redirección de USB genérico
Habilitada de forma predeterminada	Sí	No
Configuración para acceso de sólo lectura	Sí	No
Acceso a dispositivo cifrado	Sí, si el cifrado se desbloquea antes de acceder al dispositivo	Sí
Dispositivo a 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 USB genérica 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 USB genérica 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 usando la redirección USB genérica. Para obtener más información, consulte el artículo CTX123015 de Knowledge Center.

> **Nota**
>
> Se admite la redirección USB en conexiones de poco ancho de banda: por ejemplo, conexiones de 50 kbps. Sin embargo, no se admite copiar archivos de gran tamaño.

Controlar el acceso a archivos con la asignación de unidades del cliente

Puede controlar si los usuarios pueden copiar archivos desde sus entornos virtuales a sus dispositivos de usuario. De manera predeterminada, los archivos y carpetas de las unidades asignadas del cliente están disponibles en modo de lectura/escritura dentro de la sesión.

Si quiere impedir que los usuarios agreguen o modifiquen archivos y carpetas de los dispositivos de cliente asignados, habilite la configuración de directiva **Acceso de lectura solamente a unidades del cliente**. Al agregar esta configuración a una directiva, compruebe que la configuración “Redirección de unidades del cliente” está establecida en **Permitida** y también se ha agregado a la directiva.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Imprimir

March 8, 2019

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

> **Nota:**
>
> Puede obtener información sobre los cambios en los nombres de producto aquí.

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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, proporciona respaldo de 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 de servidor 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

formato optimizado y comprimido, lo que minimiza el uso de red y mejora la experiencia del usuario.

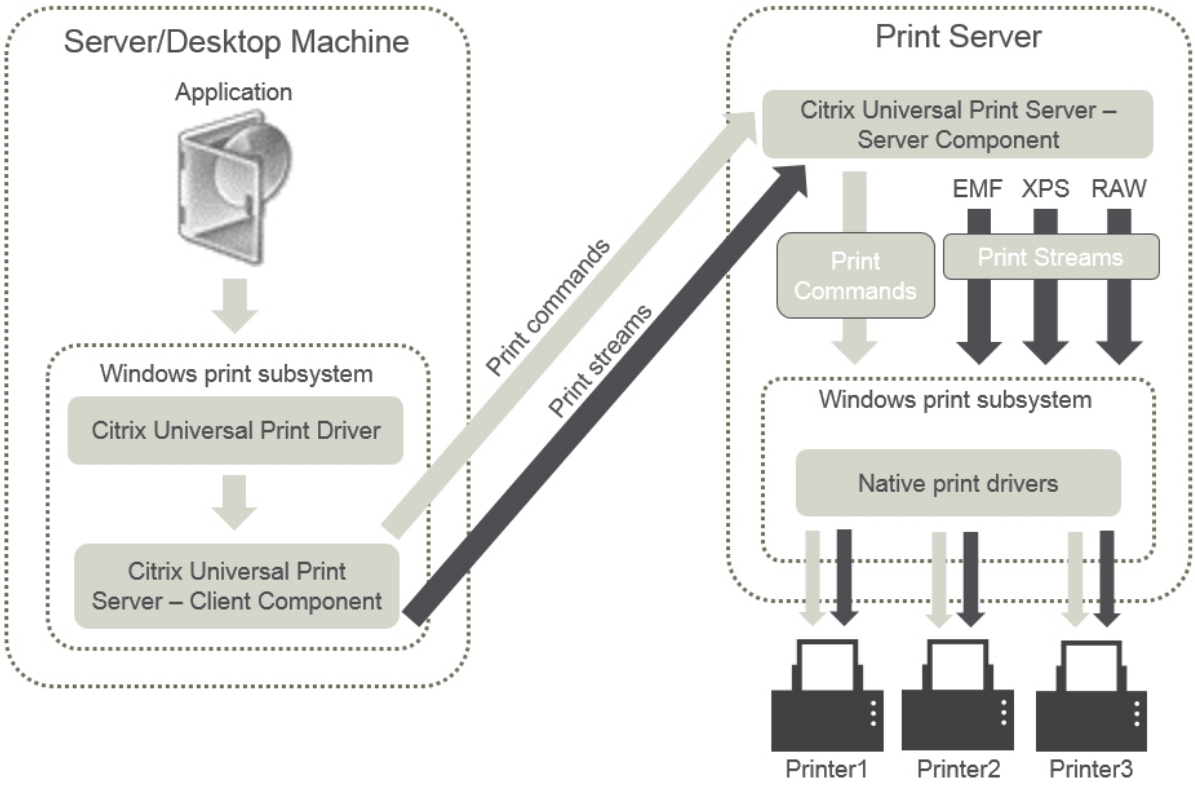
La función de Universal Print Server consta de:

Un componente de cliente, **UPClient** - Habilite UPClient en cada máquina con sistema operativo de servidor que aprovisione las impresoras de red de sesión y use el controlador de impresión universal.

Un componente de servidor, **UPServer** - Instale UPServer en cada servidor de impresión que aprovisiona las impresoras de red de sesión y utiliza el controlador de impresión universal para las impresoras de sesión (independientemente de si las impresoras de sesión están o no aprovisionadas centralmente).

Para obtener información acerca de la instalación y los requisitos de Universal Print Server, consulte los artículos Requisitos del sistema e Instalar.

La siguiente ilustración muestra el flujo de trabajo típico que tiene una impresora de red en un entorno con Universal Print Server.



Al habilitar Citrix Universal Print Server, se aprovechan automáticamente todas las impresoras de red que están conectadas gracias a la detección automática.

> **Nota:**
>
> Universal Print Server también se admite en VDI-in-a-Box 5.3. Para obtener más información acerca de la instalación de Universal Print Server con VDI-in-a-Box, consulte la documentación

© 1999-2019 Citrix Systems, Inc. All rights reserved.

de VDI-in-a-Box.

- **Creación automática** La *Creación automática* hace referencia a las impresoras que se crean automáticamente al comienzo de cada sesión. Se pueden actualizar automáticamente tanto las impresoras de red remotas como las impresoras de cliente conectadas localmente. Considere la posibilidad de crear automáticamente solo la impresora predeterminada del cliente para entornos con un gran número de impresoras por usuario. La creación automática de un número menor de impresoras produce una sobrecarga menor (consume menos memoria y CPU) en máquinas con sistema operativo de servidor. 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 de servidor mediante la configuración de directiva Asignación y compatibilidad de controladores de impresora.

Enrutamiento de trabajos de impresión

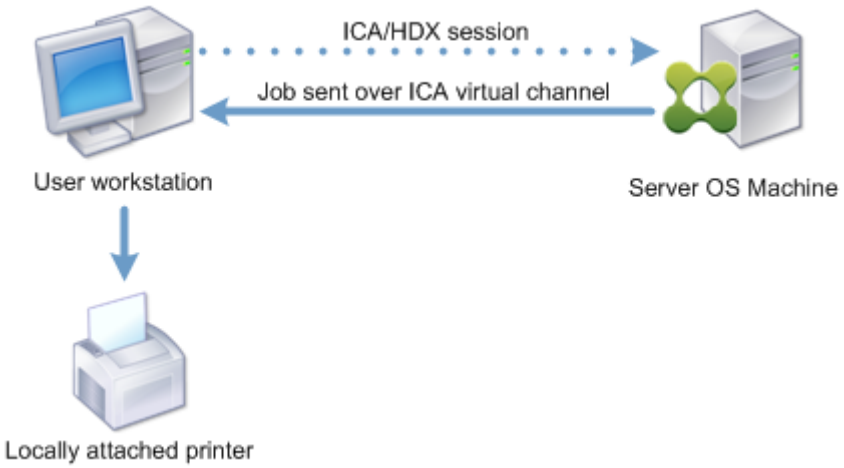
El término ruta de impresión incluye la ruta por la que se enrutan los trabajos de impresión y la ubicación donde se administran dichos trabajos en cola. Ambos aspectos de este concepto son importantes. El enrutamiento afecta al tráfico de red. La administración de la cola de impresión afecta a la utilización 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Impresoras conectadas localmente

El sistema enruta los trabajos a impresoras conectadas localmente desde la máquina de SO de servidor, 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

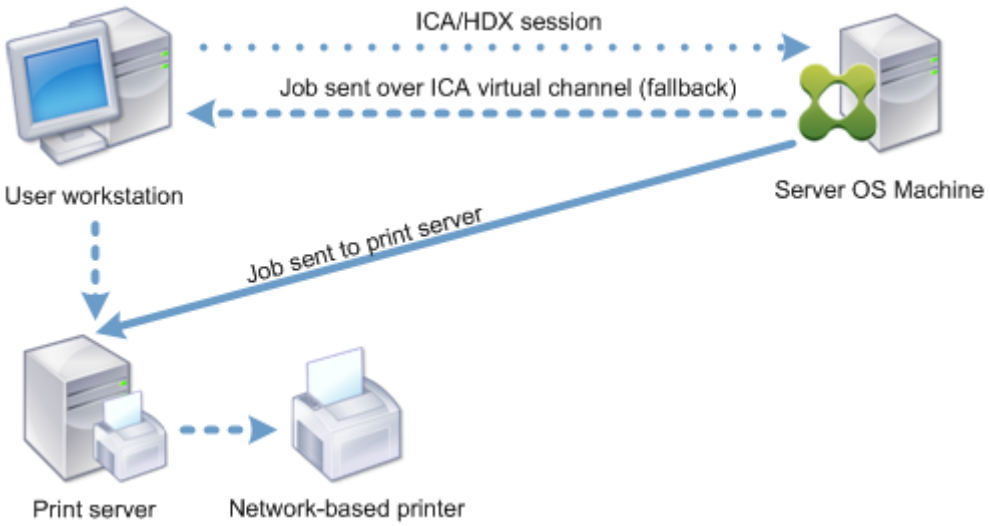
De forma predeterminada, todos los trabajos de impresión destinados a impresoras de red se enrutan desde la máquina con sistema operativo de servidor, pasan por la red y terminan directamente en el servidor de impresión. No obstante, los trabajos de impresión se enrutan automáticamente sobre la conexión 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 de servidor.

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



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 a VDA 7.17 (o una versión posterior respaldada), 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 respalda los siguientes formatos de impresión:

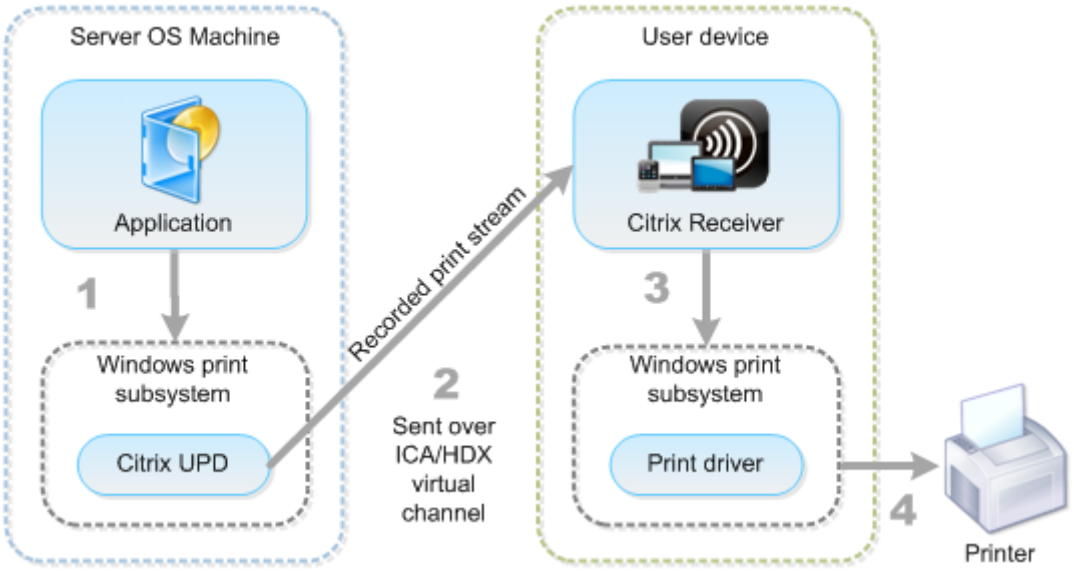
© 1999-2019 Citrix Systems, Inc. All rights reserved.

- 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 características avanzadas de impresión, tales como el grapado y la selección del origen del papel. Estas características 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.

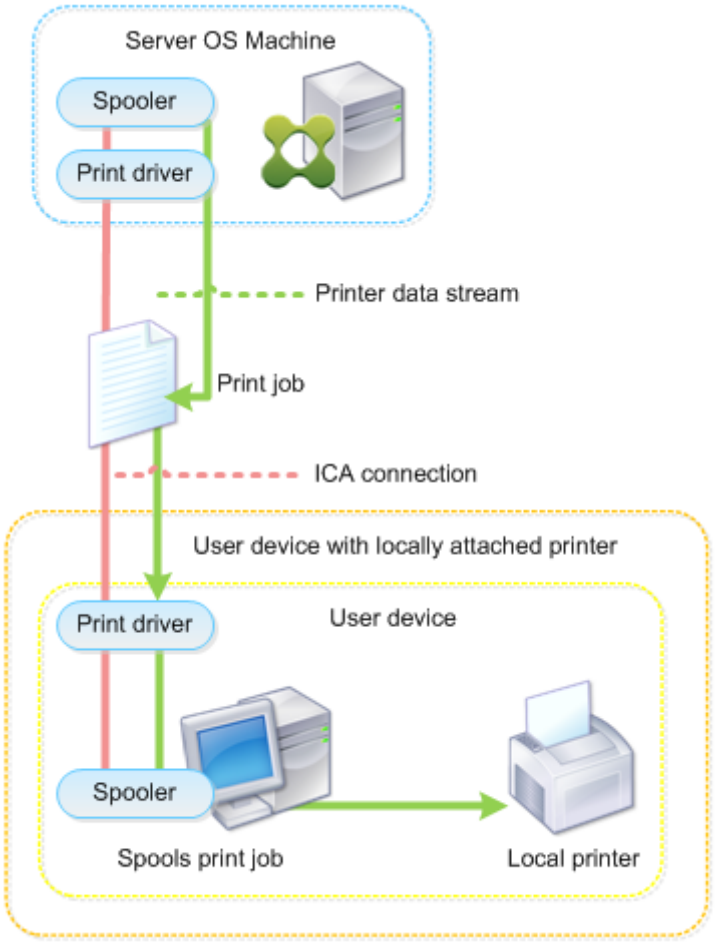


© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 de servidor. 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 de servidor 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 de servidor.
- Si creará o no listas de compatibilidad de controladores.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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

December 4, 2018

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.

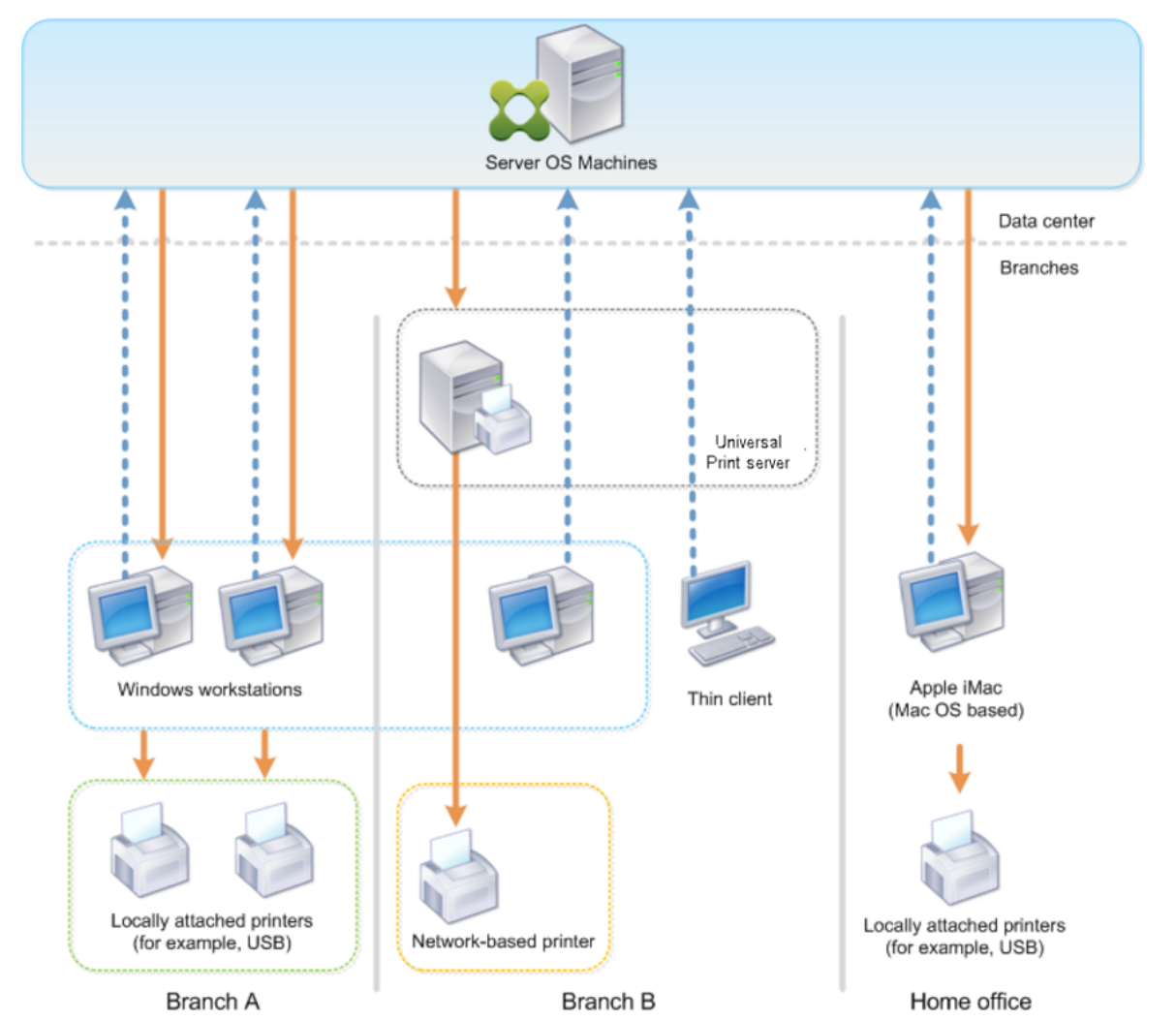
Ejemplo de implementación de impresión

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- 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 de servidor. 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 de servidor 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Prácticas recomendadas, consideraciones de seguridad y operaciones predeterminadas

March 8, 2019

Procedimientos recomendados

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 de servidor.
- 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 termi-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

nación 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 enruta 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 enruta sobre el canal ICA y a través del dispositivo del usuario).
- El sistema enruta todos los trabajos de impresión enviados a la cola de impresoras de red directamente desde máquinas con sistema operativo de servidor. Si el sistema no puede enrutar los trabajos a través de la red, los enruta 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 de servidor.

  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.
- El sistema usa la versión de Windows del controlador de impresora si está disponible en la máquina con sistema operativo de servidor. Si el controlador de impresora no está disponible,

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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

October 3, 2018

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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 de servidor. 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 de servidor.
- **En la máquina con sistema operativo de servidor:** 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 de servidor 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 de servidor.

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

January 29, 2019

Citrix Universal Print Server

Para determinar la mejor solución de impresión para el entorno, tenga en cuenta lo siguiente:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- 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 respaldo de 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 proporciona respaldo 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 de servidor, 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 UpServer 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 Instalar mediante 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 escritorio Windows o SO de servidor Windows.
2. Extraiga el VDA siguiendo las instrucciones de línea de comandos descritas en Instalar mediante 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 modifica el Registro de forma incorrecta, podrían generarse problemas graves que pueden provocar la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

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**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

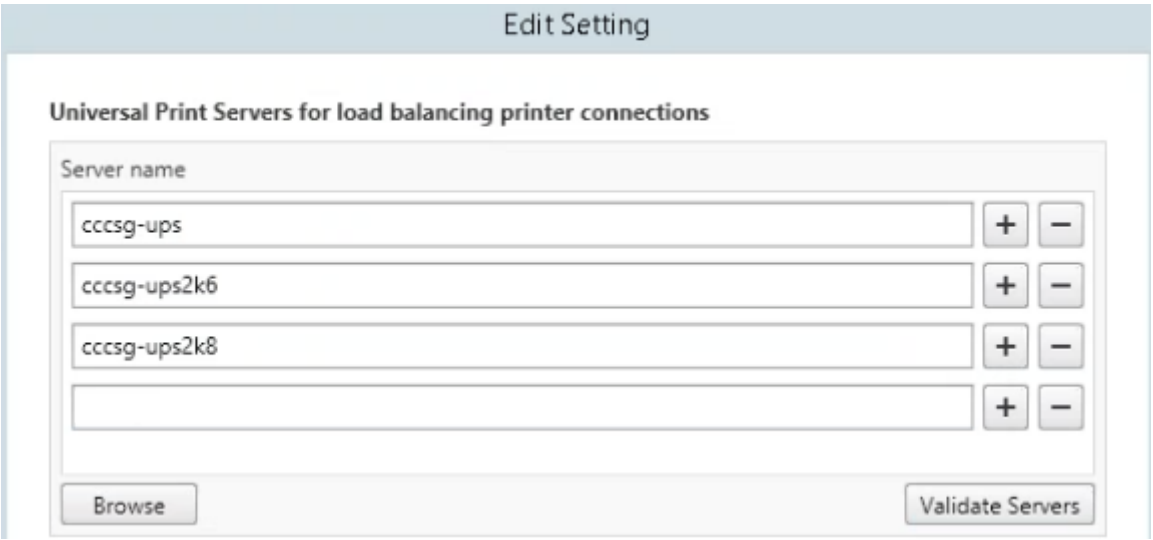
- **Puerto del servicio Web de Universal Print Server (HTTP/SOAP)**. Especifica el número de puerto TCP utilizado por el proceso de escucha de Universal Print Server para solicitudes HTTP/-SOAP entrantes. El valor predeterminado es **8080**.

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:

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 (kpbs)**. 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 usando 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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.

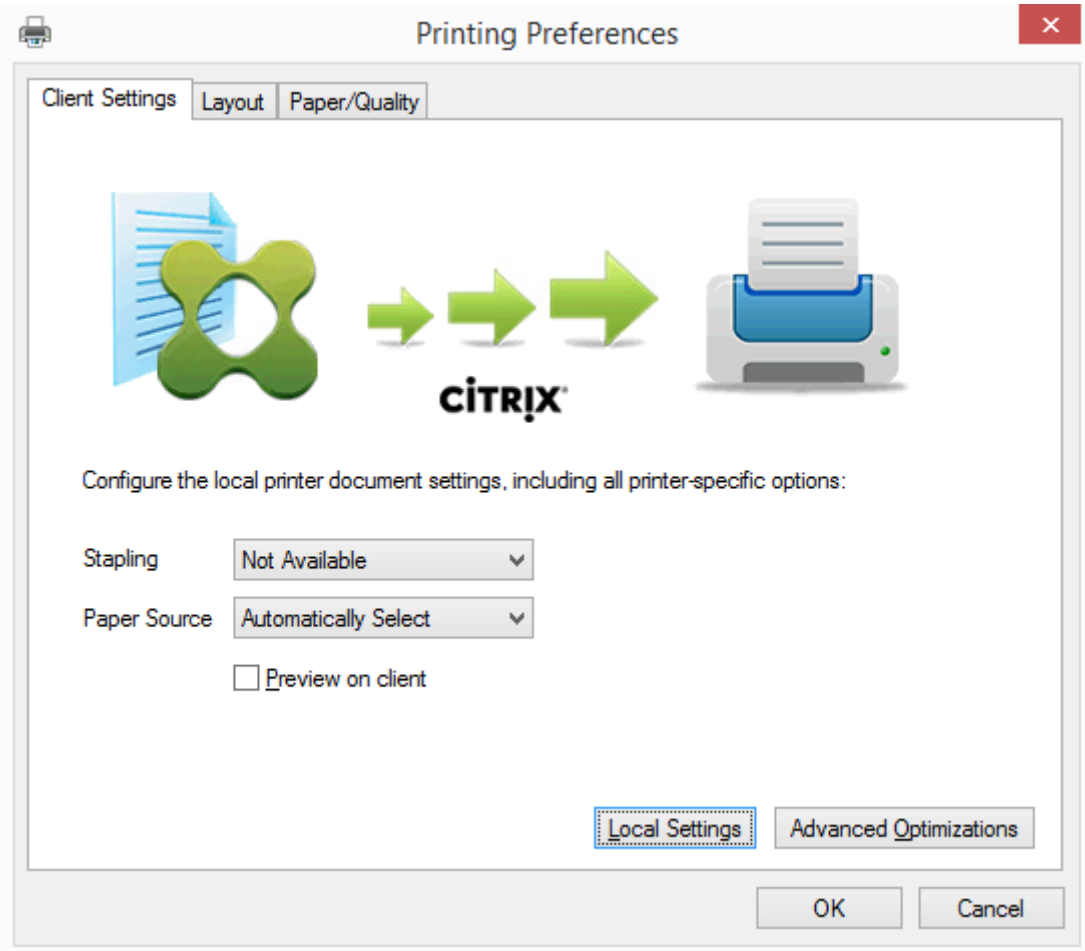
Configuración de directiva	Interacción
Redirección de impresoras del cliente, Crear automáticamente las impresoras del cliente	Después de habilitar Universal Print Server, las impresoras de red del cliente se crean mediante el controlador de impresión universal en lugar de los controladores nativos. 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 características 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



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 características 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 respalda la generación en el lado del cliente.

Para obtener más información acerca de Universal Print Server, consulte CTX200328.

Impresoras del cliente creadas automáticamente

Se suministran estas soluciones de impresión universal para las impresoras cliente:

- **Impresora universal de Citrix**: Una impresora genérica, creada al comienzo de las sesiones, que no está vinculada a ningún dispositivo de impresión. La Impresora universal de Citrix no es necesaria para enumerar las impresoras del cliente disponibles durante el inicio de sesión, lo que puede reducir notablemente el uso de los recursos y el tiempo que tarda en iniciarse la sesión del usuario. La Impresora universal puede imprimir en cualquier dispositivo de impresión del cliente.

  Es posible que la Impresora universal de Citrix no funcione en todos los dispositivos de usuario ni todas las aplicaciones Citrix Workspace de su entorno. La Impresora universal de Citrix requiere un entorno de Windows y no es compatible con Citrix Offline Plug-in o las aplicaciones que se entregan por streaming al cliente. Considere la posibilidad de usar impresoras de cliente creadas automáticamente y el controlador de impresión universal para esos entornos.

  Si quiere usar una solución de impresión universal para las aplicaciones Citrix Workspace que no sean de Windows, use uno de los demás controladores de impresión universal que están basados en PostScript/PCL y se instalan automáticamente.

- **Controladores de impresora universal de Citrix**: Un controlador de impresora universal que es independiente del dispositivo. Si configura el controlador de impresión universal de Citrix, el sistema usa el controlador de impresión universal EMF de forma predeterminada.

  El controlador de impresión universal de Citrix también puede crear trabajos de impresión más pequeños que controladores de impresora anteriores o menos avanzados. No obstante, puede que sea necesario usar el controlador específico del dispositivo para optimizar los trabajos de impresión para la impresora especializada.

Configurar la impresión universal Utilice las siguientes configuraciones de directiva Citrix para configurar la impresión universal. Para obtener más información, consulte la ayuda en pantalla de las configuraciones de directiva.

- Uso de controladores de impresión universal. Especifica cuándo se usa la impresión universal.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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

December 14, 2018

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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 de servidor. 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 de servidor. 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 respalda 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,

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 de servidor, 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 de servidor 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 usando 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 de servidor.

- 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 seguimiento 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

	Ruta de impresión	Ubicación
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 de servidor)	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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> **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.

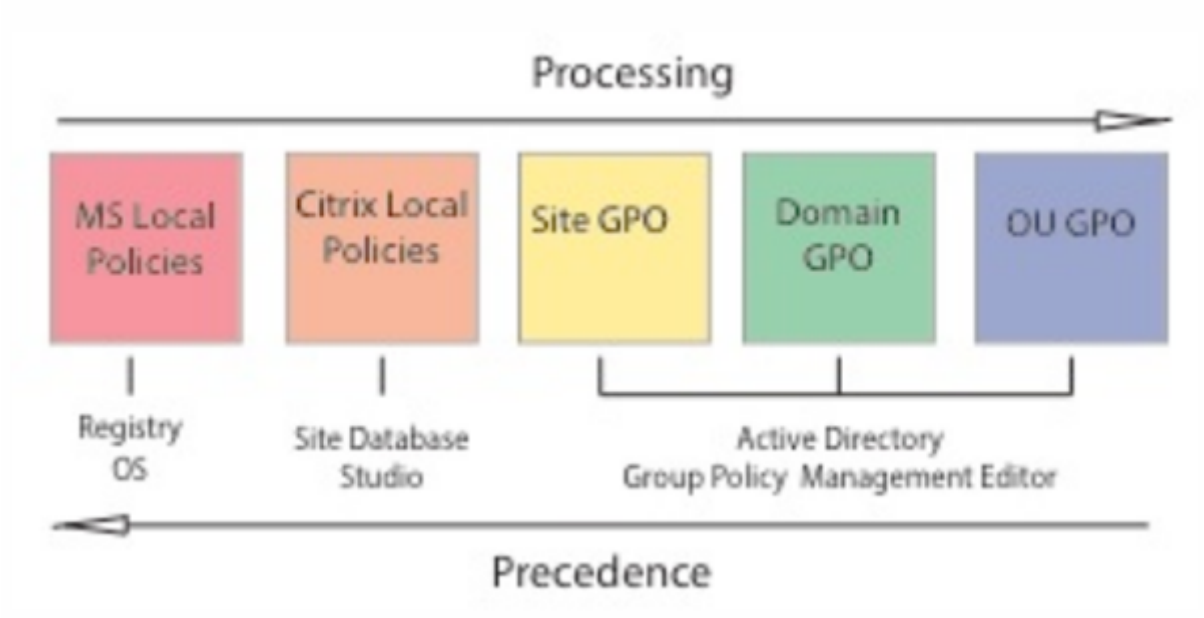
Directivas

December 4, 2018

> **Nota:**
>
> Puede obtener información sobre los cambios en los nombres de producto aquí.

Las directivas son un conjunto de configuraciones que definen la forma en que se administran las sesiones, el ancho de banda y la seguridad para un grupo de usuarios, dispositivos o tipos de conexión.

Puede aplicar configuraciones de directiva a las máquinas físicas y virtuales o a los usuarios. Puede aplicar configuraciones a usuarios individuales a un nivel local, o a grupos de seguridad en Active Directory. Las configuraciones definen criterios y reglas específicos. A menos que se asignen directivas específicamente, las configuraciones se aplican a todas las conexiones.



Puede aplicar las directivas en diferentes niveles de la red. Las configuraciones de directiva colocadas en el nivel de objeto de directiva de grupo (GPO) de unidad organizativa (OU) tienen precedencia en la red. Las directivas a nivel de grupo GPO del dominio anulan las directivas de GPO del sitio que, a su vez, anulan las directivas en conflicto que haya en los niveles de directivas locales de Citrix y de Microsoft.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Todas las directivas locales de Citrix se crean y administran desde la consola de Citrix Studio y se almacenan en la base de datos de configuración del sitio. Las directivas de grupo se crean y administran utilizando la consola Microsoft Management Console (GPMC) y se almacenan en Active Directory. Las Directivas locales de Microsoft se crean en el sistema operativo y se guardan en el Registro de Windows.

Studio usa un asistente de Modelado para ayudar a los administradores a comparar los parámetros de configuración incluidos en las plantillas y las directivas, de modo que puedan eliminar parámetros redundantes o conflictivos. Los administradores pueden configurar objetos de directiva de grupo (GPO) mediante la Consola de administración de directivas de grupo y aplicarlos a un conjunto de usuarios de destino en diferentes niveles de la red.

Estos GPO se guardan en Active Directory, y el acceso a la administración de estas configuraciones, por lo general, está restringido para la mayoría del equipo de TI por motivos de seguridad.

Las configuraciones se fusionan según su condición y prioridad. Una configuración inhabilitada anula una configuración habilitada de menor prioridad. Las configuraciones de directiva sin definir se omiten y no anulan a 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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

December 14, 2018

Configure directivas de Citrix para controlar el acceso de los usuarios y los entornos de sesión. Las directivas de Citrix son el método más eficaz para controlar los parámetros de conexión, seguridad y ancho de banda. Puede crear directivas para grupos de usuarios, dispositivos o tipos de conexión específicos. Cada directiva puede contener varias configuraciones.

Herramientas para trabajar con las directivas de Citrix

Puede utilizar las siguientes herramientas para trabajar con directivas de Citrix.

- **Studio**: Si usted es un administrador Citrix y no tiene permisos para administrar directivas de grupo, utilice Studio para crear directivas para su sitio. Las directivas creadas con Studio se almacenan en la base de datos del sitio y las actualizaciones se envían al escritorio virtual cuando el escritorio virtual se registra con el broker o cuando un usuario se conecta a ese escritorio virtual.
- **Editor de directivas de grupo local** (complemento de Microsoft Management Console): Si su entorno de red utiliza Active Directory y usted tiene permisos para administrar las directivas de grupo, puede usar el Editor de directivas de grupo local para crear directivas para un sitio. Las configuraciones que defina afectarán a los objetos de directiva de grupo (GPO) que especifique en la Consola de administración de directivas de grupo.

> **Importante**
>
> Debe usar el Editor de directivas de grupo local para definir algunas configuraciones de directiva, incluidas las relacionadas con el registro de los VDA en el Controller, y las relacionadas con servidores de Microsoft App-V.

Procesamiento de directivas y precedencia

Las configuraciones de directiva de grupo se procesan en el orden siguiente:

1. GPO locales

© 1999-2019 Citrix Systems, Inc. All rights reserved.

2. GPO del sitio de XenDesktop o XenApp (almacenados en la base de datos del sitio)
3. GPO de sitio
4. GPO de dominio
5. Unidades organizativas

No obstante, en caso de un conflicto, las configuraciones de directiva que se procesan las últimas pueden anular a las procesadas con anterioridad. Esto significa que las configuraciones de directiva toman precedencia en el orden siguiente:

1. Unidades organizativas
2. GPO de dominio
3. GPO de sitio
4. GPO del sitio de XenDesktop o XenApp (almacenados en la base de datos del sitio)
5. GPO locales

Por ejemplo, un administrador de Citrix usa Studio para crear una directiva (directiva A) que habilita la redirección de archivos del cliente para los empleados de ventas de la empresa. Al mismo tiempo, otro administrador usa el Editor de directivas de grupo para crear una directiva (directiva B) que inhabilita la redirección de archivos del cliente para los empleados de ventas. Cuando los empleados de ventas inician sesión en los escritorios virtuales, se aplica la directiva B y la directiva A se omite porque la directiva B se procesó a nivel del dominio y la directiva A se procesa en el nivel de objeto de directiva de grupo de sitio de XenApp o XenDesktop.

No obstante, cuando un usuario inicia una sesión ICA o RDP, la configuración de sesión de Citrix anula la misma configuración definida en una directiva de Active Directory o mediante la Configuración de host de sesión de Escritorio remoto. Esto incluye los parámetros relacionados con la configuración típica de conexión del cliente RDP, como Tapiz del escritorio, Animación de menús y Ver contenido de las ventanas al arrastrar.

Cuando se utilizan varias directivas, puede priorizar las que contienen configuraciones conflictivas; consulte Comparar, priorizar, modelar y solucionar problemas de directivas para obtener más información.

Flujo de trabajo para las directivas de Citrix

El proceso para la configuración de directivas es el siguiente:

1. Cree la directiva.
2. Configure los parámetros de la configuración de directiva.
3. Asigne la directiva a los objetos de usuario y máquina.
4. Dé una prioridad a la directiva.
5. Compruebe que la directiva funciona ejecutando el asistente de Modelado de Directivas de grupo de Citrix.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Explorar las directivas y las configuraciones de Citrix

En el Editor de directivas de grupo local, las directivas y las configuraciones aparecen en dos categorías: Configuración de equipo y Configuración de usuario. Cada categoría tiene un nodo de Directivas de Citrix. Consulte la documentación de Microsoft para obtener más detalles sobre cómo explorar y usar este complemento.

En Studio, las configuraciones de directiva se ordenan en categorías según la funcionalidad o la característica a la que afectan. Por ejemplo, la sección Profile Management contiene las configuraciones de directiva de Profile Management.

- Las configuraciones de equipo (configuraciones de directiva que se aplican a las máquinas) definen el comportamiento de los escritorios virtuales y se aplican cuando se inicia un escritorio virtual. Estas configuraciones se aplican incluso cuando no hay sesiones de usuario activas en el escritorio virtual. Las configuraciones de usuario definen la experiencia del usuario al conectarse mediante ICA. Las directivas de usuario se aplican cada vez que un usuario se conecta o reconecta mediante ICA. Las directivas de usuario no se aplican cuando un usuario se conecta a través de RDP o inicia sesión directamente en la consola.

  Para acceder a las directivas, sus configuraciones y plantillas, seleccione Directivas en el panel de navegación de Studio.

  - La ficha **Directivas** muestra todas las directivas. Cuando se selecciona una directiva, las etiquetas a la derecha muestran: Información general (el nombre, la prioridad, su estado habilitado o inhabilitado y una descripción), Configuraciones (lista de configuraciones definidas) y Asignada a (objetos de usuario y máquina a los que la directiva esté asignada en ese momento). Para obtener más información, consulte Creación de directivas.
  - La ficha **Plantillas** enumera las plantillas suministradas por Citrix y las plantillas que usted haya creado. Cuando se selecciona una plantilla, las fichas a la derecha muestran: Descripción (para qué se puede usar la plantilla) y Configuraciones (lista de configuraciones definidas). Para obtener más información, consulte Plantillas de directiva.
  - La ficha **Comparación** permite comparar las configuraciones de una directiva o de una plantilla con las de otras directivas o plantillas. Por ejemplo, puede que quiera verificar los valores de configuración para asegurar que se cumplen las directrices recomendadas. Para obtener más información, consulte Comparación, prioridad, modelado y solución de problemas de directivas.
  - En la ficha **Modelado**, puede simular escenarios de conexión con directivas de Citrix. Para obtener más información, consulte Comparación, prioridad, modelado y solución de problemas de directivas.

  Para buscar una configuración dentro de una directiva o una plantilla:

  1. Seleccione la directiva o la plantilla.
  2. Seleccione Modificar directiva o Modificar plantilla en el panel Acciones.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

3. En la página Configuraciones, comience a escribir el nombre de la configuración.

Puede limitar la búsqueda si selecciona una versión específica del producto, seleccionando una categoría (por ejemplo, el Ancho de banda) o marcando la casilla Ver solo seleccionadas o eligiendo buscar solo entre las configuraciones que se han agregado a la directiva seleccionada. Para realizar una búsqueda sin filtro, seleccione Todas las configuraciones.

- Para buscar una configuración dentro de una directiva:

1. Seleccione la directiva.
2. Seleccione la ficha Configuraciones y comience a escribir el nombre de la configuración.

Puede limitar la búsqueda mediante la selección de una versión específica del producto o seleccionando una categoría. Para realizar una búsqueda sin filtro, seleccione Todas las configuraciones.

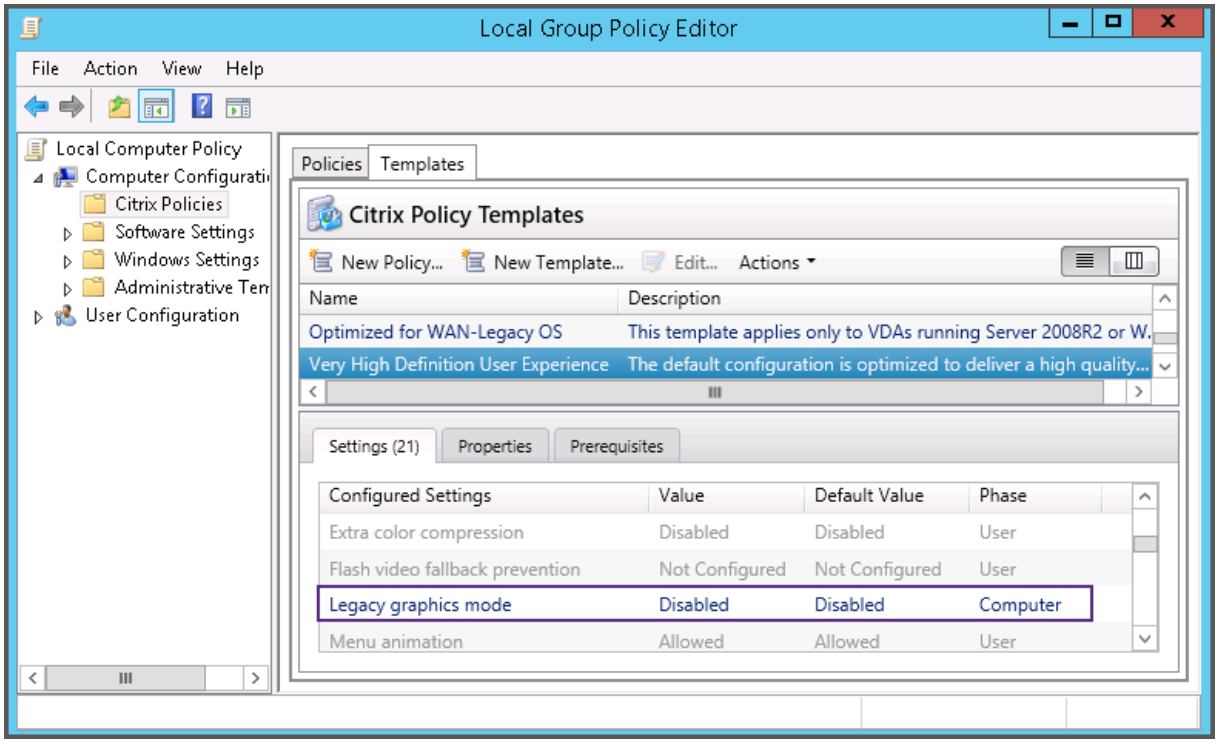
Una vez creada, una directiva es completamente independiente de la plantilla utilizada. Puede usar el campo de descripción de una nueva directiva para realizar un seguimiento de la plantilla de origen utilizada.

En Studio, las directivas y las plantillas se muestran en una única lista, independientemente de si contienen configuraciones de usuario, equipo o ambos, y se pueden aplicar tanto con filtros de usuario como con filtros de equipo.

En el Editor de directivas de grupo, las configuraciones de equipo y de usuario se deben aplicar de forma independiente incluso aunque se hayan creado a partir de una plantilla con los dos tipos de configuración. En este ejemplo, se ha optado por usar una plantilla de experiencia de usuario de definición muy alta en la configuración de equipo:

- El modo de gráficos antiguo es una configuración de equipo que se usará en una directiva creada a partir de esta plantilla.
- Las configuraciones de usuario, en gris, no se usarán en una directiva creada a partir de esta plantilla.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Plantillas de directiva

March 8, 2019

Las plantillas son un punto de partida para la creación de directivas a partir de opciones iniciales predefinidas. Las plantillas integradas de Citrix, optimizadas para condiciones de red o entornos específicos, se pueden utilizar como:

- Un borrador para crear unas directivas y plantillas propias que se compartirán entre diferentes sitios.
- Una referencia para una comparación más fácil de los resultados entre las implementaciones, ya que podrá citar los resultados; por ejemplo, "[…] cuando se usa la plantilla X o Y de Citrix […]".
- Un método para comunicar directivas al servicio de asistencia de Citrix o a terceros de confianza mediante la importación o exportación de plantillas.

Las plantillas de directivas se pueden importar o exportar. Para obtener plantillas adicionales y actualizaciones de las plantillas integradas, consulte CTX202000.

Para conocer los aspectos a tener en cuenta cuando se utilicen plantillas para crear directivas, consulte CTX202330.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

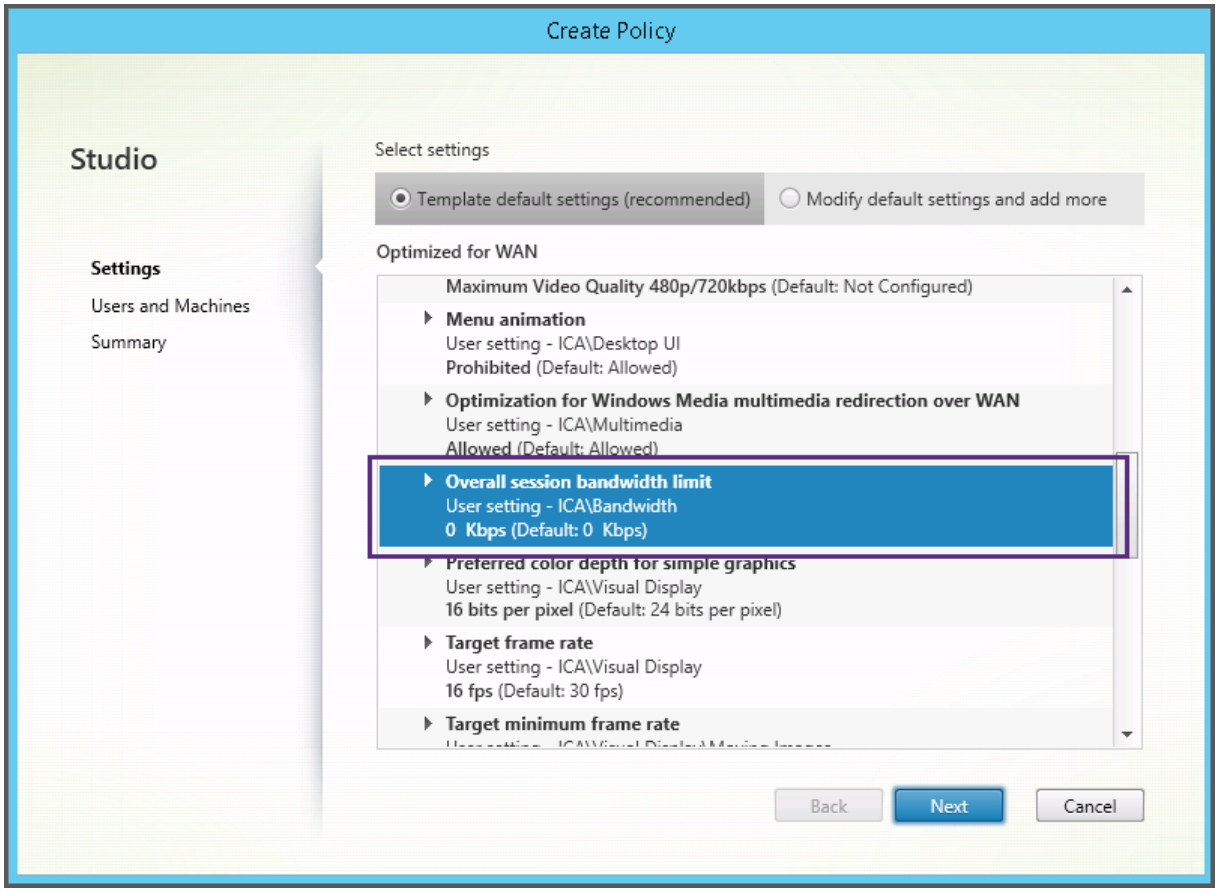
Plantillas integradas de Citrix

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 el 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 XenDesktop 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 con 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 XenApp y XenDesktop. Esta plantilla incluye opciones de configuración que inhabilitarán 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, verá 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 WAN. En este caso, en la plantilla se ofrece la opción de configuración para que el administrador entienda que esta opción se puede aplicar.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Si trabaja con una implementación (administración de directivas y agentes VDA) anteriores 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.

> **Nota**
>
> Citrix crea y actualiza las plantillas integradas. No se puede modificar ni eliminar estas plantillas.

Crear y administrar plantillas mediante Studio

Para crear una nueva plantilla basada a su vez en una plantilla:

1. Seleccione **Directivas** en el panel de navegación de Studio.
2. Haga clic en la ficha **Plantillas** y seleccione la plantilla a partir de la cual creará la nueva.
3. Seleccione **Crear plantilla** en el panel Acciones.
4. Seleccione y configure las configuraciones de directiva que desea incluir en la plantilla. Quite cualquier otra configuración que no desee incluir. Introduzca un nombre para la plantilla.

Después de hacer clic en **Finalizar**, la nueva plantilla aparecerá en la ficha **Plantillas**.

Para crear una nueva plantilla basada en una directiva:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

1. Seleccione **Directivas** en el panel de navegación de Studio.
2. Seleccione la ficha **Directivas** y, a continuación, seleccione la directiva a partir de la cual desea crear la nueva plantilla.
3. Seleccione **Guardar como plantilla** en el panel Acciones.
4. Seleccione y defina las configuraciones de directiva que desea incluir en la plantilla. Quite cualquier otra configuración que no desee incluir. Introduzca un nombre y una descripción para la nueva plantilla y haga clic en **Finalizar**.

Para importar una plantilla:

1. Seleccione **Directivas** en el panel de navegación de Studio.
2. Seleccione la ficha **Plantillas** y seleccione **Importar plantilla**.
3. Seleccione el archivo de plantilla a importar y, a continuación, haga clic en **Abrir**. Si importa una plantilla que se llama igual que otra plantilla existente, puede elegir entre sobrescribir esta última o guardar la plantilla importada con otro nombre generado automáticamente.

Para exportar una plantilla:

1. Seleccione **Directivas** en el panel de navegación de Studio.
2. Seleccione la ficha **Plantillas** y seleccione **Exportar plantilla**.
3. Seleccione la ubicación donde desea guardar la plantilla y haga clic en **Guardar**.

Se creará un archivo .gpt en la ubicación especificada.

Crear y administrar plantillas mediante el Editor de directivas de grupo

En el Editor de directivas de grupo, expanda Configuración del equipo o Configuración de usuario. Expanda el nodo Directivas y seleccione Directivas de Citrix. Elija la acción adecuada.

Tarea	Instrucción
Crear una nueva plantilla a partir de una directiva existente	En la ficha Directivas, seleccione la directiva y, a continuación, seleccione Acciones> Guardar como plantilla.
Crear una directiva a partir de una plantilla existente	En la ficha Plantillas, seleccione la plantilla y, a continuación, haga clic en Nueva directiva.
Crear una nueva plantilla a partir de una plantilla existente	En la ficha Plantillas, seleccione la plantilla y, a continuación, haga clic en Nueva plantilla.
Importar una plantilla	En la ficha Plantillas, seleccione Acciones > Importar.
Exportar una plantilla	En la ficha Plantillas, seleccione Acciones > Exportar.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Tarea	Instrucción
Ver la configuración de la plantilla	En la ficha Plantillas, seleccione la plantilla y, a continuación, haga clic en la ficha Configuraciones.
Ver un resumen de las propiedades de la plantilla	En la ficha Plantillas, seleccione la plantilla y, a continuación, haga clic en la ficha Propiedades.
Ver requisitos previos de la plantilla	En la ficha Plantillas, seleccione la plantilla y, a continuación, haga clic en la ficha Requisitos previos.

Plantillas y administración delegada

Las plantillas de directiva se almacenan en la máquina donde se ha instalado el paquete de administración de directivas. Esta máquina es la máquina de Delivery Controller o la máquina de administración de objetos de directiva de grupo, ni la base de datos del sitio de XenApp y XenDesktop. Esto significa que los archivos de plantilla de directiva se controlan mediante permisos administrativos de Windows en lugar de los roles y los ámbitos de la administración delegada del sitio.

Como resultado, un administrador con permisos de solo lectura en el sitio puede, por ejemplo, crear plantillas nuevas. Sin embargo, debido a que las plantillas son archivos locales, no se realiza ningún cambio real en el entorno.

Las plantillas personalizadas solo están visibles para la cuenta de usuario que las crea y se guardan en el perfil de usuario de Windows. Para dar mayor visibilidad a una plantilla personalizada, cree una directiva a partir de ella o expórtela a una ubicación compartida.

Crear directivas

January 29, 2019

Antes de crear una directiva, decida a qué grupo de usuarios o dispositivos debe afectar. Puede crear una directiva según las funciones laborales del usuario, el tipo de conexión, el dispositivo de usuario o la ubicación geográfica. De forma alternativa, puede utilizar los mismos criterios que utiliza para las directivas de grupo de Active Directory de Windows.

Si ya creó una directiva aplicable a un grupo, considere la posibilidad de modificar dicha directiva para agregarle las configuraciones apropiadas, en lugar de crear otra directiva nueva. Evite la creación

© 1999-2019 Citrix Systems, Inc. All rights reserved.

de una directiva nueva exclusivamente para habilitar una configuración específica o para excluir la aplicación de la directiva a determinados usuarios.

Al crear una nueva directiva, puede basarla en las configuraciones de una plantilla de directiva y personalizarlas según sea necesario, o puede crearla sin usar plantilla y agregar las configuraciones que necesite.

En Citrix Studio, las nuevas directivas creadas se establecen como inhabilitadas a menos que se marque explícitamente la casilla Habilitar directiva.

Configuraciones de directiva

Las configuraciones de directiva pueden estar habilitadas, inhabilitadas o sin configurar. De forma predeterminada, las configuraciones de directiva no están definidas; es decir, que no están agregadas a una directiva. La configuración solamente puede aplicarse cuando se agrega a una directiva.

Algunas configuraciones de directiva pueden tener uno de los siguientes estados:

- Permitida o Prohibida, permite o impide la acción controlada por la configuración. En algunos casos, se permite o se impide que los usuarios administren la acción de la configuración en la sesión. Por ejemplo, si se define la configuración Animación de menús como Permitida, los usuarios pueden controlar las animaciones de los menús en su entorno de cliente.
- Habilitada o Inhabilitada, habilita o inhabilita la configuración. Si se inhabilita una configuración, no se habilita en ninguna directiva de menor prioridad.

Asimismo, algunas configuraciones controlan la eficacia de otras configuraciones dependientes. Por ejemplo, la configuración Redirección de unidades del cliente controla si los usuarios pueden acceder a las unidades de sus dispositivos. Para permitir que los usuarios accedan a sus unidades de red, es necesario agregar tanto esta configuración como la configuración Unidades de red del cliente a la directiva. Si la configuración Redirección de unidades del cliente está inhabilitada, los usuarios no pueden acceder a sus unidades de red aunque la configuración Unidades de red del cliente esté habilitada.

En general, los cambios de configuraciones de directiva que afectan a máquinas surten efecto cuando se reinicia el escritorio virtual o cuando un usuario inicia una sesión. Los cambios de configuraciones de directiva que afectan a usuarios surten efecto la próxima vez que el usuario inicia una sesión. Si se utiliza Active Directory, las configuraciones de directiva se actualizan cuando Active Directory vuelve a evaluar las directivas en intervalos regulares de 90 minutos y se aplican cuando se reinicia el escritorio virtual o cuando un usuario inicia sesión.

Para algunas configuraciones de directiva, puede especificar o seleccionar un valor cuando se las agrega a una directiva. Puede limitar la configuración de un determinado parámetro seleccionando Usar el valor predeterminado; esta opción impide configurar el parámetro y permite usar solo el valor

© 1999-2019 Citrix Systems, Inc. All rights reserved.

predeterminado al aplicar la configuración de directiva, independientemente del valor que se hubiera introducido antes de seleccionar Usar el valor predeterminado.

Recomendaciones:

- Asigne las directivas a grupos y no a usuarios individuales. Si asigna directivas a un grupo, las asignaciones se actualizan automáticamente cuando se agregan o se quitan usuarios.
- No habilite configuraciones que puedan entrar en conflicto o que se superpongan en Configuración de host de sesión de Escritorio remoto. En algunos casos, Configuración de host de sesión de Escritorio remoto ofrece funciones similares a las configuraciones de directiva de Citrix. Siempre que sea posible, mantenga la consistencia entre todas las configuraciones (habilitadas o inhabilitadas) para facilitar la solución de problemas.
- Inhabilite las directivas que no use. Las directivas sin configuración generan una actividad de procesamiento innecesaria.

Asignaciones de directiva

Al crear una directiva, hay que asignarla a ciertos objetos de usuario y máquina; dicha directiva se aplica a las conexiones según criterios o reglas específicos. Por lo general, es posible agregar tantas asignaciones como se desee a una directiva, según una combinación de criterios. Si no se especifica ninguna asignación, la directiva se aplica a todas las conexiones.

En la siguiente tabla se muestran las asignaciones disponibles:

Nombre de asignación	Aplica una directiva según
Control de acceso	Condiciones de control de acceso del cliente. *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.
Citrix CloudBridge	Indica si la sesión del usuario se inicia a través de Citrix CloudBridge. Nota: Puede agregar solo una asignación de Citrix CloudBridge a una directiva.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre de asignación	Aplica una directiva según
Dirección IP del cliente	Dirección IP del dispositivo del usuario, utilizado para conectarse a la sesión. Ejemplos de IPv4: 12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24. Ejemplos de IPv6: 2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54
Nombre del cliente	Nombre del dispositivo de usuario. Coincidencia exacta: ClientABCName. Uso de comodines: Client*Name.
Grupo de entrega	Pertenencia a un grupo de entrega.
Tipo de grupo de entrega	Tipo de escritorio o aplicación: escritorio privado, escritorio compartido, aplicación privada o aplicación compartida.
Unidad organizativa (UO)	Unidad organizativa.
Etiqueta	Etiquetas. **Nota:** Para que las directivas se apliquen correctamente cuando utilice etiquetas, instale la revisión hotfix disponible en CTX142439.
Usuario o grupo	Nombre de usuario o grupo.

Cuando un usuario inicia sesión, se identifican todas las directivas que coinciden con las asignaciones para la conexión. Las directivas se ordenan por prioridad y se comparan varias instancias de cualquier configuración. Cada configuración se aplica según la clasificación de prioridades de la directiva. Toda configuración de directiva que esté inhabilitada prevalece sobre las configuraciones habilitadas de menor prioridad. Las configuraciones de directiva que no están configuradas se ignoran.

Importante: Si configura las directivas de Active Directory y Citrix mediante la Consola de administración de directivas de grupo, es posible que las asignaciones y las configuraciones no se apliquen de la forma esperada. Para obtener más información, consulte CTX127461.

De forma predeterminada se proporciona una directiva “Sin filtro”.

- Si utiliza Studio para administrar las directivas de Citrix, las configuraciones que agregue a la directiva sin filtro se aplican a todos los servidores, escritorios y conexiones de un sitio.
- Si utiliza el Editor de directivas de grupo local para administrar las directivas de Citrix, las configuraciones que se agreguen a la directiva sin filtro se aplican a todos los sitios y conexiones que abarquen los objetos de directiva de grupo (GPO) que contienen la directiva. Por ejemplo,

© 1999-2019 Citrix Systems, Inc. All rights reserved.

la unidad organizativa Ventas contiene un GPO denominado Ventas-EE. UU. que incluye a todos los miembros del equipo de ventas de los Estados Unidos. El GPO Ventas-EE. UU. tiene configurada una directiva sin filtro que incluye varias configuraciones de directiva de usuario. Cuando el administrador de Ventas-EE. UU. inicia sesión en el sitio, la configuración de la directiva sin filtro se aplica automáticamente a la sesión, ya que el usuario es miembro del GPO Ventas-EE. UU.

El modo de una asignación determina si la directiva se aplica exclusivamente a las conexiones que coinciden con todos los criterios de la asignación. Si el modo está establecido en Permitir (Allow) (valor predeterminado), la directiva se aplica solamente a las conexiones que coinciden con los criterios de la asignación. Si el modo está establecido en Denegar (Deny), la directiva se aplica si la conexión no coincide con las asignaciones del filtro. Los siguientes ejemplos ilustran cómo los modos de las asignaciones afectan a las directivas de Citrix cuando hay varias asignaciones.

- **Ejemplo: Asignaciones del mismo tipo en modos distintos:** En las directivas con dos asignaciones del mismo tipo, donde una está establecida en Permitir y la otra en Denegar, la asignación establecida en Denegar tiene precedencia, siempre que la conexión satisfaga ambas asignaciones. Por ejemplo:

  La directiva 1 incluye las siguientes asignaciones:

  - La asignación A especifica el grupo Ventas, con el modo Permitir
  - La asignación B especifica la cuenta del jefe de Ventas, con el modo Denegar

  Como el modo de la asignación B es Denegar, no se aplica la directiva cuando el jefe de Ventas inicia sesión en el sitio, aunque este usuario sea miembro del grupo Ventas.

- **Ejemplo: Asignaciones de diferentes tipos con modos iguales:** En las directivas con dos o más asignaciones de diferentes tipos, establecidas en Permitir, la conexión debe satisfacer al menos una asignación de cada tipo para que se aplique la directiva. Por ejemplo:

  La directiva 2 incluye las siguientes asignaciones:

  - La asignación C es una asignación de usuario que especifica el grupo Ventas con el modo Permitir
  - La asignación D es una asignación de dirección IP del cliente que especifica 10.8.169.* (la red de la empresa) con el modo Permitir

  Cuando el jefe de Ventas inicia sesión en el sitio desde la oficina, se aplica la directiva, ya que la conexión satisface ambas asignaciones.

  La directiva 3 incluye las siguientes asignaciones:

  - La asignación E es una asignación de usuario que especifica el grupo Ventas con el modo Permitir
  - La asignación F es una asignación de control de acceso que especifica condiciones de conexión de NetScaler Gateway con el modo Permitir

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Cuando el jefe de Ventas inicia sesión en el sitio desde la oficina, no se aplica la directiva, ya que la conexión no satisface la asignación F.

Crear una directiva basada en una plantilla mediante Studio

1. Seleccione Directivas en el panel de navegación de Studio.
2. Seleccione la ficha Plantillas y seleccione la plantilla.
3. Seleccione Crear directiva con una plantilla en el panel Acciones.
4. De forma predeterminada, la nueva directiva utiliza todos los valores de configuración predeterminados en la plantilla (el botón Usar configuraciones de plantilla está seleccionado). Si quiere cambiar configuraciones, seleccione Modificar y agregar más configuraciones predeterminadas y, a continuación, agregue o quite configuraciones.
5. Especifique cómo se aplica la directiva, seleccionando una de las siguientes opciones:
   - Asignar a objetos de usuario y máquina seleccionados; a continuación, elija los objetos de usuario y máquina a los que aplicar la directiva.
   - Asignar a Todos los objetos del sitio, para aplicar la directiva a todos los objetos de usuario y máquina en el sitio.
6. Introduzca un nombre para la directiva (o acepte el predeterminado). Conviene que el nombre dado a la directiva esté basado en a quién o a qué afecta; por ejemplo, “Departamento de Contabilidad” o “Usuarios remotos”. Si lo desea, puede proporcionar una descripción.

   La directiva está habilitada de forma predeterminada; se puede inhabilitar. Si la directiva está habilitada, se aplica de inmediato a los usuarios que inician sesión en el sitio. Si se inhabilita, la directiva no se aplica. Si necesita establecer la prioridad de una directiva o agregar configuraciones en otro momento, puede inhabilitar la directiva hasta que esté listo para aplicarla.

Crear una directiva basada en una plantilla mediante Studio

1. Seleccione Directivas en el panel de navegación de Studio.
2. Seleccione la ficha Plantillas y seleccione la plantilla.
3. Seleccione Crear directiva con una plantilla en el panel Acciones.
4. De forma predeterminada, la nueva directiva utiliza todos los valores de configuración predeterminados en la plantilla (el botón Usar configuraciones de plantilla está seleccionado). Si quiere cambiar configuraciones, seleccione Modificar y agregar más configuraciones predeterminadas y, a continuación, agregue o quite configuraciones.
5. Especifique cómo se aplica la directiva, seleccionando una de las siguientes opciones:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Asignar a objetos de usuario y máquina seleccionados; a continuación, elija los objetos de usuario y máquina a los que aplicar la directiva.
- Asignar a Todos los objetos del sitio, para aplicar la directiva a todos los objetos de usuario y máquina en el sitio.

6. Introduzca un nombre para la directiva (o acepte el predeterminado). Conviene que el nombre dado a la directiva esté basado en a quién o a qué afecta; por ejemplo, "Departamento de Contabilidad" o "Usuarios remotos". Si lo desea, puede proporcionar una descripción.

   La directiva está habilitada de forma predeterminada; se puede inhabilitar. Si la directiva está habilitada, se aplica de inmediato a los usuarios que inician sesión en el sitio. Si se inhabilita, la directiva no se aplica. Si necesita establecer la prioridad de una directiva o agregar configuraciones en otro momento, puede inhabilitar la directiva hasta que esté listo para aplicarla.

Crear una directiva mediante Studio

1. Seleccione Directivas en el panel de navegación de Studio.
2. Seleccione la ficha Directivas.
3. Seleccione Crear directiva en el panel Acciones.
4. Agregue y defina configuraciones de directiva.
5. Especifique cómo quiere aplicar la directiva, seleccionando una de las siguientes opciones:

   - Asignar a objetos de usuario y máquina seleccionados; a continuación, elija los objetos de usuario y máquina a los que aplicar la directiva.
   - Asignar a Todos los objetos del sitio, para aplicar la directiva a todos los objetos de usuario y máquina en el sitio.

6. Introduzca un nombre para la directiva (o acepte el predeterminado). Conviene que el nombre dado a la directiva esté basado en a quién o a qué afecta; por ejemplo, "Departamento de Contabilidad" o "Usuarios remotos". Si lo desea, puede proporcionar una descripción.

   La directiva está habilitada de forma predeterminada; se puede inhabilitar. Si la directiva está habilitada, se aplica de inmediato a los usuarios que inician sesión en el sitio. Si se inhabilita, la directiva no se aplica. Si necesita establecer la prioridad de una directiva o agregar configuraciones en otro momento, puede inhabilitar la directiva hasta que esté listo para aplicarla.

Crear y administrar directivas con el Editor de directivas de grupo

En el Editor de directivas de grupo, expanda Configuración del equipo o Configuración de usuario. Expanda el nodo Directivas y seleccione Directivas de Citrix. Elija la acción adecuada.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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.
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.

Comparar, priorizar, modelar y solucionar problemas de directivas

October 3, 2018

Puede utilizar varias directivas para personalizar el entorno y responder a las necesidades de los usuarios según su función laboral, su ubicación geográfica o su tipo de conexión. Por ejemplo, es posible que, por motivos de seguridad, deba establecer restricciones en los grupos de usuarios que trabajan regularmente con datos confidenciales. Puede crear una directiva para evitar que los usuarios guarden archivos con información confidencial en sus unidades de cliente locales. No obstante, si algunos de los miembros del grupo de usuarios necesitan acceder a las unidades locales, puede crear otra directiva para permitirles el acceso a esos usuarios en particular. A continuación, puede clasificar y dar prioridad a las dos directivas para establecer cuál de ellas tiene preferencia.

Cuando se utilizan varias directivas, debe determinar cuál es su prioridad, cómo crear las excepciones y cómo ver la directiva vigente cuando hay un conflicto de directivas.

En general, las directivas anulan configuraciones similares definidas para todo el sitio, para Delivery Controllers específicos o en el dispositivo del usuario. La excepción a este principio es la seguridad. La

© 1999-2019 Citrix Systems, Inc. All rights reserved.

configuración de cifrado más exigente en su entorno, incluidos el sistema operativo y la configuración de remedo más restrictiva, siempre anulan otras configuraciones y directivas.

Las directivas de Citrix interactúan con directivas configuradas en su sistema operativo. En un entorno de Citrix, los parámetros de Citrix sobrescriben los parámetros similares configurados en una directiva de Active Directory o mediante Configuración de host de sesión de Escritorio remoto. Esto incluye las configuraciones relacionadas con la configuración típica de conexión del cliente del Protocolo de escritorio remoto (RDP), como Tapiz del escritorio, Animación de menús y Ver contenido de las ventanas al arrastrar. En el caso de algunas configuraciones de directiva, como Secure ICA, la configuración de las directivas debe coincidir con la configuración del sistema operativo. Si se configura un nivel de cifrado de mayor prioridad en otro lugar, la configuración de directiva Secure ICA que especifique en la directiva o al entregar una aplicación o un escritorio puede anularse.

Por ejemplo, los parámetros de cifrado especificados al crear grupos de entrega deben estar al mismo nivel que los parámetros de cifrado especificados en todo el entorno.

Nota: En el segundo salto de los casos de doble salto, cuando un VDA de SO de escritorio se conecta a un VDA de SO de servidor, las directivas de Citrix actúan en el VDA de SO de escritorio como si fuera el dispositivo del usuario. Por ejemplo, si las directivas están configuradas para guardar imágenes en caché en el dispositivo del usuario, las imágenes guardadas en el segundo salto del escenario de doble salto se guardan en caché en la máquina VDA de SO de escritorio.

Comparar directivas y plantillas

Puede comparar las configuraciones de una directiva o de una plantilla con las de otras directivas o plantillas. Por ejemplo, puede que necesite verificar los valores de configuración para asegurar que se cumplen las directrices recomendadas. También puede comparar las configuraciones de una directiva o plantilla con las configuraciones predeterminadas proporcionadas por Citrix.

1. Seleccione Directivas en el panel de navegación de Studio.
2. Haga clic en la ficha Comparación y, a continuación, haga clic en Seleccionar.
3. Seleccione las directivas o plantillas que desea comparar. Para incluir los valores predeterminados en la comparación, marque la casilla Comparar con la configuración predeterminada.
4. Haga clic en Comparar, las configuraciones definidas se mostrarán en columnas.
5. Para ver todas las configuraciones, seleccione Mostrar todas las configuraciones. Para volver a la vista predeterminada, seleccione Mostrar configuraciones en común.

Priorizar directivas

La asignación de prioridades en las directivas le permite definir la prioridad de las directivas cuando contienen configuraciones conflictivas. Cuando un usuario inicia sesión, se identifican todas las directivas que coinciden con las asignaciones para la conexión. Las directivas se ordenan por prioridad

© 1999-2019 Citrix Systems, Inc. All rights reserved.

y se comparan varias instancias de cualquier configuración. Cada configuración se aplica según la clasificación de prioridades de la directiva.

Usted asigna la prioridad de las directivas asignándoles diferentes números de prioridad en Studio. De forma predeterminada, las nuevas directivas tienen la prioridad más baja. Si hay conflictos en la configuración de las directivas, las directivas de mayor prioridad (el número de prioridad 1 es el máximo) anulan las de menor prioridad. Las configuraciones se combinan según su prioridad y su condición (por ejemplo, si la configuración está habilitada o inhabilitada). Una configuración inhabilitada anula otra configuración de menor prioridad que esté habilitada. Las configuraciones de directiva que no estén configuradas se omiten y no anulan ninguna configuración de menor prioridad.

1. Seleccione Directivas en el panel de navegación de Studio. Asegúrese de que la ficha Directivas está seleccionada.
2. Seleccione una directiva.
3. Seleccione Prioridad baja o Prioridad alta en el panel Acciones.

Excepciones

Al crear directivas para grupos de usuarios, dispositivos de usuario o máquinas, es posible que deba crear excepciones en alguna configuración de directiva para determinados miembros del grupo. Para crear excepciones, debe:

- Crear una directiva exclusiva para los miembros del grupo que necesitan las excepciones y luego dar mayor prioridad a esta directiva que a la directiva de la totalidad del grupo.
- Usar el modo Denegar para una asignación agregada a la directiva

Una asignación con el modo Denegar aplica una directiva solo a las conexiones que no coinciden con los criterios de asignación. Por ejemplo, una directiva contiene las siguientes asignaciones:

- La asignación A es una asignación de dirección IP del cliente que especifica el intervalo 208.77.88.* con el modo Permitir
- La asignación B es una asignación de usuario que especifica una cuenta de usuario determinada con el modo Denegar

La directiva se aplica a todos los usuarios que inician sesión en el sitio con las direcciones IP incluidas en el intervalo indicado en la asignación A. Sin embargo, la directiva no se aplica al usuario que inicia sesión en el sitio con la cuenta especificada en la asignación B, aunque al equipo del usuario tenga una dirección IP que se encuentre en el intervalo especificado en la asignación A.

Determinar las directivas que se aplican a una conexión

En ocasiones, una conexión no responde según lo previsto debido a que se aplican varias directivas. Si se aplica una directiva de mayor prioridad a una conexión, esta puede anular la configuración definida

© 1999-2019 Citrix Systems, Inc. All rights reserved.

en la directiva original. Es posible determinar cómo se combinan las configuraciones de directiva finales para una conexión mediante el cálculo del Conjunto resultante de directivas o RSOP (Resultant Set of Policies).

El Conjunto resultante de directivas se puede calcular de diversas maneras:

- Usando el asistente de Modelado de Directivas de grupo Citrix para simular un caso de conexión y observar la forma en que se aplicarían las directivas de Citrix. Puede especificar condiciones para un caso de conexión, por ejemplo, un controlador de dominio, usuarios, valores de evidencia de asignaciones de directiva de Citrix y parámetros de entorno simulados, como una conexión de red lenta. El informe generado por el asistente incluye una lista de las directivas de Citrix que se aplicarían en el caso especificado. Si está conectado a Controller como un usuario del dominio, el asistente calcula el conjunto resultante de directivas usando tanto la configuración de directivas del sitio como los objetos de directiva de grupo (GPO) de Active Directory.
- Use los Resultados de directivas de grupo para obtener un informe donde se describen las directivas de Citrix vigentes para un usuario o un Controller específico. La herramienta Resultados de directivas de grupo ayuda a evaluar el estado actual de los GPO en el entorno y genera un informe donde se describe la forma en que se aplican estos objetos, incluidas las directivas de Citrix, a un usuario y un Controller específicos.

Puede iniciar el asistente de Modelado de Directivas de grupo Citrix desde el panel Acciones de Studio. Puede ejecutar cualquiera de las dos herramientas desde la Consola de administración de directivas de grupo de Windows.

Si ejecuta el asistente de Modelado de Directivas de grupo Citrix o la herramienta Resultados de directivas de grupo desde la Consola de administración de directivas de grupo, no se incluyen las configuraciones de directiva del sitio creadas con Studio en el grupo de directivas resultante.

Para asegurarse de obtener el grupo de directivas resultante más completo, Citrix recomienda iniciar el asistente de Modelado de Directivas de grupo Citrix desde Studio, a menos que cree las directivas usando solo la Consola de administración de directivas de grupo.

Usar el Asistente de modelado de directivas de grupo Citrix

Abra el Asistente de modelado de directivas de grupo Citrix mediante uno de los procedimientos siguientes:

- Seleccione Directivas en el panel de navegación de Studio, seleccione la ficha Modelado y, a continuación, seleccione Iniciar asistente de modelado en el panel Acciones.
- Abra la Consola de administración de directivas de grupo (gpmc.msc), haga clic con el botón secundario en el nodo Modelado de Directivas de grupo Citrix del panel del árbol y seleccione Asistente de modelado de Directivas de grupo Citrix.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Siga las instrucciones del asistente para seleccionar el controlador de dominio, los usuarios, los equipos, los parámetros del entorno y los criterios de asignación de Citrix que desee usar en la simulación. Al hacer clic en Finalizar, el asistente presenta un informe de los resultados del modelado. En Studio, el informe aparece en el panel central, en la ficha Modelado.

Para ver el informe, seleccione Ver informe de modelado.

Solucionar problemas de directivas

Los usuarios, las direcciones IP y otros objetos asignados pueden tener varias directivas que se aplican de forma simultánea. Esto puede ocasionar conflictos en los que puede que una directiva no se comporte como se espera. Cuando ejecuta el asistente de Modelado de Directivas de grupo Citrix o la herramienta Resultados de directivas de grupo, es posible que detecte que no se aplican directivas a las conexiones de usuario. Cuando esto ocurre, los usuarios que se conectan a sus aplicaciones y escritorios en condiciones que coinciden con los criterios de evaluación de directivas no se ven afectados por ninguna configuración de directiva. Esta situación ocurre cuando:

- Ninguna de las directivas tiene asignaciones que coinciden con los criterios de evaluación de la directiva.
- Las directivas que coinciden con la asignación no tienen ninguna configuración definida.
- Las directivas que coinciden con la asignación están inhabilitadas.

Si desea aplicar configuraciones de directiva a las conexiones que cumplen un criterio determinado, asegúrese de lo siguiente:

- Las directivas que desea aplicar a esas conexiones están habilitadas.
- Las directivas que desea aplicar tienen definidas las configuraciones adecuadas.

Configuraciones predeterminadas de directivas

March 14, 2019

Las tablas siguientes enumeran configuraciones de directiva, sus valores predeterminados y las versiones de Virtual Delivery Agent (VDA) a las que se pueden aplicar.

ICA

Nombre	Configuración predeterminada	VDA
Transporte adaptable	No; Usar si se prefiere	Desde VDA 7.13 hasta 7.15; desde VDA 7.16 hasta la actual

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
Redirección del portapapeles del cliente	Se permite	Todas las versiones de VDA
Inicios de escritorio	Prohibida	VDA para SO de servidor, 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 de servidor, desde la versión 7 hasta la actual
Formatos permitidos de escritura en el portapapeles del cliente	No se han especificado formatos	Desde VDA 7.6 hasta la actual
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	Habilitada	Las versiones de VDA desde 7.16 hasta la actual; para VDA 7.14 y LTSR 7.15, configure este parámetro mediante el Registro.

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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
Error de impedimento para el respaldo de vídeo Flash (*.swf)		Desde VDA 7.6 FP3 hasta la actual

ICA/Sonido

Nombre	Configuración predeterminada	VDA
Sonido Plug and Play	Se permite	VDA para SO de servidor, desde la versión 7 hasta la actual
Calidad de sonido	Alto – sonido de alta definición	Todas las versiones de VDA
Redirección de sonido del cliente	Se permite	Todas las versiones de VDA
Redirección de micrófonos del cliente	Se permite	Todas las versiones de VDA

ICA/Reconexión automática de clientes

Nombre	Configuración predeterminada	VDA
Transporte de sonido en tiempo real sobre UDP	Se permite	Todas las versiones de VDA
Reconexión automática de clientes	Se permite	Todas las versiones de VDA
Autenticación para reconexión automática de clientes	No requerir autenticación	Todas las versiones de VDA
Registro de reconexión automática de clientes	No registrar sucesos de reconexión automática	Todas las versiones de VDA

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	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 de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, 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 de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, desde la versión 7 hasta la actual
Límite de ancho de banda de redirección del portapapeles	0 Kbps	Todas las versiones de VDA
Porcentaje límite de ancho de banda de redirección del portapapeles	0	Todas las versiones de VDA

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	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 Feature Pack 1, VDA para SO de servidor 7 y VDA para SO de escritorio desde la versión 7 hasta la actual, VDA para SO de servidor y VDA para SO de escritorio
Porcentaje límite de ancho de banda de aceleración multimedia HDX MediaStream	0	VDA 5.5, 5.6 FP1, VDA para SO de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, 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 de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, desde la versión 7 hasta la actual

ICA/Redirección de contenido bidireccional

Nombre	Configuración predeterminada	VDA
Permitir redirección de contenido bidireccional	Prohibida	Desde VDA 7.13 hasta la actual
Direcciones URL permitidas para redirigir al cliente	vacío	Desde VDA 7.13 hasta la actual
Direcciones URL permitidas para redirigir al VDA	vacío	Desde VDA 7.13 hasta la actual

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
Redirección de cliente a host (VDA) y redirección de contenido de cliente a cliente		Utilice la plantilla administrativa de GPO de la aplicación Citrix Workspace.

ICA/Redirección de contenido de explorador Web

Nombre	Configuración predeterminada	VDA
Redirección de contenido de explorador Web	Se permite	Desde VDA 7.16 hasta la actual
Configuración de lista ACL para redirección de contenido del explorador Web	`https://www.youtube.com/*`	Desde VDA 7.16 hasta la actual
Configuración de proxy para redirección de contenido del explorador Web	vacío	Desde VDA 7.16 hasta la actual

ICA/Sensores del cliente

Nombre	Configuración predeterminada	VDA
Permitir que las aplicaciones usen la ubicación física del dispositivo cliente	Prohibida	VDA 5.6 FP1, VDA para SO de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, desde la versión 7 hasta la actual

ICA/Interfaz de usuario de escritorio

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 escritorio desde la versión 7 hasta 7.15
Calidad de gráficos de composición del escritorio	Medio	VDA 5.6, VDA para SO de escritorio 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	Habilitada	Todas las versiones de VDA
Intervalo de cálculo del tiempo de retorno ICA	15 segundos	Todas las versiones de VDA
Cálculo del tiempo de retorno ICA para conexiones inactivas	Inhabilitada	Todas las versiones de VDA

ICA/Enhanced Desktop Experience

Nombre	Configuración predeterminada	VDA
Enhanced Desktop Experience	Se permite	VDA para SO de servidor, desde la versión 7 hasta la actual

ICA/Redirección de archivos

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
Conectar automáticamente las unidades del cliente	Se permite	Todas las versiones de VDA
Redirección de unidades del cliente	Se permite	Todas las versiones de VDA
Unidades fijas del cliente	Se permite	Todas las versiones de VDA
Unidades de disco flexible del cliente	Se permite	Todas las versiones de VDA
Unidades de red del cliente	Se permite	Todas las versiones de VDA
Unidades ópticas del cliente	Se permite	Todas las versiones de VDA
Unidades extraíbles del cliente	Se permite	Todas las versiones de VDA
Redirección del host al cliente	Inhabilitada	VDA para SO de servidor, desde la versión 7 hasta la actual
Conservar las letras de unidad del cliente	Inhabilitada	VDA 5, 5.5, 5.6 FP1, VDA para SO de escritorio, desde la versión 7 hasta la actual
Acceso de lectura solamente a unidades del cliente	Inhabilitada	VDA 5.5, 5.6 FP1, VDA para SO de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, desde la versión 7 hasta la actual
Redirección de carpetas especiales	Se permite	Solo implementaciones de Interfaz Web; VDA para SO de servidor, desde la versión 7 hasta la versión actual
Usar escrituras asíncronas	Inhabilitada	Todas las versiones de VDA

ICA/Gráficos

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
Permitir compresión sin pérdida visual	Inhabilitada	Desde VDA 7.6 hasta la actual
Límite de memoria de presentación	65536 Kb	VDA 5, 5.5, 5.6 FP1, VDA para SO de escritorio, desde la versión 7 hasta la actual
Preferencia de degradación de presentación	Degradar primero la profundidad de color	Todas las versiones de VDA
Vista previa de ventanas dinámicas	Habilitada	VDA 5.5, 5.6 FP1, VDA para SO de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, desde la versión 7 hasta la actual
Caché de imágenes	Habilitada	VDA 5.5, 5.6 FP1, VDA para SO de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, desde la versión 7 hasta la actual
Modo de gráficos antiguo	Inhabilitada	VDA para SO de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, 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	Inhabilitada	VDA para SO de servidor, desde la versión 7 hasta la actual
Optimizar para cargas de trabajo de gráficos 3D	Inhabilitada	Desde VDA 7.17 hasta la actual
Cola y descarte	Habilitada	Todas las versiones de VDA
Usar códec de vídeo para compresión	Usar códec de vídeo si se prefiere	Desde VDA 7.6 FP3 hasta la actual
Usar codificación por hardware para códec de vídeo	Habilitada	Desde VDA 7.11 hasta la actual

© 1999-2019 Citrix Systems, Inc. All rights reserved.

ICA/Gráficos/Almacenamiento en caché

Nombre	Configuración predeterminada	VDA
Umbral de caché persistente	3 000 000 bps	VDA para SO de servidor, desde la versión 7 hasta la actual

ICA/Gráficos/Framehawk

Nombre	Configuración predeterminada	VDA
Canal de presentación Framehawk	Inhabilitada	Desde VDA 7.6 FP2 hasta la actual
Intervalo de puertos del canal de presentación Framehawk	3224, 3324	Desde VDA 7.6 FP2 hasta la actual

ICA/Keep Alive

Nombre	Configuración predeterminada	VDA
Tiempo de espera de ICA Keep Alive	60 segundos	Todas las versiones de VDA
ICA Keep Alive	No enviar mensajes de ICA Keep Alive	Todas las versiones de VDA

ICA/Acceso a aplicaciones locales

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
Permitir acceso a aplicaciones locales	Prohibida	VDA para SO de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, desde la versión 7 hasta la actual
Lista negra de redirección de URL	No se especifica ningún sitio	VDA para SO de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, desde la versión 7 hasta la actual
Lista blanca de redirección de URL	No se especifica ningún sitio	VDA para SO de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, 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 de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, desde la versión 7 hasta la actual
Iniciar escritorio con optimización táctil	Se permite	VDA 5.6 FP1; VDA para SO de servidor, desde la versión 7 hasta la actual; VDA para SO de escritorio, desde la versión 7 hasta la actual Esta configuración está inhabilitada y no está disponible para máquinas Windows 10 y Windows Server 2016.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
Control remoto de cuadros combinados	Prohibida	VDA 5.6 FP1, VDA para SO de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, 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 de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, desde la versión 7 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 de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, desde la versión 7 hasta la actual
Usar GPU para optimizar redirección de medios de Windows Media sobre WAN	Prohibida	VDA para SO de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, desde la versión 7 hasta la actual
Prevención de respaldo 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 de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, desde la versión 7 hasta la actual

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
Redirección de Windows Media	Se permite	Todas las versiones de VDA
Tamaño del búfer para la redirección de Windows Media	5 segundos	Desde VDA 5, 5.5, 5.6 FP1 hasta la actual
Uso del tamaño de búfer para redirección de Windows Media	Inhabilitada	Desde VDA 5, 5.5, 5.6 FP1 hasta la actual

ICA/Conexiones de multisecuencia

Nombre	Configuración predeterminada	VDA
Sonido sobre UDP	Se permite	VDA para SO de servidor, desde la versión 7 hasta la actual
Intervalo de puertos UDP de sonido	16500, 16509	VDA 5.5, 5.6 FP1, VDA para SO de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, 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 de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, desde la versión 7 hasta la actual
Configuración de equipo para multisecuencia	Inhabilitada	VDA 5.5, 5.6 FP1, VDA para SO de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, desde la versión 7 hasta la actual

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
Configuración de usuario para multisecuencia	Inhabilitada	VDA 5.5, 5.6 FP1, VDA para SO de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, desde la versión 7 hasta la actual

ICA/Redirección de puertos

Nombre	Configuración predeterminada	VDA
Conectar automáticamente puertos COM del cliente	Inhabilitada	Todas las versiones de VDA; para las versiones desde VDA 7.0 hasta la versión 7.8, configure este parámetro mediante el Registro.
Conectar automáticamente puertos LPT del cliente	Inhabilitada	Todas las versiones de VDA; para las versiones desde VDA 7.0 hasta la versión 7.8, configure este parámetro mediante el Registro.
Redirección de puertos COM del cliente	Prohibida	Todas las versiones de VDA; para las versiones desde VDA 7.0 hasta la versión 7.8, configure este parámetro mediante el Registro.
Redirección de puertos LPT del cliente	Prohibida	Todas las versiones de VDA; para las versiones desde VDA 7.0 hasta la versión 7.8, configure este parámetro mediante el Registro.

ICA/Impresión

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
Redirección de impresoras del cliente	Se permite	Todas las versiones de VDA
Impresora predeterminada	Definir la impresora principal del cliente como la impresora predeterminada	Todas las versiones de VDA
Asignaciones de impresora	La impresora actual del usuario se usa como predeterminada durante la sesión	Todas las versiones de VDA
Preferencia de registro de sucesos de creación automática de impresoras	Registrar errores y advertencias	Todas las versiones de VDA
Impresoras de la sesión	No se especifica ninguna impresora	Todas las versiones de VDA
Esperar a que se creen las impresoras (escritorio)	Inhabilitada	Todas las versiones de VDA

ICA/Impresión/Impresoras del cliente

Nombre	Configuración predeterminada	VDA
Crear automáticamente las impresoras del cliente	Crear automáticamente todas las impresoras cliente	Todas las versiones de VDA
Crear automáticamente una impresora universal genérica	Inhabilitada	Todas las versiones de VDA
Nombres de impresora del cliente	Nombres de impresora estándar	VDA 5.6
Conexiones directas con servidores de impresión	Habilitada	Todas las versiones de VDA
Asignación y compatibilidad de controladores de impresora	No se especifica ninguna regla	Todas las versiones de VDA

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	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	Habilitada	Todas las versiones de VDA
Preferencia de controlador universal	EMF; XPS; PCL5c; PCL4; PS	Todas las versiones de VDA
Uso de controladores de impresión universal	Usar impresión universal solo si el controlador solicitado no está disponible	Todas las versiones de VDA

ICA/Impresión/Universal Print Server

Nombre	Configuración predeterminada	VDA
Habilitar Universal Print Server	Inhabilitada	Todas las versiones de VDA
Puerto del flujo de datos de impresión de Universal Print Server (CGP)	7229	Todas las versiones de VDA
Límite de ancho de banda del flujo de entrada de impresión de Universal Print Server (kpbs)	0	Todas las versiones de VDA

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	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
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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

ICA/Seguridad

Nombre	Configuración predeterminada	VDA
Nivel de cifrado mínimo de SecureICA	Básico	VDA para SO de servidor, 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 de servidor, desde la versión 7 hasta la actual

ICA/Límites de sesión

Nombre	Configuración predeterminada	VDA
Temporizador de sesión desconectada	Inhabilitada	VDA 5, 5.5, 5.6 FP1, VDA para SO de escritorio, 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 escritorio, desde la versión 7 hasta la actual
Temporizador de conexión de sesión	Inhabilitada	VDA 5, 5.5, 5.6 FP1, VDA para SO de escritorio, 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 escritorio, desde la versión 7 hasta la actual
Temporizador de sesión inactiva	Habilitado	VDA 5, 5.5, 5.6 FP1, VDA para SO de escritorio, desde la versión 7 hasta la actual

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
Intervalo de temporizador de sesiones inactivas	1440 minutos	VDA 5, 5.5, 5.6 FP1, VDA para SO de escritorio, 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	Habilitada	VDA para SO de servidor, desde la versión 7 hasta la actual
Usar la hora local del cliente	Usar zona horaria del servidor	Todas las versiones de VDA

ICA/Dispositivos TWAIN

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
Redirección de dispositivos TWAIN del cliente	Se permite	VDA 5.5, 5.6 FP1, VDA para SO de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, desde la versión 7 hasta la actual
Nivel de compresión TWAIN	Medio	VDA 5.5, 5.6 FP1, VDA para SO de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, 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
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 de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, desde la versión 7 hasta la actual

ICA/Presentación visual

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, 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 de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, desde la versión 7 hasta la actual
Compresión de imágenes en movimiento	Habilitada	VDA 5.5, 5.6 FP1, VDA para SO de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, desde la versión 7 hasta la actual
Nivel de compresión progresiva	Ninguna	VDA 5.5, 5.6 FP1, VDA para SO de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, 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 de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, desde la versión 7 hasta la actual

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
Velocidad de fotogramas mínima de destino	10 fps	VDA 5.5, 5.6 FP1, VDA para SO de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, desde la versión 7 hasta la actual

ICA/Presentación visual/Imágenes fijas

Nombre	Configuración predeterminada	VDA
Compresión de color adicional	Inhabilitada	Todas las versiones de VDA
Umbral de compresión de color adicional	8192 Kbps	Todas las versiones de VDA
Compresión intensa	Inhabilitada	Todas las versiones de VDA
Nivel de compresión con pérdida	Medio	Todas las versiones de VDA
Valor de umbral de compresión con pérdida	2 147 483 647 Kbps	Todas las versiones de VDA

ICA/WebSockets

Nombre	Configuración predeterminada	VDA
Conexiones con WebSockets	Prohibida	VDA para SO de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, desde la versión 7 hasta la actual

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
Número de puerto de WebSockets	8008	VDA para SO de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, 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 de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, desde la versión 7 hasta la actual

Administración de carga

Nombre	Configuración predeterminada	VDA
Tolerancia de inicios de sesión simultáneos	2	VDA para SO de servidor, desde la versión 7 hasta la actual
Uso de CPU	Inhabilitada	VDA para SO de servidor, 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 de servidor, desde la versión 7 hasta la actual
Uso del disco	Inhabilitada	VDA para SO de servidor, desde la versión 7 hasta la actual
Número máximo de sesiones	250	VDA para SO de servidor, desde la versión 7 hasta la actual
Uso de memoria	Inhabilitada	VDA para SO de servidor, desde la versión 7 hasta la actual

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
Carga base de uso de memoria	Carga cero: 768 MB	VDA para SO de servidor, desde la versión 7 hasta la actual

Profile Management/Parámetros avanzados

Nombre	Configuración predeterminada	VDA
Inhabilitar configuración automática	Inhabilitada	Todas las versiones de VDA
Cerrar la sesión del usuario si hay algún problema	Inhabilitada	Todas las versiones de VDA
Reintentos de acceso a archivos bloqueados	5	Todas las versiones de VDA
Procesar cookies de Internet al cerrar la sesión	Inhabilitada	Todas las versiones de VDA

Profile Management/Parámetros básicos

Nombre	Configuración predeterminada	VDA
Reescritura activa	Inhabilitada	Todas las versiones de VDA
Habilitar Profile Management	Inhabilitada	Todas las versiones de VDA
Grupos excluidos	Inhabilitada. Se procesan los miembros de todos los grupos de usuarios.	Todas las versiones de VDA
Respaldo para perfiles sin conexión	Inhabilitada	Todas las versiones de VDA
Ruta al almacén de usuarios	Windows	Todas las versiones de VDA
Procesar inicios de sesión de administradores locales	Inhabilitada	Todas las versiones de VDA

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
Grupos procesados	Inhabilitada. 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	Inhabilitada. Se procesan todos los grupos de usuarios especificados en Grupos procesados	Todas las versiones de VDA
Habilitar configuración multiplataforma	Inhabilitada	Todas las versiones de VDA
Ruta de definiciones multiplataforma	Inhabilitada. No se especifica ninguna ruta.	Todas las versiones de VDA
Ruta del almacén de configuración multiplataforma	Inhabilitada. Se usa Windows\PM_CM.	Todas las versiones de VDA
Origen para crear configuración multiplataforma	Inhabilitada	Todas las versiones de VDA

Profile Management/Sistema de archivos/Exclusiones

Nombre	Configuración predeterminada	VDA
Lista de exclusión de directorios	Inhabilitada. Se sincronizan todas las carpetas del perfil de usuario.	Todas las versiones de VDA
Lista de exclusión de archivos	Inhabilitada. Se sincronizan todos los archivos del perfil de usuario.	Todas las versiones de VDA

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Profile Management/Sistema de archivos/Sincronización

Nombre	Configuración predeterminada	VDA
Directorios a sincronizar	Inhabilitada. Solo se sincronizan las carpetas no excluidas.	Todas las versiones de VDA
Archivos a sincronizar	Inhabilitada. Solo se sincronizan los archivos no excluidos.	Todas las versiones de VDA
Carpetas a reflejar	Inhabilitada. No se refleja ninguna carpeta.	Todas las versiones de VDA

Profile Management/Redirección de carpetas

Nombre	Configuración predeterminada	VDA
Conceder acceso a administradores	Inhabilitada	Todas las versiones de VDA
Incluir nombre de dominio	Inhabilitada	Todas las versiones de VDA

Profile Management/Redirección de carpetas/AppData(Roaming)

Nombre	Configuración predeterminada	VDA
Ruta de AppData(Roaming)	Inhabilitada. 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 directiva Ruta de AppData(Roaming).	Todas las versiones de VDA

Profile Management/Redirección de carpetas/Contactos

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
Ruta de Contactos	Inhabilitada. 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 directiva Ruta de Contactos.	Todas las versiones de VDA

Profile Management/Redirección de carpetas/Escritorio

Nombre	Configuración predeterminada	VDA
Ruta de Escritorio	Inhabilitada. No se especifica ninguna ubicación.	Todas las versiones de VDA
Parámetros de redirección para Escritorio	El contenido se redirige a la ruta UNC especificada en la configuración de directiva Ruta de Escritorio.	Todas las versiones de VDA

Profile Management/Redirección de carpetas/Documentos

Nombre	Configuración predeterminada	VDA
Ruta de Documentos	Inhabilitada. 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 directiva Ruta de Documentos.	Todas las versiones de VDA

Profile Management/Redirección de carpetas/Descargas

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
Ruta de Descargas	Inhabilitada. 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 directiva Ruta de Descargas.	Todas las versiones de VDA

Profile Management/Redirección de carpetas/Favoritos

Nombre	Configuración predeterminada	VDA
Ruta de Favoritos	Inhabilitada. No se especifica ninguna ubicación.	Todas las versiones de VDA
Parámetros de redirección para Favoritos	El contenido se redirige a la ruta UNC especificada en la configuración de directiva Ruta de Favoritos.	Todas las versiones de VDA

Profile Management/Redirección de carpetas/Vínculos

Nombre	Configuración predeterminada	VDA
Ruta de Vínculos	Inhabilitada. 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 directiva Ruta de Enlaces.	Todas las versiones de VDA

Profile Management/Redirección de carpetas/Música

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
Ruta de Música	Inhabilitada. No se especifica ninguna ubicación.	Todas las versiones de VDA
Parámetros de redirección para Música	El contenido se redirige a la ruta UNC especificada en la configuración de directiva Ruta de Música.	Todas las versiones de VDA

Profile Management/Redirección de carpetas/Imágenes

Nombre	Configuración predeterminada	VDA
Ruta de Imágenes	Inhabilitada. No se especifica ninguna ubicación.	Todas las versiones de VDA
Parámetros de redirección para Imágenes	El contenido se redirige a la ruta UNC especificada en la configuración de directiva Ruta de Imágenes.	Todas las versiones de VDA

Profile Management/Redirección de carpetas/Juegos guardados

Nombre	Configuración predeterminada	VDA
Ruta de Juegos guardados	Inhabilitada. 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 directiva Ruta de Juegos guardados.	Todas las versiones de VDA

Profile Management/Redirección de carpetas/Búsquedas

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
Ruta de Búsquedas	Inhabilitada. 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 directiva Ruta de Búsquedas.	Todas las versiones de VDA

Profile Management/Redirección de carpetas/Menú Inicio

Nombre	Configuración predeterminada	VDA
Ruta de Menú Inicio	Inhabilitada. No se especifica ninguna ubicación.	Todas las versiones de VDA
Parámetros de redirección para Menú Inicio	El contenido se redirige a la ruta UNC especificada en la configuración de directiva Ruta de Menú Inicio.	Todas las versiones de VDA

Profile Management/Redirección de carpetas/Vídeos

Nombre	Configuración predeterminada	VDA
Ruta de Vídeos	Inhabilitada. 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 directiva Ruta de Vídeos.	Todas las versiones de VDA

Profile Management/Parámetros de registro

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
Acciones de Active Directory	Inhabilitada	Todas las versiones de VDA
Información común	Inhabilitada	Todas las versiones de VDA
Advertencias comunes	Inhabilitada	Todas las versiones de VDA
Habilitar registro	Inhabilitada	Todas las versiones de VDA
Acciones del sistema de archivos	Inhabilitada	Todas las versiones de VDA
Notificaciones del sistema de archivos	Inhabilitada	Todas las versiones de VDA
Cierre de sesión	Inhabilitada	Todas las versiones de VDA
Inicio de sesión	Inhabilitada	Todas las versiones de VDA
Tamaño máximo del archivo de registro	1 048 576	Todas las versiones de VDA
Ruta al archivo de registro	Inhabilitada. Los archivos de registro se guardan en la ubicación predeterminada: %SystemRoot%\System32 \Logfiles\UserProfileManager.	Todas las versiones de VDA
Información de usuario personalizada	Inhabilitada	Todas las versiones de VDA
Valores de directivas al iniciar y cerrar la sesión	Inhabilitada	Todas las versiones de VDA
Acciones del Registro del sistema	Inhabilitada	Todas las versiones de VDA
Diferencias en el Registro del sistema al cerrar la sesión	Inhabilitada	Todas las versiones de VDA

Management/Profile Management/Gestión de perfiles

Nombre	Configuración predeterminada	VDA
Demora antes de eliminar perfiles en caché	0	Todas las versiones de VDA

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
Eliminar perfiles guardados en caché local al cerrar la sesión	Inhabilitada	Todas las versiones de VDA
Gestión de conflictos de perfiles locales	Usar el perfil local	Todas las versiones de VDA
Migración de perfiles existentes	Locales y móviles	Todas las versiones de VDA
Ruta al perfil de plantilla	Inhabilitada. Los perfiles de usuario nuevos se crean a partir del perfil de usuario predeterminado en el equipo en el que el usuario inicia una sesión por primera vez.	Todas las versiones de VDA
El perfil de plantilla anula el perfil local	Inhabilitada	Todas las versiones de VDA
El perfil de plantilla sobrescribe el perfil móvil	Inhabilitada	Todas las versiones de VDA
Perfil de plantilla utilizado como perfil de Citrix obligatorio para todos los inicios de sesión	Inhabilitada	Todas las versiones de VDA

Profile Management/Registro del sistema

Nombre	Configuración predeterminada	VDA
Lista de exclusión	Inhabilitada. 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	Inhabilitada. Todas las claves del Registro en el subárbol HKCU se procesan cuando un usuario cierra la sesión.	Todas las versiones de VDA

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Profile Management/Perfiles de usuario de streaming

Nombre	Configuración predeterminada	VDA
Guardar siempre en caché	Inhabilitada	Todas las versiones de VDA
Tamaño de caché	0 Mb	Todas las versiones de VDA
Streaming de perfiles	Inhabilitada	Todas las versiones de VDA
Grupos de perfiles de usuarios de streaming	Inhabilitada. 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 tiendas	VDA para SO de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, desde la versión 7 hasta la actual

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 de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, desde la versión 7 hasta la actual

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
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	Habilitada	VDA para SO de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, desde la versión 7 hasta la actual
Usar solo el registro de Controller con IPv6	Inhabilitada	VDA para SO de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, 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	Habilitada	VDA 5.5, 5.6 Feature Pack 1
Parámetros de calidad de HDX 3D Pro		VDA 5.5, 5.6 Feature Pack 1

Virtual Delivery Agent/Monitoring

Nombre	Configuración predeterminada	VDA
Habilitar supervisión de procesos	Inhabilitada	Desde VDA 7.11 hasta la actual

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
Habilitar supervisión de recursos	Habilitada	Desde VDA 7.11 hasta la actual

IP virtual

Nombre	Configuración predeterminada	VDA
Respaldo para bucle invertido de IP virtual	Inhabilitada	Desde VDA 7.6 hasta la actual
Lista de programas para bucle invertido de IP virtual	Ninguna	Desde VDA 7.6 hasta la actual

Referencia para configuraciones de directivas

January 29, 2019

> **Nota:**
>
> Puede obtener información sobre los cambios en los nombres de producto aquí.

Las directivas contienen configuraciones que se aplican cuando éstas se implementan. Las descripciones de esta sección también indican si se requieren configuraciones adicionales para habilitar una función y si hay configuraciones similares.

Referencia rápida

Las siguientes tablas muestran las configuraciones que se pueden definir en una directiva. Busque la tarea que desea realizar en la columna de la izquierda y, a continuación, localice la configuración correspondiente en la columna de la derecha.

Dispone de una lista completa de todas las configuraciones de directiva en formato CHM (HTML compilado) y formato CSV. Estos archivos están disponibles en la carpeta `\program files\citrix\grouppolicy`, presente en el servidor donde está instalado el broker (Delivery Controller). También puede descargar la versión más reciente de las configuraciones de directivas haciendo clic aquí.

Sonido

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para esta tarea	Use esta configuración de directiva
Controlar si se permite el uso de varios dispositivos de sonido	Sonido Plug and Play
Controlar si se permite la entrada de sonido desde los micrófonos del dispositivo del usuario	Redirección de micrófonos del cliente
Controlar la calidad de sonido en el dispositivo de usuario	Calidad de sonido
Controlar la asignación de sonido a los altavoces del dispositivo de usuario	Redirección de sonido del cliente

Ancho de banda para dispositivos de usuario

Para limitar el ancho de banda utilizado para	Use esta configuración de directiva
Asignación de sonido del cliente	Límite de ancho de banda de redirección de sonido o Porcentaje límite de ancho de banda de redirección de sonido
Cortar y pegar utilizando el 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para limitar el ancho de banda utilizado para	Use esta configuración de directiva
Dispositivos USB	Límite de ancho de banda de redirección de dispositivos USB del cliente o Porcentaje límite de ancho de banda de redirección de dispositivos USB del cliente

Redirección de dispositivos del cliente y dispositivos del usuario

Para esta tarea	Use esta configuración de directiva
Controlar si se conectan las unidades del dispositivo del usuario cuando los usuarios inician sesión en el servidor	Conectar automáticamente las unidades del cliente
Controlar la transferencia de datos mediante cortar y pegar entre el servidor y el portapapeles local	Redirección del portapapeles del cliente
Controlar la forma en que se deben asignar las unidades del dispositivo del usuario	Redirección de unidades del cliente
Controlar si los discos duros local de los usuarios están disponibles en una sesión	Unidades fijas del cliente y Redirección de unidades del cliente
Controlar si las unidades de disco flexible locales de los usuarios están disponibles en una sesión	Unidades de disco flexible del cliente y Redirección de unidades del cliente
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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para esta tarea	Use esta configuración de directiva
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

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 se genera contenido Flash en las sesiones	Comportamiento predeterminado de Flash

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para esta tarea	Use esta configuración de directiva
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 respaldo de vídeo de Flash; Error de impedimento para el respaldo de 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 el respaldo para 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para esta tarea	Use esta configuración de directiva
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 roaming	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 directiva de ICA

March 14, 2019

La sección ICA contiene configuraciones de directiva relacionadas con las conexiones de escucha ICA y la asignación del portapapeles.

Transporte adaptable

Esta configuración permite o impide el transporte de datos sobre EDT como opción principal u opción de recurrir a TCP (como método secundario).

De forma predeterminada, el transporte adaptable está habilitado (**Preferido**), y se usa EDT cuando sea posible (cuando no sea posible, se recurre a TCP). Si se ha inhabilitado y la quiere habilitar, siga este procedimiento.

1. En Studio, habilite la configuración de directiva “Transporte adaptable HDX”. Asimismo, se recomienda no habilitar esta funcionalidad como una directiva universal para todos los objetos del sitio.
2. Para habilitar esta configuración de directiva, establezca la opción en **Preferido** y, a continuación, haga clic en **Aceptar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nivel de preferencia medio. Se utiliza el transporte adaptable por EDT cuando sea posible; cuando no lo sea, se recurre a TCP.

Modo de diagnóstico. Se obliga el uso de EDT y la opción de recurrir a TCP está inhabilitada. Esta configuración se recomienda solamente para la solución de problemas.

Desactivado. Se obliga el uso de TCP y EDT está inhabilitado.

Para obtener más información, consulte Transporte adaptable.

Tiempo de espera de inicio de la aplicación

Esta configuración especifica el tiempo (en milisegundos) que una sesión debe esperar para que se inicie la primera aplicación. Si el inicio de la aplicación supera este período de tiempo, la sesión se termina.

Puede elegir el tiempo predeterminado (10 000 milisegundos) o puede especificar una cantidad de tiempo en milisegundos.

Redirección del portapapeles del cliente

Esta configuración permite o impide la asignación del portapapeles del dispositivo del usuario al portapapeles del servidor.

La redirección del portapapeles está permitida de forma predeterminada.

Para impedir la transferencia de datos mediante cortar y pegar entre una sesión y el portapapeles local, seleccione **Prohibida**. Los usuarios podrán seguir copiando y pegando datos entre aplicaciones ejecutadas en sesiones.

Después de permitir esta configuración, configure el ancho de banda máximo permitido que el portapapeles puede consumir en una conexión de cliente. Utilice los parámetros **Límite de ancho de banda de redirección del portapapeles** o **Porcentaje límite de ancho de banda de redirección del portapapeles**.

Formatos permitidos de escritura en el portapapeles del cliente

Cuando el parámetro **Restringir escritura en el portapapeles del cliente** está **habilitado**, los datos del portapapeles del host no se pueden compartir con el punto final cliente. Puede usar esta 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:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

Los siguientes formatos personalizados están predefinidos en XenApp y XenDesktop y Citrix Virtual Apps and Desktops:

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

El formato HTML está inhabilitado de forma predeterminada. Para habilitar esta funcionalidad:

- Compruebe que la configuración **Redirección del portapapeles del cliente** está **permitida**.
- Compruebe que la configuración **Restringir escritura en el portapapeles del cliente** está **habilitada**.
- Agregue una entrada para **CF_HTML** (y otros formatos que quiera admitir) en la opción **Formatos permitidos de escritura en el portapapeles del cliente**.

Puede agregar más formatos personalizados. El nombre del formato personalizado debe coincidir con los formatos para registrar con el sistema. Los nombres de formato distinguen entre mayúsculas y minúsculas.

Esta configuración no se aplicará si **Redirección del portapapeles del cliente** o **Restringir escritura**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

en el portapapeles del cliente están configuradas como **Prohibidas**.

> **Nota**
>
> Si se permite copiar contenido en formato HTML al portapapeles (en otras palabras, si se habilita el formato CF_HTML), se copian los scripts del origen del contenido al destino. Antes de proceder a copiar contenido, compruebe el origen de datos para saber si confiar en él. Si copia contenido que contiene scripts, solo se activarán si guarda el archivo de destino como HTML y lo ejecuta.

Restringir escritura en el portapapeles del cliente

Si esta configuración está **permitida**, los datos del portapapeles del host no se pueden compartir con el punto final cliente. Puede permitir algunos formatos específicos, habilitando la configuración **Formatos permitidos de escritura en el portapapeles del cliente**.

De forma predeterminada, esta configuración está prohibida.

Restringir escritura en el portapapeles de la sesión

Cuando esta configuración está **permitida**, los datos del portapapeles del cliente no se pueden compartir con la sesión del usuario. Puede permitir algunos formatos específicos, habilitando el parámetro **Formatos permitidos de escritura en el portapapeles de la sesión**.

De forma predeterminada, esta configuración está prohibida.

Formatos permitidos de escritura en el portapapeles de la sesión

Cuando la configuración **Restringir escritura en el portapapeles de la sesión** está **permitida**, los datos de portapapeles del cliente no se pueden compartir con las aplicaciones de la sesión. Puede usar esta configuración para permitir que formatos específicos de datos se puedan compartir con el portapapeles de la sesión.

Los siguientes formatos de portapapeles están definidos por el sistema:

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE
- CF_HTML

Los siguientes formatos personalizados están predefinidos en XenApp y XenDesktop y Citrix Virtual Apps and Desktops:

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8

El formato HTML está inhabilitado de forma predeterminada. Para habilitar esta funcionalidad:

- Compruebe que la configuración **Redirección del portapapeles del cliente** está **permitida**.
- Compruebe que la configuración **Restringir escritura en el portapapeles de la sesión** está **habilitada**.
- Agregue una entrada para **CF_HTML** (y otros formatos que quiera admitir) en la opción **Formatos permitidos de escritura en el portapapeles de la sesión**.

Puede agregar más formatos personalizados. El nombre del formato personalizado debe coincidir con los formatos para registrar con el sistema. Los nombres de formato distinguen entre mayúsculas y minúsculas.

Esta configuración no se aplicará si Redirección del portapapeles del cliente o Restringir escritura en el portapapeles de la sesión están configuradas como prohibidas.

> **Nota**
>
> Si se permite copiar contenido en formato HTML al portapapeles (en otras palabras, si se habilita el formato CF_HTML), se copian los scripts del origen del contenido al destino. Antes de proceder a copiar contenido, compruebe el origen de datos para saber si confiar en él. Si copia contenido que contiene scripts, solo se activarán si guarda el archivo de destino como HTML y lo ejecuta.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Inicios de escritorio

Esta configuración permite o impide que usuarios no administrativos que formen parte del grupo de usuarios con acceso directo en un VDA se conecten a ese VDA mediante conexiones ICA.

De forma predeterminada, los usuarios no administradores no pueden conectarse a estas sesiones.

Esta configuración no afecta a usuarios no administrativos que formen parte del grupo de usuarios con acceso directo en un VDA y que usen una conexión RDP. Estos usuarios pueden conectarse al VDA tanto si esta configuración está habilitada como si no. Esta configuración no afecta a usuarios no administrativos que no formen parte del grupo de usuarios con acceso directo en un VDA. Estos usuarios no pueden conectarse al VDA tanto si esta configuración está habilitada como si no.

Tiempo de espera de la conexión de escucha ICA

> **Nota**
>
> Esta configuración solo se aplica a las versiones siguientes de Virtual Delivery Agent: 5.0, 5.5 y 5.6 Feature Pack 1.

Esta configuración permite especificar el tiempo de espera máximo para establecer conexiones que usan el protocolo ICA.

El tiempo de espera predeterminado es de 120000 milésimas de segundo, es decir, dos minutos.

Número de puerto de escucha ICA

Esta configuración permite especificar el número de puerto TCP/IP que usará el protocolo ICA en el servidor.

De forma predeterminada, el número de puerto es el 1494.

Los números de puerto válidos deben estar entre 0 y 65 535, y no deben coincidir con otros números de puerto conocidos. Si cambia el número de puerto, vuelva a iniciar el servidor para que se aplique el nuevo valor. Si cambia el número de puerto en el servidor, también deberá cambiarlo en cada aplicación Citrix Workspace o plug-in que se conecte a ese servidor.

Demora en inicio de comprobador de cierre de sesión

Esta configuración especifica la duración que tendrá la demora antes de iniciar el comprobador del cierre de sesión. Utilice esta directiva para establecer el tiempo (en segundos) que espera una sesión de cliente antes de desconectar la sesión.

Esta configuración también aumenta el tiempo necesario para que un usuario cierre la sesión en el servidor.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Iniciar programas no publicados durante la conexión del cliente

Esta configuración especifica si se permite iniciar aplicaciones iniciales a través de RDP en el servidor.

De manera predeterminada, no se permite iniciar aplicaciones iniciales a través de RDP en el servidor.

Configuraciones de directiva de alternar del modo tableta

El modo tableta optimiza la apariencia y el comportamiento de las tiendas de aplicaciones, las aplicaciones Win32 y el shell de Windows en el VDA. El escritorio virtual cambia automáticamente al modo tableta cuando un usuario se conecta a él desde dispositivos de formato pequeño (como teléfonos, tabletas o cualquier dispositivo táctil).

Si esta directiva está inhabilitada, el VDA permanecerá en todo momento en el modo en que lo defina el usuario, sin importar el tipo de cliente.

Configuraciones de directiva de Reconexión automática de clientes

October 3, 2018

La sección “Reconexión automática de clientes” contiene configuraciones para controlar la reconexión automática de las sesiones.

Reconexión automática de clientes

Esta configuración permite o impide la reconexión automática de un cliente tras la interrupción de la conexión.

A partir de Citrix Receiver para Windows 4.7 y la aplicación Citrix Workspace 1808, la Reconexión automática de clientes solo usa las configuraciones de directiva de Citrix Studio. Las actualizaciones de estas directivas en Studio sincronizan la Reconexión automática de clientes desde el servidor hasta el cliente. En caso de versiones anteriores de Citrix Receiver para Windows, para configurar la Reconexión automática de clientes, use una directiva de Studio y modifique el Registro o el archivo default.ica.

La Reconexión automática de clientes permite a los usuarios reanudar el trabajo en el punto en que se interrumpió su conexión. La reconexión automática detecta las conexiones interrumpidas y luego vuelve a conectar a los usuarios a sus sesiones.

Si no usa la cookie de la aplicación Citrix Workspace que contiene la clave del ID de sesión y las credenciales, la reconexión automática puede derivar en el inicio de una nueva sesión. Es decir, se inicia una nueva sesión en vez de reconectarse a una sesión existente. La cookie no se utiliza si está caducada,

© 1999-2019 Citrix Systems, Inc. All rights reserved.

por ejemplo, por retrasos en la reconexión o si las credenciales tienen que volver a introducirse. No hay reconexión automática de clientes si los usuarios se desconectan voluntariamente.

La ventana de la sesión se oscurece mientras tiene lugar una reconexión. Aparece un temporizador que muestra el tiempo restante antes de volver a conectarse a la sesión. Cuando se supera el tiempo de espera, la sesión se desconecta.

En las sesiones de aplicaciones, cuando la Reconexión automática está permitida, en el área de notificaciones aparece un temporizador que indica el tiempo restante antes de volver a conectarse a la sesión. La aplicación Citrix Workspace intenta reconectarse a la sesión hasta que lo logra o hasta que el usuario cancela los intentos de reconexión.

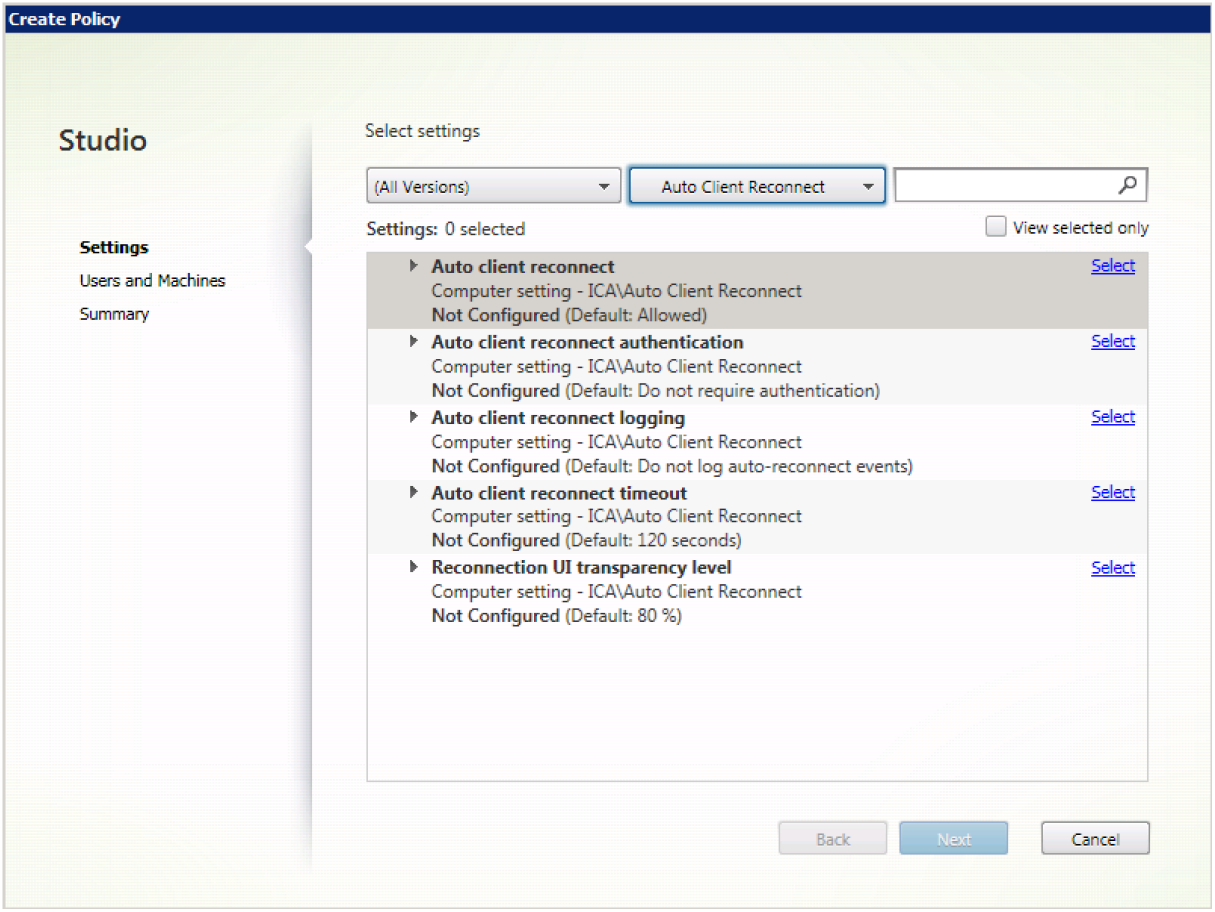
Para las sesiones de usuario, cuando la Reconexión automática está permitida, la aplicación Citrix Workspace intenta volver a conectarse a la sesión durante un período de tiempo especificado, a menos que se produzca una reconexión o el usuario cancele el intento de reconexión. De forma predeterminada, este período es de dos minutos. Para cambiar este período, modifique la directiva.

De forma predeterminada, la Reconexión automática de clientes está permitida.

Para inhabilitar la Reconexión automática de clientes:

1. Inicie Citrix Studio.
2. Abra la directiva **Reconexión automática de clientes**.
3. Establezca la directiva en **Prohibida**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Autenticación para reconexión automática de clientes

Esta configuración hace necesaria la autenticación para las reconexiones automáticas de clientes.

Cuando un usuario inicia sesión por primera vez, sus credenciales se cifran y se almacenan en la memoria. Además, se crea una cookie con la clave de cifrado. La cookie se envía a la aplicación Citrix Workspace. Cuando esta configuración está definida, las cookies no se utilizan. En su lugar, aparece un cuadro de diálogo que solicita que los usuarios introduzcan sus credenciales cuando la aplicación Citrix Workspace intenta volver a conectarse automáticamente.

De forma predeterminada, la autenticación no es necesaria.

Para cambiar la autenticación de la Reconexión automática de clientes:

1. Inicie Citrix Studio.
2. Abra la directiva **Autenticación para reconexión automática de clientes**.
3. Habilite o inhabilite la autenticación.
4. Elija **Aceptar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Registro de reconexión automática de clientes

Esta configuración habilita o inhabilita el registro de las reconexiones automáticas de clientes en el registro de sucesos.

Cuando se habilita la captura de registros, el Registro del sistema del servidor recopila información sobre los sucesos de reconexión automática correctos y fallidos. Un sitio no proporciona los registros combinados de sucesos de reconexión que han tenido lugar en todos los servidores.

De forma predeterminada, el registro está inhabilitado.

Para cambiar la captura de registros de Reconexión automática de clientes:

1. Inicie Citrix Studio.
2. Abra la directiva **Registro de reconexión automática de clientes**.
3. Habilite o inhabilite la captura de registros.
4. Elija **Aceptar**.

Tiempo de espera de la Reconexión automática de clientes

De forma predeterminada, el tiempo de espera de la Reconexión automática de clientes está establecido en 120 segundos. El valor máximo configurable de tiempo de espera para la Reconexión automática de clientes es de 300 segundos.

Para cambiar el tiempo de espera de la Reconexión automática de clientes:

1. Inicie Citrix Studio.
2. Abra la directiva **Tiempo de espera de la reconexión automática de clientes**.
3. Cambie el valor del tiempo de espera.
4. Elija **Aceptar**.

Nivel de transparencia de la interfaz de usuario durante la reconexión

Puede usar la directiva de Studio para configurar el nivel de opacidad que se aplica a la ventana de sesión de XenApp o XenDesktop durante el tiempo de reconexión de la fiabilidad de la sesión.

De manera predeterminada, el nivel de transparencia de la interfaz de usuario es del 80%.

Para modificar el nivel de opacidad de la interfaz de usuario durante una reconexión:

1. Inicie Citrix Studio.
2. Abra la directiva **Nivel de transparencia de la interfaz de usuario durante la reconexión**.
3. Cambie el valor.
4. Elija **Aceptar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Sonido

October 3, 2018

La sección “Sonido” contiene las configuraciones que permiten que los dispositivos de usuario reciban y envíen sonido en las sesiones, sin disminuir su rendimiento.

Transporte de sonido en tiempo real sobre UDP

Esta configuración permite o impide la transmisión y la recepción de sonido entre el VDA y el dispositivo del usuario a través de RTP mediante el protocolo UDP. Cuando esta configuración está inhabilitada, el sonido se envía y recibe sobre TCP.

De forma predeterminada, el sonido sobre UDP está permitido.

Sonido Plug and Play

Esta configuración permite o impide el uso de varios dispositivos de sonido para grabar y reproducir sonido.

De forma predeterminada, el uso de varios dispositivos de sonido está permitido.

Esta configuración solo se aplica a máquinas de SO de servidor Windows.

Calidad de sonido

Esta configuración especifica el nivel de calidad de sonido recibido en las sesiones de usuario.

De forma predeterminada, la calidad de sonido está establecida en Alta: sonido de alta definición.

Para controlar la calidad del sonido, seleccione una de las siguientes opciones:

- Seleccione Baja: para conexiones de baja velocidad, para las conexiones con ancho de banda reducido. Los sonidos enviados al dispositivo del usuario se comprimen hasta 16 Kbps. Esta compresión resulta en una disminución importante de la calidad del sonido pero permite un rendimiento razonable en conexiones con poco ancho de banda.
- Seleccione Media: optimizado para voz para entregar aplicaciones VoIP o para entregar aplicaciones multimedia en conexiones de red difíciles, con líneas de menos de 512 Kbps o que presentan una congestión y pérdida de paquetes significativas. Este códec ofrece una mayor rapidez de codificación, por lo que es ideal para usarlo con programas softphone y aplicaciones de comunicaciones unificadas, cuando se necesita un procesamiento de medios en el lado del servidor.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

El sonido enviado al dispositivo del usuario se comprime hasta 64 Kbps. Esta compresión provoca un ligero descenso en la calidad del sonido que se reproduce en el dispositivo del usuario, pero la latencia es menor y se consume poco ancho de banda. Si la calidad VoIP no es satisfactoria, compruebe que la configuración de directiva "Transporte de sonido en tiempo real sobre UDP" esté establecida en "Permitida".

Actualmente, RTP (transporte en tiempo real) sobre UDP solo recibe respaldo cuando se selecciona esta calidad de sonido. Use esta calidad de sonido incluso para la entrega de aplicaciones multimedia en conexiones de red con poco ancho de banda (inferior a 512 Kbps), y cuando hay congestión de tráfico y pérdida de datos en la red.

- Elija Alta: sonido de alta definición para las conexiones en las cuales no hay problemas de ancho de banda y la calidad del sonido es importante. Los clientes pueden ejecutar el sonido sin compresión adicional. Los sonidos se comprimen con un nivel alto de calidad manteniendo una calidad de nivel CD, y usando hasta 112 Kbps de ancho de banda. La transmisión de tal cantidad de datos puede ocasionar un incremento en la utilización de la CPU y congestionar la red.

El ancho de banda solo se utiliza cuando el sonido se graba o reproduce. Si se graba y se reproduce al mismo tiempo, el consumo de ancho de banda se duplica.

Para especificar el ancho de banda máximo, configure las configuraciones de directiva Límite de ancho de banda de redirección de sonido o Porcentaje límite de ancho de banda de redirección de sonido.

Redirección de sonido del cliente

Esta configuración especifica si las aplicaciones alojadas en el servidor puede reproducir sonidos mediante un dispositivo de sonido instalado en el dispositivo del usuario. Esta configuración también especifica si los usuarios pueden grabar una entrada de sonido.

La redirección del sonido está permitida de forma predeterminada.

Una vez habilitada esta configuración, es posible limitar el ancho de banda utilizado para la reproducción o la grabación de sonido. Limitar el ancho de banda utilizado para el sonido permite mejorar el rendimiento de las aplicaciones, pero también reduce la calidad de sonido. El ancho de banda solo se utiliza cuando el sonido se graba o reproduce. Si se graba y se reproduce al mismo tiempo, el consumo de ancho de banda se duplica. Para especificar el ancho de banda máximo, configure las configuraciones de directiva Límite de ancho de banda de redirección de sonido o Porcentaje límite de ancho de banda de redirección de sonido.

En las máquinas con SO de servidor Windows, compruebe también que la configuración Sonido Plug and Play está habilitada para respaldar varios dispositivos de sonido.

Importante: Cuando la Redirección de sonido del cliente está Prohibida, toda la función de sonido de HDX queda inhabilitada.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Redirección de micrófonos del cliente

Esta configuración habilita o inhabilita la redirección de micrófonos del cliente. Cuando está habilitada, los usuarios pueden usar un micrófono para grabar entradas de sonido en una sesión.

De forma predeterminada, se permite la redirección de micrófonos.

Por motivos de seguridad, se alerta a los usuarios cuando haya servidores sin relación de confianza con el dispositivo intentando acceder a sus micrófonos. Los usuarios podrán aceptar o no el acceso. Los usuarios pueden inhabilitar la alerta en la aplicación Citrix Workspace.

En las máquinas con SO de servidor Windows, compruebe también que la configuración Sonido Plug and Play está habilitada para respaldar varios dispositivos de sonido.

Si se inhabilita la configuración Redirección de sonido del cliente en el dispositivo del usuario, esta regla no tiene ningún efecto.

Configuraciones de directiva de Ancho de banda

January 29, 2019

La sección “Ancho de banda” contiene configuraciones que se pueden definir para evitar problemas de rendimiento relacionados con el uso del ancho de banda de las sesiones de cliente.

Importante: Tenga en cuenta que se pueden producir resultados inesperados si se usan estas configuraciones de directiva con las configuraciones de directiva 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, en kilobits por segundo, para la reproducción o la grabación de sonido en una sesión de usuario.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Porcentaje límite de ancho de banda de redirección de sonido, se aplicará el más restrictivo (el de valor más bajo).

Porcentaje límite de ancho de banda de redirección de sonido

Esta configuración permite especificar el límite máximo permitido de ancho de banda para la reproducción y la grabación de sonido, como porcentaje del ancho de banda total de la sesión.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Límite de ancho de banda de redirección de sonido, se aplicará el más restrictivo (el de valor más bajo).

Si usa esta configuración, también debe definir la configuración Límite de ancho de banda global de la sesión, que indica el ancho de banda total disponible para las sesiones de cliente.

Límite de ancho de banda de redirección de dispositivos USB del cliente

Esta configuración especifica el ancho de banda máximo permitido, en kilobits por segundo, para la redirección de dispositivos USB hacia y desde el cliente.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Porcentaje límite de ancho de banda de redirección de dispositivos USB del cliente, se aplicará el más restrictivo (el de valor más bajo).

Porcentaje límite de ancho de banda de redirección de dispositivos USB del cliente

Esta configuración especifica el ancho de banda máximo permitido para la redirección de dispositivos USB hacia y desde el cliente como un porcentaje del ancho de banda total de la sesión.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Límite de ancho de banda de redirección de dispositivos USB del cliente, se aplicará el más restrictivo (el de valor más bajo).

Si usa esta configuración, también debe definir la configuración Límite de ancho de banda global de la sesión, que indica el ancho de banda total disponible para las sesiones de cliente.

Límite de ancho de banda de redirección del portapapeles

Esta configuración permite especificar el valor máximo permitido de ancho de banda, en kilobits por segundo, para la transferencia de datos entre una sesión y el portapapeles local.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Porcentaje límite de ancho de banda de redirección del portapapeles, se aplicará el más restrictivo (el de valor más bajo).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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; consulteConfigurar 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; consulteConfigurar la redirección de puertos COM y puertos LPT mediante el Registro.

Esta configuración permite especificar el valor máximo permitido de ancho de banda para el acceso a puertos COM en una conexión de cliente, como porcentaje del ancho de banda total de la sesión.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Límite de ancho de banda de redirección de puertos COM, se aplicará el más restrictivo (el de valor más bajo).

Si define esta configuración, también debe definir la configuración Límite de ancho de banda global de la sesión, que indica el ancho de banda total disponible para las sesiones de cliente.

Límite de ancho de banda de redirección de archivos

Esta configuración permite especificar el valor máximo permitido de ancho de banda, en kilobits por segundo, para el acceso a una unidad del cliente en una sesión de usuario.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Porcentaje límite de ancho de banda de redirección de archivos, se aplicará el más restrictivo (el de valor más bajo).

Porcentaje límite de ancho de banda de redirección de archivos

Esta configuración permite especificar el límite máximo permitido de ancho de banda para el acceso a unidades del cliente como porcentaje del ancho de banda total de la sesión.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Límite de ancho de banda de redirección de archivos, se aplicará el más restrictivo (el de valor más bajo).

Si usa esta configuración, también debe definir la configuración Límite de ancho de banda global de la sesión, que indica el ancho de banda total disponible para las sesiones de cliente.

Límite de ancho de banda de aceleración multimedia HDX MediaStream

Esta configuración especifica el límite de ancho de banda máximo permitido, en kilobits por segundo, para entregar por streaming sonido y vídeo mediante la aceleración multimedia HDX MediaStream.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Porcentaje límite de ancho de banda de aceleración multimedia HDX MediaStream, se aplicará el más restrictivo (el de valor más bajo).

Porcentaje límite de ancho de banda de aceleración multimedia HDX MediaStream

Esta configuración especifica el ancho de banda máximo permitido para entregar por streaming sonido y vídeo mediante la aceleración multimedia HDX MediaStream como porcentaje del ancho de banda total de la sesión.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración “Límite de ancho de banda de aceleración multimedia HDX MediaStream”, se aplicará el más restrictivo (el de valor más bajo).

Si usa esta configuración, también debe definir la configuración Límite de ancho de banda global de la sesión, que indica el ancho de banda total disponible para las sesiones de cliente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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; consulteConfigurar la redirección de puertos COM y puertos LPT mediante el Registro.

Esta configuración permite especificar el valor máximo permitido de ancho de banda, en kilobits por segundo, para trabajos de impresión mediante un puerto LPT en una sesión de usuario individual.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Porcentaje límite de ancho de banda de redirección de puertos LPT, se aplicará el más restrictivo (el de valor más bajo).

Porcentaje límite de ancho de banda de redirección de puertos LPT

Nota: Para los agentes Virtual Delivery Agent 7.0 a 7.8, configure esta configuración con el Registro; consulteConfigurar la redirección de puertos COM y puertos LPT mediante el Registro.

Esta configuración permite especificar el límite de ancho de banda para los trabajos de impresión mediante un puerto LPT en una sesión de cliente individual como porcentaje del ancho de banda total de la sesión.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Límite de ancho de banda de redirección de puertos LPT, se aplicará el más restrictivo (el de valor más bajo).

Si usa esta configuración, también debe definir la configuración Límite de ancho de banda global de la sesión, que indica el ancho de banda total disponible para las sesiones de cliente.

Límite de ancho de banda global de la sesión

Esta configuración permite especificar el total de ancho de banda disponible, en kilobits por segundo, para las sesiones de usuario.

El límite de ancho de banda máximo que puede imponerse es de 10 Mbps (10000 Kbps). De forma predeterminada, no se especifica ningún valor máximo (cero).

Al limitar el ancho de banda de las conexiones de cliente, se puede mejorar el rendimiento cuando otras aplicaciones fuera de la conexión de cliente compiten por un ancho de banda limitado.

Límite de ancho de banda de redirección de impresoras

Esta configuración permite especificar el valor máximo permitido de ancho de banda, en kilobits por segundo, para el acceso a impresoras del cliente en una sesión de usuario.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Porcentaje límite de ancho de banda de redirección de impresoras, se aplicará el más restrictivo (el de valor más bajo).

Porcentaje límite de ancho de banda de redirección de impresoras

Esta configuración permite especificar el valor máximo permitido de ancho de banda para el acceso a impresoras del cliente como porcentaje del ancho de banda total de la sesión.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Límite de ancho de banda de redirección de impresoras, se aplicará el más restrictivo (el de valor más bajo).

Si usa esta configuración, también debe definir la configuración Límite de ancho de banda global de la sesión, que indica el ancho de banda total disponible para las sesiones de cliente.

Límite de ancho de banda de redirección de dispositivos TWAIN

Esta configuración permite especificar el valor máximo permitido ancho de banda, en kilobits por segundo, para el control de dispositivos de imágenes TWAIN desde aplicaciones publicadas.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Porcentaje límite de ancho de banda de redirección de dispositivos TWAIN, se aplicará el más restrictivo (el de valor más bajo).

Porcentaje límite de ancho de banda de redirección de dispositivos TWAIN

Esta configuración permite especificar el valor máximo permitido de ancho de banda para el control de dispositivos de imágenes TWAIN desde aplicaciones publicadas como porcentaje del ancho de banda total de la sesión.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Límite de ancho de banda de redirección de dispositivos TWAIN, se aplicará el más restrictivo (el de valor más bajo).

Si usa esta configuración, también debe definir la configuración Límite de ancho de banda global de la sesión, que indica el ancho de banda total disponible para las sesiones de cliente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Redirección de contenido bidireccional

October 3, 2018

La sección “Redirección de contenido bidireccional” contiene configuraciones para habilitar o inhabilitar la redirección de URL entre el host y el cliente y viceversa. Las directivas de servidor se configuran en Citrix Studio, y las directivas de cliente se configuran en la plantilla administrativa de objeto de directiva de grupo de la aplicación Citrix Workspace.

A pesar de que Citrix también ofrece la redirección del host al cliente y el Acceso a aplicaciones locales para la redirección del cliente a la URL, le recomendamos usar la redirección de contenido bidireccional para clientes de Windows unidos a un dominio.

La redirección de contenido bidireccional requiere Citrix Virtual Apps and Desktops 1808, o bien, XenApp o XenDesktop 7.13 o posterior más la aplicación Citrix Workspace 1808 o posterior, o bien, Citrix Receiver para Windows 4.7 o posterior.

> **Importante**
>
> - Compruebe que las reglas de redirección no resultan en un bucle. Por ejemplo, si las reglas de cliente al VDA se establecen en https://www.citrix.com y las reglas del VDA al cliente se establecen en la misma URL, puede producirse un bucle infinito.
> - Solo se admiten puntos finales unidos a un dominio.
> - La funcionalidad de redirección de URL solo admite direcciones URL explícitas (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 usando). No se admiten acortadores de enlaces.
> - La redirección de contenido bidireccional solo admite Internet Explorer de 8 a 11. Internet Explorer se debe usar en el dispositivo de usuario y el VDA.
> - El complemento del explorador Internet Explorer es necesario para la redirección de contenido bidireccional. Para obtener más información, consulte Registrar complementos del explorador Web.
> - Si la redirección falla debido a problemas de lanzamiento de la sesión, no hay ningún mecanismo alternativo.
> - Si hay dos aplicaciones con el mismo nombre simplificado que están configuradas para usar varias cuentas de StoreFront, se utiliza un nombre simplificado de la cuenta principal de StoreFront para el inicio.
> - Solo admite la aplicación Citrix Workspace para Windows.
> - Solo se abre una nueva ventana de explorador Web cuando la dirección URL se redirige al cliente. Cuando la dirección URL se redirige al VDA, si el explorador Web ya está abierto, la URL redirigida se abre en una nueva pestaña.
> - Se admiten enlaces incrustados en archivos como PDF, mensajes de correo electrónico y

© 1999-2019 Citrix Systems, Inc. All rights reserved.

documentos.
- Esta característica funciona en sesiones de escritorio y sesiones de aplicación, a diferencia de la redirección de URL del Acceso a aplicaciones locales, que funciona solo en las sesiones de escritorio.
- Si el Acceso a aplicaciones locales está habilitado para la redirección de URL (ya sea en el VDA o el cliente), la redirección de contenido bidireccional no tiene efecto.

Redirección del host al cliente y del cliente al host

Use Studio para configurar las directivas de redirección de host a cliente (cliente) y de host a host (VDA).

La redirección de contenido bidireccional está **prohibida** de forma predeterminada.

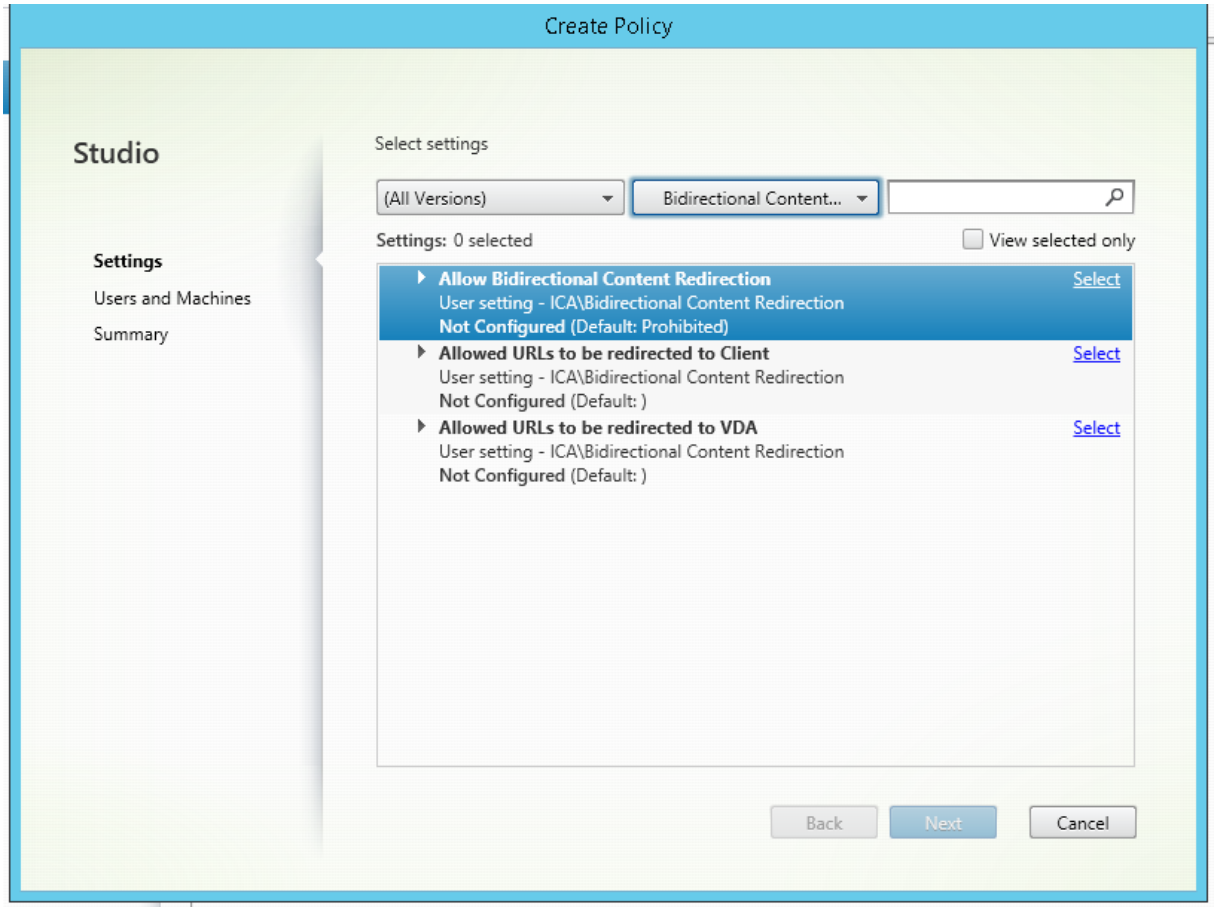
Para habilitar la redirección de contenido bidireccional

Al incluir direcciones URL, puede especificar una sola dirección URL o una lista de direcciones URL, delimitadas por punto y coma. Puede utilizar un asterisco (*) como comodín en el nombre de dominio. Por ejemplo:

http://*.citrix.com; http://www.google.com

1. Inicie Citrix Studio.
2. Abra la directiva **Redirección de contenido bidireccional**.
3. Seleccione **Permitir redirección de contenido bidireccional**, elija **Permitida** y haga clic en **Aceptar**. Si no permite esta opción, no podrá completar este procedimiento.
4. Seleccione **Direcciones URL permitidas para redirigir al cliente** y especifique una dirección URL, una lista de direcciones URL, o bien, elija el valor predeterminado.
5. Seleccione **Direcciones URL permitidas para redirigir al VDA** y especifique una dirección URL, una lista de direcciones URL, o bien, elija el valor predeterminado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Redirección de cliente a host (VDA) y de cliente a cliente

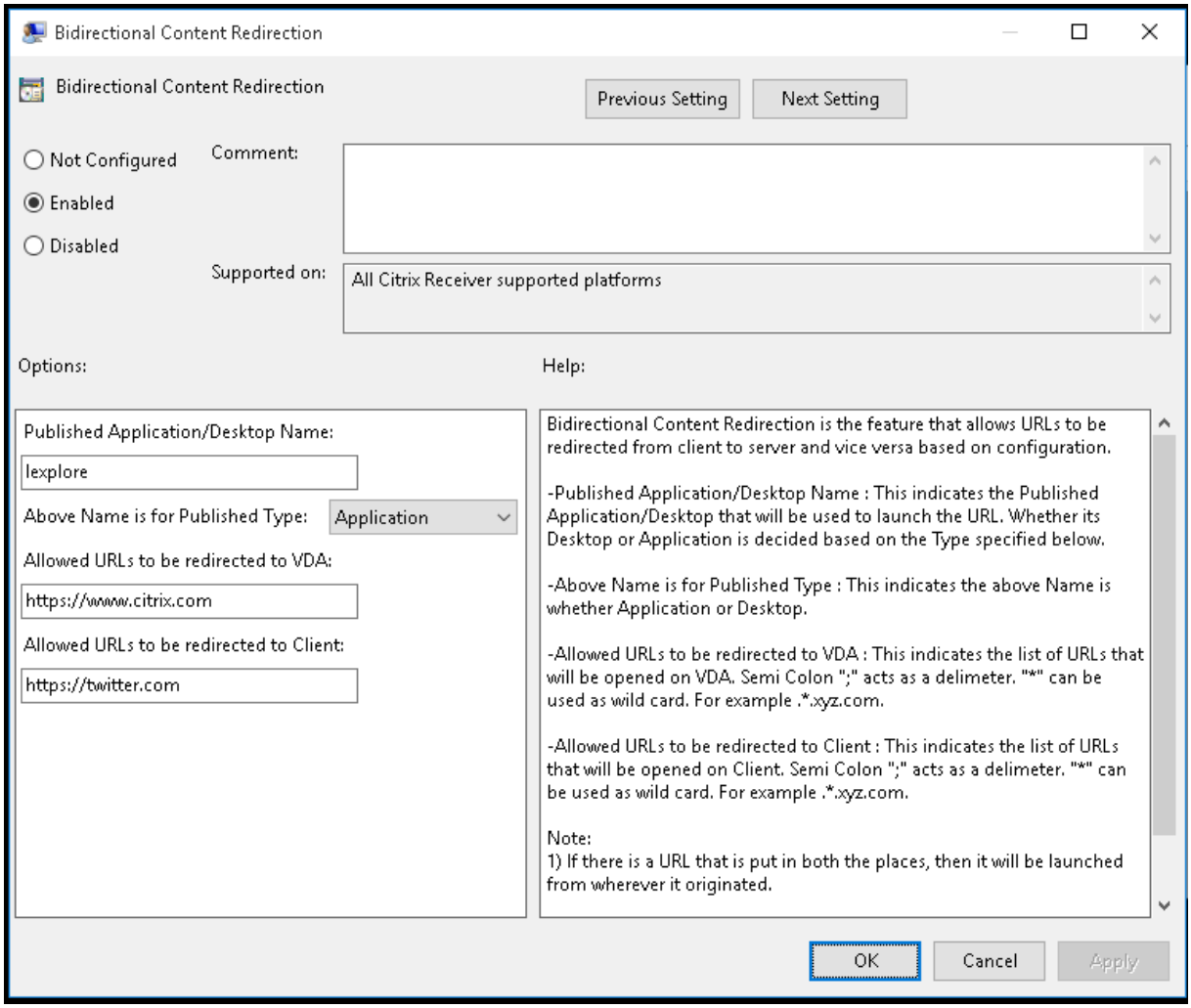
Utilice la plantilla administrativa del GPO de la aplicación Citrix Workspace para configurar la redirección de cliente a host (VDA) y de cliente a cliente (cliente).

Para habilitar la redirección de contenido bidireccional

Al incluir direcciones URL, puede especificar una sola dirección URL o una lista de direcciones URL, delimitadas por punto y coma. Puede utilizar un asterisco (*) como comodín.

Para obtener más información, consulte Configurar la redirección de contenido bidireccional en la documentación de la aplicación Citrix Workspace.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Registrar complementos del explorador Web

El complemento del explorador Internet Explorer es necesario para la redirección de contenido bidireccional.

Puede usar los siguientes comandos para registrar y cancelar el registro de un complemento de Internet Explorer:

- Para registrar un complemento de Internet Explorer en un dispositivo cliente: \redirector.exe /regIE
- Para cancelar el registro de un complemento de Internet Explorer en un dispositivo cliente: \redirector.exe /unregIE
- Para registrar un complemento de Internet Explorer en un VDA: \VDARedirector.exe /regIE
- Para cancelar el registro de un complemento de Internet Explorer en un VDA: \VDARedirector.exe /unregIE

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Por ejemplo, el siguiente comando registra el complemento de Internet Explorer en un dispositivo que ejecuta la aplicación Citrix Workspace.

C:\Archivos de programa\Citrix\ICA Client\redirector.exe/regIE

El siguiente comando registra el complemento de Internet Explorer en un VDA para sistemas operativos de servidor Windows.

C:\Archivos de programa (x86)\Citrix\System32\VDARedirector.exe /regIE

Configuraciones de directiva de Redirección de contenido de explorador Web

March 14, 2019

La sección “Redirección de contenido de explorador Web” contiene configuraciones para definir esta característica.

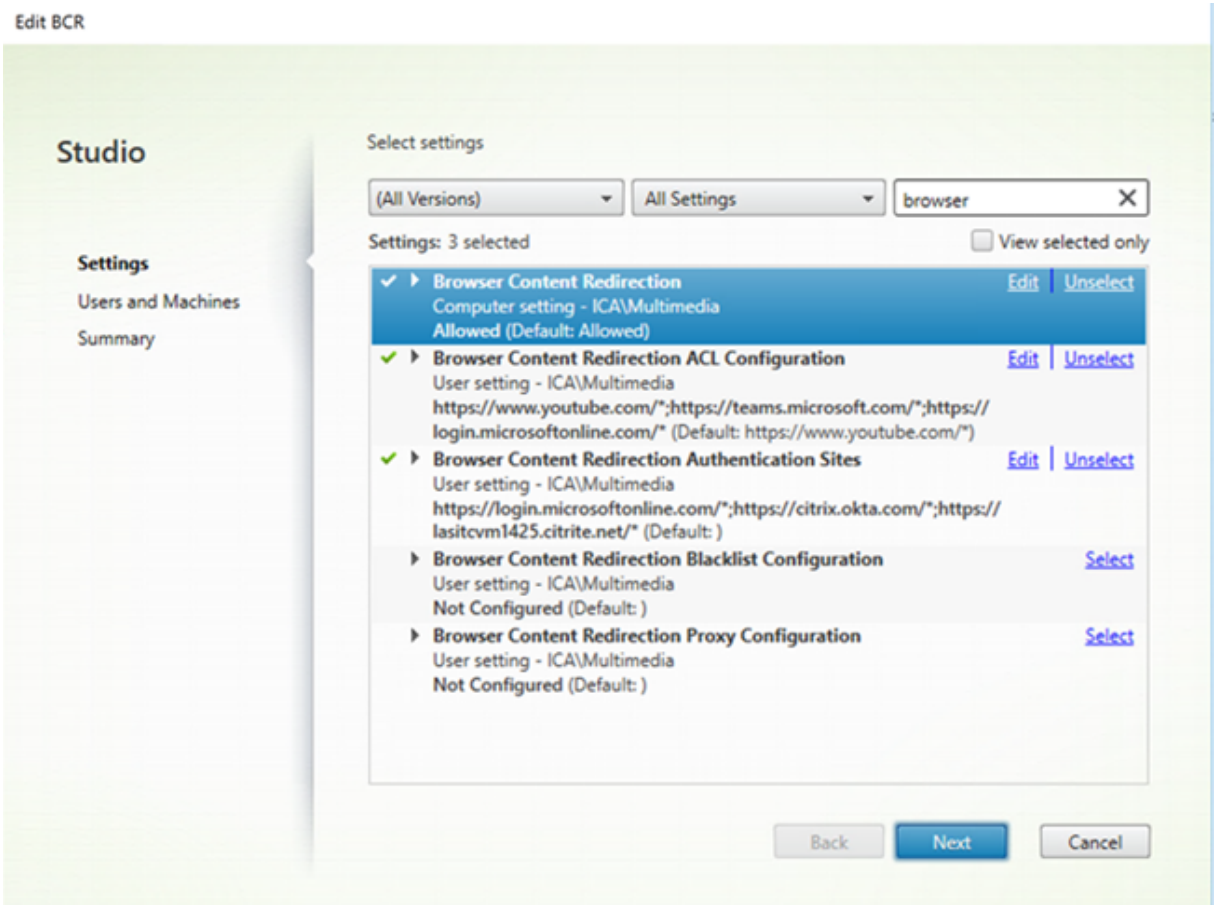
Con la redirección de contenido del explorador Web, puede controlar y optimizar el modo en que Citrix Virtual Apps and Desktops entregan contenido de los exploradores Web (por ejemplo, contenido HTML5) a los usuarios. Solo se redirige el área visible del explorador Web donde se muestra el contenido.

La Redirección de vídeo HTML5 y la Redirección de contenido del explorador Web son funciones independientes. Las directivas de redirección de vídeo HTML5 no son necesarias para que esta característica funcione, pero se usa el servicio Citrix HDX HTML5 Video Redirection Service para la redirección de contenido del explorador Web. Para obtener más información, consulte Redirección de contenido de explorador Web.

Configuraciones de directivas:

En Citrix Studio, están disponibles las siguientes configuraciones de directiva para la característica Redirección de contenido de explorador Web. Estas directivas pueden anularse con claves de Registro en el VDA, aunque esas claves de Registro son opcionales.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



TLS 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 conseguir esta redirección y mantener la integridad TLS de la página Web, el servicio Citrix HDX HTML5 Video Redirection Service genera dos certificados personalizados en el almacén de certificados del VDA.

HdxVideo.js utiliza Secure WebSockets para comunicarse con WebSocketService.exe que se ejecuta en el VDA. Este proceso se ejecuta en el sistema local y realiza la terminación SSL y la asignación de sesiones de usuario.

WebSocketService.exe escucha en 127.0.0.1 en el puerto 9001.

> **Advertencia**
>
> Si se modifica el Registro de forma incorrecta, se pueden generar problemas graves que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resol-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> verse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Redirección de contenido de explorador Web

De forma predeterminada, la aplicación Citrix Workspace intenta obtener y generar el contenido en el cliente. Si falla la opción de obtener y generar el contenido en el cliente, se intenta generar contenido en el lado del servidor. Si también habilita la directiva "Configuración de proxy para redirección de contenido de explorador Web", la aplicación Citrix Workspace solo intenta la opción de obtener contenido en el servidor y generar contenido en el cliente.

De forma predeterminada, esta configuración está Permitida.

Opciones de invalidación del Registro para configuraciones de directiva (la ruta del Registro varía en función de la arquitectura del VDA):

\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediastream
O
\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediastream

Nombre: WebBrowserRedirection

Tipo: DWORD

Valor:

1 = Se permite la redirección de contenido del explorador web.

0 = Se prohíbe la redirección de contenido del explorador web.

Configuraciones de directiva para la lista de control de acceso en la redirección de contenido de explorador Web

Use esta configuración para definir una lista de control de acceso (ACL) con las direcciones URL que pueden utilizar la redirección de contenido del explorador Web y las direcciones URL a las que se deniega el acceso a la redirección de contenido del explorador Web.

Las direcciones URL autorizadas son aquellas URL cuyo contenido se redirige al cliente.

Se permite el carácter comodín *, salvo en el protocolo o en la parte de dirección de dominio de la URL.

Permitido: `http://www.xyz.com/index.html`, `https://www.xyz.com/*`, `http://www.xyz.com/*videos*`

No permitido: `http://*.xyz.com/`

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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/*`

Opciones de invalidación del Registro para configuraciones de directiva (la ruta del Registro varía en función de la arquitectura del VDA):

\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediastream
O
\HKEY_LOCAL_MACHINE\Citrix\HdxMediastream

Nombre: WebBrowserRedirectionAcl

Tipo: REG_MULTI_SZ

Para obtener más información, consulte el artículo CTX238236 de Knowledge Center.

Sitios de autenticación para la Redirección de contenido de explorador Web

Use esta configuración para definir una lista de direcciones URL. Los sitios redirigidos mediante la Redirección de contenido de explorador Web utilizan esa lista para autenticar usuarios. La configuración especifica las URL para las que la Redirección de contenido de explorador Web permanece activa (se redirige el contenido) cuando se navega más allá de una URL incluida en una lista blanca.

Un ejemplo típico es un sitio Web que relega la autenticación a un proveedor de identidades (IdP). Por ejemplo, el sitio Web `www.xyz.com` 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 blanca, y luego utiliza los sitios de autenticación de Redirección de contenido de explorador Web para incluir `www.xyz.okta.com` en la lista blanca.

Opciones de anulación de Registro en el VDA para configuraciones de directiva:

\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediastream

O bien:

\HKEY_LOCAL_MACHINE\Citrix\HdxMediastream

Nombre: WebBrowserRedirectionAuthenticationSites

Tipo: REG_MULTI_SZ

Para obtener más información, consulte el artículo CTX238236 de Knowledge Center.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configuración de lista negra para la redirección de contenido del explorador web

Esta configuración funciona junto con la configuración de la lista ACL de redirección de contenido del explorador Web. Si las URL están presentes en la configuración de la ACL de redirección de contenido del explorador Web y en la configuración de la lista negra, la configuración de la lista negra 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 negra cuyo contenido del explorador Web no se redirige al cliente, sino que se genera en el servidor.

Se permite el carácter comodín *, salvo en el protocolo o en la parte de dirección de dominio de la URL.

Permitido: `http://www.xyz.com/index.html`, `https://www.xyz.com/*`, `http://www.xyz.com/*videos*`

No permitido: `http://*.xyz.com/`

Puede lograr una mayor granularidad si especifica rutas en la URL. Por ejemplo, si especifica `https://www.xyz.com/sports/index.html`, solo index.html se incluye en la lista negra.

\HKLM\SOFTWARE\Wow6432Node\Citrix\HdxMediastream

O bien:

\HKLM\SOFTWARE\Citrix\HdxMediastream

Nombre: WebBrowserRedirectionBlacklist

Tipo: REG_MULTI_SZ

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 un número de puerto y una dirección de proxy válidos, 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 el valor predeterminado, la aplicación Citrix Workspace intenta obtener contenido en el cliente y generarlo en el cliente.

De forma predeterminada, esta configuración está prohibida.

Opciones de invalidación del Registro para configuraciones de directiva (la ruta del Registro varía en función de la arquitectura del VDA):

\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediastream
O
\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediastream

© 1999-2019 Citrix Systems, Inc. All rights reserved.

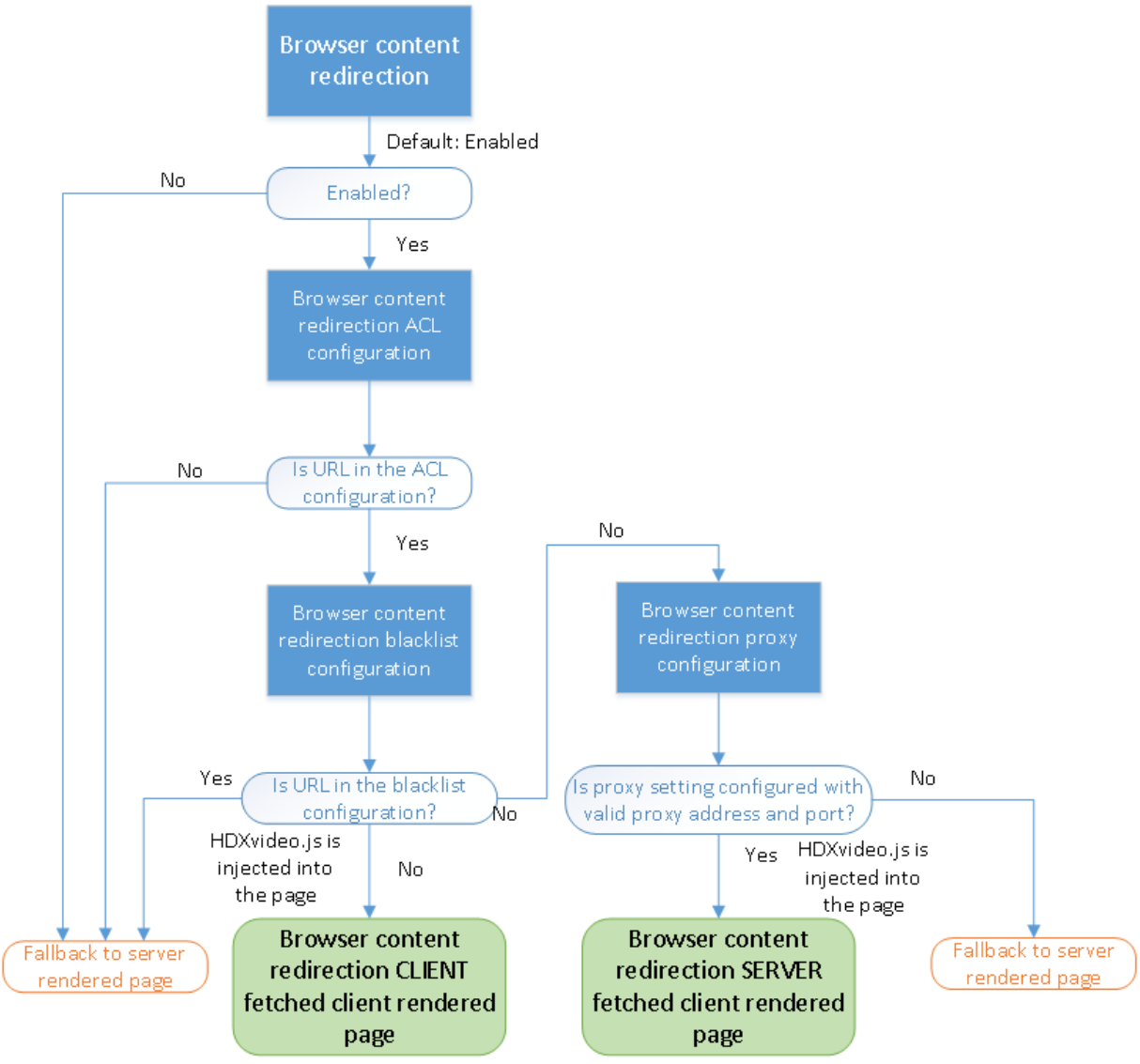
Nombre: WebBrowserRedirectionProxyAddress

Tipo: REG_SZ

Patrón permitido: `http://\<hostname/ip address\>:\<port\>`

Ejemplo: `http://proxy.example.citrix.com:80`

Insertar HDXVideo.js para redirigir contenido del explorador Web



HdxVideo.js se inserta en la página Web utilizando 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

El objeto BHO decide si insertar HdxVideo.js en una página determinada. La decisión se basa en directivas administrativas mostradas en el gráfico anterior.

Después de que se haya decidido insertar JavaScript y redirigir el contenido del explorador Web al cliente, la página Web del Internet Explorer presente en el VDA se queda vacía. Dejar vacío **document.body.innerHTML** elimina el cuerpo entero de la página Web en el VDA. La página está lista para enviarse al cliente, donde se verá en el explorador superpuesto (Hdxbrowser.exe).

Configuraciones de directiva de Sensores del cliente

December 14, 2018

La sección “Sensores del cliente” contiene configuraciones de directiva para controlar cómo se gestiona la información de sensor del dispositivo móvil en una sesión de usuario.

Permitir que las aplicaciones usen la ubicación física del dispositivo cliente

Esta configuración determina si las aplicaciones que se ejecutan en la sesión de un dispositivo móvil pueden usar la ubicación física del dispositivo de usuario.

De forma predeterminada, no se permite el uso de la información de ubicación.

Cuando esta configuración está prohibida, los intentos de una aplicación por obtener información de ubicación tendrán como resultado “permiso denegado”.

Cuando esta configuración está permitida, el usuario puede prohibir el uso de la información de ubicación denegando la solicitud de la aplicación Citrix Workspace para acceder a la ubicación. Los dispositivos Android y iOS 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 respalde 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

  - Dar al usuario la opción de borrar la información de ubicación que almacena la aplicación en caché. (La aplicación Citrix Workspace no almacena en caché la información de ubicación.)
- Una aplicación con información de ubicación habilitada debe gestionar la complejidad de la información de ubicación, de manera que los datos obtenidos sean apropiados para los fines de la aplicación en particular y cumplan con las normas aplicables en todas las jurisdicciones pertinentes.
- Aplicar una conexión segura (por ejemplo, con TLS o una red VPN) es imprescindible para usar los servicios de ubicación. Conecte la aplicación Citrix Workspace a servidores de confianza.
- Consulte la información legal referente al uso de servicios de ubicación.

Configuraciones de directiva de Interfaz de usuario de escritorio

October 3, 2018

La sección “Interfaz de usuario de escritorio” contiene configuraciones que controlan los efectos visuales, como el papel tapiz del escritorio, las animaciones de menús y las imágenes de arrastrar y colocar, a fin de administrar el ancho de banda utilizado en las conexiones del cliente. Se puede mejorar el rendimiento sobre conexiones WAN limitando el uso de ancho de banda.

> **Importante**
>
> En esta versión, no se admiten el modo de gráficos antiguos ni la redirección de composición del escritorio (DCR). Esa directiva se incluye solo para la compatibilidad con versiones anteriores cuando se usa XenApp 7.15 LTSR y XenDesktop 7.15 LTSR, así como las versiones anteriores de VDA con Windows 7 y Windows 2008 R2.

Redirección de composición del escritorio

Esta configuración especifica si se debe usar la capacidad de procesamiento de la unidad de procesamiento de gráficos (GPU) o el procesador de gráficos integrado (IGP) en el dispositivo del usuario en la generación de gráficos locales de DirectX para proporcionar a los usuarios una experiencia de escritorio de Windows más fluida. Cuando está habilitada, la 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, la 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Calidad de gráficos de composición del escritorio

Esta configuración especifica la calidad de los gráficos utilizados para la redirección de composición del escritorio.

El valor predeterminado es “Alta”.

Elija la calidad entre las opciones Alta, Media, Baja o Sin pérdida.

Tapiz del escritorio

Esta configuración permite o evita que se muestre el tapiz del escritorio en las sesiones de los usuarios.

De forma predeterminada, las sesiones de usuario pueden mostrar el tapiz del escritorio.

Para inhabilitar el tapiz del escritorio y reducir el ancho de banda necesario para las sesiones de usuario, seleccione Prohibida cuando agregue esta configuración a una directiva.

Animación de menús

Esta configuración permite o evita la animación de menús en las sesiones de los usuarios.

La animación de menús está permitida de forma predeterminada.

Animación de menús es una configuración de preferencia personal de Microsoft para facilitar el acceso. Cuando está habilitado, provoca que el menú aparezca tras una breve demora, ya sea con un desplazamiento o un fundido. Aparece un icono de flecha en la parte inferior del menú. El menú se muestra al apuntar a dicha flecha.

La animación de menús se habilita en un escritorio si esta configuración de directiva se define como Permitida y la configuración de preferencia personal de animación de menús de Microsoft está habilitada.

Nota: Los cambios en la configuración de preferencia personal de animación de menús de Microsoft son cambios hechos en el escritorio. Si el escritorio está configurado para descartar los cambios cuando finalice la sesión, un usuario que haya habilitado las animaciones de menú durante la sesión no verá animaciones de menú en sesiones subsiguientes en ese escritorio. Si los usuarios requieren animaciones de menú, habilite la configuración de Microsoft en la imagen maestra del escritorio para garantizar que el escritorio conserva los cambios del usuario.

Ver contenido de las ventanas al arrastrar

Esta configuración permite o evita que se muestre el contenido de las ventanas al arrastrarlas por la pantalla.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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

October 3, 2018

La sección Supervisión de usuario final contiene configuraciones de directiva para medir el tráfico de la sesión.

Cálculo del tiempo de retorno ICA

Esta configuración determina si se realizan cálculos del tiempo de retorno ICA para las conexiones activas.

De forma predeterminada, los cálculos para las conexiones activas están habilitados.

De forma predeterminada, el inicio de cada medición de tiempo de retorno ICA espera hasta que se detecte tráfico que indique la interacción del usuario. La duración de esta espera puede ser indefinida y su función es evitar que se produzca tráfico ICA con el único fin de medir tiempos de retorno de ICA.

Intervalo de cálculo del tiempo de retorno ICA

Esta configuración permite especificar la frecuencia, en segundos, para el cálculo del tiempo de retorno ICA.

De forma predeterminada, el tiempo de retorno ICA se calcula cada 15 segundos.

Cálculo del tiempo de retorno ICA para conexiones inactivas

Esta configuración determina si se realizan cálculos del tiempo de retorno ICA para las conexiones inactivas.

De forma predeterminada, no se realizan cálculos para las conexiones inactivas.

De forma predeterminada, el inicio de cada medición de tiempo de retorno ICA espera hasta que se detecte tráfico que indique la interacción del usuario. La duración de esta espera puede ser indefinida y su función es evitar que se produzca tráfico ICA con el único fin de medir tiempos de retorno de ICA.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configuración de directiva de Enhanced Desktop Experience

October 3, 2018

Con la configuración de directiva Enhanced Desktop Experience, las sesiones que se ejecutan en sistemas operativos de servidor tienen el mismo aspecto que los escritorios locales con Windows 7, lo que proporciona a los usuarios una mejor experiencia de escritorio.

De forma predeterminada, esta configuración está permitida.

Si ya existe un perfil de usuario con el tema Windows clásico en el escritorio virtual, habilitar esta directiva no proporciona una mejor experiencia de escritorio para ese usuario. Si un usuario con un perfil con el tema Windows 7 inicia sesión en un escritorio virtual que ejecuta Windows Server 2012 para el que esta directiva esté sin configurar o inhabilitada, el usuario ve un mensaje de error que indica que no se pudo aplicar el tema.

En ambos casos, el problema se resuelve restableciendo el perfil de usuario.

Si la directiva cambia de habilitada a inhabilitada en un escritorio virtual con sesiones de usuario activas, la apariencia de las sesiones es inconsistente con la experiencia de escritorio de Windows 7 y Windows clásico. Para evitar este problema, debe reiniciar el escritorio virtual después de cambiar esta configuración de directiva. También debe eliminar los perfiles móviles del escritorio virtual. Citrix también recomienda eliminar otros perfiles de usuario del escritorio virtual a fin de evitar inconsistencias entre perfiles.

Si se utilizan perfiles de usuario móviles en el entorno, asegúrese de que la función Enhanced Desktop Experience está habilitada o inhabilitada para todos los escritorios virtuales que comparten un perfil.

Citrix no recomienda el uso compartido de los perfiles móviles entre los escritorios virtuales con sistemas operativos de servidor y de cliente. Los perfiles para sistemas operativos de cliente y sistemas operativos de servidor difieren y el uso compartido de perfiles móviles entre ambos tipos de SO puede dar lugar a incoherencias en las propiedades de los perfiles cuando el usuario pasa de uno a otro.

Configuraciones de directiva de Redirección de archivos

January 29, 2019

La sección “Redirección de archivos” contiene configuraciones relacionadas con la asignación y la optimización de unidades del cliente.

Conectar automáticamente las unidades del cliente

Esta configuración permite o impide la conexión automática de unidades del cliente cuando los usuarios inician sesión.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 USB genérica.

Si está habilitada, los usuarios pueden guardar archivos en todas las unidades del cliente. Si está inhabilitada, se impide cualquier redirección de archivos, independientemente del estado de las configuraciones individuales de redirección de archivos, como Unidades de disco flexible del cliente y Unidades de red del cliente.

Configuraciones de directiva relacionadas:

- Unidades de disco flexible del cliente
- Unidades ópticas del cliente
- Unidades fijas del cliente
- Unidades de red del cliente
- Unidades extraíbles del cliente

Unidades fijas del cliente

Esta configuración permite o impide que los usuarios accedan a las unidades fijas del dispositivo del usuario o guarden archivos en ellas.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

De forma predeterminada, el acceso a las unidades fijas del cliente está permitido.

Al agregar esta configuración a una directiva, compruebe que la configuración Redirección de unidades del cliente está presente y establecida en la opción Permitida. Si esta configuración está inhabilitada, no se asignan las unidades fijas del cliente y los usuarios no pueden acceder a ellas de forma manual, independientemente del estado de la configuración Unidades fijas del cliente.

Para garantizar que las unidades fijas se conecten automáticamente cuando los usuarios inician sesión, configure Conectar automáticamente las unidades del cliente.

Unidades de disco flexible del cliente

Esta configuración permite o impide que los usuarios accedan a las unidades de disco flexible del dispositivo del usuario o guarden archivos en ellas.

De forma predeterminada, el acceso a las unidades de disco flexible del cliente está permitido.

Al agregar esta configuración a una directiva, compruebe que la configuración Redirección de unidades del cliente está presente y establecida en la opción Permitida. Si esta configuración está inhabilitada, no se asignan las unidades de disco flexible del cliente y los usuarios no pueden acceder a ellas de forma manual, independientemente del estado de la configuración Unidades de disco flexible del cliente.

Para garantizar que las unidades de disco flexible se conecten automáticamente cuando los usuarios inician sesión, configure Conectar automáticamente las unidades del cliente.

Unidades de red del cliente

Esta configuración permite o impide que los usuarios accedan a las unidades de red (remotas) o guarden archivos en ellas mediante el dispositivo del usuario.

De forma predeterminada, el acceso a las unidades de red del cliente está permitido.

Al agregar esta configuración a una directiva, compruebe que la configuración Redirección de unidades del cliente está presente y establecida en la opción Permitida. Si esta configuración está inhabilitada, no se asignan las unidades de red del cliente y los usuarios no pueden acceder a ellas de forma manual, independientemente del estado de la configuración Unidades de red del cliente.

Para garantizar que las unidades de red se conecten automáticamente cuando los usuarios inician sesión, configure Conectar automáticamente las unidades del cliente.

Unidades ópticas del cliente

Esta configuración permite o impide que los usuarios tengan acceso a las unidades de CD-ROM, DVD-ROM y BD-ROM en el dispositivo del usuario o guarden archivos en ellas.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

De forma predeterminada, el acceso a las unidades ópticas del cliente está permitido.

Al agregar esta configuración a una directiva, compruebe que la configuración Redirección de unidades del cliente está presente y establecida en la opción Permitida. Si esta configuración está inhabilitada, no se asignan las unidades ópticas del cliente y los usuarios no pueden acceder a ellas de forma manual, independientemente del estado de la configuración Unidades ópticas del cliente.

Para garantizar que las unidades ópticas se conecten automáticamente cuando los usuarios inician sesión, configure Conectar automáticamente las unidades del cliente.

Unidades extraíbles del cliente

Esta configuración permite o impide que los usuarios accedan a las unidades USB del dispositivo del usuario o guarden archivos en ellas.

De forma predeterminada, el acceso a las unidades extraíbles del cliente está permitido.

Al agregar esta configuración a una directiva, compruebe que la configuración Redirección de unidades del cliente está presente y establecida en la opción Permitida. Si esta configuración está inhabilitada, no se asignan las unidades extraíbles del cliente y los usuarios no pueden acceder a ellas de forma manual, independientemente del estado de la configuración Unidades extraíbles del cliente.

Para garantizar que las unidades extraíbles se conecten automáticamente cuando los usuarios inician sesión, configure Conectar automáticamente las unidades del cliente.

Redirección del host al cliente

Esta configuración habilita o inhabilita las asociaciones de tipos de archivos para direcciones URL y contenido multimedia que se abren en el dispositivo del usuario. Si está inhabilitada, el contenido se abre en el servidor.

De forma predeterminada, la asociación de tipos de archivo está inhabilitada.

Cuando se habilita esta configuración, los siguientes tipos de direcciones URL se abren de forma local:

- Protocolo HTTP
- Protocolo HTTP seguro (HTTPS)
- Real Player y QuickTime (RTSP)
- Real Player y QuickTime (RTSPU)
- Real Player (PNM) antiguo
- Microsoft Media Server (MMS)

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Conservar las letras de unidad del cliente

Esta configuración habilita o inhabilita la asignación de unidades del cliente a la misma letra de unidad en la sesión.

De forma predeterminada, las letras de las unidades del cliente no se conservan.

Al agregar esta configuración a una directiva, compruebe que la configuración Redirección de unidades del cliente está presente y establecida en la opción Permitida.

Acceso de lectura solamente a unidades del cliente

Esta configuración permite o impide que los usuarios y las aplicaciones creen o modifiquen archivos o carpetas en las unidades de cliente asignadas.

De forma predeterminada, los archivos y las carpetas en las unidades de cliente asignadas se pueden modificar.

Si se establece en Habilitada, se podrá acceder a los archivos y las carpetas con permisos de solo lectura.

Al agregar esta configuración a una directiva, compruebe que la configuración Redirección de unidades del cliente está presente y establecida en la opción Permitida.

Redirección de carpetas especiales

Esta configuración permite o impide que los usuarios de la aplicación Citrix Workspace y de la Interfaz Web vean las carpetas especiales locales Documentos y Escritorio desde una sesión.

De forma predeterminada, la redirección de carpetas especiales está permitida.

Esta configuración impide la redirección de carpetas especiales para los objetos filtrados mediante una directiva, independientemente de las configuraciones de otras secciones. Cuando se prohíbe esta configuración, se omiten las configuraciones relacionadas especificadas para StoreFront, la Interfaz Web o la aplicación Citrix Workspace.

Para definir qué usuarios podrán usar la redirección de carpetas especiales, seleccione Permitida e incluya esta configuración en una directiva filtrada para los usuarios que desee. Esta configuración sobrescribe cualquier otra configuración de redirección de carpetas especiales.

Como la redirección de carpetas especiales interactúa con el dispositivo del usuario, las configuraciones de directiva que impiden que los usuarios accedan a sus discos duros locales o guarden archivos en ellos también impiden el funcionamiento de la redirección de carpetas especiales.

Al agregar esta configuración a una directiva, compruebe que la configuración “Unidades fijas del cliente” esté presente y establecida en Permitida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Usar escrituras asíncronas

Esta configuración habilita o inhabilita las escrituras asíncronas en los discos.

De forma predeterminada, las escrituras asíncronas están inhabilitadas.

En redes WAN, caracterizadas por mucho ancho de banda y latencia alta, las escrituras asíncronas pueden acelerar la transferencia de archivos y la escritura en los discos del cliente. Sin embargo, si hay un error de conexión o de disco, el archivo o los archivos del cliente que se vayan a escribir pueden terminar en un estado indefinido. Si esto sucede, aparecerá una ventana emergente con la lista de archivos afectados. El usuario puede entonces corregir el error, por ejemplo, puede reanudar la transferencia interrumpida de archivos al volver a conectarse o cuando se corrija el error en el disco.

Citrix recomienda habilitar la escritura asíncrona solamente para usuarios que necesiten conexiones remotas con buena velocidad de acceso a los archivos y en las que el usuario pueda recuperar fácilmente los archivos o datos perdidos cuando haya problemas de conexión o errores en el disco.

Al agregar esta configuración a una directiva, compruebe que la configuración Redirección de unidades del cliente está presente y establecida en la opción Permitida. Si esta configuración está inhabilitada, no se realizan escrituras asíncronas.

Configuraciones de directiva de Redirección de Flash

December 14, 2018

La sección Redirección de Flash contiene configuraciones de directiva para gestionar el contenido Flash en las sesiones de usuario.

Aceleración de Flash

Esta configuración habilita o inhabilita la opción de generar el contenido Flash en los dispositivos del usuario en lugar del servidor. De forma predeterminada, la generación del contenido Flash en el cliente está habilitada.

Nota: Esta configuración se usa para la redirección de Flash antigua con Citrix Online Plug-in 12.1.

Cuando está habilitada, esta configuración reduce la carga de red y de servidor al generar el contenido Flash en el dispositivo del usuario. Además, la configuración Lista de compatibilidad de URL de Flash hace que el contenido Flash de sitios Web específicos se genere en el servidor.

En el dispositivo del usuario, la configuración “Habilitar la redirección de HDX MediaStream para Flash en el dispositivo de usuario” también debe estar habilitada.

Si esta configuración está inhabilitada, el contenido Flash de todos los sitios Web, independientemente de la URL, se genera en el servidor. Para permitir que solamente determinados sitios Web

© 1999-2019 Citrix Systems, Inc. All rights reserved.

puedan generar el contenido Flash en el dispositivo del usuario, configure la Lista de compatibilidad de URL de Flash.

Lista de colores de fondo de Flash

Esta configuración permite establecer colores clave para determinadas URL.

De forma predeterminada, no hay colores clave especificados.

Los colores clave aparecen en el fondo del contenido Flash generado en el cliente y ayudan a detectar regiones visibles. El color clave especificado debe ser poco común; de lo contrario, es posible que la detección de regiones visibles no funcione correctamente.

Las entradas válidas consisten en una URL (con caracteres comodín optativos al comienzo o al final) seguida de un código hexadecimal de color RGB de 24 bits. Por ejemplo: http://citrix.com 000003.

Compruebe que la URL especificada es la URL del contenido Flash, que puede diferir de la URL del sitio Web.

> **Advertencia**
>
> El uso incorrecto del Editor del Registro del sistema puede causar problemas graves que pueden hacer necesaria la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del Registro antes de editarlo.

En máquinas de agente VDA con Windows 8 o Windows 2012, puede que esta configuración no establezca los colores clave de la URL. Si esto ocurre, modifique el Registro en la máquina de agente VDA.

Para máquinas de 32 bits, use este parámetro de Registro:
[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer] “ForceHDXFlashEnabled”=dword:00000001

Para máquinas de 64 bits, use este parámetro de Registro:
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer] “ForceHDXFlashEnabled”=dword:00000001

Compatibilidad con versiones anteriores de Flash

Esta configuración habilita o inhabilita el uso de las funciones de redirección originales de versiones anteriores de Flash con versiones antiguas de la aplicación Citrix Workspace (antes denominado Citrix Online Plug-in).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

De manera predeterminada, esta configuración está habilitada.

En el dispositivo del usuario, la configuración “Habilitar la redirección de HDX MediaStream para Flash en el dispositivo de usuario” también debe estar habilitada.

Las funciones de redirección de Flash de segunda generación están habilitadas para usarlas con Citrix Receiver 3.0. Las funciones de redirección antiguas reciben respaldo para su uso con Citrix Online Plug-in 12.1. Para garantizar que se usan las funciones de redirección de Flash de segunda generación, tanto el servidor como el dispositivo del usuario deben tener habilitada la redirección de Flash de segunda generación. Si la redirección antigua está habilitada o en el servidor o en el dispositivo del usuario, se usarán las funciones de redirección antiguas.

Comportamiento predeterminado de Flash

Esta configuración establece el comportamiento predeterminado de la aceleración de Flash de segunda generación.

De manera predeterminada, la aceleración de Flash está habilitada.

Para definir esta configuración, elija alguna de estas opciones:

- Habilitar aceleración de Flash.Se usa la redirección de Flash.
- Bloquear reproductor de Flash.No se usa la redirección de Flash ni la generación en el lado del servidor. El usuario no puede ver ningún contenido Flash.
- Inhabilitar aceleración de Flash.No se usa la redirección de Flash. El usuario puede ver el contenido Flash generado en el servidor si se ha instalado en el servidor una versión de Adobe Flash Player para Windows Internet Explorer compatible con el contenido.

Esta configuración se puede anular para determinadas páginas Web e instancias de Flash basándose en la configuración de la Lista de compatibilidad de URL de Flash. Además, la configuración Habilitar la redirección de HDX MediaStream para Flash en el dispositivo de usuario también debe estar habilitada en el dispositivo del usuario.

Registro de sucesos de Flash

Esta configuración permite que los sucesos de Flash se capturen en el registro de sucesos de la aplicación de Windows.

De forma predeterminada, el registro está permitido.

En los equipos con Windows 7 o Windows Vista, aparece un registro específico de redirección de Flash en el nodo del registro de aplicaciones y servicios.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Respaldo inteligente de Flash

Esta configuración habilita o inhabilita los intentos automáticos de utilizar la generación en el lado del servidor para instancias del reproductor de Flash para las que la generación en el lado del cliente no sea necesaria o empeore la experiencia del usuario.

De manera predeterminada, esta configuración está habilitada.

Umbral de latencia de Flash

Esta configuración especifica un umbral entre 0 y 30 milésimas de segundo para determinar dónde se genera el contenido de Adobe Flash.

De forma predeterminada, el umbral es de 30 milésimas de segundo.

Durante el inicio, HDX MediaStream para Flash mide la latencia actual entre el servidor y el dispositivo del usuario. Si la latencia es inferior al umbral, se usa HDX MediaStream para Flash a fin de generare el contenido Flash en el dispositivo del usuario. Si la latencia es superior al umbral, el servidor de red genera el contenido si hay un reproductor de Adobe Flash disponible.

Cuando habilite esta configuración, compruebe que la configuración Compatibilidad con versiones anteriores de Flash esté presente y establecida en Habilitada.

Nota: Se aplica solo cuando se usa la redirección de Flash de HDX MediaStream en modo Legacy (funciones antiguas).

Impedimento para recurrir al vídeo Flash

Esta configuración especifica si un contenido “pequeño” de Flash se reproduce y, en caso de que lo haga, cómo se generará y cómo lo verán a los usuarios.

De manera predeterminada, esta configuración no está definida.

Para definir esta configuración, elija alguna de estas opciones:

- **Solo contenido pequeño.** Solo se genera contenido de respaldo inteligente en el servidor; el resto del contenido Flash se reemplazará por un error *.swf.
- **Solo contenido pequeño con un cliente compatible.** Solo se genera contenido de respaldo inteligente en el servidor si el cliente está usando la redirección de Flash; el resto del contenido se reemplazará por un error *.swf.
- **Sin contenido del lado del servidor.** Todo el contenido presente en el servidor se reemplazará por un error *swf.

Para usar esta configuración de directiva, debe especificar un archivo de error *.swf. Este error *.swf reemplazará cualquier contenido que usted no quiera que se genere en el agente VDA.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Error de impedimento para el respaldo de vídeo Flash (*.swf)

Esta configuración especifica la URL del mensaje de error que se mostrará a los usuarios en lugar de las instancias de Flash cuando se utilicen las directivas de administración de carga en el servidor. Por ejemplo:

http://domainName.tld/sample/path/error.swf

Lista de URL para obtener contenido Flash del lado del servidor

Esta configuración especifica sitios Web cuyo contenido Flash se puede descargar en el servidor y transferir luego al dispositivo del usuario para generarse allí.

De forma predeterminada, no hay ningún sitio especificado.

Esta configuración se utiliza cuando el dispositivo del usuario no tiene acceso directo a Internet, sino que es el servidor el que suministra esa conexión. Además, el dispositivo del usuario debe tener habilitada la configuración "Habilitar obtención de contenido del lado del servidor".

La redirección de Flash de segunda generación incluye una opción de respaldo para obtener contenido del lado del servidor para archivos de Flash .swf. Si el dispositivo del usuario no puede obtener contenido Flash de un sitio Web y el sitio Web está incluido en la lista de URL para obtener contenido Flash del lado del servidor, la obtención se produce automáticamente.

Cuando agregue direcciones URL a la lista:

- Agregue la URL de la aplicación Flash en lugar de la página HTML superior que inicia el reproductor de Flash.
- Use un asterisco (*) al comienzo o al final de la URL como comodín.
- Use un carácter comodín al final para permitir todas las URL secundarias (`http://www.citrix.com/*`).
- Los prefijos `http://` y `https://` se usan cuando existen, pero no son necesarios en las entradas de la lista.

Lista de compatibilidad de URL de Flash

Esta configuración especifica las reglas que determinan si el contenido Flash de ciertos sitios Web se genera en el dispositivo del usuario, se genera en el servidor o se bloquea y, por tanto, no se genera.

De forma predeterminada, no se especifica ninguna regla.

Cuando agregue direcciones URL a la lista:

- Establezca un orden de prioridad en la lista situando las URL, acciones y ubicaciones de generación de contenido más importantes en la parte superior.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Use un asterisco (*) al comienzo o al final de la URL como comodín.
- Use un carácter comodín al final para hacer referencia a todas las URL secundarias (`http://www.citrix.com/*`).
- Los prefijos `http://` y `https://` se usan cuando existen, pero no son necesarios en las entradas de la lista.
- Agregue a esta lista los sitios Web cuyo contenido de Flash no se genera correctamente en el dispositivo del usuario, y seleccione la opción Generar en servidor o la opción Bloquear.

Configuraciones de directiva de Gráficos

March 8, 2019

La sección Gráficos contiene configuraciones de directiva para controlar la gestión de imágenes en las sesiones de usuario.

Permitir compresión sin pérdida visual

Esta configuración permite usar compresión sin pérdida visual en lugar de compresión sin pérdida verdadera para los gráficos. La compresión sin pérdida visual mejora el rendimiento en mayor medida que la compresión sin pérdida verdadera, con una pérdida menor que no se nota a la vista. Esta configuración cambia el modo en que se usan los valores de la configuración Calidad visual.

De forma predeterminada, esta configuración está inhabilitada.

Indicador de estado de gráficos

Esta configuración definirá el indicador del estado de gráficos que se va a ejecutar en la sesión del usuario. Lo que permitirá ver datos sobre el modo de gráficos en uso, incluido el proveedor de gráficos, el codificador, la codificación por hardware, la calidad de imagen, el estado de pantalla progresiva y la compresión sin pérdida de texto.

De forma predeterminada, el indicador del modo de gráficos está inhabilitado. Esta configuración sustituye al indicador de compresión sin pérdida. En las versiones anteriores de Citrix Virtual Apps and Desktops, se habilita el indicador de compresión sin pérdida en lugar del indicador del modo de gráficos.

Límite de memoria de presentación

Esta configuración permite especificar el tamaño máximo de búfer para vídeo, en kilobytes, asignado a la sesión.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

El límite de memoria de presentación predeterminado es de 65536 kilobytes.

Permite especificar el tamaño máximo de búfer para vídeo, en kilobytes, asignado a la sesión. Especifique una cifra en kilobytes de 128 a 4 194 303. El valor máximo (4,194,303) no limita la memoria de presentación. La memoria de presentación predeterminada es de 65536 kilobytes. Si se utiliza mayor profundidad de color y mayor resolución para las conexiones, se necesitará más memoria. En el modo de gráficos antiguos, si se alcanza el límite de memoria, la presentación se degrada según esté definida la configuración Preferencia de degradación de presentación.

Para las conexiones que requieran mayor profundidad de color y mayor resolución, aumente el límite. Puede calcular la memoria máxima necesaria con la siguiente ecuación:

Profundidad de memoria en bytes = (profundidad de color en bits por píxel) / 8) x (resolución vertical en píxeles) x (resolución horizontal en píxeles).

Por ejemplo, si la profundidad de color es 32, la resolución vertical es 600 y la resolución horizontal es 800, la memoria máxima necesaria es (32 / 8) x (600) x (800) = 1 920 000 bytes, por lo que habría que establecer el límite de memoria de presentación en 1920 KB.

Las profundidades de color que no son de 32 bits solo están disponibles si la configuración de directiva Modo de gráficos antiguo está habilitada.

HDX asigna solo la cantidad de memoria de presentación necesaria para cada sesión. Por lo tanto, si tan solo algunos usuarios necesitan más memoria de la predeterminada, no hay ningún impacto negativo en la escalabilidad si se aumenta el límite de memoria de presentación.

Preferencia de degradación de presentación

Nota: Para Virtual Delivery Agent 7.x, esta configuración de directiva solo se aplica cuando la configuración de directiva Modo de gráficos antiguo está habilitada.

Esta configuración permite especificar que la profundidad de color o la resolución sean las primeras características en degradarse cuando se alcance el límite de memoria para la presentación.

De forma predeterminada, se degrada primero la profundidad de color.

Cuando se alcanza el límite de memoria para presentación, se puede reducir la calidad de la imagen presentada e indicar si se degradará primero la profundidad de color o la resolución. Cuando se degrada primero la profundidad de color, se usan menos colores para las imágenes. Cuando se degrada primero la resolución, se muestran las imágenes con menos píxeles por pulgada.

Para notificar a los usuarios de la degradación de la profundidad de color o de la resolución, defina la configuración Notificar al usuario cuando se degrada la presentación.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Vista previa de ventanas dinámicas

Esta configuración permite habilitar o inhabilitar la presentación de las ventanas integradas en los modos de vista previa Rotar, 3D rotado, Barra de tareas y Vistazo.

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 secciones de imágenes y su recuperación a medida que se necesitan, permite que el desplazamiento por la imagen sea más suave, reduce la cantidad de datos transmitidos por la red y reduce el procesamiento necesario en el dispositivo del usuario.

De forma predeterminada, el almacenamiento en caché de imágenes está habilitado.

Nota: La configuración de almacenamiento en caché de imágenes controla el modo en que se almacenan y se recuperan las imágenes; no controla si las imágenes se almacenan o no. Las imágenes se almacenan en caché si la configuración Modo de gráficos antiguo está habilitada.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 antiguo 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 recibe respaldo en los VDA con Windows 7 y Windows Server 2008 R2.

El modo de gráficos antiguo no recibe respaldo en Windows 8.x, 10 o Windows Server 2012, 2012 R2 y 2016.

Consulte CTX202687 para ver más información sobre la optimización de los modos de gráficos y directivas en XenApp y XenDesktop 7.6 FP3 o versiones posteriores.

Profundidad de color máxima permitida

Nota: Para Virtual Delivery Agent 7.x, esta configuración de directiva solo se aplica cuando la configuración de directiva Modo de gráficos antiguo está habilitada.

Esta configuración permite especificar la profundidad de color máxima permitida para una sesión.

De manera predeterminada, la profundidad de color máxima permitida es de 32 bits por píxel.

Esta configuración se aplica solo a conexiones y controladores Thinwire. No se aplica a agentes VDA que tienen un controlador de pantalla principal que no sea Thinwire, como los agentes VDA que usan un controlador Windows Display Driver Model (WDDM) en calidad de controlador de pantalla principal. Para agentes VDA con SO de escritorio que utilicen un controlador WDDM como controlador de pantalla principal (como Windows 8), esta configuración no tiene ningún efecto. Para agentes VDA con SO de servidor Windows que utilicen un controlador WDDM (como Windows Server 2012 R2), esta configuración puede impedir que los usuarios se conecten a los VDA.

Una mayor profundidad de color requerirá más memoria. Para que se degrade la profundidad de color cuando se alcanza el límite de memoria, configure Preferencia de degradación de presentación. Cuando se degrada la profundidad de color, se usan menos colores para las imágenes.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 reemplazadas por otra imagen.

De manera predeterminada, la configuración “Cola y descarte” está habilitada.

Así se 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 aplicará como el códec predeterminado para todo. Si selecciona **Para áreas en cambio constante**, el códec de vídeo se usará para las áreas donde haya cambios constantes en pantalla, mientras que para los demás datos se usará 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 está respaldada 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 mucho vídeo 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 volverá 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 escritorio.

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 se ha habilitado, “Sin pérdida de texto” tiene prioridad sobre la codificación por hardware NVENC.

Se admite el uso selectivo del códec de hardware H.264 para áreas en cambio constante.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 escritorio y agentes VDA para SO de servidor.

Se admiten los procesadores de gráficos Intel Iris Pro de la familia de procesadores Intel Broadwell y versiones posteriores. Se requiere el SDK del codificador de hardware Intel Iris Pro; puede descargarse desde el 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 puede definir esta configuración de directiva por usuario o por máquina.

Configuraciones de directiva de Almacenamiento en caché

December 14, 2018

La sección Almacenamiento en caché contiene configuraciones de directiva que permiten el almacenamiento en caché de los datos de imágenes en los dispositivos de usuario cuando el ancho de banda es limitado en las conexiones con el cliente.

Umbral de caché persistente

Nota: Para Virtual Delivery Agent 7.x, esta configuración de directiva solo se aplica cuando la configuración de directiva Modo de gráficos antiguo está habilitada.

Esta configuración almacena en caché los mapas de bits en las unidades de disco duro del dispositivo del usuario. Esto permite la reutilización de imágenes grandes de sesiones anteriores que se usan con frecuencia.

De manera predeterminada, el valor umbral es de 3000000 bits por segundo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Este valor representa el umbral por debajo del cual tendrá efecto la función de caché persistente. Es decir, con el valor predeterminado, los mapas de bits se almacenan en caché en el disco duro del dispositivo del usuario cuando el ancho de banda está por debajo de 3000000 bps.

Configuraciones de directiva de Framehawk

October 3, 2018

La sección Framehawk contiene configuraciones de directiva para habilitar y configurar el canal de presentación Framehawk en el servidor.

Canal de presentación Framehawk

Cuando se habilita, el servidor intenta usar el canal virtual Framehawk para la presentación remota de entradas y gráficos del usuario. Ese canal de presentación usará UDP para ofrecer una mejor experiencia de usuario en redes con grandes pérdidas de paquetes y latencia alta. Sin embargo, también puede utilizar más recursos y ancho de banda del servidor que otros modos gráficos.

De forma predeterminada, el canal de presentación Framehawk está inhabilitado.

Intervalo de puertos del canal de presentación Framehawk

Esta configuración de directiva permite especificar el intervalo de números de puerto UDP (con el formato *número de puerto más bajo,número de puerto más alto*) que el VDA utiliza para intercambiar datos del canal de presentación Framehawk con el dispositivo de usuario. El agente VDA intenta utilizar todos los puertos, comenzando por el de número más bajo y subiendo en cada intento subsiguiente. El puerto gestiona el tráfico de entrada y salida.

De forma predeterminada, el intervalo de puertos es 3224,3324.

Configuraciones de directiva de Keep Alive

October 3, 2018

La sección Keep Alive contiene configuraciones de directiva para gestionar los mensajes de ICA Keep Alive.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Tiempo de espera de ICA Keep Alive

Esta configuración permite especificar cuántos segundos deben transcurrir entre los mensajes sucesivos de ICA Keep Alive.

El intervalo predeterminado para los mensajes de Keep Alive es de 60 segundos.

Especifique un intervalo entre 1 y 3600 segundos para el envío de mensajes de ICA Keep Alive. No configure esto si tiene un software de supervisión de red que se encarga de cerrar las conexiones inactivas.

ICA Keep Alive

Esta configuración habilita o inhabilita el envío periódico de mensajes de ICA Keep Alive.

De manera predeterminada, no se envían mensajes de Keep Alive.

Si se habilita esta configuración, se evita la desconexión de las conexiones interrumpidas. Si el servidor no detecta ninguna actividad, esta configuración evita que los Servicios de Escritorio remoto (RDS) desconecten la sesión. El servidor envía mensajes de Keep Alive cada pocos segundos para detectar si la sesión está activa. Si la sesión ya no está activa, el servidor la marca como desconectada.

La función ICA Keep Alive no funciona si se usa Fiabilidad de la sesión. Configure ICA Keep Alive únicamente para conexiones que no usen Fiabilidad de la sesión.

Configuraciones de directiva relacionadas: Conexiones de fiabilidad de la sesión.

Configuraciones de directiva de Acceso a aplicaciones locales

October 3, 2018

La sección “Acceso a aplicaciones locales” contiene configuraciones de directiva para gestionar la integración de las aplicaciones de los usuarios instaladas localmente con las aplicaciones alojadas en un entorno de escritorios alojados.

Permitir acceso a aplicaciones locales

Esta configuración permite o impide la integración de las aplicaciones de usuarios instaladas localmente con las aplicaciones alojadas en un entorno de escritorios alojados.

Cuando un usuario inicia una aplicación instalada localmente, la aplicación parece ejecutarse en su escritorio virtual, aunque en realidad se está ejecutando de forma local.

De forma predeterminada, el acceso a aplicaciones locales está prohibido.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Lista negra de redirección de URL

Esta configuración especifica los sitios Web que se redirigen y se inician en el explorador Web local. Pueden incluirse los sitios Web que requieren información regional (como msn.com o news-google.com), o bien, sitios Web con contenido multimedia enriquecido que se genera mejor en el dispositivo del usuario.

De forma predeterminada, no hay ningún sitio especificado.

Lista blanca 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

October 3, 2018

La sección Experiencia móvil contiene configuraciones de directiva para la gestión de Citrix Mobility Pack.

Presentación automática del teclado

Esta configuración habilita o inhabilita la presentación automática del teclado en las pantallas de los dispositivos móviles.

De manera predeterminada, la presentación automática del teclado está inhabilitada.

Iniciar escritorio con optimización táctil

Esta configuración está inhabilitada y no está disponible para máquinas Windows 10 o Windows Server 2016.

Esta configuración determina el comportamiento general de la interfaz de la aplicación Citrix Workspace, ya que permite o prohíbe una interfaz táctil intuitiva, optimizada para dispositivos tipo tableta.

De forma predeterminada, se utiliza una interfaz táctil intuitiva.

Para usar solo la interfaz de Windows, defina esta configuración de directiva como Prohibida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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

January 29, 2019

La sección Multimedia contiene configuraciones de directiva para gestionar la transmisión por streaming de sonido y vídeo HTML5 y Windows a las sesiones de usuario.

> **Advertencia**
>
> Si modifica el Registro de forma incorrecta, pueden producirse problemas graves, que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

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

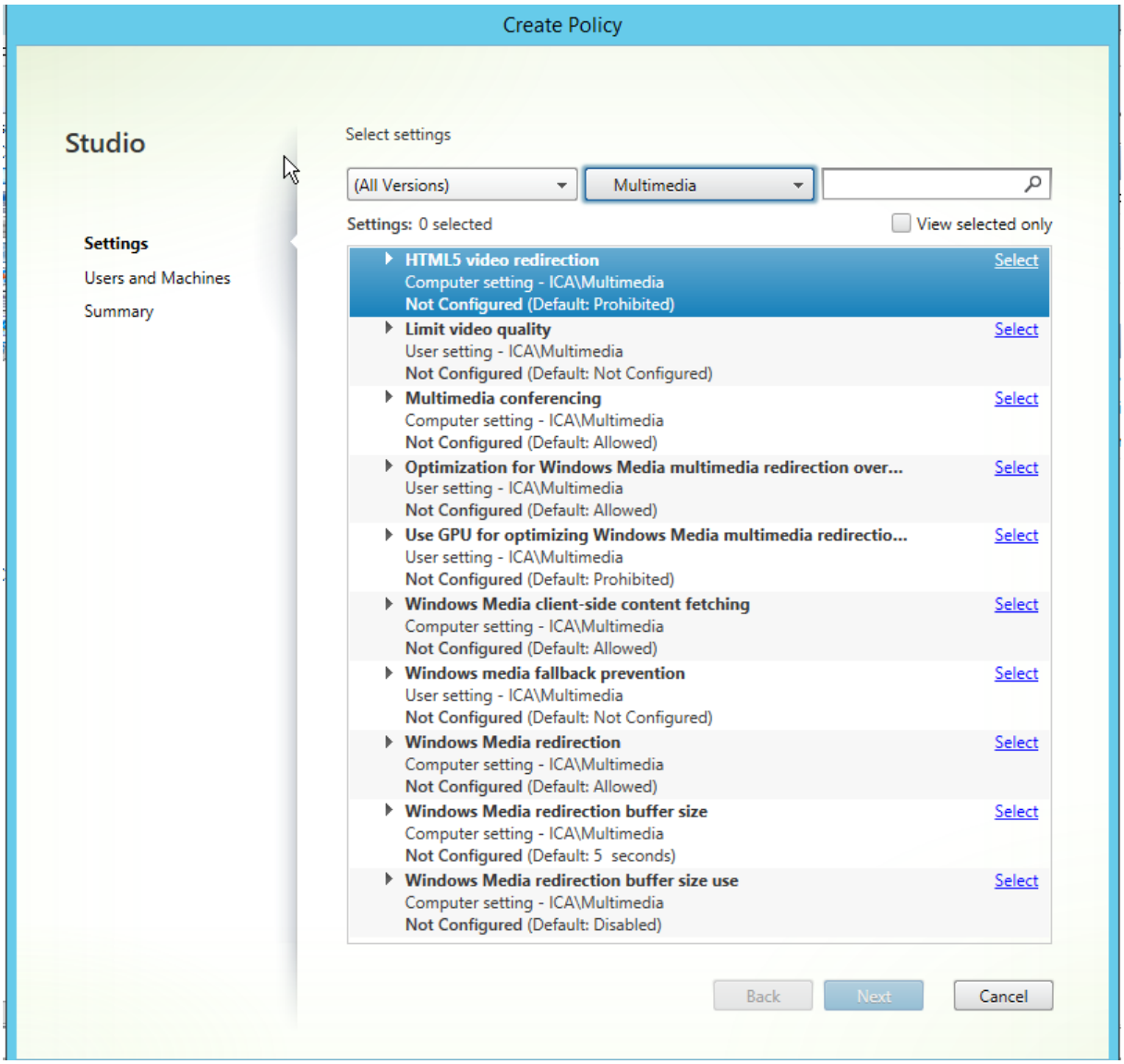
Para buscar el ID de sesión del usuario actual (User Session ID), emita el comando **qwinsta** desde la línea de comandos de Windows.

Redirección de vídeo HTML5

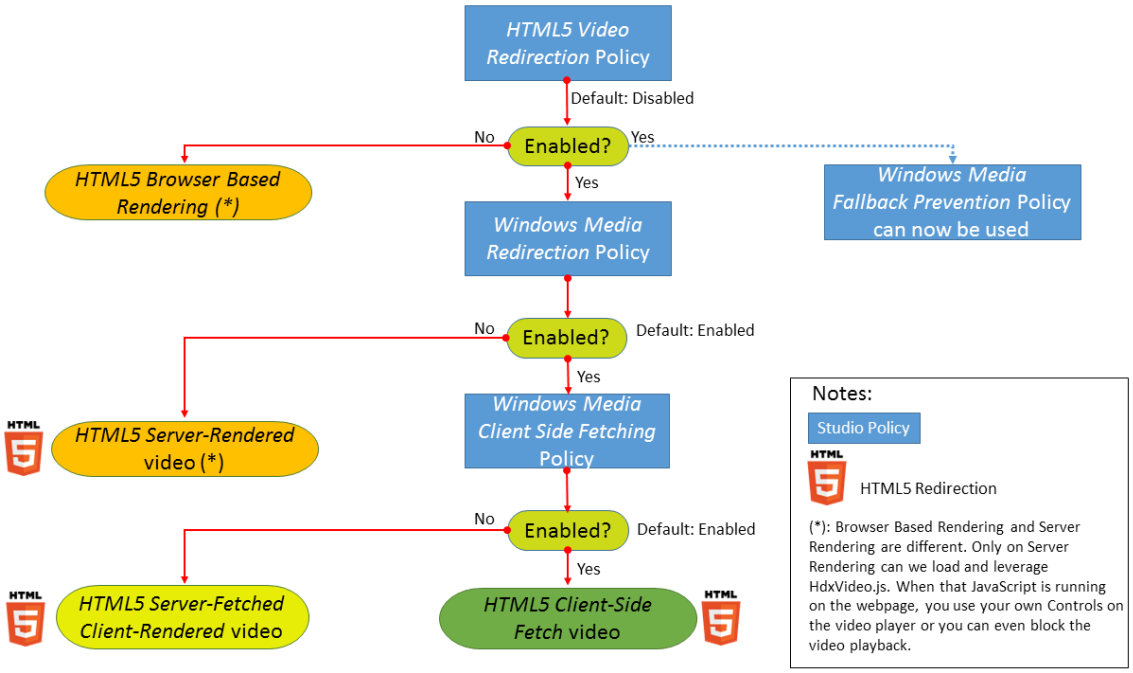
Controla y optimiza el modo en que los servidores Citrix Virtual Apps and Desktops entregan contenido multimedia Web de HTML5 a los usuarios.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

De forma predeterminada, esta configuración está inhabilitada.



© 1999-2019 Citrix Systems, Inc. All rights reserved.



En esta versión, esta funcionalidad está disponible solo para las páginas Web controladas. Requiere agregar JavaScript a las páginas Web que tengan contenido multimedia para HTML5 disponible; por ejemplo, vídeos en un sitio interno de formación.

Para configurar la redirección de vídeo HTML5:

1. Copie el archivo **HdxVideo.js** de %Archivos de programa%/Citrix/ICA Service/HTML5 Video Redirection en la instalación del VDA a la ubicación de la página Web interna.
2. Inserte esta línea en la página Web (si la página Web tiene otros scripts, incluya **HdxVideo.js** antes de ellos):
   `<script src=”HdxVideo.js”type=”text/javascript”\></script>`

Nota: Si HdxVideo.js no está en la misma ubicación que la página Web, utilice el atributo **src** para especificar la ruta completa a él.

Si no se agrega JavaScript a las páginas Web controladas y el usuario reproduce un vídeo HTML5, Citrix Virtual Apps and Desktops recurrirán a la generación en el lado del servidor.

Debe estar permitida la ***Redirección de Windows Media*** para que la Redirección de vídeo HTML5 funcione correctamente. Esta directiva es obligatoria para Obtención en servidor, generación en cliente, y es necesaria para Obtención del lado del cliente (que a su vez requiere que *Obtención de contenido de Windows Media en el lado del cliente* esté permitida).

Microsoft Edge no admite esta función.

HdxVideo.js reemplaza los controles del reproductor HTML5 del explorador por los suyos propios. Para comprobar que la directiva Redirección de vídeo HTML5 está en vigor para un determinado sitio

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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
- sonido
- pantalla completa

Dispone de una página para pruebas de redirección de vídeo HTML5 en https://www.citrix.com/virtualization/hdx/html5-redirect.html.

TLS y la redirección de vídeos HTML5

Puede usar la redirección de vídeo HTML5 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 conseguir esta redirección y mantener la integridad TLS de la página Web, el servicio Citrix HDX HTML5 Video Redirection Service genera dos certificados personalizados en el almacén de certificados del VDA.

HdxVideo.js utiliza Secure WebSockets para comunicarse con WebSocketService.exe que se ejecuta en el VDA. Este proceso se ejecuta en el sistema local y realiza la terminación SSL y la asignación de sesiones de usuario.

WebSocketService.exe escucha en 127.0.0.1 en el puerto 9001.

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*.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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.

Conferencia multimedia

Esta configuración permite o impide el uso de tecnología optimizada de redirección para cámara Web mediante aplicaciones de videoconferencia.

De forma predeterminada, el respaldo para videoconferencia está permitido.

Al agregar esta configuración a una directiva, compruebe que la configuración Redirección de Windows Media esté presente y establecida en Permitida (opción predeterminada).

Si hace uso de 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 videoconferencia. 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 videoconferencia.

Esta directiva no es necesaria cuando la cámara Web se redirige utilizando la redirección USB genérica. 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.Esta configuración permite la transcodificación multimedia en tiempo real, lo que permite la transmisión por streaming de medios de sonido y vídeo a dispositivos móviles en condiciones degradadas de red y mejora la experiencia del usuario al mejorar la entrega del contenido de Windows Media a través de redes WAN.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

De forma predeterminada, la entrega de contenido de Windows Media a través de WAN está optimizada.

Al agregar esta configuración a una directiva, asegúrese de que la configuración **Redirección de Windows Media** esté presente y establecida en **Permitida**.

Cuando esta configuración está habilitada, la transcodificación de multimedia en tiempo real se implementa automáticamente según sea necesario para la transmisión multimedia por streaming y proporciona una experiencia de usuario fluida incluso en condiciones de conexión extremas.

Usar GPU para optimizar redirección de medios de Windows Media sobre WAN

Esta configuración 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 está respaldada en las GPU de NVIDIA.

De forma predeterminada, el uso de la GPU en el VDA para optimizar la entrega de contenido de Windows Media a través de WAN está prohibido.

Al agregar esta configuración a una directiva, compruebe que las configuraciones Redirección de Windows Media y Optimización de la redirección de medios de Windows Media sobre WAN estén presentes y establecidas como Permitidas.

Prevención de respaldo de Windows Media

Esta configuración solo se aplica a Windows Media, no a HTML5. Para que funcione con HTML5, establezca la directiva **Redirección de vídeo HTML** en **Permitida**.

Los administradores pueden usar la directiva Prevención de respaldo 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**.

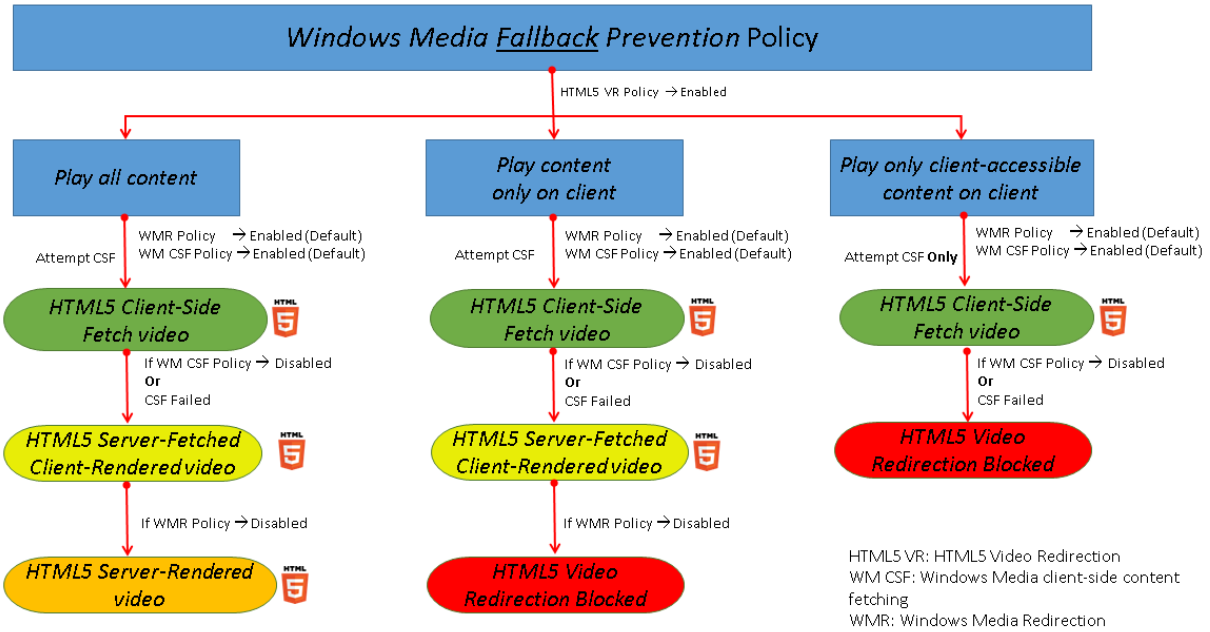
Para definir esta configuración, elija alguna de estas opciones:

- **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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Reproducir solo el contenido accesible por el cliente**. Solo intentar la obtención de contenido del lado del cliente. Si no se realiza correctamente, no se reproduce el contenido.

Si el contenido no se reproduce, aparece el mensaje de error “La empresa ha bloqueado el vídeo debido a falta de recursos” en la ventana del reproductor (durante una periodo predeterminado de 5 segundos).



La duración de este mensaje de error puede ajustarse con la siguiente clave de Registro en el VDA. Si no existe la entrada del Registro, se usa la duración predeterminada (5 segundos).

La ruta del Registro varía en función de la arquitectura del VDA:

\HKLM\SOFTWARE\Wow6432Node\Citrix\HdxMediastream

O bien

\HKLM\SOFTWARE\Citrix\HdxMediastream

Clave del Registro:

Nombre: VideoLoadManagementErrDuration

Tipo: DWORD

Intervalo: 1 - hasta el límite DWORD (predeterminado = 5)

Unidad: segundos

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Obtención de contenido de Windows Media en el lado del cliente

Esta configuración solo se aplica a Windows Media, no a HTML5. Esta configuración permite a un dispositivo de usuario distribuir por streaming los archivos multimedia directamente desde su proveedor de origen en Internet o Intranet, en vez de hacerlo a través del servidor host de XenApp o XenDesktop.

De forma predeterminada, esta configuración está **Permitida**. Cuando se habilita esta configuración, se mejora el uso de la red y la escalabilidad del servidor porque se transfiere el procesamiento del medio desde el servidor host al dispositivo del usuario. También elimina la necesidad de tener instalado un software de infraestructura multimedia avanzado, como Microsoft DirectShow o Media Foundation, en el dispositivo del usuario; el dispositivo del usuario requiere solo la capacidad de reproducir un archivo a partir de una URL.

Al agregar esta configuración a una directiva, asegúrese de que la configuración **Redirección de Windows Media** esté presente y establecida en **Permitida**. Si **Redirección de Windows Media** está inhabilitada, también está inhabilitada la distribución por streaming de archivos multimedia al dispositivo del usuario directamente desde el proveedor de origen.

Redirección de Windows Media

Esta configuración se aplica a HTML5 y Windows Media. Controla y optimiza el modo en que los servidores entregan audio y vídeo por streaming a los usuarios.

De forma predeterminada, esta configuración está **Permitida**. Para HTML5, esta configuración no se aplica si la directiva **Redirección de vídeo HTML5** está **Prohibida**.

Cuando se habilita esta configuración, se aumenta la calidad de sonido y vídeo que se genera desde el servidor a un nivel comparable al del sonido y el vídeo ejecutados localmente en un dispositivo del usuario. El servidor transmite por streaming el material multimedia al cliente en el formato original comprimido y deja que el dispositivo del usuario lo descomprima y lo genere.

La función de redirección de Windows Media optimiza los archivos multimedia codificados con códecs que cumplen con las normas DirectShow de Microsoft, DirectX Media Objects (DMO) y Media Foundation. Para reproducir un archivo multimedia específico, el dispositivo del usuario debe tener un códec compatible con el formato de cifrado del archivo multimedia.

De forma predeterminada, el audio está inhabilitado en la aplicación Citrix Workspace. Para permitir que los usuarios ejecuten aplicaciones multimedia en sesiones ICA, habilite el audio u otorgue permisos a los usuarios para que lo habiliten en su interfaz de la aplicación Citrix Workspace.

Seleccione **Prohibida** solamente si la reproducción multimedia con la redirección de Windows Media resulta ser peor que cuando se genera usando la compresión básica de ICA y el sonido normal. Esta

© 1999-2019 Citrix Systems, Inc. All rights reserved.

situación no es habitual, pero puede ocurrir en condiciones de ancho de banda bajo; por ejemplo, con medios que tengan una frecuencia de fotogramas clave muy baja.

Tamaño del búfer para la redirección de Windows Media

Esta configuración es antigua y no se aplica a HTML5.

Esta configuración permite especificar un tamaño de búfer de entre 1 y 10 segundos para la aceleración multimedia.

El tamaño predeterminado es de 5 segundos.

Uso del tamaño de búfer para redirección de Windows Media

Esta configuración es antigua y no se aplica a HTML5.

Esta configuración habilita o inhabilita el uso del tamaño del búfer especificado en **Tamaño del búfer para la redirección de Windows Media**.

De forma predeterminada, no se usa el tamaño de búfer especificado.

Si esta configuración está inhabilitada o el Tamaño del búfer para la redirección de Windows Media no se ha configurado, el servidor usa el valor de búfer predeterminado (5 segundos).

Configuraciones de directiva de Conexiones de multisecuencia

January 29, 2019

La sección “Conexiones de multisecuencia” contiene configuraciones de directiva para gestionar las prioridades de Calidad de servicio (QoS) cuando hay varias conexiones ICA en una sesión.

Sonido sobre UDP

Esta configuración permite o impide el sonido sobre UDP en el servidor.

De forma predeterminada, el sonido sobre UDP está inhabilitado en el servidor.

Cuando está habilitada, esta configuración abre un puerto UDP en el servidor para dar respaldo a todas las conexiones configuradas para usar el Transporte de sonido en tiempo real sobre UDP.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Intervalo de puertos UDP de sonido

Esta configuración especifica el intervalo de números de puerto (con el formato "número de puerto más bajo,número de puerto más alto") que Virtual Delivery Agent (VDA) utiliza para intercambiar datos de paquetes de audio con el dispositivo del usuario. VDA intenta utilizar cada par de puertos UDP para intercambiar datos con el dispositivo del usuario, comenzando por el número menor y aumentando en incrementos de 2 en cada intento subsiguiente. Cada puerto gestiona tanto el tráfico de entrada como el de salida.

De forma predeterminada, este valor está establecido en 16500,16509.

Directiva Puertos múltiples

Esta configuración especifica los puertos TCP que deben usarse para el tráfico ICA y establece la prioridad de red para cada puerto.

De forma predeterminada, el puerto primario (2598) tiene prioridad Alta.

Cuando configure los puertos, puede asignarles las siguientes prioridades:

- Muy alta: Para las actividades en tiempo real, como conferencias con cámaras Web.
- Alta: Para los elementos interactivos, como la pantalla, el teclado y el puntero.
- Media: Para procesos con gran cantidad de datos, como la asignación de unidades del cliente.
- Baja: Para las actividades en segundo plano, como la impresión.

Cada puerto debe tener una prioridad exclusiva. Por ejemplo, no puede asignar la prioridad Muy alta a dos puertos, como CGP puerto 1 y CGP puerto 3.

Para quitar un puerto del sistema de prioridades, defina el número de puerto como 0. El puerto primario no puede eliminarse y no se puede modificar su nivel de prioridad.

Después de definir esta configuración, reinicie el servidor. Esta configuración solo tiene efecto después de haber habilitado la configuración de directiva Configuración de equipo para multisecuencia.

Configuración de equipo para multisecuencia

Esta configuración habilita o inhabilita la multisecuencia en el servidor.

De forma predeterminada, la multisecuencia está inhabilitada.

Si usa Citrix SD-WAN con respaldo para multisecuencia en el entorno, no es necesario definir esta configuración. Defina esta configuración de directiva cuando esté usando enrutadores externos o versiones antiguas de Branch Repeater para conseguir el nivel de Calidad de servicio (QoS) que necesite.

Cuando defina esta configuración, reinicie el servidor para que los cambios tengan efecto.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> **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.

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.

Configuraciones de directiva de Redirección de puertos

October 3, 2018

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Conectar automáticamente puertos LPT del cliente

Esta configuración habilita o inhabilita la conexión automática de los puertos LPT en los dispositivos del usuario cuando este inicia sesión en un sitio.

Los puertos LPT del cliente no se conectan automáticamente de forma predeterminada.

Redirección de puertos COM del cliente

Esta configuración permite o impide el acceso a los puertos COM en el dispositivo del usuario.

La redirección de puertos COM está prohibida de forma predeterminada.

Configuraciones de directiva relacionadas:

- Límite de ancho de banda de redirección de puertos COM
- Porcentaje límite de ancho de banda de redirección de puertos COM

Redirección de puertos LPT del cliente

Esta configuración permite o impide el acceso a los puertos LPT en el dispositivo del usuario.

La redirección de puertos LPT está prohibida de forma predeterminada.

Los puertos LPT solo se utilizan por aplicaciones antiguas que envían trabajos de impresión a los puertos LPT y no a los objetos de impresión del dispositivo de usuario. La mayoría de las aplicaciones que se utilizan hoy en día pueden enviar trabajos de impresión a objetos de impresora. Esta configuración de directiva solo es necesaria para los servidores que alojan aplicaciones antiguas que imprimen en puertos LPT.

Tenga en cuenta que, aunque la redirección de puertos COM del cliente es bidireccional, la redirección de puertos LPT es solo de salida y se limita a \\client\LPT1 y \\client\LPT2 en una sesión ICA.

Configuraciones de directiva relacionadas:

- Límite de ancho de banda de redirección de puertos LPT
- Porcentaje límite de ancho de banda de redirección de puertos LPT

Configuraciones de directiva de Impresión

March 8, 2019

La sección Impresión contiene configuraciones de directiva para administrar la impresión del cliente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 en el 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 en el 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 desea crear automáticamente. Después de agregar la impresora, puede aplicar parámetros personalizados para la sesión actual en cada inicio de sesión.

Preferencia de registro de sucesos de creación automática de impresoras

Esta configuración permite especificar los sucesos que se registran durante el proceso de creación automática de impresoras. Puede optar por no registrar los errores ni las advertencias, registrar solamente los errores o registrar los errores y las advertencias.

De forma predeterminada, se registran los errores y las advertencias.

Un ejemplo de advertencia es un suceso en el cual no se pudo instalar el controlador original de una impresora y se instaló el controlador de impresión universal. Para utilizar controladores de impresión universal en esta circunstancia, configure Uso de controladores de impresión universal en Usar solo impresión universal o Usar impresión universal solo si el controlador solicitado no está disponible.

Impresoras de la sesión

Esta configuración permite especificar qué impresoras de red se crearán automáticamente en una sesión. Dentro de la sesión ICA/HDX, Citrix Print Manager Service (CpSvc.exe) crea una conexión de impresora de red durante el inicio de sesión para cada impresora de red especificada en la configuración de directiva **Impresoras de la sesión**. Elimina las impresoras durante el cierre de sesión. De forma predeterminada, no hay impresoras especificadas.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 Citrix Virtual Apps debe tener instalados los controladores de impresora nativos.

Cuando se utiliza Citrix Universal Print Server, Citrix Print Manager Service crea las conexiones de las impresoras de red mediante controladores de impresora nativos, el controlador de impresora universal de Citrix o el controlador de impresora universal XPS de Citrix. El controlador que usted utiliza está controlado por la configuración de directiva Uso de controladores de impresión universal.

Actualmente, todos los controladores de impresora de Windows están dentro de la versión v3 o v4 de controlador. Para obtener más información, consulte Support for the Microsoft V3 and V4 Printer Driver Architectures (Compatibilidad para las arquitecturas de las versiones v3 y v4 de los controladores de impresora de Microsoft).

Para agregar impresoras de sesión y comprobar si aparecen en las sesiones, siga el procedimiento siguiente:

1. En Citrix Studio, vaya a la ficha **Directivas**.
2. Habilite la directiva de impresión de sesión en el cuadro de diálogo **Modificar directiva**.
3. En la directiva, agregue la impresora de sesión. Para agregar impresoras, escriba la ruta UNC de la impresora que desea 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 Citrix Virtual Apps o la directiva se ha creado pero no se ha habilitado.

   > Nota:
   >
   > Si el controlador de impresora no se ha instalado en el servidor Citrix Virtual Apps, es posible que experimente el error más común con las impresoras de sesión: que los administradores se olviden de instalar el controlador de impresora en el servidor Citrix Virtual Apps.

5. Inicie el escritorio publicado y agregue manualmente la impresora de sesión en **Dispositivos e impresoras > Panel de control**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

6. Si esto falla, investigue la comunicación entre el servidor Citrix Virtual Apps y el servidor de impresión. Si hace falta, realice una prueba con RDP.

Esperar a que se creen las impresoras (escritorio de servidor)

Esta configuración permite o impide la demora al conectarse a una sesión para dar tiempo a que las impresoras de escritorio del servidor se creen automáticamente.

De forma predeterminada, no hay una espera en la conexión.

Configuraciones de directiva de Impresoras del cliente

January 29, 2019

La sección Impresoras del cliente contiene configuraciones de directiva para las impresoras del cliente, como configuraciones para la creación automática de impresoras, la conservación de ciertas propiedades de la impresora y la conexión a servidores de impresión.

Crear automáticamente las impresoras del cliente

Esta configuración permite especificar qué impresoras se crearán automáticamente. Esta configuración anula los parámetros predeterminados de creación automática de impresoras del cliente.

Todas las impresoras del cliente se crean automáticamente de forma predeterminada.

Esta configuración se aplica solamente si la configuración Redirección de impresoras del cliente está presente y establecida en Permitida.

Al agregar esta configuración a una directiva, seleccione una de las siguientes opciones:

- Crear automáticamente todas las impresoras del cliente. Crea de forma automática todas las impresoras del dispositivo del usuario.
- Crear automáticamente solo la impresora predeterminada del cliente. Crea de forma automática solo la impresora seleccionada como predeterminada en el dispositivo del usuario.
- Crear automáticamente solo las impresoras locales (no de red) del cliente. Crea de forma automática solo las impresoras conectadas directamente con el dispositivo del usuario por un puerto LPT, COM, USB, TCP/IP u otro puerto local.
- No crear automáticamente las impresoras del cliente. Desactiva la creación automática de todas las impresoras del cliente cuando el usuario inicia sesión. Esto hace que los parámetros de creación automática de impresoras del cliente de los Servicios de Escritorio remoto reemplacen esta configuración en las directivas que tengan menor prioridad.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Crear automáticamente una impresora universal genérica

Nota: Hay revisiones hotfix que solucionan problemas relacionados con esta configuración de directiva en los artículos CTX141565 y CTX141566 de Knowledge Center.

Esta configuración habilita o inhabilita la creación automática del objeto de impresora universal de Citrix genérico (Citrix Universal Printer) para las sesiones en las que se usa un dispositivo de usuario compatible con la impresión universal.

De forma predeterminada, el objeto genérico de impresora universal no se crea automáticamente.

Configuraciones de directiva relacionadas:

- Uso de controladores de impresión universal
- Preferencia de controlador universal

Crear automáticamente la impresora universal de PDF

Este parámetro habilita o inhabilita la creación automática de Citrix PDF Printer para sesiones usando la aplicación Citrix Workspace para Windows (a partir de VDA 7.19), la aplicación Citrix Workspace para HTML5 o la aplicación Citrix Workspace para Chrome.

De forma predeterminada, la impresora Citrix PDF Printer no se crea automáticamente.

Nombres de impresora del cliente

Esta configuración permite seleccionar la convención de nomenclatura que se aplicará a las impresoras del cliente creadas automáticamente.

De forma predeterminada, se utilizan nombres de impresoras estándar.

Seleccione Nombres de impresoras estándar para usar nombres de impresora similares a “HPLaserJet 4 de nombre_cliente en sesión 3”.

Seleccione Nombres de impresoras antiguos para usar nombres similares a los asignados a las impresoras cliente más antiguas y mantener la compatibilidad con versiones anteriores para usuarios o grupos que utilicen MetaFrame Presentation Server 3.0 u otra versión anterior. Un ejemplo de nombre de impresora antiguo es: “Cliente/nombre_cliente#/HPLaserJet 4”. Esta opción es menos segura.

Nota: Esta opción se ofrece únicamente para mantener la compatibilidad con versiones anteriores de XenApp y XenDesktop.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Conexiones directas con servidores de impresión

Esta configuración habilita o inhabilita las conexiones directas desde el escritorio virtual o desde el servidor que aloja las aplicaciones con un servidor de impresión para las impresoras del cliente alojadas en un recurso compartido de red accesible.

Las conexiones directas están habilitadas de forma predeterminada.

Habilite las conexiones directas si el servidor de impresión en red no está en una red WAN desde el escritorio virtual o servidor que aloja las aplicaciones. La comunicación directa da como resultado una impresión más rápida si el servidor de impresión en red y el escritorio virtual o servidor que aloja las aplicaciones están en la misma LAN.

Inhabilite las conexiones directas si es una red WAN o si el ancho de banda es limitado o tiene mucha latencia. Los trabajos de impresión se enrutan a través del dispositivo del usuario, desde donde se los redirige hacia el servidor de impresión en red. Los datos enviados al dispositivo del usuario se comprimen, por lo que se consume menos ancho de banda al transmitir los datos en la WAN.

Si hay dos impresoras de red con un mismo nombre, se usará la que esté en la misma red que el dispositivo del usuario.

Asignación y compatibilidad de controladores de impresora

Esta configuración permite especificar reglas de sustitución de controladores para impresoras creadas automáticamente.

Esta configuración está definida para excluir Microsoft OneNote y el escritor de documentos XPS de la lista de impresoras cliente creadas automáticamente.

Al definir estas reglas, es posible permitir o impedir la creación de impresoras con un controlador específico. También es posible permitir que las impresoras creadas usen solamente controladores de impresión universal. La sustitución de controladores sobrescribe (o asigna) los nombres de los controladores proporcionados por el dispositivo cliente y sustituyéndolo por un controlador equivalente en el servidor. Este proceso permite que las aplicaciones del servidor tengan acceso a las impresoras cliente que tienen los mismos controladores que el servidor pero distintos nombres de controladores.

Puede agregar una asignación de controlador, editar una existente, sobrescribir la configuración personalizada para una asignación, quitar una asignación o cambiar el orden de entradas de controlador en la lista. Al agregar una asignación, se debe especificar el nombre del controlador de la impresora cliente y luego seleccionar el controlador de servidor con el que desea sustituirlo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Retención de las propiedades de impresora

Esta configuración permite especificar si se almacenan las propiedades de la impresora y dónde se almacenan.

De forma predeterminada, el sistema determina si las propiedades de la impresora se almacenan en el dispositivo del usuario, si está disponible, o en el perfil del usuario.

Al agregar esta configuración a una directiva, seleccione una de las siguientes opciones:

- Guardado solo en el dispositivo cliente se utiliza para los dispositivos de usuario que cuentan con un perfil obligatorio o móvil que no se guarda. Elija esta opción solo si todos los servidores de la comunidad están ejecutando XenApp 5 o una versión posterior y los usuarios usan Citrix Online Plug-in versiones 9 a 12.x, o Citrix Receiver 3.x.
- Conservado solo en el perfil de usuario se utiliza para los dispositivos de usuarios con un ancho de banda limitado (ya que reduce el tráfico de red) e inicios de sesión lentos o para los usuarios que tienen plug-ins antiguos. Esta opción almacena las propiedades de la impresora en el perfil del usuario existente en el servidor y evita cualquier intercambio de propiedades con el dispositivo del usuario. Utilice esta opción con MetaFrame Presentation Server 3.0 o una versión anterior y el cliente de MetaFrame Presentation Server 8.x o anterior. Tenga en cuenta que esto solo se puede aplicar si se utiliza un perfil móvil de Servicios de Escritorio remoto (RDS).
- Guardado en perfil solo si no se guarda en el cliente permite que el sistema determine dónde almacenar las propiedades de la impresora. Las propiedades de la impresora se almacenan en el dispositivo del usuario, cuando está disponible, o en el perfil del usuario. Aunque esta opción ofrece más flexibilidad, puede hacer que el inicio de sesión se prolongue y que parte del ancho de banda se utilice para realizar las comprobaciones del sistema.
- No conservar las propiedades de impresora. Evita que se almacenen las propiedades de la impresora.

Impresoras del cliente retenidas o restauradas

Esta configuración habilita o inhabilita la conservación y la recreación de impresoras en el dispositivo del usuario. De forma predeterminada, las impresoras del cliente se conservan y se restauran automáticamente.

Las impresoras conservadas son impresoras creadas por el usuario que se vuelven a crear, o se recuerdan, al iniciar la sesión siguiente. Cuando Citrix Virtual Apps vuelve a crear una impresora conservada, aplica todas las configuraciones de directiva, excepto Crear automáticamente las impresoras del cliente.

Las impresoras restauradas son impresoras configuradas íntegramente por un administrador, con un estado guardado que queda vinculado de forma permanente con un puerto del cliente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Controlador de impresora universal PDF de Citrix

El controlador de impresora universal PDF de Citrix (o Citrix PDF Universal Printer) permite a los usuarios imprimir documentos abiertos con aplicaciones alojadas o aplicaciones ejecutadas en escritorios virtuales entregados por Citrix Virtual Apps and Desktops. Cuando un usuario selecciona la opción Citrix PDF Printer, el controlador convierte el archivo a PDF y transfiere el PDF al dispositivo local. El PDF se abre para verlo e imprimirlo en una impresora conectada localmente. PDF es uno de los formatos que respalda 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

October 3, 2018

La sección Controladores contiene configuraciones de directiva relacionadas con los controladores de impresoras.

Instalación automática de controladores de impresora

> **Nota**
>
> Esta directiva no respalda agentes VDA en esta versión.

Esta configuración habilita o inhabilita la instalación automática de los controladores de impresora del conjunto de controladores integrados de Windows o de paquetes de controladores del host mediante pnputil.exe /a.

De forma predeterminada, estos controladores se instalan según se requieren.

Preferencia de controlador universal

Esta configuración especifica el orden en el que se usan los controladores de impresión universal, comenzando por la primera entrada en la lista.

De forma predeterminada, el orden de preferencia es:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- EMF
- XPS
- PCL5c
- PCL4
- PS

Es posible agregar, modificar o eliminar controladores y cambiar el orden de los controladores en la lista.

Uso de controladores de impresión universal

Esta configuración permite especificar cuándo se usa la impresión universal.

De forma predeterminada, la impresión universal se utiliza exclusivamente si el controlador solicitado no está disponible.

La impresión universal emplea controladores de impresora genéricos en lugar de controladores específicos de modelos de impresora, lo que simplifica la gestión de los controladores en los equipos host. La disponibilidad de los controladores de impresión universal depende de la capacidad del software del dispositivo de usuario, del host y del servidor de impresión. En algunas configuraciones, es posible que la impresión universal no esté disponible.

Al agregar esta configuración a una directiva, seleccione una de las siguientes opciones:

- Usar solo los controladores específicos de la impresora indica que la impresora cliente usa solamente los controladores estándar específicos de modelo de impresora, los cuales se crean automáticamente al iniciar sesión. Si el controlador solicitado no está disponible, la impresora cliente no podrá crearse de forma automática.
- Usar solo impresión universal. Especifica que no se usen los controladores específicos del modelo de impresora. Solo se usan controladores de impresión universal para crear impresoras.
- Usar impresión universal solo si el controlador solicitado no está disponible utiliza los controladores estándar específicos del modelo de impresora para la creación de impresoras, si están disponibles. Si el controlador no está disponible en el servidor, la impresora cliente se crea automáticamente usando un controlador de impresora universal adecuado.
- Usar controladores específicos de la impresora solo si la impresión universal no está disponible usa el controlador de impresión universal si está disponible. Si el controlador no está disponible en el servidor, la impresora cliente se crea de forma automática con el controlador específico del modelo de impresora adecuado.

Configuraciones de directiva de Universal Print Server

October 3, 2018

© 1999-2019 Citrix Systems, Inc. All rights reserved.

La sección Universal Print Server contiene configuraciones de directiva para administrar el servidor de impresión universal (Universal Print Server).

Habilitar Universal Print Server

Esta configuración habilita o inhabilita la funcionalidad de Universal Print Server en el escritorio virtual o en el servidor que aloja aplicaciones. Aplique esta configuración de directiva a las unidades organizativas (OU) que contienen los escritorios o servidores virtuales que alojan las aplicaciones.

De forma predeterminada, Universal Print Server está inhabilitado.

Al agregar esta configuración a una directiva, seleccione una de las siguientes opciones:

- **Habilitado, con respaldo de la impresión remota nativa de Windows**. Cuando es posible, Universal Print Server proporciona servicios a las conexiones con impresoras de red. Si Universal Print Server no está disponible, se usa el proveedor de impresión de Windows. El proveedor de impresión de Windows sigue administrando todas las impresoras que fueron creadas previamente con dicho proveedor.
- **Habilitado, sin respaldo de la impresión remota nativa de Windows**. Solo Universal Print Server proporciona servicios a las conexiones con impresoras de red. Si Universal Print Server no está disponible, la conexión con la impresora de red falla. Esta configuración inhabilita en efecto la impresión en red a través del proveedor de impresión de Windows. Las impresoras creadas previamente con el proveedor de impresión de Windows no se crearán mientras exista una directiva que contenga esta configuración.
- **Inhabilitada**. La funcionalidad de Universal Print Server está inhabilitada. No se intenta conectar con Universal Print Server al conectar con una impresora de red con un nombre UNC. Las conexiones con impresoras remotas continúan usando 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Límite de ancho de banda del flujo de entrada de impresión de Universal Print Server (kpbs)

Esta configuración especifica el límite superior (en kilobits por segundo) de la velocidad de transferencia de datos de impresión entregados desde cada trabajo de impresión a Universal Print Server usando CGP. Aplique esta configuración de directiva a las unidades organizativas que contienen el escritorio virtual o el servidor que aloja aplicaciones.

De forma predeterminada, el valor es 0, lo cual no especifica un límite superior.

Puerto del servicio Web de Universal Print Server (HTTP/SOAP)

Esta configuración especifica el número de puerto TCP que utiliza el agente de escucha (HTTP/SOAP) del servicio Web de Universal Print Server. Universal Print Server es un componente optativo que permite el uso de controladores de impresión universal de Citrix para la impresión en red. Cuando se utiliza Universal Print Server, los comandos de impresión se envían de los hosts de Citrix Virtual Apps and Desktops a Universal Print Server mediante SOAP a través de HTTP. Esta configuración modifica el puerto TCP predeterminado en que Universal Print Server escucha las solicitudes HTTP/SOAP entrantes.

Debe configurar de la misma manera el puerto HTTP del host y del servidor de impresión. Si los puertos no tienen la misma configuración, el software del host no se conectará a Universal Print Server. Esta configuración cambia el VDA en Citrix Virtual Apps and Desktops. Además, debe cambiar el puerto predeterminado en Universal Print Server.

De forma predeterminada, el número de puerto es el 8080.

Los números de puerto válidos deben estar en el intervalo de 0 a 65535.

Universal Print Servers para equilibrio de carga

Esta configuración enumera los servidores de impresión universal que se usarán para equilibrar la carga de las conexiones de impresora establecidas al comienzo de las sesiones, después de evaluar otras configuraciones de impresión de Citrix. Para optimizar la creación de impresoras, Citrix recomienda que todos los servidores de impresión tengan el mismo conjunto de impresoras compartidas. No hay límite máximo para la cantidad de servidores de impresión que se pueden agregar para el equilibrio de carga.

Esta configuración también implementa la detección de fallos de impresora para la conmutación por error y la recuperación de conexiones de impresora. La disponibilidad de los servidores de impresión se comprueba periódicamente. Si se detecta un error del servidor, ese servidor se quita del esquema de equilibrio de carga y las conexiones de impresora en ese servidor se redistribuyen entre los otros

© 1999-2019 Citrix Systems, Inc. All rights reserved.

servidores de impresión disponibles. Cuando el servidor de impresión que falló se recupera, se lo devuelve al esquema de equilibrio de carga.

Haga clic en **Validar servidores** para comprobar: que cada servidor es un servidor de impresión, que la lista no contiene nombres de servidor duplicados y que todos los servidores tienen un conjunto idéntico de impresoras compartidas instaladas. Esta operación puede tardar varios minutos.

Umbral para servidores Universal Print Server fuera de servicio

Esta configuración especifica cuánto tiempo debe esperar el equilibrador de carga a que se recupere un servidor de impresión no disponible antes de determinar que ese servidor está fuera de línea permanentemente y redistribuir su carga en otros servidores de impresión disponibles.

El valor umbral predeterminado es de 180 segundos.

Configuraciones de directiva de Impresión universal

December 14, 2018

La sección Impresión universal contiene configuraciones de directiva para administrar la impresión universal.

Modo de procesamiento EMF de la impresión universal

Esta configuración controla el método de procesamiento del archivo de cola de impresión EMF en el dispositivo de usuario Windows.

De forma predeterminada, los registros EMF se envían directamente a la impresora.

Al agregar esta configuración a una directiva, seleccione una de las siguientes opciones:

- Reprocesar EMF para la impresora fuerza el reprocesamiento del archivo de cola de EMF y su envío a través del subsistema GDI en el dispositivo del usuario. Puede usar esta configuración para los controladores que requieren el reprocesamiento de EMF pero que puede que no se seleccionen automáticamente en una sesión.
- Enviar directamente a la cola de impresión, cuando se usa con el controlador de impresora universal de Citrix, asegura que los registros EMF se envíen a la cola y se entreguen al dispositivo del usuario para el procesamiento. Normalmente, estos archivos de cola de impresión EMF se transfieren directamente a la cola de impresión del cliente. Para las impresoras y controladores que son compatibles con el formato EMF, este es el método de impresión más rápido.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Límite de compresión de imagen para la impresión universal

Esta configuración define la calidad máxima y el nivel de compresión mínimo disponibles para las imágenes impresas con el controlador de impresora universal de Citrix.

De forma predeterminada, el límite de compresión de imagen está definido en Mejor calidad (compresión sin pérdida).

Si se ha seleccionado Sin compresión, la compresión está inhabilitada para la impresión EMF solamente.

Al agregar esta configuración a una directiva, seleccione una de las siguientes opciones:

- Sin compresión
- Mejor calidad (compresión sin pérdida)
- Alta calidad
- Calidad estándar
- Calidad reducida (compresión máxima)

Cuando agregue esta configuración a una directiva que incluye ya la configuración Valores predeterminados de optimización de impresión universal, tenga en cuenta lo siguiente:

- Si el nivel de compresión en Límite de compresión de imagen para la impresión universal es inferior al nivel definido en Valores predeterminados de optimización de impresión universal, las imágenes se comprimen según el nivel definido en la configuración Límite de compresión de imagen para la impresión universal.
- Si la compresión está inhabilitada, las opciones Calidad de imagen deseada y Habilitar la compresión intensa de la configuración Valores predeterminados de optimización de impresión universal no tienen ningún efecto en la directiva.

Valores predeterminados de optimización de impresión universal

Esta configuración especifica los valores predeterminados para la optimización de la impresión cuando se crea el controlador de impresión universal para una sesión.

- Calidad de imagen deseada especifica el límite predeterminado de compresión de imagen aplicable a la impresión universal. De forma predeterminada, la Calidad estándar está habilitada, de manera que los usuarios solo pueden imprimir imágenes con la compresión de calidad estándar o reducida.
- Habilitar la compresión intensa habilita o inhabilita la reducción de ancho de banda más allá del nivel de compresión definido por Calidad de imagen deseada, sin pérdida de calidad de imagen. La compresión intensa está inhabilitada de forma predeterminada.
- La configuración de Almacenamiento en caché de imágenes y fuentes especifica si las imágenes y fuentes que aparecen varias veces en el flujo de impresión se almacenan en caché, para que

© 1999-2019 Citrix Systems, Inc. All rights reserved.

cada imagen individual se envíe solo una vez a la impresora. De forma predeterminada, las fuentes e imágenes incrustadas se almacenan en caché. Tenga en cuenta que estas configuraciones solo se aplican si el dispositivo del usuario respalda 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 reciben respaldo con la impresión EMF. En el caso de la impresión XPS, solo se respalda el uso de la opción Calidad de imagen deseada.

Cuando agregue esta configuración a una directiva que incluye ya la configuración Límite de compresión de imagen para la impresión universal, tenga en cuenta lo siguiente:

- Si el nivel de compresión en Límite de compresión de imagen para la impresión universal es inferior al nivel definido en Valores predeterminados de optimización de impresión universal, las imágenes se comprimen según el nivel definido en la configuración Límite de compresión de imagen para la impresión universal.
- Si la compresión está inhabilitada, las opciones Calidad de imagen deseada y Habilitar la compresión intensa de la configuración Valores predeterminados de optimización de impresión universal no tienen ningún efecto en la directiva.

Preferencia de vista previa en impresión universal

Esta configuración permite especificar si se usará la función de vista previa de impresión para las impresoras universales genéricas o creadas automáticamente.

De forma predeterminada, no se utiliza la vista previa de impresión para estas impresoras.

Al agregar esta configuración a una directiva, seleccione una de las siguientes opciones:

- No usar vista previa en las impresoras de creación automática o universales genéricas
- Usar vista previa solo para impresoras de creación automática
- Usar vista previa solo para impresoras universales genéricas
- Usar vista previa para impresoras de creación automática y universales genéricas

Límite de calidad de la impresión universal

Esta configuración especifica la cantidad máxima de puntos por pulgada (ppp) disponibles para generar los productos impresos en una sesión.

De forma predeterminada, Sin límite está habilitado, y permite a los usuarios seleccionar la calidad de impresión máxima permitida por la impresora a la que están conectados.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Cuando esta configuración está definida, limita la calidad de impresión máxima disponible para los usuarios en términos de resolución de salida. Tanto la calidad de impresión misma como la capacidad de calidad de impresión de la impresora a la que se conectan los usuarios quedan limitadas por el parámetro configurado. Por ejemplo, si se configura como Resolución media (600 ppp), los usuarios están limitados a imprimir con una calidad máxima de 600 ppp y la configuración Calidad de impresión en la ficha Avanzado del cuadro de diálogo Impresora universal muestra parámetros de resolución solo hasta la calidad media inclusive (600 ppp).

Al agregar esta configuración a una directiva, seleccione una de las siguientes opciones:

- Borrador (150 ppp)
- Baja resolución (300 ppp)
- Resolución media (600 ppp)
- Alta resolución (1200 ppp)
- Sin límite

Configuraciones de directiva de Seguridad

October 3, 2018

La sección Seguridad contiene la configuración de directiva para configurar el cifrado de sesiones y el cifrado de los datos de inicio de sesión.

Nivel de cifrado mínimo de SecureICA

Esta configuración permite especificar el nivel mínimo de cifrado para los datos de sesión enviados entre el servidor y el dispositivo de usuario.

Importante: Para Virtual Delivery Agent 7.x, esta configuración de directiva se puede usar solo para habilitar el cifrado de los datos de inicio de sesión con el cifrado RC5 de 128 bits. Hay otras configuraciones que se proporcionan únicamente para la compatibilidad con versiones anteriores de Citrix Virtual Apps and Desktops.

Para VDA 7.x, el cifrado de los datos de inicio de sesión se configura usando 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 usando 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 usando un cifrado RC5 de 128 bits y cifra la conexión de cliente usando un cifrado básico.
- RC5 (40 bits). Cifra la conexión de cliente usando un cifrado RC5 de 40 bits.
- RC5 (56 bits). Cifra la conexión de cliente usando un cifrado RC5 de 56 bits.
- RC5 (128 bits). Cifra la conexión de cliente usando un cifrado RC5 de 128 bits.

La configuración especificada para el cifrado cliente-servidor puede interactuar con cualquier otra configuración de cifrado existente en el entorno y en el sistema operativo Windows. Si se establece un cifrado de alta prioridad en un servidor o un dispositivo de usuario, se pueden sobrescribir las configuraciones especificadas en los recursos publicados.

Se pueden elevar los niveles de cifrado para proteger aún más las comunicaciones y la integridad de los mensajes de ciertos usuarios. Si una directiva exige un nivel de cifrado mayor, se impide la conexión de Citrix Receivers que usen un nivel de cifrado inferior.

SecureICA no realiza ninguna autenticación ni comprueba la integridad de los datos. Para proporcionar un cifrado integral de extremo a extremo para su sitio, use SecureICA con cifrado TLS.

SecureICA no utiliza algoritmos compatibles con FIPS. Si esto supone algún problema, configure el servidor y Citrix Receivers para que no utilicen SecureICA.

Por motivos de confidencialidad, SecureICA usa el cifrado de bloques RC5 como se describe en RFC 2040. El tamaño del bloque es de 64 bits (un múltiplo de unidades de palabras de 32 bits). La longitud de la clave es de 128 bits. La cantidad de rondas es 12.

Configuraciones de directiva de Límites de servidor

December 4, 2018

La sección Límites de servidor contiene la configuración de directiva para controlar las conexiones inactivas.

Intervalo de temporizador de servidor inactivo

Esta configuración determina cuánto tiempo, en milésimas de segundo, se mantendrá una sesión de usuario ininterrumpida si este no realiza entradas.

De forma predeterminada, las conexiones inactivas no se desconectan (intervalo de temporizador de servidor inactivo = 0). Citrix recomienda establecer este valor a un mínimo de 60 000 milisegundos (60 segundos).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para mostrar la directiva, seleccione **Versiones múltiples**, borre las versiones de SO de escritorio 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

January 29, 2019

La sección **Límites de sesión** contiene configuraciones de directiva para controlar el tiempo que las sesiones pueden permanecer conectadas antes de un cierre forzoso.

> **Importante:**
>
> Estos valores no se aplican a agentes VDA de Windows Server.

Temporizador de sesión desconectada

Esta configuración habilita o inhabilita un temporizador para determinar cuánto tiempo permanece desconectado y bloqueado un escritorio antes de que se cierre la sesión. Si esto minutero está habilitado, el sesion desconectada se desconecta cuando el minutero expira .

De forma predeterminada, las sesiones desconectadas no se cierran.

Intervalo de temporizador de sesiones desconectadas

Esta configuración especifica cuánto tiempo, en minutos, puede permanecer desconectado y bloqueado un escritorio antes de que se cierre la sesión.

De forma predeterminada, este período es de 1440 minutos (24 horas).

Establecer límite de tiempo para sesiones desconectadas

Establecer límite de tiempo para sesiones desconectadas es una directiva de Microsoft. Esta directiva está disponible en **Consola de administración de directivas de grupo** en **Configuración de usuario**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> Directivas > Plantillas administrativas> Componentes de Windows> Servicios de Escritorio remoto> Host de sesión de Escritorio remoto> Límites de tiempo para sesiones.

Habilite las siguientes dos configuraciones:

- Establecer el tiempo para sesiones desconectadas.
- Finalizar sesión cuando se alcancen los límites de tiempo.

Para obtener más información sobre esta directiva, consulte Microsoft KB - Límites de tiempo de sesión.

Temporizador de conexión de sesión

Esta configuración habilita o inhabilita un temporizador para especificar la duración máxima de una conexión sin interrupciones entre un dispositivo del usuario y un escritorio. Si este temporizador está habilitado, la sesión se desconecta o se cierra cuando caduca el temporizador. La configuración de **Finalizar sesión cuando se alcancen los límites de tiempo** determina el siguiente estado de la sesión.

De manera predeterminada, este temporizador está inhabilitado.

Intervalo de temporizador de conexión de sesiones

Esta configuración especifica el número máximo de minutos de una conexión sin interrupciones entre un dispositivo del usuario y un escritorio.

De forma predeterminada, la duración máxima es 1440 minutos (24 horas).

Temporizador de sesión inactiva

Esta configuración habilita o inhabilita un temporizador que especifica cuánto tiempo se puede mantener ininterrumpida una conexión entre un dispositivo de usuario y un escritorio si el usuario no suministra ninguna entrada. Cuando caduca este temporizador , la sesión se coloca en el estado desconectado y el **temporizador desesión desconectado se aplica .** Si el **Temporizador de sesión desconectada** está inhabilitado, la sesión se cierra.

De manera predeterminada, este temporizador está habilitado.

Intervalo de temporizador de sesiones inactivas

Esta configuración especifica cuánto tiempo se mantiene ininterrumpida la conexión entre el dispositivo del usuario y un escritorio si el usuario no realiza entradas.

De forma predeterminada, las conexiones inactivas se mantienen durante 1440 minutos (24 horas).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Fiabilidad de la sesión

March 8, 2019

La sección Fiabilidad de la sesión contiene las configuraciones de directiva para gestionar las conexiones que usan fiabilidad de la sesión.

Conexiones de fiabilidad de la sesión

Esta configuración permite o impide que las sesiones permanezcan abiertas durante una pérdida de conectividad de red. La Reconexión automática de clientes, junto con la Fiabilidad de la sesión, permiten a los usuarios reconectarse automáticamente a sus sesiones de la aplicación Citrix Workspace después de recuperarse de una interrupción en la red. De forma predeterminada, la Fiabilidad de la sesión está permitida.

Para la aplicación de Citrix Workspace 1808 y versiones posteriores y Citrix Receiver para Windows 4.7 y versiones posteriores, la configuración de Studio se aplica en el cliente. La directiva de Studio reemplaza el objeto de directiva de grupo deCitrix Receiver en los clientes . Las actualizaciones de estas directivas en Studio sincronizan la Fiabilidad de la sesión desde el servidor hasta el cliente.

> **Nota:**
>
> - Cuando se trata de Citrix Receiver para Windows 4.7 y versiones posteriores o aplicaciones Citrix Workspace para Windows, establezca la directiva en Studio.
> - Cuando se trata de Citrix Receiver para Windows anterior a 4.7, establezca directivas en Studio y en la plantilla del objeto de directiva de grupo de Citrix Receiver en el cliente para un comportamiento uniforme.

Cuando la conectividad de red se ve interrumpida, la fiabilidad de la sesión mantiene las sesiones activas y en la pantalla del usuario. Los usuarios siguen viendo la aplicación que están utilizando hasta que vuelve la conexión.

Con la función Fiabilidad de la sesión, la sesión permanece activa en el servidor. Para indicar que se ha perdido la conectividad, la pantalla del usuario se oscurece. La sesión del usuario puede quedar congelada durante la interrupción y puede reanudar la interacción con la aplicación después de restablecerse la conexión de red. La función Fiabilidad de la sesión reconecta a los usuarios sin pedirles que repitan la autenticación.

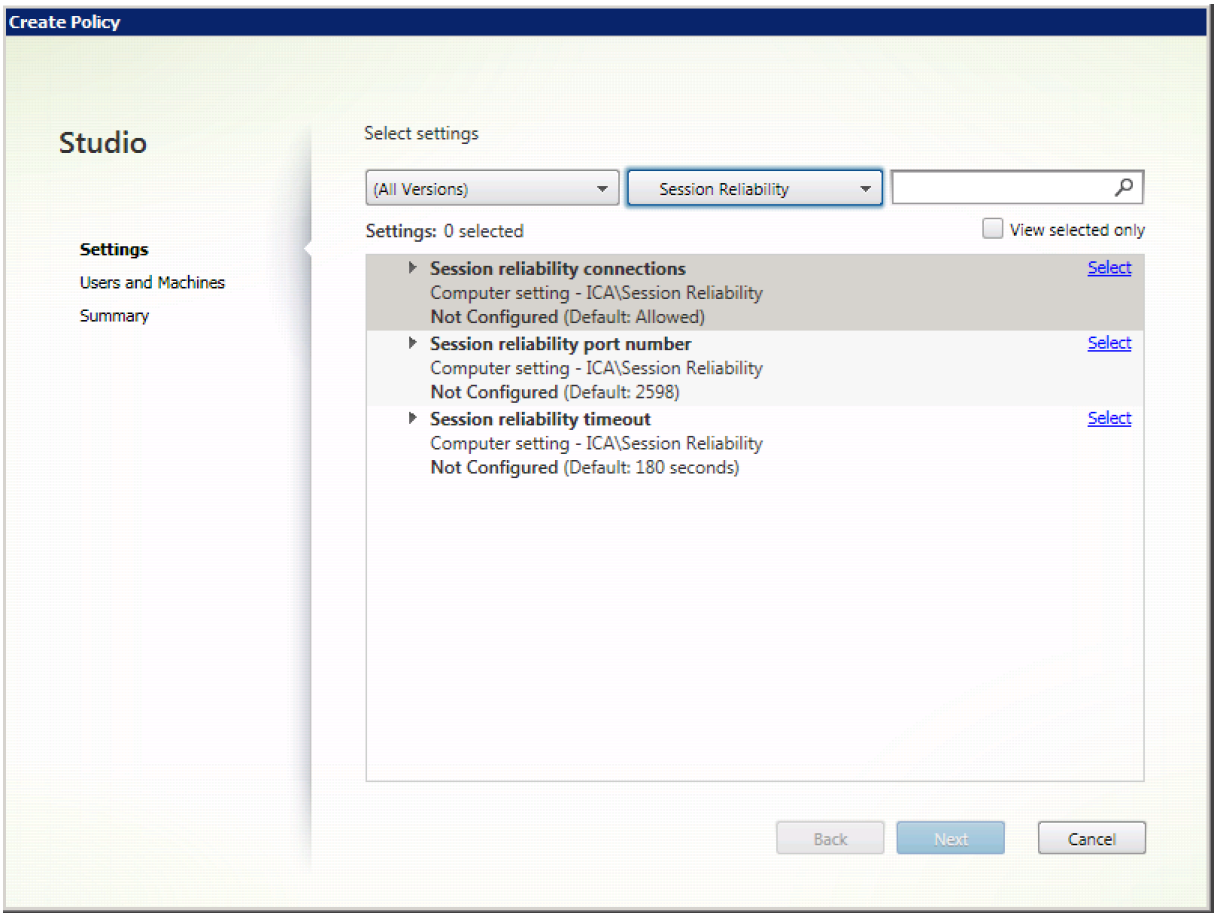
Si usa tanto la fiabilidad de la sesión como la reconexión automática de clientes, las dos actúan de manera secuencial. La Fiabilidad de la sesión cierra (o desconecta) la sesión del usuario una vez haya trascurrido el tiempo especificado en Tiempo de espera de fiabilidad de la sesión. A continuación, se aplicará la configuración de directiva de Reconexión automática de clientes y se intentará reconectar al usuario con la sesión desconectada.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

De forma predeterminada, la Fiabilidad de la sesión está permitida.

Para inhabilitar la fiabilidad de la sesión:

1. Inicie Citrix Studio.
2. Abra la directiva **Conexiones de fiabilidad de la sesión**.
3. Establezca la directiva en **Prohibida**.



Número de puerto para fiabilidad de la sesión

Esta configuración especifica el número de puerto TCP para conexiones de fiabilidad de la sesión entrantes.

De forma predeterminada, el número de puerto es el 2598.

Para cambiar el número de puerto de Fiabilidad de la sesión:

1. Inicie Citrix Studio.
2. Abra la directiva **Número de puerto para fiabilidad de la sesión**.
3. Modifique el número de puerto.
4. Haga clic en **Aceptar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Tiempo de espera de fiabilidad de la sesión

Esta configuración especifica el tiempo en segundos que el proxy de fiabilidad de la sesión espera a que se reconecte un usuario, antes de dejar que la sesión sea desconectada.

Aunque se puede alargar el tiempo que se mantiene abierta una sesión, esta función está diseñada para la comodidad del usuario, por lo que no le pedirá que repita la autenticación. Cuanto más tiempo permanezca abierta la sesión, mayor será la probabilidad de que el usuario deje el dispositivo sin supervisión, por lo que podría ser potencialmente accesible a usuarios no autorizados.

De forma predeterminada, el tiempo de espera es de 180 segundos (3 minutos).

Para modificar el tiempo de espera de Fiabilidad de la sesión:

1. Inicie Citrix Studio.
2. Abra la directiva **Tiempo de espera de fiabilidad de la sesión**.
3. Cambie el valor del tiempo de espera.
4. Haga clic en **Aceptar**.

Configuraciones de directiva de Marca de agua de la sesión

October 3, 2018

La sección “Marca de agua de la sesión” contiene configuraciones para definir esta característica. 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Incluir dirección IP del cliente

Cuando habilita esta configuración, la sesión muestra la dirección IP del cliente actual como una marca de agua.

De forma predeterminada, “Incluir dirección IP del cliente” está inhabilitado.

Incluir la hora de la conexión

Cuando habilita esta configuración, la marca de agua de la sesión muestra la hora de la conexión. El formato es: aaaa/mm/dd hh:mm. La hora que aparece se basa en el reloj del sistema y la zona horaria.

De forma predeterminada, “Incluir la hora de la conexión” está inhabilitado.

Incluir nombre de usuario de inicio de sesión

Cuando habilita esta configuración, la sesión muestra el nombre del usuario que ha iniciado la sesión como una marca de agua. El formato es: NOMBREDEUSUARIO@NOMBREDEDOMINIO. Recomendamos que el nombre de usuario tenga un máximo de 20 caracteres. Si un nombre de usuario contiene más de 20 caracteres, pueden aparecer fuentes de caracteres demasiado pequeñas o puede haber truncamiento de caracteres, con lo que disminuye la eficacia de la marca de agua.

De forma predeterminada, “Incluir nombre de usuario de inicio de sesión” está habilitado.

Incluir nombre de host del VDA

Cuando habilita esta configuración, la sesión muestra el nombre de host del VDA perteneciente a la sesión ICA actual como una marca de agua.

De forma predeterminada, “Incluir nombre de host del VDA” está habilitado.

Incluir dirección IP del VDA

Cuando habilita esta configuración, la sesión muestra la dirección IP del VDA perteneciente a la sesión ICA actual como una marca de agua.

De forma predeterminada, “Incluir dirección IP del VDA” está inhabilitado.

Estilo de la marca de agua de la sesión

Esta configuración controla si se muestra una sola etiqueta de texto de la marca de agua o varias etiquetas. Elija **Múltiple** o **Única** en el menú desplegable **Valor**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

La opción **Múltiple** muestra cinco etiquetas de marca de agua en la sesión. Una en el centro y cuatro en las esquinas.

La opción **Única** muestra una sola etiqueta de marca de agua en el centro de la pantalla de la sesión.

De forma predeterminada, el "Estilo de la marca de agua de la sesión" es "Múltiple".

Texto personalizado de la marca de agua

Esta configuración especifica una cadena de texto personalizada (por ejemplo, el nombre corporativo) a mostrar en la marca de agua de la sesión. Cuando configura una cadena no vacía, el texto se muestra en una nueva línea que se agrega a la información ya habilitada en la marca de agua.
La cantidad máxima de caracteres que puede contener el texto personalizado de la marca de agua es de 25 caracteres Unicode. Si configura una cadena más larga, se truncará a los 25 caracteres.

No hay texto predeterminado.

Transparencia de la marca de agua

Puede especificar una opacidad de la marca de agua que oscile entre 0 y 100. Cuanto mayor sea el valor especificado, más opaca será la marca de agua.

De forma predeterminada, el valor es 17.

Parámetros de directiva de control de zona horaria

January 29, 2019

La sección Control de zona horaria contiene parámetros de directiva relacionados con la hora local usada para las sesiones.

Calcular hora local para clientes antiguos

Este parámetro habilita o inhabilita el cálculo de la zona horaria local de los dispositivos del usuario que envían información inexacta sobre la zona horaria al servidor.

De forma predeterminada, el servidor calcula la zona horaria local cuando es necesario.

Este parámetro está diseñado para su uso con versiones anteriores de Citrix Receiver o clientes ICA que no envían al servidor información detallada acerca de la zona horaria. Cuando se usa con instancias de Citrix Receiver que envían al servidor información detallada acerca de la zona horaria, como las versiones respaldadas de Citrix Receiver para Windows, esta configuración no tiene ningún efecto.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Usar la hora local del cliente

Este parámetro permite determinar la configuración de zona horaria de la sesión del usuario. Las opciones son la zona horaria de la sesión de usuario (zona horaria del servidor) o la zona horaria del dispositivo de usuario (zona horaria del cliente).

De forma predeterminada, se usa la zona horaria de la sesión del usuario.

Para activar esta configuración, habilite el parámetro **Permitir redirección de zona horaria** en el Editor de directivas de grupo. Este parámetro se encuentra en **Directiva de equipo local** > **Configuración del equipo** > **Plantillas administrativas** > **Componentes de Windows** > **Servicios de Escritorio remoto** > **Host de sesión de Escritorio remoto** > **Redirección de dispositivo o recurso**.

Si el VDA es un VDA de SO de escritorio que se ejecuta en un SO de servidor, establezca el derecho de usuario local **Cambiar zona horaria** en **Todos**. Este derecho de usuario se puede encontrar en **Directiva del equipo local** > **Configuración del equipo** > **Parámetros de Windows** > **Parámetros de seguridad** > **Directivas locales** > **Asignación de derechos de usuario**.

> **Nota:**
>
> En un SO de escritorio, los **usuarios** se incluyen en la asignación de derechos de usuario **Cambiar zona horaria**, aunque no en un SO de servidor. En un SO de servidor, la zona horaria se sincroniza utilizando la siguiente directiva de grupo: Configuración del equipo\Plantillas administrativas\Componentes de Windows\Servicios de Escritorio remoto\Host de sesión de Escritorio remoto\Redirección de dispositivo o recurso\Permitir redirección de zona horaria. Esta directiva no se aplica cuando el servidor no es un host de sesión de Escritorio remoto en el VDA del SO de servidor (instalado con el comando `/ServerVDI`). En un SO de servidor, de forma predeterminada y por diseño, los usuarios no tienen el derecho local de cambiar la zona horaria.

Configuraciones de directiva de Dispositivos TWAIN

October 3, 2018

La sección Dispositivos TWAIN contiene configuraciones de directiva relacionadas con la asignación de dispositivos TWAIN del cliente, tales como cámaras digitales o escáneres, y con la optimización de la transferencia de imágenes del servidor al cliente.

> **Nota**
>
> TWAIN 2.0 se respalda con Citrix Receiver para Windows 4.5.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Redirección de dispositivos TWAIN del cliente

Esta configuración permite o impide el acceso de los usuarios a los dispositivos TWAIN del dispositivo del usuario desde aplicaciones de tratamiento de imágenes alojadas en servidores. De forma predeterminada, la redirección de dispositivos TWAIN está permitida.

Configuraciones de directiva relacionadas:

- Nivel de compresión TWAIN
- Límite de ancho de banda de redirección de dispositivos TWAIN
- Porcentaje límite de ancho de banda de redirección de dispositivos TWAIN

Nivel de compresión TWAIN

Esta configuración permite especificar el nivel de compresión para la transferencia de imágenes del cliente al servidor. Utilice Baja para obtener la mejor calidad de imagen, Media para una calidad de imagen intermedia o Alta para una imagen de baja calidad. De forma predeterminada, se aplica la compresión media.

Configuraciones de directiva de Dispositivos USB

March 8, 2019

La sección **Dispositivos USB** contiene las configuraciones de directiva para gestionar la redirección de archivos para dispositivos USB.

Reglas de optimización de dispositivos USB del cliente

Las reglas referentes a la optimización de dispositivos USB del cliente se pueden aplicar a los dispositivos para inhabilitar la optimización o para cambiar el modo de optimización.

Cuando el usuario conecta un dispositivo USB, el host comprueba si la configuración de la **directiva USB** permite el dispositivo. Si el dispositivo está permitido, el host comprueba luego las **reglas de optimización para dispositivos USB del cliente** definidas para el dispositivo. Si no se especifica ninguna regla, el dispositivo no está optimizado. El modo de captura (04) es el modo recomendado para los dispositivos de firma. Para otros dispositivos cuyo rendimiento se degrada con la latencia alta, los administradores pueden habilitar el modo interactivo (02). Consulte las descripciones de los modos disponibles en la tabla de este artículo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Tenga en cuenta

- 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 configurado previamente el respaldo a 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	Description
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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre de la etiqueta	Description
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, se 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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	Description
VID	Identificador del proveedor tomado del descriptor del dispositivo
PID	Identificador del producto tomado del descriptor del dispositivo
REL	Identificador de la versión tomado del descriptor del dispositivo
Class	Clase, tomada del descriptor del dispositivo o de un descriptor de la interfaz
Subclass	Subclase, tomada del descriptor del dispositivo o de un descriptor de la interfaz
Prot	Protocolo tomado del descriptor del dispositivo o de un descriptor de la interfaz

Al crear reglas de directivas, recuerde:

- Las reglas no distinguen entre mayúsculas y minúsculas.
- Las reglas pueden tener un comentario optativo al final que se introduce con el signo #.
- Se ignoran las líneas en blanco y las que son exclusivamente de comentario.
- Las etiquetas deben utilizar el operador de coincidencia = (por ejemplo, VID=067B_).
- Cada regla debe comenzar en una línea nueva o formar parte de una lista de reglas, separadas por punto y coma.
- Consulte los códigos de clase USB que están disponibles en el sitio Web de USB Implementers Forum, Inc.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 el respaldo de USB está habilitado y la configuración de las preferencias de usuario para USB está definida para conectar automáticamente los dispositivos USB.

> Nota:
>
> En Receiver para Windows 4.2, los dispositivos USB también se redirigen automáticamente cuando se trabaja en modo Desktop Appliance y la barra de conexión no está presente. En versiones anteriores de Citrix Receiver para Windows, los dispositivos USB también se redirigen automáticamente cuando funcionan en modo de dispositivo de escritorio o con aplicaciones alojadas en máquinas virtuales (VM).

No siempre es mejor redirigir todos los dispositivos USB. Los usuarios pueden redirigir explícitamente dispositivos seleccionándolos en la lista de dispositivos USB que no se redirigen automáticamente. Para evitar que los dispositivos USB se incluyan o redirijan, use DeviceRules en el dispositivo de punto final del cliente o en el VDA. Consulte las Guías de administración para obtener más detalles.

> Precaución
>
> Utilizar el Editor del Registro de forma incorrecta puede provocar problemas graves que podrían conllevar la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Parámetros de preferencias de usuario para la redirección automática de dispositivos USB

Directiva:

1. Abra el **Editor de directivas de grupo local** y vaya a **Plantillas administrativas > Componentes de Citrix > Citrix Receiver > Uso remoto de dispositivos cliente > Uso remoto de USB genérico**.
2. Abra **Nuevos dispositivos USB**, seleccione **Habilitado** y haga clic en **Aceptar**.
3. Abra **Dispositivos USB existentes**, seleccione **Habilitado** y haga clic en **Aceptar**.

Citrix Receiver:

1. Vaya a **Preferencias de Citrix Receiver > Conexiones**.
2. Asegúrese de que las siguientes opciones estén seleccionadas:
   - Conectar dispositivos automáticamente al comenzar una sesión
   - Cuando se conecta un nuevo dispositivo mientras se ejecuta una sesión, conectar el dispositivo automáticamente.
3. Haga clic en **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, y se espera que las impresoras avanzadas con funciones de escaneo, por ejemplo, puedan tener que redirigirse con la ayuda del respaldo USB para funcionar correctamente.

Utilice este Registro para establecer si las impresoras simples se redirigen automáticamente:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Nombre: AutoRedirectPrinters

Tipo: DWORD

Datos: 00000000

El valor predeterminado es 0 (no redirige automáticamente). Al establecer un valor distinto de cero se permite que el soporte USB redirija las impresoras USB simples.

También puede implementar directivas de Active Directory en esta clave de Registro y anular el valor que no corresponda a la directiva si ambos están presentes:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nombre: AutoRedirectAudio

Tipo: DWORD

Datos: 00000000

Redirección de dispositivos de sonido simples

Al igual que las impresoras simples, la mejor experiencia de usuario se logra utilizando el canal virtual de audio dedicado de ICA para enviar datos de audio desde dispositivos de sonido simples. Sin embargo, es posible que deba redirigir algunos dispositivos especializados mediante el soporte USB. Los datos heurísticos se utilizan para determinar qué dispositivos son dispositivos de sonido simples.

Utilice este Registro para establecer si los dispositivos de sonido simples se redirigen automáticamente:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Nombre: AutoRedirectAudio

Tipo: DWORD

Datos: 00000000

El valor predeterminado es 0 (no redirige automáticamente). Al establecer un valor distinto de cero, redirige los dispositivos de sonido simples mediante el respaldo 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 utilizando 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 ser redirigido con respaldo de USB genérico.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 el respaldo 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 usando un respaldo USB genérico, mientras que se puede configurar si se usa la asignación de unidades del cliente.

Dispositivo de memoria USB con redireccionamiento 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 utilizando 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 USB genérica es necesaria para clientes que no son de Windows (por ejemplo, clientes de Linux) y casos en los que el cliente ha restringido (bloqueado) el acceso de los usuarios a las funciones locales en el cliente. La redirección USB genérica puede redirigir cualquier dispositivo de almacenamiento USB sin cifrado de hardware a las sesiones de VDA del SO de escritorio y SO de servidor.

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 de SO de escritorio y SO de servidor. Una nueva mejora de funciones introducida en Citrix Virtual Apps and Desktops

© 1999-2019 Citrix Systems, Inc. All rights reserved.

7 1808 admite el redireccionamiento USB genérico de dispositivos de memoria USB con cifrado de hardware en sesiones de VDA de SO de escritorio y SO de servidor.
Una vez que se redirige el dispositivo, ninguna de sus unidades de disco 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 utilizando el canal virtual dedicado, como el canal virtual TWAIN, que también realiza la optimización. Estos dispositivos deben cumplir con los estándares de la industria. Si un dispositivo no es conforme o si no se usa de acuerdo con las intenciones originales, la redirección USB genérica podría ser la única forma de usar el dispositivo. Los datos heurísticos se utilizan para determinar qué dispositivos son dispositivos simples de imagen fija.

Utilice esta clave de Registro para establecer si los dispositivos simples de imagen fija se redirigen automáticamente:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices

Nombre: AutoRedirectImage

Tipo: DWORD

Datos: 00000000

El valor predeterminado es 0 (no redirige automáticamente). Al establecer un valor distinto de cero, redirige los dispositivos simples de imagen fija mediante el USB genérico.

También puede utilizar las directivas de Active Directory para implementar este valor en la siguiente clave de Registro y anular el valor que no corresponda a la directiva si ambos están presentes:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices

Nombre: AutoRedirectImage

Tipo: DWORD

Datos: 00000000

Parámetros específicos del dispositivo

Los procesos heurísticos utilizados para seleccionar dispositivos optimizables de Citrix (como impresoras, dispositivos de sonido, vídeo, almacenamiento e imágenes fijas) no siempre coinciden con lo que usted desea. Es posible que desee controlar la redirección automática de los dispositivos que no figuran en la lista anterior. Puede controlar la redirección automática según el dispositivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Por ejemplo, no es necesario redireccionar el lector de códigos de barras DemoTech 2.000 mediante el respaldo 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 utilizando las directivas de Active Directory en esta clave de Registro. Anula el valor que no corresponda a la directiva si ambos están presentes:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678

Nombre: AutoRedirect

Tipo: DWORD

Datos: 00000000

La configuración de AutoRedirect específica del dispositivo tiene prioridad sobre los valores más generales de AutoRedirectXXX explicados anteriormente. Los procesos heurísticos predeterminados para dispositivos optimizados de Citrix pueden malinterpretar un dispositivo como genérico. Por lo tanto, establezca el valor de AutoRedirect específico del dispositivo en 1 para redirigirlo automáticamente.

Configuraciones de directiva de Presentación visual

December 4, 2018

La sección Presentación visual contiene configuraciones de directiva para controlar la calidad de las imágenes enviadas desde los escritorios virtuales al dispositivo del usuario.

Profundidad de color preferida para gráficos simples

Esta configuración de directiva se encuentra disponible en las versiones de VDA 7.6 FP3 y las versiones posteriores. La opción de 8 bits está disponible en las versiones de VDA 7.12 y las versiones posteriores.

Esta configuración hace posible reducir la profundidad de color en los gráficos sencillos que se envían a través de la red. Reducir el color a 8 o 16 bits por píxel ofrece una mejora potencial de la capacidad de

© 1999-2019 Citrix Systems, Inc. All rights reserved.

respuesta en conexiones de poco ancho de banda, a costa de una pequeña degradación de la calidad de imagen. La profundidad de color de 8 bits no se admite cuando la configuración de directiva Usar códec de vídeo para compresión está definida en "Para la pantalla entera".

El valor predeterminado es la profundidad de color preferida de 24 bits por píxel.

Los VDA vuelven a la profundidad de color de 24 bits (predeterminada) si la opción de 8 bits se aplica a VDA 7.11 y versiones anteriores.

Velocidad de fotogramas de destino

Esta configuración especifica la cantidad máxima de fotogramas por segundo que se envían desde el escritorio virtual al dispositivo de usuario.

De forma predeterminada, el valor máximo es 30 fotogramas por segundo.

Establecer una cantidad alta de fotogramas por segundo (por ejemplo, 30) mejora la experiencia del usuario, pero requiere más ancho de banda. Reducir la cantidad de fotogramas por segundo (por ejemplo, a 10) maximiza la escalabilidad del servidor a expensas de la experiencia del usuario. Para los dispositivos de usuario con CPU lentas, especifique un valor inferior para mejorar la experiencia de usuario.

La velocidad máxima permitida es de 60 fotogramas por segundo.

Calidad visual

Esta configuración especifica la calidad visual de las imágenes que se muestran en el dispositivo del usuario.

De forma predeterminada, se establece en Media.

Para especificar la calidad de la imagen, seleccione una de las siguientes opciones:

- **Baja:** Se recomienda para redes con ancho de banda limitado donde la calidad visual se puede sacrificar para ganar en interactividad
- **Media:** Ofrece la mejor eficiencia de rendimiento y de ancho de banda en la mayoría de los casos de uso
- **Alta:** Opción recomendada cuando se requiere calidad de imagen sin pérdida
- **Gradual sin pérdida:** Envía imágenes con pérdida al dispositivo de usuario durante los períodos de mayor actividad en la red, e imágenes sin pérdida cuando la actividad en la red disminuye. Esta configuración mejora el rendimiento en conexiones de ancho de banda limitado.
- **Siempre sin pérdida:** En situaciones en que resulta totalmente necesario conservar la calidad de la imagen, seleccione "Siempre sin pérdida" para que nunca se envíen datos incompletos al dispositivo del usuario. Por ejemplo, al mostrar radiografías, donde una pérdida de calidad sería inaceptable.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Imágenes en movimiento

December 14, 2018

La sección Imágenes en movimiento contiene configuraciones que le permiten quitar o modificar la compresión para imágenes dinámicas.

Calidad de imagen mínima

Nota: Para Virtual Delivery Agent 7.x, esta configuración de directiva solo se aplica cuando la configuración de directiva Modo de gráficos antiguo está habilitada.

Esta configuración especifica la calidad de imagen mínima aceptable para la pantalla adaptable. Cuanto menor sea la compresión que se utilice, mayor es la calidad de las imágenes que se muestran. Elija la compresión entre las opciones Superalta, Muy alta, Alta, Normal y Baja.

De forma predeterminada, esta opción se establece en Normal.

Compresión de imágenes en movimiento

Esta configuración especifica si se habilita o no la pantalla adaptable. La pantalla adaptable ajusta automáticamente la calidad de imagen de los vídeos y las diapositivas de transición de las presentaciones según el ancho de banda disponible. Si la pantalla adaptable está habilitada, los usuarios pueden ver presentaciones de ejecución fluida, sin pérdida de calidad.

De manera predeterminada, la función de pantalla adaptable está habilitada.

Desde la versión 7.0 hasta la versión 7.6 de VDA, esta opción de configuración se aplica solo cuando el modo de gráficos antiguo está habilitado. Para VDA 7.6 FP1 y versiones posteriores, esta opción de configuración se aplica cuando el modo de gráficos antiguo está habilitado, o bien cuando el modo de gráficos antiguo está inhabilitado y no se usa ningún códec de vídeo para comprimir los gráficos.

Cuando el modo de gráficos antiguo está habilitado, la sesión debe reiniciarse para que los cambios de la directiva surtan efecto. La pantalla adaptable y la presentación progresiva se excluyen mutuamente; es decir, habilitar la pantalla adaptable inhabilita la presentación progresiva y viceversa. Sin embargo, tanto la presentación progresiva como la pantalla adaptable se pueden inhabilitar al mismo tiempo. La presentación progresiva, como función de versiones anteriores, no se recomienda para XenApp o XenDesktop. Establecer un umbral de presentación progresiva inhabilitará la pantalla adaptable.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nivel de compresión progresiva

Nota: Para Virtual Delivery Agent 7.x, esta configuración de directiva solo se aplica cuando la configuración de directiva Modo de gráficos antiguo está habilitada.

Esta configuración permite una presentación inicial con menor detalle pero más rápida.

De forma predeterminada, no se aplica la compresión progresiva.

La imagen más detallada aparece cuando está ya disponible, definida por la configuración de compresión con pérdida normal. Use la compresión Muy alta o Superalta para una presentación mejorada de gráficos que usan mucho ancho de banda, como las fotografías.

Para que la compresión progresiva sea efectiva, el nivel de compresión debe ser mayor que el definido en la configuración Nivel de compresión con pérdida.

Nota: Un mayor nivel de compresión asociado a la compresión progresiva también mejora la interactividad de imágenes dinámicas en las conexiones de cliente. La calidad de una imagen dinámica, como un modelo tridimensional en movimiento, disminuye temporalmente hasta que la imagen deja de moverse; en ese momento, se aplica la configuración del nivel de compresión con pérdida normal.

Configuraciones de directiva relacionadas:

- Valor de umbral de compresión progresiva
- Compresión intensa progresiva

Valor de umbral de compresión progresiva

Nota: Para Virtual Delivery Agent 7.x, esta configuración de directiva solo se aplica cuando la configuración de directiva Modo de gráficos antiguo está habilitada.

Esta configuración indica el valor máximo de ancho de banda (en kilobits por segundo), para una conexión a la que se aplica la compresión progresiva. Se aplica exclusivamente a las conexiones de cliente con un ancho de banda menor.

El umbral predeterminado es de 2 147 483 647 kilobits por segundo.

Configuraciones de directiva relacionadas:

- Valor de umbral de compresión progresiva
- Compresión intensa progresiva

Velocidad de fotogramas mínima de destino

Esta configuración especifica la velocidad de fotogramas por segundo mínima que el sistema intenta mantener para imágenes dinámicas cuando la conexión cuenta con poco ancho de banda.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

De forma predeterminada, el valor es de 10 fps.

Desde la versión 7.0 hasta la versión 7.6 de VDA, esta opción de configuración se aplica solo cuando el modo de gráficos antiguo está habilitado. A partir de la versión 7.6 FP1 de VDA, esta opción de configuración se aplica cuando el modo de gráficos antiguo está habilitado o inhabilitado.

Configuraciones de directiva de Imágenes fijas

December 14, 2018

La sección Imágenes fijas contiene configuraciones que permiten quitar o modificar la compresión para imágenes estáticas.

Compresión de color adicional

Esta configuración habilita o inhabilita el uso de la compresión de color adicional en imágenes enviadas a través de conexiones cliente que tienen una limitación de ancho de banda, con lo que se mejora la capacidad de respuesta al reducir la calidad de las imágenes presentadas.

De forma predeterminada, la compresión de color adicional está inhabilitada.

Cuando está habilitada, la compresión adicional de color se aplica solamente cuando el ancho de banda de la conexión del cliente está por debajo del valor especificado en Umbral de compresión de color adicional. Cuando el ancho de banda de la conexión de cliente es superior al umbral o la configuración está Inhabilitada, no se aplica la compresión.

Umbral de compresión de color adicional

Nota: Para Virtual Delivery Agent 7.x, esta configuración de directiva solo se aplica cuando la configuración de directiva Modo de gráficos antiguo está habilitada.

Esta configuración indica el valor máximo de ancho de banda de una conexión (en kilobits por segundo), por debajo del cual se aplicará la compresión de color adicional. Si el ancho de banda de la conexión de cliente cae por debajo del valor establecido, se aplica la compresión de color adicional (si está habilitada).

El umbral predeterminado es de 8192 kilobits por segundo.

Compresión intensa

Nota: Para Virtual Delivery Agent 7.x, esta configuración de directiva solo se aplica cuando la configuración de directiva Modo de gráficos antiguo está habilitada.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Esta configuración habilita o inhabilita la reducción del ancho de banda más allá de la compresión progresiva sin reducir la calidad de la imagen, utilizando 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. Está respaldada en la aplicación Citrix Workspace, pero no tiene ningún efecto en otros plug-ins.

Configuraciones de directiva relacionadas:

- Nivel de compresión progresiva
- Valor de umbral de compresión progresiva

Nivel de compresión con pérdida

Nota: Para Virtual Delivery Agent 7.x, esta configuración de directiva solo se aplica cuando la configuración de directiva Modo de gráficos antiguo está habilitada.

Esta configuración permite controlar el grado de compresión con pérdida de información usado para las imágenes transmitidas a través de conexiones de cliente que tienen un ancho de banda limitado. En tales casos, la presentación de imágenes sin comprimir puede tardar mucho.

De forma predeterminada, se utiliza una compresión media.

Para mejorar la capacidad de respuesta al usar imágenes que consumen mucho ancho de banda, use la compresión alta. En aquellos casos en los que es muy importante mantener toda la información de la imagen, como, por ejemplo, al ver imágenes de rayos X en situaciones en las que no es aceptable perder calidad, se recomienda no utilizar compresión con pérdida.

Configuración de directiva relacionada: Valor de umbral de compresión con pérdida

Valor de umbral de compresión con pérdida

Nota: Para Virtual Delivery Agent 7.x, esta configuración de directiva solo se aplica cuando la configuración de directiva Modo de gráficos antiguo está habilitada.

Esta configuración indica el valor máximo de ancho de banda (en kilobits por segundo) de una conexión a la que se aplicará compresión con pérdida.

El umbral predeterminado es de 2 147 483 647 kilobits por segundo.

Si se agrega la configuración Nivel de compresión con pérdida a una directiva y no se especifica ningún umbral, se puede incrementar la velocidad de presentación de mapas de bits con gran nivel de detalle, tales como fotografías, en una LAN.

Configuración de directiva relacionada: Nivel de compresión con pérdida

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de WebSockets

October 3, 2018

La sección “WebSockets” contiene configuraciones de directiva para acceder con la aplicación Citrix Workspace para HTML5 a los escritorios virtuales y las aplicaciones alojadas. La función WebSockets aumenta la seguridad y reduce la sobrecarga al llevar a cabo una comunicación bidireccional entre las aplicaciones basadas en exploradores Web y los servidores, sin abrir varias conexiones HTTP.

Conexiones con WebSockets

Esta configuración permite o prohíbe conexiones de WebSockets.

De forma predeterminada, las conexiones de WebSockets están prohibidas.

Número de puerto de WebSockets

Esta configuración identifica el puerto para conexiones entrantes de WebSocket.

De forma predeterminada, el valor es de 8008.

Lista de servidores de origen de WebSockets de confianza

Esta configuración proporciona una lista separada por comas de los servidores de origen de confianza (suele ser la aplicación Citrix Workspace para Web), expresados como direcciones URL. El servidor solo acepta conexiones de WebSockets procedentes de alguna de estas direcciones.

De forma predeterminada, se utiliza el carácter comodín * para confiar en todas las URL de la aplicación Citrix Workspace para Web.

Para escribir una dirección en la lista, use la siguiente sintaxis:

<protocolo>://<Nombre de dominio completo del host>:[puerto]

El protocolo debe ser HTTP o HTTPS. Si no se especifica el puerto, se usa el puerto 80 para HTTP y el puerto 443 para HTTPS.

El carácter comodín * se puede utilizar en la URL si no se trata de una dirección IP (10.105..).

Configuraciones de directiva de Administración de carga

October 3, 2018

© 1999-2019 Citrix Systems, Inc. All rights reserved.

La sección Administración de carga contiene configuraciones de directiva para habilitar y configurar la administración de carga entre los servidores que entregan máquinas con SO de servidor 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

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 100.

De manera predeterminada, esta configuración está habilitada.

Uso de memoria

Esta configuración especifica el nivel de uso de la memoria (como un porcentaje) alcanzado el cual, el servidor notifica carga completa. Cuando está habilitada, el valor predeterminado en el que el servidor notifica carga completa es del 90%.

De forma predeterminada, esta configuración está inhabilitada y el uso de la memoria queda excluido al calcular la carga.

Carga base de uso de memoria

Esta configuración especifica una aproximación del uso de memoria del sistema operativo base y define, en MB, el uso de memoria por debajo del cual se considera que el servidor tiene carga cero.

De forma predeterminada, este valor está establecido en 768 MB.

Configuraciones de directiva de Profile Management

January 22, 2019

La sección “Profile Management” contiene configuraciones de directiva para habilitar la administración de perfiles del componente Profile Management y especificar qué grupos incluir y excluir en el procesamiento de Profile Management.

Otra información, como los nombres de los parámetros del archivo INI equivalentes y la versión de Profile Management necesaria para cualquier configuración de directiva en particular, está disponible en Directivas de Profile Management.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Parámetros avanzados de directiva

October 3, 2018

La sección “Parámetros avanzados” contiene configuraciones de directiva relacionadas con una configuración avanzada de Profile Management.

Inhabilitar configuración automática

Esta configuración permite a Profile Management examinar el entorno; por ejemplo, para comprobar la presencia de discos Personal vDisk y configurar la directiva de grupo como corresponda. Solo se ajustan las directivas de Profile Management en el estado “No configurado”, por lo que todas las personalizaciones realizadas anteriormente se conservan. Esta función aumenta la velocidad de implementación y simplifica la optimización. La función no requiere ninguna configuración, pero puede inhabilitar la configuración automática al actualizar (para conservar la configuración de versiones anteriores) o durante la solución de problemas. La configuración automática no funciona en entornos de XenApp u otros.

De forma predeterminada, la configuración automática está permitida.

Si esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, la configuración automática se activa, por lo que la configuración de Profile Management puede cambiar si el entorno cambia.

Cerrar la sesión del usuario si hay algún problema

Esta configuración permite a Profile Management cerrar la sesión de un usuario si ocurre algún problema; por ejemplo, si el almacén de usuarios no está disponible. Cuando está habilitada, aparece un mensaje de error para el usuario antes de que se cierre la sesión. Cuando está inhabilitada, los usuarios reciben un perfil temporal.

De forma predeterminada, esta configuración está inhabilitada y los usuarios reciben un perfil temporal si se produce algún problema.

Si esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo .ini, se ofrece un perfil temporal.

Reintentos de acceso a archivos bloqueados

Esta configuración especifica la cantidad de intentos que realiza Profile Management para acceder a archivos bloqueados.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

De forma predeterminada, este valor está establecido en cinco reintentos.

Si esta configuración no está definida 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.

Procesar cookies de Internet al cerrar la sesión

Esta configuración permite que Profile Management procese el archivo index.dat al cerrar sesión para quitar las cookies de Internet que quedan en el sistema de archivos después de una exploración prolongada que puede provocar una sobrecarga del perfil. Al habilitarla, los cierres de sesión tardan más, de manera que se recomienda habilitarla solamente si es necesario.

De forma predeterminada, esta configuración está inhabilitada y Profile Management no procesa el archivo index.dat al cerrar la sesión.

Si esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo .ini, no se procesará el archivo index.dat.

Parámetros básicos de directiva

December 14, 2018

La sección “Parámetros básicos” contiene configuraciones de directiva relacionadas con una configuración básica de Profile Management.

Reescritura activa

Esta configuración permite sincronizar archivos y carpetas modificados (pero no los parámetros del Registro) con el almacén de usuarios durante una sesión antes de cerrarla.

De forma predeterminada, la sincronización con el almacén de usuarios durante una sesión está inhabilitada.

Si esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se considera habilitada.

Habilitar Profile Management

Esta configuración habilita Profile Management para procesar los inicios y los cierres de sesión.

De forma predeterminada, esta configuración está inhabilitada para facilitar la implementación.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Importante: Citrix recomienda habilitar Profile Management únicamente después de realizar todas las demás tareas de instalación y probar cómo funcionan los perfiles de usuario de Citrix en su entorno.

Si esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si la configuración no está definida ni aquí ni en el archivo INI, Profile Management no procesa los perfiles de usuario de Windows de ninguna manera.

Grupos excluidos

Esta configuración especifica qué grupos locales de equipo y de dominio (locales, globales y universales) se excluyen en el procesamiento de Profile Management.

Cuando está habilitada, Profile Management no procesa los miembros de los grupos de usuarios especificados.

De forma predeterminada, esta configuración está inhabilitada y se procesan los miembros de todos los grupos de usuarios.

Especifique los grupos de dominio así: <NOMBRE DE DOMINIO>\<NOMBRE DE GRUPO>.

Si esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se procesan los miembros de todos los grupos de usuarios.

Respaldo para perfiles sin conexión

Esta configuración habilita el respaldo para perfiles sin conexión, lo que permite que los perfiles se sincronicen con el almacén de usuarios en la primera oportunidad tras una desconexión de red.

De forma predeterminada, el respaldo para perfiles sin conexión está inhabilitado.

Esta configuración se aplica a usuarios de equipos portátiles o dispositivos móviles que utilicen el servicio de roaming. Cuando se produce una desconexión de red, los perfiles permanecen intactos en el equipo portátil o dispositivo móvil, incluso luego de reiniciar o hibernar. A medida que los usuarios móviles trabajan, su perfil se actualiza de forma local y se sincroniza con el almacén de usuarios cuando se vuelve a establecer la conexión de red.

Si esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se inhabilita el respaldo a perfiles sin conexión.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Ruta al almacén de usuarios

Esta configuración especifica la ruta al directorio (el almacén de usuarios) en el que se guardan las configuraciones de usuario, como, por ejemplo, los parámetros de Registro y los archivos sincronizados.

De forma predeterminada, se utiliza el directorio de Windows de la unidad principal.

Si esta configuración está inhabilitada, la configuración de usuario se guarda en el subdirectorio de Windows del directorio principal.

La ruta puede:

- Ser 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.
- Ser una **ruta UNC absoluta**. Esta ruta especifica generalmente un recurso compartido del servidor o un espacio de nombres DFS.
- **Estar inhabilitada o sin configurar**. En este caso, se asume el valor #homeDirectory#\Windows.

Utilice los siguientes tipos de variables al definir esta configuración de directiva:

- Variables de entorno del sistema entre signos de porcentaje (por ejemplo, %ProfVer%). Tenga en cuenta que 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 de Profile Management.

También puede usar las variables de entorno de usuario %username% y %userdomain% y crear atributos personalizados para definir las variables organizativas, como la ubicación o los 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$%USERNAME%.%USERDOMAIN%!CTX_PROFILEVER!!CTX_OSBITNESS! podría expandirse a \\server\profiles$\JohnSmith.DOMAINCONTROLLER1\v2x64

Importante: Independientemente de los atributos o las variables que utilice, compruebe que este parámetro se expande hasta la carpeta del nivel inmediatamente superior al de la carpeta donde se encuentra NTUSER.DAT. Por ejemplo, si este archivo se encuentra en \\server\profiles$\JohnSmith.Finance\v2x64\UPM_Profile, defina la ruta al almacén de usuarios como \\server\profiles$\JohnSmith.Finance\v2x64, no la subcarpeta \UPM_Profile.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Si esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se utiliza el directorio Windows de la unidad del directorio principal.

Procesar inicios de sesión de administradores locales

Esta configuración especifica si se procesan los inicios de sesión de los miembros del grupo BUILTIN\Administradores. Esto permite que los usuarios del dominio con derechos de administrador local, normalmente usuarios con escritorios virtuales asignados, puedan omitir el procesamiento, y puedan iniciar sesión y solucionar problemas de Profile Management en el escritorio.

Si esta configuración está inhabilitada, o si no está configurada en sistemas operativos de servidor, Profile Management asume que deben procesarse los inicios de sesión de usuarios del dominio, pero no los de administradores locales. En sistemas operativos de escritorio los inicios de sesión de administradores locales sí se procesan.

De forma predeterminada, esta configuración está inhabilitada y los inicios de sesión de administradores locales no se procesan.

Si esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, no se procesan los inicios de sesión de administrador local.

Grupos procesados

Esta configuración permite especificar qué grupos locales del equipo y grupos de dominio (locales, globales y universales) se incluyen en el procesamiento de Profile Management.

Cuando está habilitada, Profile Management procesará solo los miembros de los grupos de usuarios especificados.

De forma predeterminada, esta configuración está inhabilitada y se procesan los miembros de todos los grupos de usuarios.

Especifique los grupos de dominio así: <NOMBRE DE DOMINIO>\<NOMBRE DE GRUPO>.

Si esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se procesan los miembros de todos los grupos de usuarios.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Multiplataforma

January 29, 2019

La sección “Multiplataforma” contiene configuraciones de directiva relacionadas con la función de configuración multiplataforma de Profile Management.

Grupos de usuarios de configuración multiplataforma

Esta configuración especifica los grupos de usuarios de Windows cuyos perfiles se procesan cuando la función de configuración multiplataforma está habilitada.

De forma predeterminada, esta configuración está inhabilitada y se procesan todos los grupos de usuarios especificados en la configuración de directiva Grupos procesados.

Si esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se procesarán todos los grupos de usuarios.

Habilitar configuración multiplataforma

Esta configuración habilita o inhabilita la función de configuración multiplataforma, que permite migrar perfiles de usuarios y hacerlos móviles cuando un usuario se conecta a la misma aplicación en sistemas operativos distintos.

De forma predeterminada, la función de configuración multiplataforma está inhabilitada.

Si esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, no se aplicarán configuraciones multiplataforma.

Ruta de definiciones multiplataforma

Esta configuración especifica la ubicación de red como una ruta UNC de los archivos de definición copiados desde el paquete de descarga.

Nota: Los usuarios deben tener acceso de lectura y los administradores acceso de escritura a esta ubicación y debe ser un recurso compartido de archivos SMB (Server Message Block) o CIFS (Common Internet File System).

De forma predeterminada, no se especifica ninguna ruta.

Si esta configuración no está definida aquí, se utiliza el valor del archivo INI.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Si esta configuración no está definida ni aquí ni en el archivo INI, no se aplicarán configuraciones multiplataforma.

Ruta del almacén de configuración multiplataforma

Esta configuración especifica la ruta al almacén de configuraciones multiplataforma, que es la carpeta donde se guardan las configuraciones multiplataforma de los usuarios. La ruta puede ser una ruta UNC o una ruta relativa al directorio principal.

Nota: Los usuarios deben tener acceso de escritura al almacén multiplataforma.

De forma predeterminada, esta configuración está inhabilitada y se utiliza la ruta Windows\PM_CP.

Si esta configuración no está definida 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.

Origen para crear configuración multiplataforma

Esta configuración especifica una plataforma como la plataforma base si la configuración está habilitada para la unidad organizativa de esa plataforma. Los datos de los perfiles de la plataforma base migran 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.

Cuando está habilitada, Profile Management migra los datos desde el perfil de plataforma única al almacén si el almacén de configuración multiplataforma contiene un archivo de definición sin datos, o bien si los datos almacenados en caché en el perfil de una plataforma única son más recientes que los datos de definición que hay en el almacén.

Importante: Si esta configuración 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 forma predeterminada, esta configuración está inhabilitada y Profile Management no migra los datos del perfil de una plataforma única al almacén.

Configuraciones de directiva de Sistema de archivos

October 3, 2018

© 1999-2019 Citrix Systems, Inc. All rights reserved.

La sección Sistema de archivos contiene configuraciones de directiva para establecer qué archivos y directorios de un perfil de usuario se sincronizan entre el sistema en el que el perfil está instalado y el almacén de usuarios.

Configuraciones de directiva de Exclusiones

October 3, 2018

La sección Exclusiones contiene configuraciones de directiva para establecer qué archivos y directorios de un perfil de usuario se excluyen del proceso de sincronización.

Lista de exclusión de directorios

Esta configuración especifica una lista de las carpetas del perfil de usuario que se ignoran durante la sincronización.

Especifique los nombres de carpeta como rutas relativas al perfil de usuario (%USERPROFILE%).

De forma predeterminada, esta configuración está inhabilitada y se sincronizan todas las carpetas del perfil de usuario.

Ejemplo: “Escritorio” ignora la carpeta Escritorio en el perfil del usuario

Si esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se sincronizan todas las carpetas del perfil de usuario.

Lista de exclusión de archivos

Esta configuración especifica una lista de archivos del perfil de usuario que se ignoran durante la sincronización.

De forma predeterminada, esta configuración está inhabilitada y se sincronizan todos los archivos del perfil de usuario.

Especifique los nombres de archivo como rutas relativas al perfil de usuario (%USERPROFILE%). Tenga en cuenta que se permiten comodines y se aplican de forma recursiva.

Ejemplo: Escritorio\Desktop.ini ignora el archivo Desktop.ini de la carpeta Escritorio

Si esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se sincronizan todos los archivos del perfil de usuario.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Sincronización

March 14, 2019

La sección Sincronización contiene configuraciones de directiva para especificar qué archivos y carpetas de un perfil de usuario se sincronizarán entre el sistema en el que el perfil está instalado y el almacén de usuarios.

Directorios a sincronizar

Esta configuración especifica los archivos que Profile Management debe incluir en el proceso de sincronización y que están ubicados en carpetas excluidas. De manera predeterminada, Profile Management sincroniza todo el contenido del perfil de usuario. No es necesario agregar las subcarpetas del perfil del usuario a la lista para incluirlas. Para obtener más información, consulte el tema general Incluir y excluir elementos.

Las rutas de la lista deben ser relativas al perfil de usuario.

Ejemplo: Escritorio\excluir\incluir hace que la subcarpeta llamada “incluir” se sincronice aun cuando la carpeta llamada “Escritorio\excluir” no se sincronice

De forma predeterminada, esta configuración está inhabilitada y no se especifica ninguna carpeta.

Si esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se sincronizarán solo las carpetas que no se han excluido del perfil de usuario.

Archivos a sincronizar

Esta configuración especifica los archivos que Profile Management debe incluir en el proceso de sincronización y que están ubicados en carpetas excluidas. De manera predeterminada, Profile Management sincroniza todo el contenido del perfil de usuario. No es necesario agregar archivos del perfil del usuario a la lista para incluirlos. Para obtener más información, consulte el tema general Incluir y excluir elementos.

Las rutas de la lista deben ser relativas al perfil de usuario. Las rutas relativas se interpretan como relativas al perfil de usuario. Es posible utilizar comodines, pero solo se permiten para los nombres de archivo. No es posible anidar los comodines y se aplican de forma recursiva.

Ejemplos:

- AppData\Local\Microsoft\Office\Access.qat especifica un archivo que se encuentra en un nivel inferior de una carpeta excluida en la configuración predeterminada

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- AppData\Local\MyApp*.cfg especifica todos los archivos con la extensión .cfg en la carpeta AppData\Local\MyApp del perfil y sus subcarpetas

De forma predeterminada, esta configuración está inhabilitada y no se especifica ningún archivo.

Si esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se sincronizan solo los archivos que no se han excluido del perfil de usuario.

Carpetas a reflejar

Esta configuración permite especificar qué carpetas relativas a la carpeta raíz de un perfil de usuario hay que reflejar. Esta configuración de directiva puede ayudar a resolver problemas relacionados con carpetas transaccionales (también conocidas como carpetas de referencia), que contienen archivos interdependientes, donde un archivo hace referencia a los otros.

El reflejo de las carpetas permite a Profile Management procesar una carpeta transaccional y su contenido como una sola entidad, evitando la sobrecarga del perfil. Tenga en cuenta que 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, 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.

Si un usuario abre dos sesiones de Internet Explorer, cada una en un servidor diferente, y consulta distintos sitios en cada sesión, las cookies de cada sitio se agregarán al servidor apropiado. Cuando el usuario se desconecte de la primera sesión (o en la mitad de una sesión, si está habilitada la función de reescritura activa), las cookies de la segunda sesión deberían sustituir aquellas de la primera sesión. Sin embargo, éstas se combinan, y las referencias a las cookies en Index.dat se vuelven obsoletas. Las consultas adicionales que se hagan en sesiones nuevas resultarán en combinaciones repetidas y en una carpeta de cookies saturada.

La posibilidad de reflejar la carpeta de cookies resuelve el problema al sobrescribir las cookies con las de la última sesión cada vez que el usuario cierra la sesión, de manera que Index.dat permanece siempre actualizado.

De forma predeterminada, esta configuración está inhabilitada y no se refleja ninguna carpeta.

Si esta configuración no está definida 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Redirección de carpetas

December 4, 2018

La sección Redirección de carpetas contiene configuraciones de directiva para especificar si desea redirigir las carpetas que suelen aparecer en perfiles a una ubicación de red compartida.

Conceder acceso a administradores

Esta configuración permite que un administrador pueda acceder al contenido de las carpetas redirigidas de un usuario.

> **Nota:**
>
> Este parámetro otorga permisos a los administradores que tienen acceso completo y sin restricciones al dominio.

De forma predeterminada, esta configuración está inhabilitada y los usuarios tienen acceso exclusivo al contenido de sus carpetas redirigidas.

Incluir nombre de dominio

Esta configuración habilita la inclusión de la variable de entorno %userdomain% como parte de la ruta UNC especificada para carpetas redirigidas.

De forma predeterminada, esta configuración está inhabilitada y la variable de entorno %userdomain% no se incluye como parte de la ruta UNC especificada para carpetas redirigidas.

Configuraciones de directiva de AppData(Roaming)

October 3, 2018

La sección AppData(Roaming) contiene configuraciones de directiva para especificar si se debe 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 este parámetro no está configurado aquí, Profile Management no redirige la carpeta especificada.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Parámetros de redirección para AppData(Roaming)

Esta configuración especifica cómo redirigir el contenido de la carpeta AppData(Roaming).

De forma predeterminada, el contenido se redirige a una ruta UNC.

Si este parámetro no está configurado aquí, Profile Management no redirige la carpeta especificada.

Configuraciones de directiva de Contactos

October 3, 2018

La sección Contactos contiene configuraciones de directiva para especificar si se debe 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

October 3, 2018

La sección Escritorio contiene configuraciones de directiva para especificar si se debe redirigir el contenido de la carpeta Escritorio a una ubicación de red compartida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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

October 3, 2018

La sección Documentos contiene configuraciones de directiva para especificar si se debe 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:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- 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

December 14, 2018

La sección Descargas contiene configuraciones de directiva para especificar si se debe 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 en 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

October 3, 2018

La sección Favoritos contiene configuraciones de directiva para especificar si se debe redirigir el contenido de la carpeta Favoritos a una ubicación de red compartida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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

October 3, 2018

La sección Vínculos contiene configuraciones de directiva para especificar si se debe 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Música

October 3, 2018

La sección Música contiene configuraciones de directiva para especificar si se debe 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.

Parámetros 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

October 3, 2018

La sección Imágenes contiene configuraciones de directiva para especificar si se debe 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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

October 3, 2018

La sección Juegos guardados contiene configuraciones de directiva para especificar si se debe 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Menú Inicio

October 3, 2018

La sección Menú Inicio contiene configuraciones de directiva para especificar si se debe 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

October 3, 2018

La sección Búsquedas contiene configuraciones de directiva para especificar si se debe 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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

October 3, 2018

La sección Vídeos contiene configuraciones de directiva para especificar si se debe 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Registro

October 3, 2018

La sección “Registro” 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 aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se registran los errores y la información general.

Información común

Esta configuración habilita o inhabilita el registro detallado de información común.

De forma predeterminada, esta configuración está inhabilitada.

Cuando habilite esta configuración, compruebe que la configuración Habilitar registro también está habilitada.

Si esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se registran los errores y la información general.

Advertencias comunes

Esta configuración habilita o inhabilita el registro detallado de advertencias comunes.

De forma predeterminada, esta configuración está inhabilitada.

Cuando habilite esta configuración, compruebe que la configuración Habilitar registro también está habilitada.

Si esta configuración no está definida aquí, se utiliza el valor del archivo INI.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Si esta configuración no está definida ni aquí ni en el archivo INI, se registran los errores y la información general.

Habilitar registro

Esta configuración habilita o inhabilita el registro de Profile Management en el modo de depuración (registro detallado). En modo de depuración, la información detallada de estado se registra en los archivos de registro ubicados en "%SystemRoot%\System32\Logfiles\UserProfileManager".

De forma predeterminada, esta configuración está inhabilitada y solo se registran los errores.

Citrix recomienda habilitar esta configuración solo cuando vaya a solucionar problemas de Profile Management.

Si esta configuración no está definida 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 esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se registran los errores y la información general.

Notificaciones del sistema de archivos

Esta configuración habilita o inhabilita el registro detallado de las notificaciones de los sistemas de archivos.

De forma predeterminada, esta configuración está inhabilitada.

Cuando habilite esta configuración, compruebe que la configuración Habilitar registro también está habilitada.

Si esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se registran los errores y la información general.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se registran los errores y la información general.

Inicio de sesión

Esta configuración habilita o inhabilita el registro detallado de los inicios de sesión de los usuarios.

De forma predeterminada, esta configuración está inhabilitada.

Cuando habilite esta configuración, compruebe que la configuración Habilitar registro también está habilitada.

Si esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se registran los errores y la información general.

Tamaño máximo del archivo de registro

Esta configuración permite especificar el valor máximo permitido para el archivo de registro de Profile Management en bytes.

De forma predeterminada, este valor está establecido en 1.048.576 bytes (1 MB).

Citrix recomienda aumentar el tamaño de este archivo a 5 MB o más si dispone de suficiente espacio en disco. Si el archivo de registro supera el tamaño máximo indicado, se elimina una copia de seguridad (.bak) del archivo, se cambia el nombre del archivo de registro a .bak y se crea un nuevo archivo de registro.

El archivo de registro se crea en %SystemRoot%\System32\Logfiles\UserProfileManager.

Si esta configuración no está definida 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Ruta al archivo de registro

Esta configuración especifica una ruta alternativa en la que guardar el archivo de registros de Profile Management.

De forma predeterminada, esta configuración está inhabilitada y los archivos de registro se guardan en la ubicación predeterminada: %SystemRoot%\System32\Logfiles\UserProfileManager.

La ruta puede corresponder a una unidad local o a una unidad remota en la red (una ruta UNC). Las rutas remotas pueden ser útiles en entornos distribuidos de gran tamaño, pero pueden crear un tráfico de red significativo, lo cual puede ser inadecuado para los archivos de registros. En el caso de máquinas virtuales aprovisionadas, con una unidad de disco duro persistente, defina una ruta local a dicha unidad. Esto garantiza que los archivos de registro se conservarán cuando la máquina se reinicie. Para máquinas virtuales sin disco duro persistente, la definición de una ruta UNC permite conservar los archivos de registros, pero la cuenta de sistema de las máquinas debe tener acceso de escritura en el punto compartido UNC. Use una ruta local para los equipos portátiles gestionados con la función de perfiles sin conexión.

Si se usa una ruta UNC para los archivos de registro, Citrix recomienda aplicar una lista de control de acceso a la carpeta donde se guardan los mismos, para garantizar que sólo tengan acceso a ellos las cuentas de los usuarios y equipos autorizados.

Si esta configuración no está definida 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 esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se registran los errores y la información general.

Valores de directivas al iniciar y cerrar la sesión

Esta configuración habilita o inhabilita el registro detallado de valores de directivas cuando un usuario inicia y cierra sesión.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se registran los errores y la información general.

Acciones del Registro del sistema

Esta configuración habilita o inhabilita el registro detallado de las acciones realizadas en el Registro del sistema.

De forma predeterminada, esta configuración está inhabilitada.

Cuando habilite esta configuración, compruebe que la configuración Habilitar registro también está habilitada.

Si esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se registran los errores y la información general.

Diferencias en el Registro del sistema al cerrar la sesión

Esta configuración habilita o inhabilita el registro detallado de las diferencias en el Registro cuando un usuario cierra sesión.

De forma predeterminada, esta configuración está inhabilitada.

Cuando habilite esta configuración, compruebe que la configuración Habilitar registro también está habilitada.

Si esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se registran los errores y la información general.

Configuraciones de directiva de Gestión de perfiles

October 3, 2018

La sección “Gestión de perfiles” contiene configuraciones de directiva para definir la forma en que Profile Management gestiona los perfiles de usuario.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Demora antes de eliminar perfiles en caché

Esta configuración especifica una extensión opcional para el intervalo de demora, en segundos, antes de que Profile Management elimine los perfiles almacenados en caché local al cerrar sesión.

Un valor de 0 elimina los perfiles inmediatamente al final del proceso de cierre de sesión. Profile Management comprueba los cierres de sesión cada minuto, por lo que un valor de 60 garantiza que los perfiles se eliminan entre uno y dos minutos después de que los usuarios hayan cerrado la sesión (dependiendo de cuando tuvo lugar la última comprobación). Ampliar la demora es útil si sabe que un proceso mantiene abiertos los archivos o el subárbol User del Registro durante el cierre de sesión. Con grandes perfiles, esto también puede acelerar el cierre de sesión.

De forma predeterminada, este valor está establecido en 0 y Profile Management elimina inmediatamente los perfiles almacenados en caché local.

Cuando habilite esta configuración, compruebe que Eliminar perfiles guardados en caché local al cerrar la sesión también está habilitada.

Si esta configuración no está definida 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 esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, los perfiles almacenados en caché no se eliminan.

Gestión de conflictos de perfiles locales

Esta configuración define el comportamiento de Profile Management si el mismo perfil de usuario consta en el almacén de usuarios y en Windows como perfil local (no un perfil de usuario de Citrix).

De forma predeterminada, Profile Management utiliza el perfil de Windows local, pero no lo cambia de ninguna manera.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se utilizan los perfiles locales existentes.

Migración de perfiles existentes

Esta configuración especifica los tipos de perfil migrados al almacén de usuarios durante el inicio de sesión si un usuario no tiene ningún perfil actual en el almacén de usuarios.

Profile Management puede migrar perfiles existentes inmediatamente durante el inicio de sesión si un usuario no tiene perfil en el almacén de usuarios. Al finalizar este proceso, Profile Management utiliza el perfil del almacén de usuarios tanto en la sesión actual como en cualquier otra sesión configurada con la ruta al mismo almacén de usuarios.

De forma predeterminada, se migran los perfiles locales y móviles al almacén de usuarios durante el inicio de sesión.

Para especificar los tipos de perfil que se migran al almacén de usuarios durante el inicio de sesión, elija una de las siguientes opciones:

- Perfiles locales y móviles
- Locales
- Roaming
- 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 esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se migran los perfiles locales y móviles existentes.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Ruta al perfil de plantilla

Esta configuración especifica la ruta al perfil que Profile Management deberá utilizar como plantilla para crear nuevos 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 \\MiServidor\MisPerfiles\plantillas\ntuser.da se definiría la ubicación como \\MiServidor\MisPerfiles\plantillas.

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 respalda 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% o %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 esta configuración no está definida 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 nuevos perfiles de usuario.

Si un usuario no tiene perfil de usuario de Citrix, pero existe un perfil de usuario local de Windows, de forma predeterminada se utiliza el perfil local (y se migra al almacén de usuarios si esto no está inhabilitado). Al habilitar esta configuración de directiva, el perfil de plantilla anula el perfil local que se usa durante la creación de nuevos perfiles de usuario.

Si esta configuración no está definida 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 nuevos perfiles de usuario.

Si un usuario no tiene perfil de usuario de Citrix, pero existe un perfil de usuario móvil de Windows, de forma predeterminada se utiliza el perfil móvil (y se migra al almacén de usuarios si esto no está

© 1999-2019 Citrix Systems, Inc. All rights reserved.

inhabilitado). Al habilitar esta configuración de directiva, el perfil de plantilla anula el perfil móvil utilizado durante la creación de nuevos perfiles de usuario.

Si esta configuración no está definida 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 nuevos 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 esta configuración no está definida 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

October 3, 2018

La sección “Registro del sistema” contiene configuraciones de directiva para especificar qué claves del Registro se incluyen o excluyen en el procesamiento de Profile Management.

Lista de exclusión

Esta configuración especifica la lista de claves de Registro en el subárbol HKCU que se excluyen del procesamiento de Profile Management cuando un usuario cierra sesión.

Cuando está habilitada, las claves especificadas en esta lista se excluyen del procesamiento cuando un usuario cierra la sesión.

De forma predeterminada, esta configuración está inhabilitada y todas las claves del Registro en el subárbol HKCU se procesan cuando un usuario cierra la sesión.

Si esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, no se excluye ninguna clave de Registro.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Lista de inclusión

Esta configuración especifica la lista de claves de Registro en el subárbol HKCU que se incluyen en el procesamiento de Profile Management cuando un usuario cierra sesión.

Cuando está habilitada, solo las claves especificadas en esta lista se procesan cuando un usuario cierra la sesión.

De forma predeterminada, esta configuración está inhabilitada y todas las claves del Registro en el subárbol HKCU se procesan cuando un usuario cierra la sesión.

Si esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se procesará toda la sección HKCU.

Configuraciones de directiva para Perfiles de usuario de streaming

October 3, 2018

La sección “Perfiles de usuario de streaming” 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 esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se considera inhabilitada.

Tamaño de caché

Esta configuración especifica un límite inferior, en megabytes, 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

De forma predeterminada, este valor está establecido en 0 (cero) y se usa la función de guardado del perfil entero en caché. Cuando la función de guardado del perfil entero en caché está habilitada, Profile Management obtiene todo el contenido del perfil en el almacén de usuarios, cuando un usuario inicia sesión, como una tarea en segundo plano.

Si esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se considera inhabilitada.

Streaming de perfiles

Esta configuración habilita o inhabilita la función de streaming de perfiles de usuario de Citrix. Cuando está habilitada, las carpetas y los archivos incluidos en un perfil se obtienen del almacén de usuarios y se envían al equipo local solo cuando los usuarios acceden a estos archivos y carpetas después de iniciar una sesión. Las entradas del Registro y los archivos del área de archivos pendientes se obtienen inmediatamente.

De forma predeterminada, el streaming de perfiles está inhabilitado.

Si esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se considera inhabilitada.

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 esta configuración no está definida aquí, se utiliza el valor del archivo INI.

Si esta configuración no está definida ni aquí ni en el archivo INI, se procesan todos los perfiles de usuario.

Para habilitar la exclusión de streaming de perfiles

Cuando la exclusión de streaming de perfiles está habilitada, Profile Management no distribuye por streaming las carpetas especificadas en la lista de exclusiones, con lo que todas las carpetas se obtienen inmediatamente desde el almacén de usuarios al equipo local cuando un usuario inicia sesión.

Para obtener más información, consulte Perfiles de usuario de streaming.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Tiempo de espera para bloqueo del área de archivos pendientes

Esta configuración especifica el período de tiempo (en días) transcurrido el cual, los archivos de los usuarios se escriben de nuevo en el almacén de usuarios desde el área de archivos pendientes en el caso de que el almacén de usuarios quede bloqueado cuando un servidor no responde. Esto evita la saturación en el área de archivos pendientes y garantiza que el almacén de usuarios siempre contenga los archivos más actualizados.

De forma predeterminada, este valor está establecido en 1 (un) día.

Si esta configuración no está definida 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.

Configuraciones de directiva de Receiver

October 3, 2018

Nota: A menos que se indique lo contrario, “Receiver” hace referencia a Citrix Receiver.

La sección Receiver contiene configuraciones de directiva que especifican una lista de las direcciones de StoreFront a insertar en Citrix Receiver para Windows ejecutado en el escritorio virtual.

Lista de cuentas de StoreFront

Esta configuración especifica una lista de las tiendas de StoreFront que los administradores pueden insertar en el Citrix Receiver para Windows que se ejecuta en el escritorio virtual. Cuando crean un grupo de entrega, los administradores pueden seleccionar qué tiendas quieren insertar en el Citrix Receiver para Windows ejecutado en los escritorios virtuales de ese grupo.

De forma predeterminada, no hay ninguna tienda especificada.

Para cada tienda, especifique la siguiente información como entradas separadas por punto y coma:

- Nombre de la tienda. El nombre que se muestra a los usuarios de la tienda.
- URL de la tienda. La dirección URL de la tienda.
- Habilitación de la tienda. Indica si la tienda está disponible para los usuarios. Aquí hay dos opciones: Sí o No.
- Descripción de la tienda. La descripción que se muestra a los usuarios de la tienda.

Por ejemplo: Tienda de Ventas;`https://sales.mycompany.com/Citrix/Store/discovery` ;Sí;Tienda para personal de Ventas

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Virtual Delivery Agent

October 3, 2018

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
- SIDs 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 registrará VDA. VDA se registrará solo en la primera dirección que coincida con la máscara de red especificada. Esta configuración solo es válida si la configuración de directiva Usar solo registro de Controller con IPv6 está habilitada.

De forma predeterminada, esta configuración está en blanco.

Puerto de registro de Controller

Use esta configuración solamente si Habilitar actualización automática de Controller está inhabilitada.

Esta configuración especifica el número de puerto TCP/IP que VDA utiliza para registrarse con un Controller cuando se usa un registro basado en el Registro del sistema.

De forma predeterminada, el número de puerto es el 80.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

SIDs de Controller

Use esta configuración solamente si Habilitar actualización automática de Controller está inhabilitada.

Esta configuración especifica una lista separada por espacios de identificadores de seguridad (SID) de Controllers que VDA usa para registrarse con un Controller cuando se usa un registro basado en el Registro del sistema. Este es un parámetro opcional que se puede usar con la configuración Controllers para restringir la lista de Controllers utilizados para el registro.

De forma predeterminada, esta configuración está en blanco.

Controllers

Use esta configuración solamente si Habilitar actualización automática de Controller está inhabilitada.

Esta configuración especifica una lista separada por espacios de nombres de dominio completos (FQDN) de Controllers que el VDA usa para registrarse con un Controller cuando se usa un registro basado en el Registro del sistema. Esta es una configuración optativa que puede utilizarse junto con la configuración SIDs de Controller.

De forma predeterminada, esta configuración está en blanco.

Habilitar actualización automática de Controller

Esta configuración permite que el VDA se registre con un Controller automáticamente después de la instalación.

Después de que el VDA se registre, el Controller con el que se registró envía una lista actualizada de los SID y FQDN del Controllers al VDA. VDA escribe esta lista en almacenamiento persistente. Cada Controller también comprueba la base de datos del sitio cada 90 minutos para verificar la información sobre los Controllers; si un Controller se ha agregado o quitado desde la última comprobación, o si se ha producido un cambio en la directiva, Controller envía listas actualizadas a los VDA registrados. Los VDA aceptarán conexiones de todos los Controllers de la lista más reciente que hayan recibido.

De manera predeterminada, esta configuración está habilitada.

Usar solo el registro de Controller con IPv6

Esta configuración controla qué tipo de dirección usa el VDA para registrarse con un Controller:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Cuando está habilitada, el VDA se registra con el Controller usando la dirección IPv6 de la máquina. Cuando el VDA se comunica con el Controller, se utiliza el siguiente orden de direcciones: dirección IP global, dirección local única (ULA), dirección local de vínculo (si no hay otras direcciones IPv6 disponibles).
- Cuando está inhabilitada, el VDA se registra y se comunica con el Controller mediante la dirección IPv4 de la máquina.

De manera predeterminada, esta configuración está inhabilitada.

GUID del sitio

Use esta configuración solamente si Habilitar actualización automática de Controller está inhabilitada.

Esta configuración especifica el identificador único global (GUID) del sitio que utiliza VDA para registrarse con un Controller cuando se usa el registro basado en Active Directory.

De forma predeterminada, esta configuración está en blanco.

Configuraciones de directiva de HDX 3D Pro

October 3, 2018

La sección HDX 3D Pro contiene configuraciones de directiva para habilitar y definir los parámetros de la herramienta de configuración de la calidad de imagen para los usuarios. La herramienta permite que los usuarios ajusten el equilibrio entre calidad de imagen y capacidad de respuesta en tiempo real para optimizar el uso del ancho de banda disponible.

Habilitar sin pérdida

Esta configuración especifica si los usuarios pueden o no habilitar e inhabilitar la compresión sin pérdida mediante la herramienta de configuración de la calidad de imagen. De forma predeterminada, los usuarios no tienen la opción de habilitar la compresión sin pérdida.

Cuando un usuario habilita la compresión sin pérdida, la calidad de imagen se establece automáticamente en el valor máximo disponible en la herramienta de configuración de la imagen. De forma predeterminada, se puede utilizar la compresión basada en CPU o GPU, según la capacidad del dispositivo del usuario y el equipo host.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Parámetros de calidad de HDX 3D Pro

Esta configuración especifica los valores mínimos y máximos que definen el intervalo de ajuste de la calidad de imagen disponible para los usuarios en la herramienta de configuración de la calidad de imagen.

Especifique valores de calidad de imagen entre 0 y 100, ambos valores incluidos. El valor máximo debe ser mayor o igual que el valor mínimo.

Configuraciones de directiva de Supervisión

January 22, 2019

La sección Supervisión contiene configuraciones de directiva para la supervisión de procesos, recursos y errores de aplicaciones.

El ámbito de estas directivas se puede definir según el sitio, el grupo de entrega, el tipo de grupo de entrega, la unidad organizativa y las etiquetas.

Directivas para la supervisión de procesos y recursos

Cada punto de datos de la CPU, la memoria y los procesos se recopila del VDA y se almacena en la base de datos de Supervisión. El envío de puntos de datos desde el VDA consume ancho de banda y su almacenamiento consume un espacio considerable en la base de datos de supervisión. Si no quiere supervisar datos de procesos o de recursos (o ninguno de los dos) de un ámbito concreto (por ejemplo, un grupo de entrega o una unidad organizativa específicos), se recomienda inhabilitar la directiva.

Habilitar supervisión de procesos

Habilite esta configuración para permitir la supervisión de procesos que se ejecutan en las máquinas con agentes VDA. Las estadísticas (por ejemplo, acerca del uso de la CPU y la memoria) se envían a Monitoring Service. Las estadísticas se utilizan para notificaciones en tiempo real e informes históricos en Director.

La opción predeterminada de esta configuración es “Inhabilitada”.

Habilitar supervisión de recursos

Habilite esta configuración para permitir la supervisión de los contadores de rendimiento en las máquinas con agentes VDA. Las estadísticas (por ejemplo, acerca de la CPU y la memoria, IOPS y la

© 1999-2019 Citrix Systems, Inc. All rights reserved.

latencia de datos) se envían a Monitoring Service. Las estadísticas se utilizan para notificaciones en tiempo real e informes históricos en Director.

La opción predeterminada de esta configuración es “Habilitada”.

Escalabilidad

Los datos de la CPU y la memoria se envían desde cada VDA a la base de datos en intervalos de 5 minutos. Los datos de procesos (si la opción está habilitada) se envían a la base de datos en intervalos de 10 minutos.Los datos de IOPS y latencia disco se envían a la base de datos cada hora.

Datos de CPU y memoria

De forma predeterminada, la opción de datos de CPU y memoria está **habilitada**. Los valores de retención de datos son los siguientes (licencia Platinum):

Granularidad de datos	Cantidad de días
Datos de 5 minutos	1 día
Datos de 10 minutos	7 días
Datos por hora	30 días
Datos diarios	90 días

Datos de IOPS y latencia de disco

Los datos de IOPS y latencia de disco están **habilitados** de forma predeterminada. Los valores de retención de datos son los siguientes (licencia Platinum):

Granularidad de datos	Cantidad de días
Datos por hora	3 días
Datos diarios	90 días

Con esta configuración de retención de datos, se necesitan aproximadamente 276 KB de espacio para almacenar los datos de la CPU, la memoria las IOPS y la latencia de disco provenientes de un VDA en un periodo de un año.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Cantidad de máquinas	Almacenamiento aproximado requerido
1	276 KB
1000	270 MB
40 000	10,6 GB

Datos de procesos

Los datos de procesos están **inhabilitados** de forma predeterminada. Se recomienda habilitar los datos de procesos en un subconjunto de máquinas si fuera necesario. La configuración predeterminada de retención para datos de procesos es la siguiente:

Granularidad de datos	Cantidad de días
Datos de 10 minutos	1 día
Datos por hora	7 días

Si se habilitan los datos de procesos, con la configuración predeterminada de retención de datos, consumirían aproximadamente 1,5 MB por cada VDA y 3 MB por cada VDA de Terminal Services (VDA de TS) en un periodo de un año.

Cantidad de máquinas	Almacenamiento aproximado requerido para el VDA	Almacenamiento aproximado requerido para el VDA de Terminal Services
1	1,5 MB	3 MB
1000	1,5 GB	3 GB

> **Nota**
>
> Estos números no incluyen el espacio de índice. Además, todos esos cálculos son aproximados y pueden variar de una implementación a otra.

Configuraciones opcionales

Puede modificar la configuración de retención predeterminada para que se adapte a sus necesidades. Sin embargo, eso consume almacenamiento extra. Al habilitar los siguientes parámetros, puede

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 de servidor. 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 **Valor** en **Ninguna**.
El valor predeterminado de esta configuración es “Solo fallos de aplicación”.

Habilitar supervisión de fallos y errores de aplicación en VDA de SO de escritorio

De forma predeterminada, solo se supervisan los fallos de las aplicaciones alojadas en agentes VDA de SO de servidor. Para supervisar los VDA de SO de escritorio, establezca la directiva en **Permitida**.
De forma predeterminada, esta configuración está establecida en **Prohibida**.

Lista de aplicaciones excluidas de la supervisión de fallos y errores

Especifique una lista de las aplicaciones que no se supervisarán para buscar fallos.
De forma predeterminada, esta lista está vacía.

Sugerencias para la planificación de almacenamiento

Directiva de grupo.Si no quiere supervisar los datos de recursos o procesos, ambos se pueden desactivar mediante la directiva de grupo. Para obtener más información, consulte la sección Directiva de grupo de Creación de directivas.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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

October 3, 2018

La sección IP virtual contiene configuraciones de directiva que controlan si las sesiones tienen su propia dirección virtual de bucle invertido.

Respaldo para bucle invertido de IP virtual

Cuando esta configuración está habilitada, cada sesión tiene su propia dirección virtual de bucle invertido. Cuando está inhabilitada, las sesiones no tienen direcciones de bucle invertido individuales.

De forma predeterminada, esta configuración está inhabilitada.

Lista de programas para bucle invertido de IP virtual

Esta configuración especifica los archivos ejecutables de aplicaciones que pueden usar direcciones virtuales de bucle invertido. Al agregar programas a la lista, especifique solamente el nombre del archivo ejecutable, no es necesario especificar la ruta completa.

De forma predeterminada, no hay archivos ejecutables especificados.

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

March 8, 2019

En las versiones de VDA desde 7.0 a 7.8, los parámetros de puertos COM y puertos LPT solo se pueden configurar utilizando el Registro. Para versiones de VDA anteriores a 7.0 y a partir de VDA 7.9, estos parámetros se pueden configurar en Studio. Para obtener más información, consulte Configuraciones de directiva de Redirección de puertos y Configuraciones de directiva de ancho de banda.

Las configuraciones de directiva de Redirección de puertos COM y puertos LPT se encuentran en HKLM\Software\Citrix\GroupPolicy\Defaults\Deprecated en la imagen o la máquina VDA.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para habilitar la redirección de puertos COM y puertos LPT, agregue nuevas claves de Registro de tipo REG_DWORD, como se muestra a continuación:

Precaución: Si modifica el Registro de forma incorrecta, podrían generarse problemas graves que pueden provocar la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Clave del Registro	Description	Valores permitidos
AllowComPortRedirection	Permitir o impedir la redirección de puertos COM	1 (Permitir) o 0 (Prohibir)
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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 para Configuration Manager 2012

October 3, 2018

La sección de Connector para 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 de servidor administradas manualmente o mediante Provisioning Services. Para esos catálogos de máquinas, el servicio Connector avisa a los usuarios cuando hay instalaciones de aplicaciones o actualizaciones de software pendientes.

En caso de catálogos administrados por MCS, use Studio para notificar a los usuarios. En caso de catálogos de máquinas con SO de escritorio administrados manualmente, utilice Configuration Manager para notificar a los usuarios. En caso de catálogos de máquinas con SO de escritorio administradas por Provisioning Services, utilice Provisioning Services para notificar a los usuarios.

Frecuencia de advertencias por adelantado

Este parámetro define el intervalo de frecuencia con que aparecen los mensajes de advertencia para los usuarios.

Los intervalos se establecen con el formato ddd.hh:mm:ss, donde:

- ddd son los días, un parámetro optativo, con un rango de 0 a 999.
- hh son las horas, con un rango de 0 a 23.
- hh son los minutos, con un rango de 0 a 59.
- hh son los segundos, con un rango de 0 a 59.

De forma predeterminada, el valor del intervalo es de 1 hora (01:00:00).

Texto del mensaje de advertencia por adelantado

Este parámetro contiene el texto a modificar del mensaje para los usuarios, donde se les notifica que va a haber actualizaciones de software o un periodo de mantenimiento para lo cual necesitan cerrar sesión.

De forma predeterminada, el mensaje contiene este texto: {TIMESTAMP} Please save your work. The server will go offline for maintenance in {TIMELEFT}.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Título del mensaje de advertencia por adelantado

Este parámetro contiene el texto editable del título del mensaje de advertencia dirigido a los usuarios.

De manera predeterminada, el título es Upcoming Maintenance.

Periodo de advertencia por adelantado

Este parámetro define el tiempo de antelación con que aparecen por primera vez los mensajes de advertencia sobre el mantenimiento.

El tiempo se establece con el formato ddd.hh:mm:ss, donde:

- ddd son los días, un parámetro optativo, con un rango de 0 a 999.
- hh son las horas, con un rango de 0 a 23.
- hh son los minutos, con un rango de 0 a 59.
- hh son los segundos, con un rango de 0 a 59.

De forma predeterminada, el valor es de 16 horas (16:00:00), lo que indica que el primer mensaje de advertencia aparece aproximadamente 16 horas antes del mantenimiento.

Texto del mensaje final de cierre de sesión forzado

Este parámetro contiene el texto editable del mensaje donde se avisa a los usuarios que se ha comenzado un cierre de sesión forzoso.

De manera predeterminada, el mensaje contiene el texto siguiente: The server is currently going offline for maintenance.

Título del mensaje final de cierre de sesión forzado

Este parámetro contiene el texto editable del título del mensaje donde se avisa a los usuarios que se ha comenzado un cierre de sesión forzoso.

De manera predeterminada, el título es Notification From IT Staff.

Periodo de gracia de cierre de sesión forzado

Este parámetro define el tiempo que transcurre desde que se notifica a los usuarios que deben cerrar sesión hasta que se aplica el cierre de sesión forzoso para procesar el mantenimiento pendiente.

El tiempo se establece con el formato ddd.hh:mm:ss, donde:

- ddd son los días, un parámetro optativo, con un rango de 0 a 999.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- hh son las horas, con un rango de 0 a 23.
- hh son los minutos, con un rango de 0 a 59.
- hh son los segundos, con un rango de 0 a 59.

De manera predeterminada, el periodo de gracia para el cierre de sesión forzoso es de 5 minutos (00:05:00).

Texto del mensaje de cierre de sesión forzado

Este parámetro contiene el texto editable 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 forzoso.

De manera predeterminada, el mensaje contiene este texto: {TIMESTAMP} Please save your work and log off. The server will go offline for maintenance in {TIMELEFT}.

Título del mensaje de cierre de sesión forzado

Este parámetro contiene el texto editable del título del mensaje de advertencia sobre el cierre de sesión forzoso.

De manera predeterminada, el título es Notification From IT Staff.

Modo administrado por imagen

El servicio Connector Agent detecta automáticamente si se está ejecutando en una máquina clonada administrada por Provisioning Services o MCS. El agente bloquea las actualizaciones de Configuration Manager en clones administrados por imagen, e instala automáticamente las actualizaciones en la imagen maestra del catálogo.

Después de actualizar una imagen maestra, use Studio para orquestar el reinicio de los clones del catálogo de MCS. El servicio Connector Agent orquesta automáticamente el reinicio de los clones del catálogo de PVS durante las ventanas de mantenimiento de Configuration Manager. Si quiere anular este comportamiento para que Configuration Manager instale el software en los clones de catálogo, cambie el modo administrado por imagen a Inhabilitado.

Texto del mensaje de reinicio

Este parámetro contiene el texto editable 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Intervalo regular para ejecutar la tarea del agente

Este parámetro determina la frecuencia con la que se ejecuta la tarea del agente Citrix Connector Agent.

El tiempo se establece con el formato ddd.hh:mm:ss, donde:

- ddd son los días, un parámetro optativo, con un rango de 0 a 999.
- hh son las horas, con un rango de 0 a 23.
- hh son los minutos, con un rango de 0 a 59.
- hh son los segundos, con un rango de 0 a 59.

De forma predeterminada, el parámetro del intervalo regular es de 5 minutos (00:05:00).

Administrar

November 29, 2018

La administración de un sitio de XenDesktop o XenApp implica diversos elementos y tareas.

Licencias

Es necesaria una conexión válida al servidor de licencias de Citrix cuando se crea un sitio. Más adelante, podrá realizar varias tareas de licencias desde Studio, como agregar licencias, cambiar sus tipos o modelos, además de gestionar a los administradores de licencias. También podrá acceder a la consola License Administration Console desde Studio.

Aplicaciones

Administre aplicaciones en grupos de entrega y, opcionalmente, en grupos de aplicaciones.

Zonas

En una implementación de puntos geográficamente alejados, puede usar zonas para mantener las aplicaciones y los escritorios más cerca de los usuarios finales, lo que mejora el rendimiento. Cuando se instala y se configura un sitio, todos los Controllers, los catálogos de máquinas y las conexiones de host están en una zona principal. Posteriormente, puede usar Studio para crear zonas satélite que contengan esos elementos. Una vez que el sitio tenga más de una zona, podrá indicar en qué zona se colocarán las conexiones de host, los catálogos de máquinas recién creados o los Controllers recién agregados. También podrá mover elementos entre zonas.

Conexiones y recursos

Si usa un hipervisor o un servicio de nube para alojar máquinas que van a entregar aplicaciones y escritorios a los usuarios, cree la primera conexión a ese hipervisor o servicio de nube al crear un sitio. Los datos de almacenamiento y red que seleccione para dicha conexión forman los *recursos*

© 1999-2019 Citrix Systems, Inc. All rights reserved.

necesarios. Posteriormente, puede cambiar esa conexión y sus recursos, además de crear nuevas conexiones. También puede administrar las máquinas que usan una conexión configurada.

Caché de host local

La Caché de host local permite que la intermediación de operaciones en un sitio continúe cuando se interrumpa la conexión entre un Delivery Controller y la base de datos del sitio.

IP virtual y bucle invertido virtual

La función de dirección IP virtual de Microsoft proporciona una dirección IP exclusiva a una aplicación publicada, asignada dinámicamente para cada sesión. La función de bucle invertido virtual permite configurar aplicaciones que dependen de la comunicación con el host local (127.0.0.1 de forma predeterminada) para utilizar una dirección de bucle invertido virtual exclusiva en el rango del host local (127.*).

Delivery Controllers

Este artículo contiene procedimientos y aspectos a tener en cuenta a la hora de agregar y quitar Controllers de un sitio. Asimismo, se describe cómo mover los Controllers a otra zona o sitio, y cómo mover un VDA a otro sitio.

Registro de VDA en Controllers

Para que un VDA pueda facilitar la entrega de aplicaciones y escritorios, debe registrarse en un Controller (establecer comunicación con él). Las direcciones del Controller se pueden especificar de varias maneras, todas ellas descritas en este artículo. Es importante que los agentes VDA tengan información actualizada a medida que se agreguen, se muevan o se eliminen Controllers del sitio.

Sesiones

El mantenimiento de la actividad de las sesiones es fundamental para ofrecer la mejor experiencia de uso. Existen varias funciones que pueden optimizar la fiabilidad de sesiones, reducir los problemas, el tiempo de inactividad y la pérdida de la productividad.

- Fiabilidad de la sesión
- Reconexión automática de clientes
- ICA Keep-Alive
- Control del espacio de trabajo
- Movilidad de sesión

Usar las búsquedas en Studio

Si quiere ver información acerca de las máquinas, las sesiones, los catálogos de máquinas, las aplicaciones o los grupos de entrega en Studio, utilice la función flexible de búsqueda.

Etiquetas

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Utilice etiquetas para identificar elementos tales como máquinas, aplicaciones, grupos y directivas. A continuación, puede ajustar determinadas operaciones para aplicarlas a elementos con una etiqueta determinada.

IPv4 o IPv6

XenApp y XenDesktop 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 usa esta solución de perfiles, consulte este artículo para obtener información general; consulte la documentación de Profile Management para obtener información detallada.

Citrix Insight Services

Citrix Insight Services (CIS) es una plataforma de Citrix para instrumentación, telemetría y generación de información empresarial.

Licencias

January 22, 2019

> **Nota:**
>
> Ni Studio ni Director admiten Citrix License Server VPX. Para obtener más información acerca de Citrix License Server VPX, consulte la documentación de Citrix Licensing.

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 información sobre otras tareas relacionadas con las licencias, consulte la documentación sobre el sistema de licencias y Licencias de varios tipos.

Debe ser un administrador total de licencias para llevar a cabo las tareas que se describen a continuación, excepto para ver la información de las licencias. Para ver la información de licencias en Studio, un administrador debe tener al menos el permiso de lectura de licencias de administración delegada; los roles de administrador total y de administrador de solo lectura integrados tienen esos permisos.

La siguiente tabla ofrece una lista de las ediciones y los modelos de licencia admitidos:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Productos	Ediciones	Modelos de licencia
Citrix Virtual Apps	Premium, Advanced, Standard	Concurrente
Citrix Virtual Desktops	Premium, Advanced, Standard	Dispositivo del usuario y Concurrente

Para ver la información de licencias, seleccione **Configuración > Licencias** en el panel de navegación de Studio. Se muestra un resumen del uso de licencias y los parámetros del sitio, junto con una lista de todas las licencias instaladas actualmente en el servidor de licencias especificado.

Para descargar una licencia de Citrix:

1. Seleccione **Configuración > Licencias** en el panel de navegación de Studio.
2. Seleccione **Asignar licencias** en el panel Acciones.
3. Introduzca el código de acceso de licencia (License Access Code) suministrado por Citrix en un mensaje de correo electrónico.
4. Seleccione un producto y haga clic en **Asignar licencias**. Todas las licencias disponibles para ese producto se asignarán y se descargarán. Una vez que se asignan y se descargan todas las licencias para un código de acceso de licencia específico, no se puede volver a usar ese código. Si tiene que llevar a cabo otras transacciones con ese código, inicie sesión en My Account.

Para agregar licencias almacenadas en el equipo local o en la red:

1. Seleccione **Configuración > Licencias** en el panel de navegación de Studio.
2. Seleccione **Agregar licencias** en el panel Acciones.
3. Vaya a un archivo de licencias y agréguelo al servidor de licencias.

Para cambiar el servidor de licencias:

1. Seleccione **Configuración > Licencias** en el panel de navegación de Studio.
2. Seleccione **Cambiar servidor de licencias** en el panel Acciones.
3. Escriba la dirección del servidor de licencias en el formato nombre:puerto, donde nombre es una dirección DNS, NetBIOS o IP. Si no especifica un número de puerto, se utiliza el puerto predeterminado (27000).

Para seleccionar el tipo de licencia que se va a utilizar:

- Al configurar el sitio, después de especificar el servidor de licencias, se le solicita que seleccione el tipo de licencia que va a utilizar. Si no existen licencias en el servidor, se selecciona automáticamente la opción para utilizar el producto durante un período de prueba de 30 días sin una licencia.
- Si existen licencias en el servidor, se muestran los detalles y se puede seleccionar una de ellas. O bien puede agregar un archivo de licencia al servidor y seleccionar ese archivo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para cambiar la edición y el modelo de licencia del producto:

1. Seleccione **Configuración > Licencias** en el panel de navegación de Studio.
2. Seleccione **Modificar edición de producto** en el panel Acciones.
3. Actualice las opciones pertinentes.

Para acceder a la consola License Administration Console, en el panel Acciones, seleccione **License Administration Console**. La consola aparece inmediatamente o bien, si el panel de mandos está configurado con la protección por contraseña, se le pedirán las credenciales de la consola License Administration Console. Para obtener más información acerca de cómo usar la consola, consulte la documentación de licencias.

Para agregar un administrador de licencias:

1. Seleccione **Configuración > Licencias** en el panel de navegación de Studio.
2. Seleccione la ficha Administradores de licencias en el panel central.
3. Seleccione **Agregar administrador de licencias** en el panel Acciones.
4. Vaya al usuario que quiere agregar como administrador y elija los permisos correspondientes.

Para modificar los permisos de un administrador de licencias o eliminarlo:

1. Seleccione **Configuración > Licencias** en el panel de navegación de Studio.
2. Seleccione la ficha Administradores de licencias en el panel central y, a continuación, seleccione el administrador en cuestión.
3. Seleccione **Modificar administrador de licencias** o **Eliminar administrador de licencias** en el panel Acciones.

Para agregar un grupo de administradores de licencias:

1. Seleccione **Configuración > Licencias** en el panel de navegación de Studio.
2. Seleccione la ficha Administradores de licencias en el panel central.
3. Seleccione **Agregar grupo de administradores de licencias** en el panel Acciones.
4. Vaya al grupo de usuarios que quiere que actúen como administradores y elija los permisos correspondientes. Cuando se agrega un grupo de Active Directory se dan permisos de administrador de licencias a los usuarios de ese grupo.

Para modificar los permisos de un grupo de administradores de licencias o eliminar el grupo:

1. Seleccione **Configuración > Licencias** en el panel de navegación de Studio.
2. Seleccione la ficha Administradores de licencias en el panel central y, a continuación, seleccione el grupo de administradores en cuestión.
3. Seleccione **Modificar grupo de administradores de licencias** o **Eliminar grupo de administradores de licencias** en el panel Acciones.

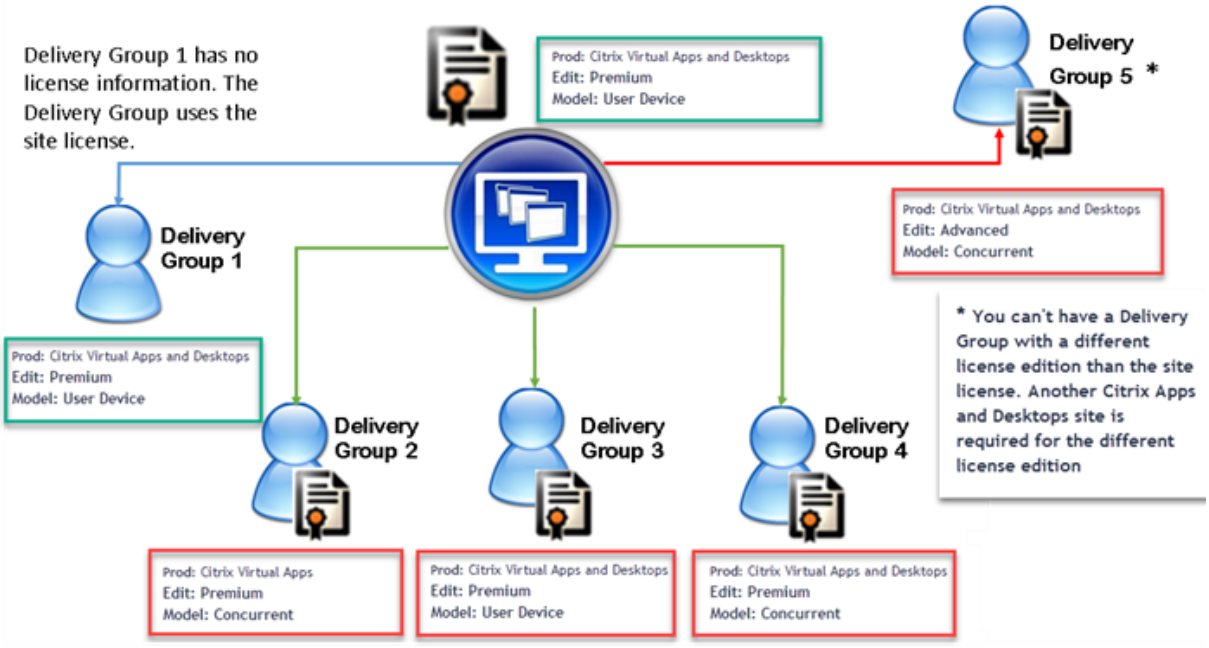
© 1999-2019 Citrix Systems, Inc. All rights reserved.

Licencias de varios tipos

March 14, 2019

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, MPS) y el modelo (UserDevice, Concurrent). Los grupos de entrega deben utilizar la edición del producto establecida para el sitio.

Si no se configura el uso de licencias de varios tipos, solo podrá utilizar tipos distintos de licencias cuando se configuren en sitios totalmente independientes. Los grupos de entrega usan la licencia del sitio.



Para determinar los grupos de entrega que consumen los distintos tipos de licencias, utilice estos cmdlets de Broker PowerShell:

- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup
- Get-BrokerDesktopGroup

Para instalar licencias, utilice:

- Citrix Studio
- Citrix Licensing Manager
- License Administration Console
- citrix.com

Las fechas de Subscription Advantage son únicas para cada archivo de licencia, producto y modelo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Los grupos de entrega que se configuren de manera diferente podrían tener diferentes fechas de Subscription Advantage entre sí.

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	Una clasificación (Concurrent o UserDevice) que especifica el modelo de licencias para el grupo.	Si está inhabilitada la activación o desactivación de la característica, 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 está inhabilitada la activación o desactivación de la característica, no se puede establecer ninguna de las propiedades.

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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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/.

Ejemplo

En este ejemplo de cmdlet de PowerShell, se representa cómo establecer varios tipos de licencias para dos grupos de entrega existentes; también se crea y se establece un tercer grupo de entrega.

Para ver el producto de licencia y el modelo de licencia asociado a un grupo de entrega, use el cmdlet de PowerShell **Get-BrokerDesktopGroup**.

1. El primer grupo de entrega se establece como XenApp y Concurrent.

   Set-BrokerDesktopGroup -Name "Delivery Group for Citrix Virtual Apps Premium Concurrent" -ProductCode MPS -LicenseModel Concurrent

2. El segundo grupo de entrega se establece como XenDesktop y Concurrent.

   Set-BrokerDesktopGroup -Name "Delivery Group for Citrix Virtual Desktops Premium Concurrent" -ProductCode XDT -LicenseModel Concurrent

3. El tercer grupo de entrega se crea y se establece como XenDesktop y UserDevice.

   New-BrokerDesktopGroup -Name "Delivery Group for Citrix Virtual Desktops Premium UserDevice" -PublishedName "MyDesktop" -DesktopKind Private -ProductCode XDT -LicenseModel UserDevice

Consideraciones especiales

Las licencias de varios tipos presentan una funcionalidad distinta de las licencias habituales de Citrix Virtual Apps and Desktops.

No hay alertas ni notificaciones de Director o Studio:

- 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.

Aplicaciones

March 8, 2019

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Introducción

Si su implementación usa solo grupos de entrega (y no grupos de aplicaciones), tiene que agregar aplicaciones a los grupos de entrega. Si también tiene grupos de aplicaciones, por lo general, debe agregar aplicaciones a los grupos de aplicaciones. Esta recomendación facilita la administración. Una aplicación siempre debe pertenecer al menos a un grupo de entrega o un grupo de aplicaciones.

En el asistente para agregar aplicaciones, seleccione uno o varios grupos de entrega, o uno o más grupos de aplicaciones, pero no ambos. Aunque puede cambiar posteriormente la asociación de una aplicación a un grupo (por ejemplo, puede mover la aplicación desde un grupo de aplicaciones a un grupo de entrega), se recomienda no hacerlo para no incrementar la complejidad. Mantenga sus aplicaciones en un tipo de grupo.

Al asociar una aplicación a más de un grupo de entrega o más de un grupo de aplicaciones, puede producirse un problema de visibilidad si no dispone de permisos suficientes para ver la aplicación en todos esos grupos. En tales casos, consulte a un administrador con más permisos o amplíe haga que amplíen su ámbito para incluir todos los grupos a los que se haya agregado la aplicación.

Si publica dos aplicaciones con el mismo nombre (quizá desde distintos grupos) para los mismos usuarios, cambie la propiedad Nombre de la aplicación (para el usuario) en Studio; de lo contrario, los usuarios verán nombres duplicados en la aplicación Citrix Workspace.

Puede cambiar las propiedades de una aplicación (parámetros) al agregarla, o más tarde. También puede cambiar la carpeta de la aplicación donde está colocada la aplicación, ya sea al agregarla, o más tarde.

Para obtener más detalles, consulte:

- Crear grupos de entrega
- Crear grupos de aplicaciones
- Etiquetas

Agregar aplicaciones

Puede agregar aplicaciones al crear un grupo de entrega o un grupo de aplicaciones; los procedimientos correspondientes se describen en los artículos Creación de grupos de entrega y Creación de grupos de aplicaciones. El procedimiento siguiente describe cómo agregar aplicaciones después de crear un grupo.

Conviene tener en cuenta lo siguiente:

- No se pueden agregar aplicaciones a grupos de entrega de acceso con Remote PC.
- El asistente para agregar aplicaciones no puede usarse para quitar aplicaciones de los grupos de entrega o de los grupos de aplicaciones. Se trata de dos operaciones diferentes.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para agregar una o varias aplicaciones:

1. Seleccione **Aplicaciones** en el panel de navegación de Studio y, a continuación, seleccione **Agregar aplicaciones** en el panel Acciones.
2. El asistente para agregar aplicaciones se inicia con la página **Introducción**, que se puede eliminar de futuros inicios de este asistente.
3. El asistente le guiará a través de las páginas Grupos, Aplicaciones y Resumen, que se describen a continuación. Cuando haya terminado con cada página, haga clic en **Siguiente** para ir a la página final.

Como alternativa al paso 1 si quiere agregar aplicaciones a un grupo de entrega o un grupo de aplicaciones:

- Para agregar aplicaciones a un solo grupo de entrega, en el paso 1, seleccione **Grupos de entrega** en el panel de navegación de Studio y, a continuación, seleccione un grupo de entrega en el panel central y, a continuación, seleccione **Agregar aplicaciones** en el panel Acciones. El asistente no mostrará la página **Grupos**.
- Para agregar aplicaciones a un solo grupo de aplicaciones, en el paso 1, seleccione **Aplicaciones** en el panel de navegación de Studio y, a continuación, seleccione un **Grupo de aplicaciones** en el panel central y, a continuación, seleccione la entrada **Agregar aplicaciones** bajo el nombre del grupo de aplicaciones en el panel Acciones. El asistente no mostrará la página **Grupos**.

Grupos

Esta página contiene una lista de todos los grupos de entrega en el sitio. Si también se han creado grupos de aplicaciones, la página muestra la lista de grupos de aplicaciones y grupos de entrega. Puede elegir de cada grupo, pero no de ambos grupos. En otras palabras, no se pueden agregar aplicaciones a un grupo de aplicaciones y a un grupo de entrega a la vez. Por lo general, si está usando grupos de aplicaciones, las aplicaciones deben agregarse a grupos de aplicaciones en lugar de grupos de entrega.

Al agregar una aplicación, se debe marcar la casilla de verificación junto a un grupo de entrega o un grupo de aplicaciones (si están disponibles) como mínimo, porque cada aplicación siempre debe estar asociada con, al menos, un grupo.

Aplicaciones

Haga clic en la lista desplegable **Agregar** para ver los orígenes de aplicación.

- **Desde el menú Inicio:** Se trata de las aplicaciones que se detectan en una máquina de los grupos de entrega seleccionados. Cuando se selecciona este origen, se abre una nueva página con una lista de aplicaciones detectadas. Marque las casillas de las aplicaciones que quiere agregar y, a continuación, haga clic en Aceptar.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Este origen no se puede seleccionar si usted (1) seleccionó grupos de aplicaciones que no tienen grupos de entrega asociados, (2) seleccionó grupos de aplicaciones con grupos de entrega asociados que no contienen máquinas, o (3) seleccionó un grupo de entrega que no contiene máquinas.

- **Definidas manualmente**: Se trata de las aplicaciones que se encuentran en el sitio o en la red. Cuando se selecciona este origen, se abre una nueva página donde se escribe la ruta al archivo ejecutable, al directorio de trabajo, los argumentos de línea de comandos opcionales y los nombres simplificados para administradores y usuarios. Después de introducir la información, haga clic en Aceptar.
- **Existentes:** Se trata de aplicaciones agregadas anteriormente al sitio. Cuando se selecciona este origen, se abre una nueva página con una lista de aplicaciones detectadas. Marque las casillas de 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 App-V o la biblioteca de aplicaciones. En la vista resultante, marque las casillas de las aplicaciones que quiere agregar y, a continuación, haga clic en Aceptar. Para obtener más información, consulte el artículo App-V.

  Este origen no se puede seleccionar si App-V no está configurado en el sitio.
- **Grupo de aplicaciones:** Grupos de aplicaciones. Cuando se selecciona este origen, se abre una nueva página con una lista de Grupos de aplicaciones. (Aunque la pantalla también lista las aplicaciones de cada grupo, solo se puede seleccionar el grupo, no las aplicaciones individualmente). Se agregarán las aplicaciones actuales del grupo y las que se agreguen a él en el futuro. Marque las casillas de 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 respaldan el uso de grupos de aplicaciones (por ejemplo, los grupos de entrega contienen máquinas de asignación estática).

Como se indica en la tabla, algunas de las entradas de la lista desplegable Agregar no se pueden seleccionar si no existe ningún origen válido de ese tipo. Los orígenes que no son compatibles (por ejemplo, no se puede agregar grupos de aplicaciones a otros grupos de aplicaciones) no se incluyen en la lista desplegable. Las aplicaciones que ya se han agregado a los grupos que eligió no se podrán seleccionar de nuevo.

Para agregar una aplicación desde un AppDisk asignado, seleccione **Desde el menú Inicio**. Si la aplicación no está disponible allí, seleccione **Definidas manualmente** y facilite los datos pertinentes. Si se produce un error de acceso a la carpeta, configúrela como “compartida” y vuelva a agregar la aplicación a través de la opción **Definidas manualmente**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Puede cambiar las propiedades de una aplicación (parámetros) en esta página, o más tarde.

De forma predeterminada, las aplicaciones que agregue se colocan en una carpeta denominada Aplicaciones. Puede cambiar la aplicación desde esta página, o más tarde. Si intenta agregar una aplicación y ya existe una con el mismo nombre en la misma carpeta, se le pedirá cambiar el nombre de la aplicación que está agregando. Puede aceptar el nuevo nombre sugerido, o rechazarlo y darle otro nombre, o seleccionar una carpeta diferente. Por ejemplo, si "app" ya existe en la carpeta Aplicaciones y usted intenta agregar otra aplicación denominada también "app" a esa carpeta, se le sugerirá el nombre "app_1".

Resumen

Si agrega como máximo 10 aplicaciones, sus nombres aparecerán en la lista **Aplicaciones para agregar**. Si agrega más de 10 aplicaciones, se indica la cantidad total.

Revise la información de resumen y, a continuación, haga clic en **Finalizar**.

Cambiar la asociación de una aplicación a un grupo

Después de agregar una aplicación, puede cambiar los grupos de entrega y los grupos de aplicaciones con los que la aplicación está asociada.

Puede arrastrar y colocar para asociar una aplicación con un grupo adicional. Esta es una alternativa al uso de comandos en el panel Acciones.

Si una aplicación está asociada a más de un grupo de entrega o más de un grupo de aplicaciones, se puede usar la prioridad de grupos para especificar el orden en que se comprueban los grupos para encontrar las aplicaciones. De forma predeterminada, todos los grupos tienen prioridad 0 (la máxima prioridad). Si los grupos tienen la misma prioridad, se les aplica el equilibrio de carga.

Una aplicación se puede asociar con grupos de entrega que contengan máquinas compartidas (no privadas) que puedan entregar aplicaciones. También puede seleccionar grupos de entrega con máquinas compartidas que entreguen solo escritorios si 1) el grupo de entrega contiene máquinas compartidas y se creó con una versión de XenDesktop 7.x anterior a 7.9 y 2) usted tiene el permiso Modificar grupo de entrega. El tipo de grupo de entrega se convierte automáticamente a "escritorios y aplicaciones" cuando se confirma la selección en el diálogo de propiedades.

1. Seleccione **Aplicaciones** en el panel de navegación de Studio y, a continuación, seleccione la aplicación en el panel central.
2. Seleccione **Propiedades** en el panel Acciones.
3. Seleccione la página **Grupos**.
4. Para agregar un grupo, haga clic en la lista desplegable **Agregar** y seleccione **Grupos de aplicaciones** o **Grupos de entrega**. (Si aún no ha creado ningún grupo de aplicaciones, la única

© 1999-2019 Citrix Systems, Inc. All rights reserved.

entrada que verá será Grupos de entrega.) A continuación, seleccione uno o varios grupos disponibles. Los grupos que no son compatibles con la aplicación, o que ya están asociados con ella, no se pueden seleccionar.

5. Para quitar un grupo, seleccione uno o varios grupos y, a continuación, haga clic en **Quitar**. Si al quitar la asociación de grupo la aplicación ya no estará asociada a ningún grupo de aplicaciones o grupo de entrega, se le alertará de que la aplicación será eliminada.
6. Para cambiar la prioridad de un grupo, seleccione el grupo y, a continuación, haga clic en **Modificar prioridad**. Seleccione un valor de prioridad y, a continuación, haga clic en **Aceptar**.
7. Cuando haya terminado, haga clic en **Aplicar** para aplicar los cambios y dejar abierta la ventana, o haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

Duplicar, habilitar o inhabilitar, cambiar de nombre o eliminar una aplicación

Las siguientes acciones están disponibles:

- **Duplicar:** Puede que necesite duplicar una aplicación para crear otra versión de esta con parámetros o propiedades diferentes. Cuando se duplica una aplicación, se le cambia el nombre de manera automática con un sufijo único y se coloca junto a la original. También puede que le convenga duplicar una aplicación para agregarla a un grupo distinto. (Después de la duplicación, el modo más sencillo de mover una aplicación es arrastrarla y colocarla en otro grupo.)
- **Habilitar o inhabilitar:** La habilitación o inhabilitación de una aplicación son acciones diferentes de habilitar o inhabilitar un grupo de entrega o un grupo de aplicaciones.
- **Cambio de nombre:** Solo se puede cambiar el nombre de una aplicación a la vez. Si intenta agregar una aplicación y ya existe una con el mismo nombre en la misma carpeta o el mismo grupo, se le pedirá que especifique un nombre diferente.
- **Eliminar**: Al eliminar una aplicación, se la quita de los grupos de aplicaciones o grupos de entrega con los que estaba asociada, pero no del origen que se utilizó para agregarla originalmente. Eliminar una aplicación es una acción diferente de quitarla de un grupo de entrega o un grupo de aplicaciones.

Para duplicar, habilitar, inhabilitar, cambiar de nombre o eliminar una aplicación:

1. Seleccione **Aplicaciones** en el panel de navegación de Studio.
2. Seleccione una o más aplicaciones en el panel central y, a continuación, seleccione la tarea correspondiente en el panel Acciones.
3. Confirme la acción, cuando se le solicite.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Quitar aplicaciones de un grupo de entrega

La aplicación debe estar asociada (pertenecer) a al menos un grupo de entrega o un grupo de aplicaciones. Si intenta quitar una aplicación de un grupo de entrega y con ello la aplicación ya no estaría asociada con ningún grupo de entrega o grupo de aplicaciones, se le notificará que la aplicación será eliminada si decide continuar. En estos casos, si quiere poder entregar la aplicación, debe volver a agregarla desde un origen válido.

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo de entrega. En el panel inferior central, seleccione la ficha **Aplicaciones** y, a continuación, la aplicación que quiere quitar.
3. Seleccione **Quitar aplicación** en el panel Acciones.
4. Confirme la eliminación.

Quitar aplicaciones de un grupo de aplicaciones

Una aplicación debe pertenecer al menos a un grupo de entrega o a un grupo de aplicaciones. Si intenta quitar una aplicación de un grupo de aplicaciones y con ello la aplicación ya no pertenecería a ningún grupo de entrega o grupo de aplicaciones, se le notificará que la aplicación será eliminada si decide continuar. En estos casos, si quiere poder entregar la aplicación, debe volver a agregarla desde un origen válido.

1. Seleccione **Aplicaciones** en el panel de navegación de Studio.
2. Seleccione el grupo de aplicaciones en el panel central y, a continuación, seleccione una o más aplicaciones en el panel central.
3. Seleccione **Quitar del grupo de aplicaciones** en el panel Acciones.
4. Confirme la eliminación.

Cambiar las propiedades de la aplicación

Solo se pueden cambiar las propiedades de una aplicación a la vez.

Para cambiar las propiedades de una aplicación:

1. Seleccione **Aplicaciones** en el panel de navegación de Studio.
2. Seleccione una aplicación y, a continuación, seleccione **Modificar propiedades de aplicación** en el panel Acciones.
3. Seleccione la página que contiene la propiedad que quiere cambiar.
4. Cuando haya terminado, haga clic en **Aplicar** para aplicar los cambios que haya realizado y dejar la ventana abierta, o bien haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

En la siguiente lista, la página se indica entre paréntesis.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Propiedad	Página
Categoría/carpeta donde aparece la aplicación en la aplicación Citrix Workspace	Entrega
Argumentos de línea de comandos; consulte Transferir parámetros a aplicaciones publicadas	Ubicación
Grupos de entrega y grupos de aplicaciones donde la aplicación está disponible	Grupos
Descripción	Identificación
Extensiones de archivo y asociación de tipos de archivo: qué extensiones abre automáticamente la aplicación	Asociación de tipos de archivos
Icono	Entrega
Palabras clave para StoreFront	Identificación
Límites: consulte Configurar límites para aplicaciones	Entrega
Nombre: los nombres que ven el usuario y el administrador	Identificación
Ruta al archivo ejecutable; consulte Transferir parámetros a aplicaciones publicadas	Ubicación
Acceso directo en el escritorio de usuario: habilitarlo o inhabilitarlo	Entrega
Visibilidad: limita qué usuarios pueden ver la aplicación en la aplicación Citrix Workspace (aunque una aplicación sea invisible, se la puede iniciar; para que además de no estar visible, tampoco esté disponible, agréguela a otro grupo)	Limitar visibilidad
Directorio de trabajo	Ubicación

Es posible que los cambios en las aplicaciones no se efectúen de cara a los usuarios actuales de las aplicaciones hasta que cierren sus sesiones.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurar límites para aplicaciones

Configurar límites para aplicaciones puede ayudarle a administrar el uso de esas aplicaciones. Por ejemplo, puede usar límites para aplicaciones si quiere controlar la cantidad de usuarios que acceden a una aplicación de forma simultánea. Del mismo modo, los límites para aplicaciones se pueden usar con el fin de controlar la cantidad de instancias simultáneas de aplicaciones que consumen muchos recursos, lo que puede ayudar a mantener el rendimiento del servidor y evitar el deterioro del servicio.

Esta función limita la cantidad de inicios de aplicaciones que usan como intermediario el Controller (por ejemplo, desde la aplicación Citrix Workspace y StoreFront), no la cantidad de aplicaciones en ejecución que se inician mediante otros métodos. Esto significa que los límites para aplicaciones ayudan a los administradores a la hora de administrar el uso simultáneo, pero no se aplican en todos los casos. Por ejemplo, no se pueden aplicar límites para aplicaciones cuando el Controller está en modo de conexión por concesión.

De forma predeterminada, no hay ningún límite en la cantidad de instancias de aplicación que pueden ejecutarse al mismo tiempo. Existen varias configuraciones de límite para las aplicaciones. Puede definir una o todas:

- La cantidad máxima de instancias simultáneas de una aplicación que hayan iniciado todos los usuarios del grupo de entrega.
- Una instancia de aplicación por usuario en el grupo de entrega.
- La cantidad máxima de instancias simultáneas de una aplicación por cada máquina (solo PowerShell).

Si se define un límite, se generará un mensaje de error cuando un usuario intente iniciar una aplicación más veces que el número del límite configurado. Si se configura más de un límite, se informa un error cuando se alcanza el primer límite.

Ejemplos de uso de los límites para aplicaciones:

- **Límite para la cantidad máxima de instancias simultáneas:** En un grupo de entrega, se configura la cantidad máxima de 15 instancias simultáneas de la aplicación Alfa. Posteriormente, los usuarios de ese grupo de entrega tienen 15 instancias de esa aplicación que se ejecutan al mismo tiempo. Si un usuario de ese grupo de entrega intenta iniciar Alfa, se generará un mensaje de error y Alfa no se iniciará porque eso superaría el límite de instancias simultáneas de aplicación (15).
- **Límite para una instancia de aplicación por usuario:** En otro grupo de entrega, se habilita la opción de una instancia por usuario para la aplicación Beta. El usuario Marcos inicia correctamente la aplicación Beta. Más tarde en la misma jornada, mientras esa aplicación se sigue ejecutando en la sesión de Marcos, este intenta iniciar otra instancia de Beta. Se generará un mensaje de error y Beta no se iniciará porque eso superaría el límite de una instancia por usuario.
- **Límites de cantidad máxima de instancias simultáneas y una instancia de aplicación**

© 1999-2019 Citrix Systems, Inc. All rights reserved.

por usuario: En otro grupo de entrega, se configura una cantidad máxima de 10 instancias simultáneas y se habilita la opción de una instancia por usuario de la aplicación Delta. Posteriormente, cuando diez usuarios de ese grupo de entrega tienen cada uno una instancia de Delta en ejecución, si otro usuario de ese grupo intenta iniciar Delta, recibirá un mensaje de error y Delta no se iniciará. Si alguno de los diez usuarios actuales intenta iniciar una segunda instancia de esa aplicación, recibirá un mensaje de error y la segunda instancia no se iniciará.

- **Cantidad máxima de instancias simultáneas por máquina y con restricciones de etiqueta:** La aplicación A tiene requisitos de licencia y rendimiento que estipulan cuántas instancias se pueden ejecutar al mismo tiempo en un servidor específico, así como cuántas instancias pueden ejecutarse simultáneamente en todos los servidores del sitio.

  El límite de instancias de aplicación por máquina afecta a todos los servidores del sitio (no solo a las máquinas en un grupo de entrega en particular). Supongamos que su sitio contiene tres servidores. Para la aplicación A, se configura el límite de 2 instancias de aplicación por máquina. Por lo tanto, no se permitirá el inicio de más de seis instancias de aplicación en todo el sitio. (Este es el límite de dos instancias de A en cada uno de los tres servidores.)

  Para restringir el uso de una aplicación a solo ciertas máquinas dentro de un grupo de entrega (además de limitar las instancias en todas las máquinas en todo el sitio), use la función de etiquetado para esas máquinas y configure el límite de cantidad máxima de instancias por máquina para esa aplicación.

Si también se inician instancias de aplicación sin Controller como broker (por ejemplo, durante la interrupción de servicios de un Controller) y se superan los límites configurados, los usuarios no podrán iniciar más instancias hasta que cierren las instancias necesarias para dejar de superar el límite. No se forzará el cierre de las instancias que superen el límite, sino que se seguirán ejecutando hasta que el usuario las cierre.

Si inhabilita la movilidad de sesión, inhabilite también el límite de una instancia de aplicación por usuario. Si habilita el límite de una instancia de aplicación por usuario, no configure uno de los dos valores que permiten sesiones nuevas en dispositivos nuevos. Para obtener información acerca de la movilidad, consulte el artículo Sesiones.

Para configurar el límite de instancias máximas por grupo de entrega y el límite de una instancia por usuario:

1. Seleccione **Aplicaciones** en el panel de navegación de Studio y, a continuación, seleccione una aplicación.
2. Seleccione **Modificar propiedades de aplicación** en el panel Acciones.
3. En la página **Entrega**, seleccione una de las siguientes opciones.
   - Puede permitir el uso ilimitado de la aplicación. No hay límite para la cantidad de instancias ejecutadas a la vez. Ésta es la opción predeterminada.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Puede establecer límites para la aplicación. Hay dos tipos de límite; especifique uno o ambos.
  - Especifique la cantidad máxima de instancias que pueden ejecutarse simultáneamente.
  - Ponga el límite de una instancia de aplicación por usuario.

4. Haga clic en **Aceptar** para aplicar el cambio y cierre el cuadro de diálogo, o pinche en **Aplicar** para aplicar el cambio y deje abierto el cuadro de diálogo.

Para configurar el límite de instancias máximas por máquina (solo PowerShell):

- En PowerShell (utilizando Remote PowerShell SDK para implementaciones de Citrix Cloud o PowerShell SDK para implementaciones locales), indique el cmdlet BrokerApplication apropiado con el parámetro MaxPerMachineInstances.
- Para obtener ayuda, use el cmdlet Get-Help. Por ejemplo:

```
Get-Help Set-BrokerApplication -Parameter MaxPerMachineInstances
```

Transferir parámetros a aplicaciones publicadas

Utilice la página **Ubicación** de las propiedades de la aplicación para introducir la línea de comandos y transferir los parámetros a las aplicaciones publicadas.

Al asociar una aplicación publicada con tipos de archivos, los símbolos "%*" (porcentaje y asterisco entre comillas) se agregan al final de la línea de comandos de la aplicación. Estos símbolos actúan como marcadores de posición para los parámetros transferidos a los dispositivos de usuario.

Si una aplicación publicada no se inicia cuando se espera, verifique que la línea de comandos contiene los símbolos correctos. De forma predeterminada, los parámetros proporcionados por los dispositivos de usuario se validan si se agregan los símbolos "%*". Para las aplicaciones publicadas que utilizan parámetros personalizados suministrados por el dispositivo de usuario, se agregan los símbolos "%**" a la línea de comandos para omitir la validación de la línea de comandos. Si los símbolos no aparecen en la línea de comandos de la aplicación, agréguelos manualmente.

Si la ruta del archivo ejecutable contiene nombres de directorios con espacios (como "C:\Archivos de programa"), 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"  "%*"
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Administrar carpetas de aplicaciones

De forma predeterminada, las aplicaciones nuevas que se agreguen a los grupos de entrega se colocan en una carpeta denominada **Aplicaciones**. Puede indicar una carpeta distinta cuando cree el grupo de entrega, cuando agregue una aplicación o más tarde.

Conviene tener en cuenta lo siguiente:

- No se puede eliminar o cambiar el nombre a la carpeta Aplicaciones, pero puede mover todas las aplicaciones que contiene a otras carpetas que cree.
- El nombre de las carpetas puede contener entre 1 y 64 caracteres. Se permiten los espacios en blanco.
- Las carpetas se pueden anidar en hasta cinco niveles.
- Las carpetas no tienen que contener aplicaciones: pueden ser carpetas vacías.
- En Studio, las carpetas se incluyen en una lista alfabética a menos que las mueva o especifique otra ubicación al crearlas.
- Puede tener más de una carpeta con el mismo nombre, siempre y cuando cada una tenga otra carpeta principal. Del mismo modo, puede tener más de una aplicación con el mismo nombre, siempre y cuando cada una esté en una carpeta diferente.
- Para poder ver las aplicaciones en las carpetas, debe tener el permiso de Ver aplicaciones. Para quitar, cambiar el nombre o eliminar una carpeta que contenga aplicaciones, debe tener el permiso de Modificar propiedades de aplicación para todas las aplicaciones que contenga dicha carpeta.
- La mayoría de los procedimientos siguientes requieren acciones mediante el panel Acciones de Studio. También puede utilizar los menús contextuales o arrastrar y colocar. Por ejemplo, si crea o mueve por error una carpeta a una ubicación, la puede arrastrar y colocar en la ubicación correcta.

Para administrar las carpetas de aplicaciones, seleccione **Aplicaciones** en el panel de navegación de Studio. Utilice la siguiente lista como guía.

- **Para ver todas las carpetas (también las anidadas):** haga clic en **Mostrar todo**, situado sobre la lista de carpetas.
- **Para crear una carpeta en el nivel más alto (no anidada):** seleccione la carpeta Aplicaciones. Para colocar la nueva carpeta en una carpeta existente distinta de Aplicaciones, seleccione esa carpeta. A continuación, seleccione **Crear carpeta** en el panel Acciones. Escriba un nombre.
- **Para cambiar una carpeta:** Seleccione esa carpeta y, a continuación, seleccione **Mover carpeta** en el panel Acciones. Solo puede mover una carpeta a la vez, a menos que la carpeta que quiere mover contenga carpetas anidadas. (La forma más fácil de mover una carpeta es arrastrarla y colocarla en el sitio correspondiente.)
- **Para cambiar el nombre de una carpeta:** Seleccione esa carpeta y, a continuación, seleccione **Cambiar nombre de carpeta** en el panel Acciones. Escriba un nombre.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Para eliminar una carpeta:** seleccione esa carpeta y, a continuación, seleccione **Eliminar carpeta** en el panel Acciones. Si elimina una carpeta que contiene aplicaciones y otras carpetas, esos objetos también se eliminarán. Cuando se elimina una aplicación, se quita la asignación de la misma del grupo de entrega; no se quita la aplicación de la máquina.
- **Para mover aplicaciones a una carpeta:** Seleccione una o varias aplicaciones. A continuación, seleccione **Mover aplicación** en el panel Acciones. Seleccione la carpeta.

También puede colocar las aplicaciones en una carpeta específica (incluso una nueva) en la página **Aplicación** de los asistentes Crear grupo de entrega y Crear grupo de aplicaciones. De forma predeterminada, las aplicaciones agregadas se colocan en la carpeta **Aplicaciones**, haga clic en **Cambiar** para seleccionar o crear una carpeta.

Controlar el inicio local de aplicaciones en escritorios publicados

Cuando los usuarios inician una aplicación publicada desde un escritorio publicado, puede controlar si la aplicación se inicia en esa sesión de escritorio o como una aplicación publicada en el mismo grupo de entrega. De forma predeterminada, se inicia la aplicación en la sesión de escritorio publicado. En PowerShell (utilizando Remote PowerShell SDK en implementaciones de Citrix Cloud o PowerShell SDK en implementaciones locales), puede cambiar esta acción.

En el cmdlet New-Broker Application o Set-BrokerApplication, use 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 esta 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:

- Esta opción solo se aplica a los escritorios y las aplicaciones publicados en el mismo grupo de entrega.
- El valor ApplicationType de la aplicación debe ser HostedOnDesktop.
- Esta opción solo está disponible a través del SDK de PowerShell apropiado. Actualmente no está disponible en la interfaz gráfica de Studio.
- Esta opción requiere, como mínimo: StoreFront 3.14, Citrix Receiver para Windows 4.11 y Delivery Controller 7.17.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Aplicaciones de la Plataforma universal de Windows

January 29, 2019

Citrix Virtual Apps and Desktops admiten aplicaciones de la Plataforma universal de Windows (UWP) con agentes VDA en máquinas Windows 10 y Windows Server 2016. Para obtener más información acerca de las aplicaciones para UWP, consulte la siguiente documentación de Microsoft:

- ¿Qué es una aplicación para la Plataforma universal de Windows (UWP)? (En inglés)
- Distribuir aplicaciones sin conexión
- Guía de aplicaciones para la Plataforma universal de Windows (UWP)

En este artículo, se utiliza el término “aplicación universal” para referirse a aplicaciones de la Plataforma universal de Windows.

Requisitos y limitaciones

Las aplicaciones universales se respaldan en agentes VDA de máquinas Windows 10 y Windows Server 2016.

Los VDA deben ser como mínimo de la versión 7.11.

Las siguientes funciones de Citrix Virtual Apps and Desktops no reciben respaldo o reciben un respaldo limitado cuando se usan aplicaciones universales:

- La asociación de tipo de archivo no está respaldada.
- La función Acceso a aplicaciones locales no está respaldada.
- 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 respaldan en aplicaciones universales.
- Comunicación remota con el centro de actividades. Las aplicaciones universales pueden usar el Centro de actividades para mostrar mensajes en la sesión. Redirija esos mensajes al dispositivo del punto final para mostrarlos al usuario.

Iniciar aplicaciones universales junto con aplicaciones no universales desde el mismo servidor no está respaldado para agentes VDA de Windows 10. Para Windows Server 2016, las aplicaciones universales y las no universales deben estar en grupos de entrega o grupos de aplicaciones diferentes.

Se enumeran todas las aplicaciones universales instaladas en la máquina; por lo tanto, Citrix recomienda inhabilitar el acceso de los usuarios a la Tienda Windows. Eso impide que un usuario acceda a unas aplicaciones universales que haya instalado otro usuario.

Durante la instalación de prueba, la aplicación universal se instala en la máquina y empieza a estar disponible para otros usuarios. Cuando algún otro usuario inicia la aplicación, esta se instala. A con-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

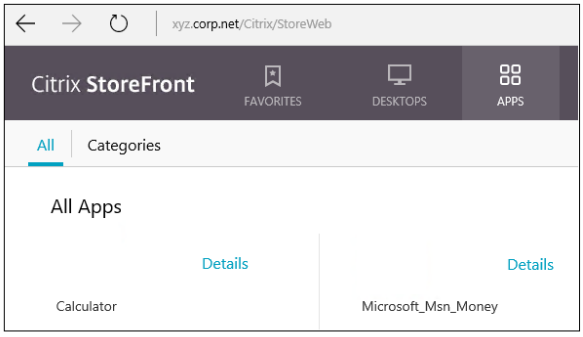
tinuación, el sistema operativo actualiza su base de datos de AppX para indicar la aplicación “como instalada” al usuario que la haya iniciado.

Cerrar correctamente una aplicación universal publicada que se haya iniciado en una ventana integrada o fija podría provocar que la sesión no se cierre y, en cambio, se cierre la sesión del usuario. En tales casos, varios procesos restantes en la sesión impiden que la sesión se cierre correctamente. Para resolver este problema, puede determinar cuál es el proceso que impide el cierre de sesión y agregarlo al valor de la clave de Registro “LogoffCheckSysModules” según las instrucciones proporcionadas en CTX891671.

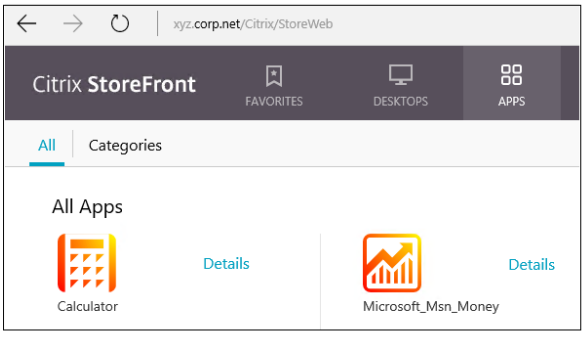
Es posible que los nombres principales y las descripciones de las aplicaciones universales no sean correctos. Modifique y corrija esas propiedades al agregar las aplicaciones a un grupo de entrega.

Consulte Problemas conocidos para resolver problemas adicionales.

Actualmente, algunas aplicaciones universales tienen iconos blancos con transparencia habilitada, lo que vuelve al icono invisible en el fondo de pantalla blanco de StoreFront. Para evitar este problema, se puede cambiar el fondo. Por ejemplo, en la máquina de StoreFront, modifique el archivo C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css. Al final del archivo, agregue `.storeapp-icon { background-image: radial-gradient( circle at top right, yellow, red ); }` . En el gráfico siguiente, se muestra un antes y un después de este ejemplo.



Before



After

En Windows Server 2016, es posible que el Administrador del servidor también se inicie cuando se inicie una aplicación de 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 más información, consulte https://blogs.technet.microsoft.com/rmilne/2014/05/30/how-to-hide-server-manager-at-logon/.

Instalar y publicar aplicaciones universales

El respaldo para las aplicaciones universales está habilitado de forma predeterminada.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para inhabilitar el uso de aplicaciones universales en un VDA, agregue el parámetro de Registro **EnableUWASeamlessSupport** a HKLM\Software\Citrix\VirtualDesktopAgent\FeatureToggle y establézcalo en **0**.

Para instalar una o más aplicaciones universales 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 https://technet.microsoft.com/en-us/itpro/windows/manage/distribute-offline-apps.
- Realice una instalación de prueba de las aplicaciones. Para obtener más información, consulte https://technet.microsoft.com/en-us/itpro/windows/deploy/sideload-apps-in-windows-10.

Para agregar (publicar) una o varias aplicaciones universales en Citrix Virtual Apps o Citrix Virtual Desktops:

1. Una vez que las aplicaciones universales estén instaladas en la máquina, agréguelas a un grupo de entrega o 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 universales que quiera publicar.
3. Continúe con el asistente o cierre el cuadro de diálogo de edición.

Desinstalar aplicaciones universales

Cuando desinstale una aplicación universal con un comando como `Remove-AppXPackage`, el elemento se desinstala solo para los administradores. Para quitar la aplicación de las máquinas de los usuarios que puedan haberlas iniciado y utilizado, debe ejecutar el comando de eliminación en cada máquina. No puede desinstalar el paquete AppX de todas las máquinas de los usuarios con un comando.

Zonas

December 4, 2018

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:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Implementar varios sitios, cada uno con su propia base de datos SQL Server del sitio.

  Se recomienda esta opción para implementaciones de empresa de gran tamaño. Se trata de varios sitios que se administran por separado, y cada uno necesita su propia base de datos SQL Server del sitio. Cada sitio es una implementación independiente de Citrix Virtual Apps.

- Configurar varias zonas en un único sitio.

  Configurar zonas puede ayudar a los usuarios de regiones remotas a conectarse a recursos sin que las conexiones recorran necesariamente grandes segmentos de red WAN. Utilizar zonas permite una administración efectiva de sitios desde una única consola de Citrix Studio, Citrix Director y la base de datos del sitio. Esto disminuye los costes de implementación, personal, licencias y operación de otros sitios que contienen bases de datos separadas en ubicaciones remotas.

  Las zonas pueden resultar útiles en implementaciones de todos los tamaños. Puede usar zonas para mantener las aplicaciones y los escritorios más cerca de los usuarios finales, lo que mejora el rendimiento. Una zona puede tener uno o varios Controllers instalados localmente por redundancia y resistencia, pero no es necesario.

  La cantidad de Controllers configurados en el sitio puede afectar al rendimiento de algunas operaciones, como agregar nuevos Controllers al sitio mismo. Para evitar este problema, se recomienda limitar la cantidad a no más de 50 zonas en su sitio de Citrix Virtual Apps o Citrix Virtual Desktops.

  Si la latencia de red de las zonas es superior a 250 milisegundos RTT, se recomienda implementar varios sitios en lugar de varias zonas.

En este artículo, el término “local” se refiere a la zona que se analiza. Por ejemplo, “un VDA se registra en el Controller local” significa que el VDA se registra en un Controller de la zona donde está situado el VDA.

Las zonas de esta versión son similares (pero no idénticas) a las zonas de XenApp 6.5 o versiones anteriores. Por ejemplo, en esta implementación de zonas, no hay recopiladores de datos. Todos los Controllers de un sitio se comunican con una base de datos del sitio situada en la zona principal. Además, la conmutación por error y las zonas favoritas funcionan de otra forma en esta versión.

Tipos de zona

Un sitio siempre tiene una zona principal. También puede tener una o varias zonas satélite. Las zonas satélite se pueden usar para: recuperación ante desastres, centros de datos geográficamente alejados, sucursales, una nube o la zona de disponibilidad de una nube.

Zona principal:

La zona principal tiene el nombre predeterminado “Principal” y contiene la base de datos SQL Server del sitio (y servidores SQL de alta disponibilidad, si los hay), Studio, Director, Citrix StoreFront, el

© 1999-2019 Citrix Systems, Inc. All rights reserved.

servidor de licencias Citrix y Citrix Gateway. La base de datos del sitio debe estar siempre en la zona principal.

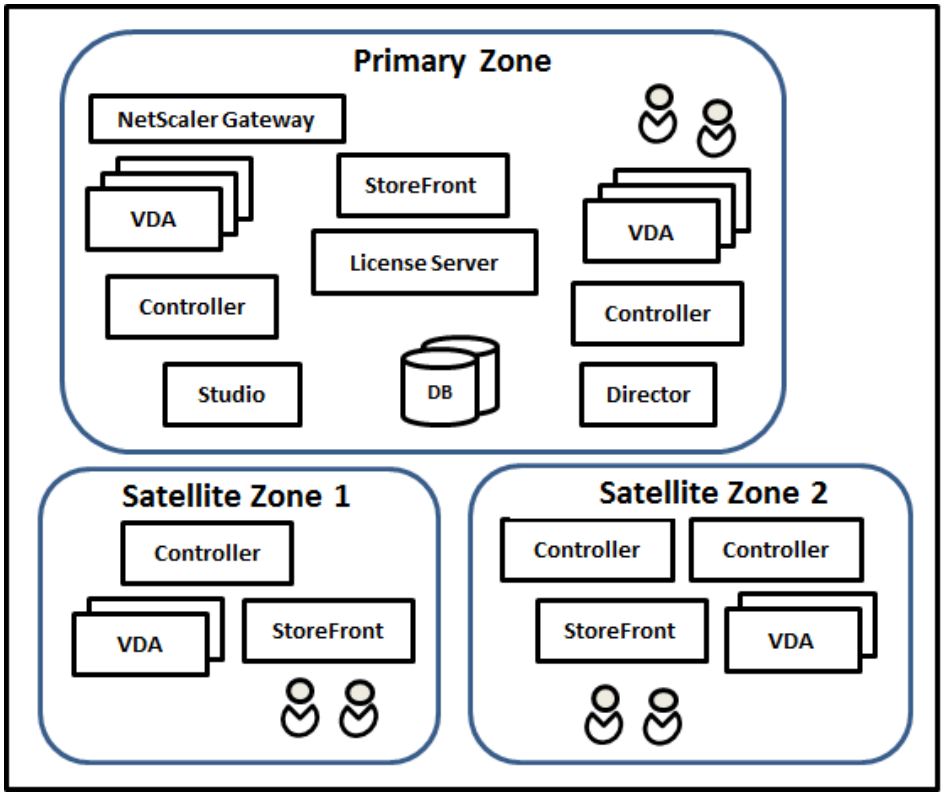
La zona principal también debe tener al menos dos Controllers para la redundancia. Asimismo, puede tener uno o varios VDA con aplicaciones estrechamente ligadas a la base de datos y la infraestructura.

Zona satélite:

Una zona satélite contiene uno o varios VDA, Controllers, servidores StoreFront y servidores Citrix Gateway. En condiciones normales, los Controllers de una zona satélite se comunican directamente con la base de datos situada en la zona principal.

Una zona satélite, especialmente una grande, también puede contener un hipervisor que se usa para aprovisionar y/o almacenar máquinas de esa zona. Al configurar una zona satélite, puede asociarle una conexión de hipervisor o servicio de nube. (Compruebe que los catálogos de máquinas que utilizan esa conexión están en la misma zona.)

Un sitio puede tener zonas satélite con distintas configuraciones, en función de sus necesidades concretas y su entorno. En la siguiente imagen, se representa una zona principal y ejemplos de zonas satélite.



En la imagen:

- **Zona principal:** Contiene dos Controllers, Studio, Director, StoreFront, el servidor de licencias y la base de datos del sitio (además de implementaciones de alta disponibilidad de SQL Server). La zona principal también contiene varios VDA y un Citrix Gateway.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Zona satélite 1: varios VDA con un Controller:** Contiene un Controller, agentes VDA y un servidor StoreFront. Los VDA de esta zona satélite se registran en el Controller local. El Controller local se comunica con la base de datos del sitio y el servidor de licencias situados en la zona principal.

  Si falla la red WAN, la función Caché de host local permite que el Controller de la zona satélite siga actuando como broker en conexiones a los VDA de esa zona. Una implementación así puede ser adecuada en una oficina donde los trabajadores utilicen un sitio local de StoreFront y el Controller local para acceder a sus recursos locales incluso aunque falle el vínculo WAN que conecta su oficina a la red de la empresa.

- **Zona satélite 2: varios VDA con Controllers redundantes:** Contiene dos Controllers, agentes VDA y un servidor StoreFront. Este es el tipo de zona más resistente. Ofrece protección contra errores simultáneos de red WAN y uno de los Controllers locales.

Dónde se registran los VDA y dónde conmutan por error los Controllers

En un sitio que contiene zonas principal y satélite, con agentes VDA como mínimo de la versión 7.7:

- Un VDA de la zona principal se registra en un Controller de la zona principal. Un VDA de la zona principal no intentará nunca registrarse en un Controller de una zona satélite.
- Un VDA de una zona satélite se registra en el Controller local, si es posible. (Este se considera el Controller favorito.) Si no hay Controllers locales disponibles (por ejemplo, debido a que no pueden aceptar más registros de VDA o porque se ha producido un error en ellos), el VDA intentará registrarse en un Controller de la zona principal. En este caso, el VDA permanecerá registrado en la zona principal incluso aunque un Controller de la zona satélite vuelva a estar disponible. Un VDA de una zona satélite no intentará nunca registrarse en un Controller de otra zona satélite.
- Cuando está habilitada la actualización automática para la detección de Controllers por parte de los VDA y se especifica una lista de direcciones de Controller durante la instalación de VDA, se selecciona aleatoriamente un Controller de esa lista para el registro inicial (independientemente de la zona en que resida ese Controller). Una vez se reinicie la máquina que contiene el VDA, ese VDA empezará el registro en un Controller de su zona local.
- Si falla un Controller de una zona satélite, si puede, conmutará por error a otro Controller local. Si no hay Controllers locales disponibles, se producirá una conmutación por error a un Controller de la zona principal.
- Si se mueve un Controller dentro o fuera de una zona y su actualización automática está habilitada, los VDA de ambas zonas recibirán listas actualizadas que indicarán qué Controllers son locales y cuáles están en la zona principal, para que los VDA sepan en cuál se pueden registrar y de cuál pueden aceptar conexiones.
- Si se mueve un catálogo de máquinas a otra zona, los VDA de ese catálogo volverán a registrarse

© 1999-2019 Citrix Systems, Inc. All rights reserved.

en los Controllers de la zona a la que se haya movido el catálogo. (Cuando mueva un catálogo a otra zona, compruebe que esa zona y la zona con la conexión de host asociada estén bien conectadas. Si hay ancho de banda limitado o alta latencia, mueva la conexión de host a la misma zona que contiene el catálogo de máquinas asociado.)

Si fallan todos los Controllers de la zona principal:

- Studio no puede conectarse al sitio.
- No se puede establecer conexiones con los VDA de la zona principal.
- El rendimiento del sitio se degradará cada vez más hasta que los Controllers de la zona principal vuelvan a estar disponibles.

En caso de sitios que contienen versiones de VDA anteriores a 7.7:

- Un VDA en una zona satélite aceptará solicitudes de Controllers de su zona local y la zona principal. (A partir de la versión 7.7, los agentes VDA pueden aceptar solicitudes de Controller de otras zonas satélite.)
- Un VDA de una zona satélite se registrará en un Controller de la zona principal o de la zona local de forma aleatoria. (A partir de la versión 7.7, los agentes VDA prefieren la zona local.)

Preferencia de zonas

Para usar la característica Preferencia de zonas, debe utilizar como mínimo StoreFront 3.7 y Citrix Gateway 11.0-65.x.

En un sitio de varias zonas, la funcionalidad Preferencia de zonas ofrece más flexibilidad al administrador para controlar qué VDA se utiliza para iniciar una aplicación o un escritorio.

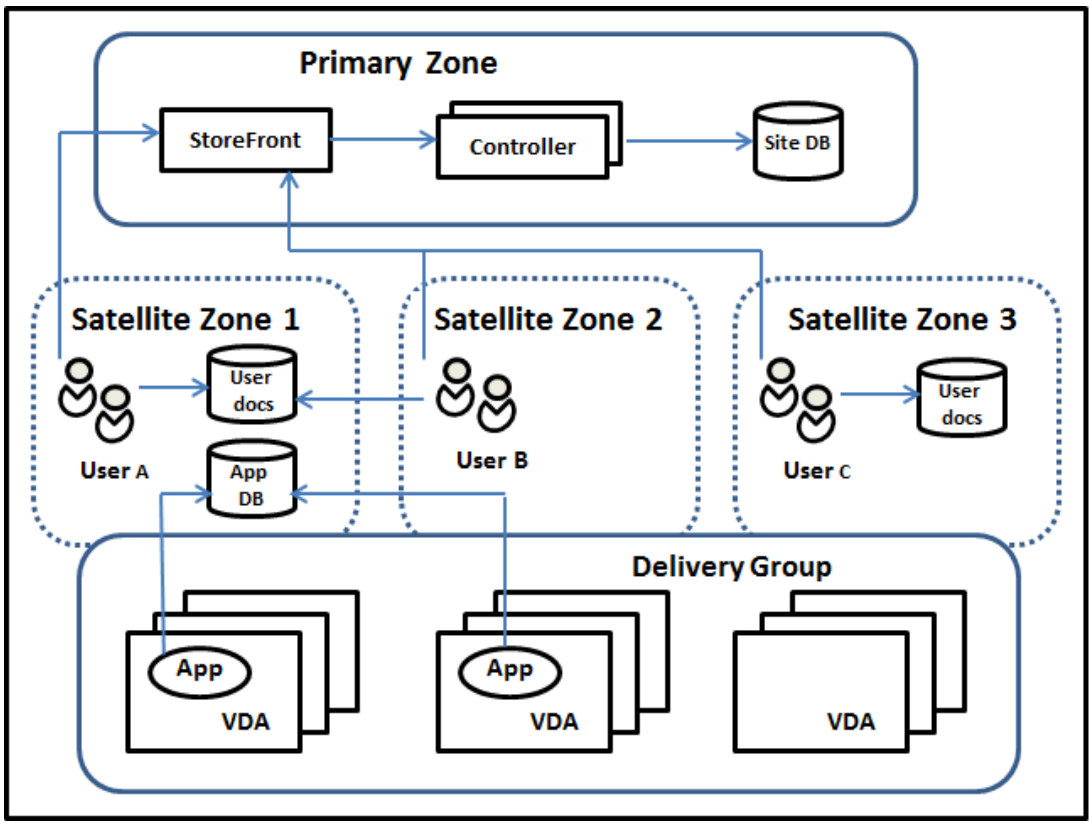
Cómo funciona la preferencia de zonas

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



En este ejemplo, los VDA están distribuidos en tres zonas satélite, pero pertenecen todos al mismo grupo de entrega. Por lo tanto, el intermediario (broker) puede elegir qué VDA usar cuando un usuario lanza una solicitud de inicio. En este ejemplo, hay varios lugares donde los usuarios pueden ejecutar sus puntos finales de la aplicación Citrix Workspace: el usuario A usa un dispositivo con la aplicación Citrix Workspace en la zona satélite 1; el usuario B usa un dispositivo en la zona satélite 2. Los documentos de los usuarios pueden almacenarse en una serie de ubicaciones; por ejemplo: ambos usuarios, A y B, utilizan un recurso compartido en la zona satélite 1, mientras que el usuario C usa un recurso de la zona satélite C. Además, una de las aplicaciones publicadas utiliza una base de datos que se encuentra en la zona satélite 1.

Para asociar un usuario o una aplicación a una zona, configure una zona particular específica para ese usuario o esa aplicación. A partir de ahí, el broker que se encuentra en el Delivery Controller usa esas asociaciones para seleccionar la zona donde se iniciará una sesión, si los recursos están disponibles. Puede:

- 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.)

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Aunque se puedan configurar las preferencias de zonas para usuarios y aplicaciones, el broker selecciona una sola zona preferida para el inicio. El orden predeterminado de prioridad para seleccionar la zona preferida es: zona particular de la aplicación > zona particular del usuario > ubicación del usuario. Puede restringir la secuencia; consulte Adaptar la preferencia de zonas. Cuando un usuario inicia una aplicación:

- Si la aplicación tiene configurada una asociación de zona (es decir, una zona particular de la aplicación), entonces la zona preferida es la zona particular de esa aplicación.
- En cambio, si la aplicación no tiene configurada una asociación de zona pero el usuario sí la tiene (una zona particular de usuario), entonces la zona preferida es la zona particular del usuario.
- Si ni la aplicación ni el usuario tienen configurada una asociación de zona, entonces la zona preferida es la zona donde el usuario ejecuta la instancia de la aplicación Citrix Workspace (la ubicación del usuario). Si esa zona no está definida, se seleccionan un VDA y una zona aleatorios. El equilibrio de carga se aplica a todos los VDA de la zona preferida. Si no hay ninguna zona preferida, el equilibrio de carga se aplica a todos los VDA del grupo de entrega.

Adaptar la preferencia de zonas

Al configurar (o quitar) la zona particular de un usuario o una aplicación, puede limitar más cómo se utilizará (o no) la preferencia de zonas.

- **Uso obligatorio de la zona particular del usuario.** En un grupo de entrega, puede especificar que una sesión deba iniciarse en la zona particular del usuario (si la tiene), sin conmutación por error a otra zona si los recursos no estuvieran disponibles en esa zona particular. Esta restricción es útil para evitar el riesgo de copia de perfiles o archivos de datos grandes entre las zonas. En otras palabras, cuando se prefiere negar el inicio de una sesión a iniciarla en otra zona.
- **Uso obligatorio de la zona particular de la aplicación.** Del mismo modo, cuando configure la zona particular de una aplicación, puede indicar que la aplicación deba iniciarse solo en esa zona, sin conmutación por error a otra zona aunque los recursos no estuvieran disponibles en la zona particular de la aplicación.
- **Sin zona particular de aplicación, e ignorar la zona particular configurada del usuario.** Si no especifica ninguna zona particular para una aplicación, también puede indicar que no se tenga en cuenta ninguna zona de usuario configurada para iniciar esa aplicación. Por ejemplo, si prefiere que los usuarios ejecuten una aplicación concreta en un VDA cercano a la máquina que están usando (donde se está ejecutando la aplicación Citrix Workspace), puede indicarlo mediante la preferencia de zona “ubicación del usuario” aunque algunos usuarios tengan otra zona particular.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Cómo afecta la preferencia de zonas al uso de sesiones

Cuando un usuario inicia una aplicación o un escritorio, el broker prefiere usar la zona preferida en lugar de usar una sesión existente.

Si el usuario que inicia la aplicación o escritorio ya tiene una sesión apropiada para el recurso que se va a iniciar (por ejemplo, una que puede usar la función de compartir sesiones para una aplicación, o bien una sesión que ya ejecuta el recurso que se va a iniciar), pero esa sesión se está ejecutando en un VDA que se encuentra en otra zona, no la preferida de la aplicación o el usuario, el sistema puede crear una nueva sesión. Con lo que el inicio se produce en la zona correcta (si tiene capacidad disponible), en vez de reconectarse a una sesión en una zona menos ventajosa para los requisitos de sesión del usuario.

Para que no exista una sesión "huérfana" con la que ya no se pueda establecer conexión, se permite volverse a conectar a las sesiones desconectadas incluso aunque estén en una zona no preferida.

El orden de preferencia para elegir una sesión para el inicio es:

1. Reconectarse a una sesión existente en la zona preferida.
2. Reconectarse a una sesión desconectada existente en una zona que no sea la preferida.
3. Iniciar una sesión nueva en la zona preferida.
4. Reconectarse una sesión conectada existente en una zona que no sea la preferida.
5. Iniciar una sesión nueva en una zona que no sea la preferida.

Otras consideraciones de preferencia de zonas

- Si configura la zona particular de un grupo de usuarios (por ejemplo, un grupo de seguridad), los usuarios de ese grupo (por pertenencia directa o indirecta) se asocian a la zona especificada. No obstante, un usuario puede pertenecer a varios grupos de seguridad y, por lo tanto, puede tener otras zonas particulares configuradas por pertenecer a otros grupos. En tales casos, la determinación de la zona particular de ese usuario puede ser ambigua.

Si un usuario tiene configurada una zona particular que no adquirió por pertenecer a grupos, esa es la zona que se usa para la preferencia de zonas. Se ignoran las asociaciones de zona que se adquieran por pertenecer a grupos.

Si el usuario tiene varias asociaciones de zonas que adquirió únicamente por pertenecer a grupos, el broker escoge una zona aleatoria de entre ellas. Tras la elección del broker, se utiliza la misma zona para los inicios subsiguientes de sesión hasta que cambie la pertenencia del usuario a los grupos.

- La preferencia de zona "ubicación del usuario" requiere que el Citrix Gateway a través del cual se conecta el dispositivo de punto final detecte la aplicación Citrix Workspace en ese dispositivo de punto final. El dispositivo Citrix Gateway debe estar configurado para asociar rangos de

© 1999-2019 Citrix Systems, Inc. All rights reserved.

direcciones IP a zonas concretas, y la identidad de la zona detectada debe transferirse a través de StoreFront al Controller.

Para obtener más información acerca de la preferencia de zonas, consulte Zone Preference Internals.

Requisitos, consejos y consideraciones

- Puede colocar los siguientes elementos en una zona: Controllers, catálogos de máquinas, conexiones de host, usuarios y aplicaciones. Si un catálogo de máquinas usa una conexión de host, el catálogo y la conexión deben estar en la misma zona. (Sin embargo, con una conexión disponible de latencia baja y ancho de banda alto, pueden estar en diferentes zonas.)
- Colocar elementos en una zona satélite afecta al modo en que el sitio interactúa con ellos y con otros objetos relacionados con esos elementos.
  - Cuando se colocan máquinas de Controller en una zona satélite, se presupone que esas máquinas tienen una buena conexión (local) con hipervisores y máquinas VDA en la misma zona satélite. Por tanto, se utilizan preferentemente los Controllers de esa zona satélite en lugar de Controllers de la zona principal para la gestión de esos hipervisores y esas máquinas VDA.
  - Cuando se coloca una conexión de hipervisor en una zona satélite, se presupone que todos los hipervisores administrados a través de esa conexión de hipervisor también residen en esa zona satélite. Por tanto, se utilizan preferentemente los Controllers de esa zona satélite en lugar de Controllers de la zona principal para la comunicación por esa conexión de hipervisor.
  - Cuando se coloca un catálogo de máquinas en una zona satélite, se presupone que todas las máquinas VDA de ese catálogo están en la zona satélite. Se utilizan preferentemente Controllers locales (en lugar de Controllers de la zona principal) cuando los VDA intentan registrarse en el sitio, después de que se haya activado el mecanismo de actualización automática de los Controllers tras el primer registro de cada VDA.
  - También se pueden asociar instancias de Citrix Gateway a zonas. A diferencia de los demás elementos que se describen aquí, esto se realiza como parte de la configuración del enrutamiento óptimo de HDX de StoreFront, en lugar de hacerse como parte de la configuración del sitio. Cuando se asocia un Citrix Gateway a una zona, se utiliza preferentemente ese Citrix Gateway cuando se utilizan las conexiones HDX a las máquinas VDA de esa zona.
- Cuando se crea un sitio de producción y, luego, se crean el primer catálogo de máquinas y el primer grupo de entrega, todos esos elementos se encuentran en la zona principal: no se pueden crear zonas satélite hasta después de completar la configuración inicial. (Si crea un sitio vacío, la zona principal contendrá al principio solo un Controller. Puede crear zonas satélite antes o después de crear un catálogo de máquinas y un grupo de entrega.)

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Cuando crea la primera zona satélite con uno o varios elementos, todos los demás elementos de su sitio siguen estando en la zona principal.
- La zona principal se denomina “Principal” de forma predeterminada, y usted puede cambiar ese nombre. Aunque la pantalla de Studio indica cuál es la zona principal, se recomienda usar un nombre de fácil identificación para la zona principal. Puede reasignar la zona principal (es decir, puede convertir otra zona en la zona principal), pero esta debe contener siempre la base de datos del sitio y los servidores de alta disponibilidad.
- La base de datos del sitio debe estar siempre en la zona principal.
- Después de crear una zona, puede mover elementos de una zona a otra. Tenga en cuenta que esta flexibilidad permite llegar a separar elementos que funcionan mejor en cercanía; por ejemplo, mover un catálogo de máquinas a otra zona que la conexión (host) que crea las máquinas del catálogo podría afectar al rendimiento. Por lo tanto, tenga en mente los posibles efectos imprevistos antes de mover elementos entre zonas. Mantenga el catálogo y la conexión de host que éste usa en la misma zona o en zonas bien conectadas (por ejemplo, conectadas a través de una red de baja latencia y alto ancho de banda).
- Para obtener un rendimiento óptimo, instale Studio y Director solo en la zona principal. Si quiere otra instancia de Studio en una zona satélite (por ejemplo, si una zona satélite que contiene Controllers se usa para la conmutación por error en caso de que la zona principal deje de ser accesible), ejecute Studio como una aplicación publicada localmente. Asimismo, puede acceder a Director desde una zona satélite porque se trata de una aplicación Web.
- Preferiblemente, Citrix Gateway de una zona satélite debe usarse para conexiones de usuario provenientes de otras zonas o ubicaciones externas, aunque puede usarse para conexiones desde dentro de la zona.
- Recuerde: Para usar la característica Preferencia de zonas, debe utilizar como mínimo StoreFront 3.7 y Citrix Gateway 11.0-65.x.
- Para obtener información más técnica y consideraciones de rendimiento, consulte Zones Deep Dive.

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Impacto de latencia en la intermediación de rendimiento

Aunque las zonas permiten a los usuarios estar en los enlaces de mayor latencia, siempre que haya un broker local, la latencia adicional influye inevitablemente en la experiencia del usuario final. Para la mayor parte de las tareas, los usuarios experimentan lentitud provocada por viajes de ida y vuelta entre los Controllers de la zona satélite y la base de datos del sitio.

En el inicio de aplicaciones, se producen demoras extras mientras el proceso de intermediación de sesiones identifica al VDA adecuado al que enviar las solicitudes de inicio de sesión.

Crear y administrar zonas

Un administrador total puede realizar todas las tareas de creación y administración de zonas. Sin embargo, también se puede crear un rol personalizado que permita crear, modificar o eliminar una zona. Mover elementos entre zonas no requiere permisos de zonas (excepto el permiso de lectura de zonas). Sin embargo, debe tener permiso para modificar los elementos que esté moviendo. Por ejemplo, para mover un catálogo de máquinas de una zona a otra, debe tener el permiso de modificar ese catálogo de máquinas. Para obtener más información, consulte el artículo Administración delegada.

Si utiliza Citrix Provisioning: La consola de Citrix Provisioning que se incluye en esta versión no reconoce zonas, por lo que Citrix recomienda usar Studio para crear catálogos de máquinas que quiera colocar en las zonas satélite. Use el asistente de Studio para crear el catálogo y especificar la zona satélite correspondiente. A continuación, utilice la consola de Citrix Provisioning para aprovisionar las máquinas de ese catálogo. (Si crea el catálogo mediante el asistente de Citrix Provisioning, este se colocará en la zona principal y deberá usar Studio para moverlo posteriormente a la zona satélite.)

Crear una zona

1. Seleccione **Configuración > Zonas** en el panel de navegación de Studio.
2. Seleccione **Crear zona** en el panel Acciones.
3. Escriba un nombre para la zona y una descripción (opcional). El nombre debe ser único dentro del sitio.
4. Seleccione los elementos que se van a colocar en la nueva zona. Puede filtrar o buscar la lista de elementos de la que seleccionarlos. También puede crear una zona vacía. Para ello, simplemente no seleccione ningún elemento.
5. Haga clic en **Guardar**.

Como alternativa a este método, puede seleccionar uno o varios elementos en Studio y, a continuación, seleccionar **Crear zona** en el panel Acciones.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Cambiar el nombre o la descripción de una zona

1. Seleccione **Configuración > Zonas** en el panel de navegación de Studio.
2. Seleccione una zona en el panel central y, a continuación, seleccione **Modificar zona** en el panel Acciones.
3. Cambie el nombre y/o la descripción de la zona. Si cambia el nombre de la zona principal, tenga en cuenta que la zona debe ser fácilmente identificable como zona principal.
4. Haga clic en **Aceptar** o en **Aplicar**.

Mover elementos de una zona a otra

1. Seleccione **Configuración > Zonas** en el panel de navegación de Studio.
2. Seleccione una zona en el panel central y, a continuación, seleccione uno o varios elementos.
3. Arrastre los elementos a la zona de destino o seleccione **Mover elementos** en el panel Acciones y, a continuación, especifique la zona a la que moverlos.

Aparecerá un mensaje de confirmación con una lista de los elementos seleccionados y preguntará si quiere moverlos a todos.

Recuerde: Si un catálogo de máquinas usa una conexión de host a un hipervisor o un servicio de nube, ambos (el catálogo y la conexión) deben estar en la misma zona. De lo contrario, el rendimiento puede verse afectado. Si mueve un elemento, mueva el otro.

Eliminar una zona

Una zona debe estar vacía antes de que se pueda eliminar. No se puede eliminar la zona principal.

1. Seleccione **Configuración > Zonas** en el panel de navegación de Studio.
2. Seleccione una zona en el panel central.
3. Seleccione **Eliminar zona** en el panel Acciones. Si la zona no está vacía (contiene elementos), se le pedirá que seleccione la zona a la que se moverán los elementos.
4. Confirme la eliminación.

Agregar una zona particular a un usuario

Configurar la zona particular de un usuario también se conoce como *agregar un usuario a una zona*.

1. Seleccione **Configuración > Zonas** en el panel de navegación de Studio y, a continuación, seleccione una zona en el panel central.
2. Seleccione **Agregar usuarios a la zona** en el panel Acciones.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

3. En el cuadro de diálogo **Agregar usuarios a la zona**, haga clic en **Agregar** y, a continuación, seleccione los usuarios y los grupos de usuarios que quiera agregar a la zona. Si especifica usuarios que ya tienen su zona particular, aparecerá un mensaje con dos opciones: **Sí**, que equivale a agregar solo a los usuarios especificados que no tengan ninguna zona particular; **No**, que equivale a volver al diálogo de selección de usuarios.
4. Haga clic en **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 edite un grupo de entrega.
2. En la página **Usuarios**, marque la casilla **Las sesiones deben iniciarse en la zona particular del usuario, si está configurada**.

Todas las sesiones que inicie un usuario de ese grupo de entrega deberán iniciarse desde las máquinas que se encuentren en la zona particular de ese usuario. Si un usuario del grupo de entrega no tiene configurada una zona particular, este parámetro no tiene ningún efecto.

Eliminar la zona particular de un usuario

Este procedimiento también se conoce como quitar un usuario de una zona.

1. Seleccione **Configuración > Zonas** en el panel de navegación de Studio y, a continuación, seleccione una zona en el panel central.
2. Seleccione **Quitar usuarios de la zona** en el panel Acciones.
3. En el cuadro de diálogo **Agregar usuarios a la zona**, haga clic en **Quitar** y, a continuación, seleccione los usuarios y los grupos que quiera quitar de la zona. Tenga en cuenta que esta acción solo quita a los usuarios de la zona; esos usuarios siguen formando parte de los grupos de entrega y los grupos de aplicaciones.
4. Confirme la eliminación cuando se le solicite.

Administrar zonas particulares de aplicaciones

Configurar la zona particular de una aplicación también se conoce como agregar una aplicación a una zona. De forma predeterminada, en un entorno de varias zonas, una aplicación no tiene ninguna zona particular.

La zona particular de una aplicación se especifica en las propiedades de la aplicación. Puede configurar las propiedades de una aplicación cuando la agregue a un grupo o más adelante. Para ello, deberá seleccionar la aplicación en Studio y modificar sus propiedades.

- Al crear un grupo de entrega, crear un grupo de aplicaciones o al agregar aplicaciones a grupos existentes, seleccione **Propiedades** en la página **Aplicaciones** del asistente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Para cambiar las propiedades de una aplicación después de agregarla, seleccione **Aplicaciones** en el panel de navegación de Studio. Seleccione una aplicación y, a continuación, seleccione **Modificar propiedades de aplicación** en el panel Acciones.

En la página **Zonas** de las propiedades o ajustes de la aplicación:

- Si quiere que la aplicación tenga una zona particular:
  - Marque el botón de opción **Usar la zona seleccionada para determinar donde se inicia esta aplicación** y, a continuación, seleccione la zona de la lista desplegable.
  - Si quiere que la aplicación solo se inicie desde la zona seleccionada (ninguna otra), marque la casilla situada debajo de la selección de zonas.
- Si no quiere que la aplicación tenga una zona particular:
  - Seleccione la opción **No configurar una zona particular para esta aplicación**.
  - Si no quiere que el broker tenga en cuenta ninguna de las zonas de usuario configuradas cuando se inicie esta aplicación, marque la casilla situada bajo el botón de opción. En ese caso, no se utilizará ninguna zona particular de aplicación o usuario para determinar dónde iniciar esta aplicación.

Otras acciones que implican especificar zonas

Cuando se agrega una conexión de host o se crea un catálogo de máquinas (aparte del momento en que se crea un sitio), se puede especificar una zona a la que se asignará el objeto, si ya se ha creado al menos una zona satélite.

En la mayoría de los casos, la zona principal es la opción predeterminada. Si utiliza Machine Creation Services para crear un catálogo de máquinas, se selecciona automáticamente la zona que esté configurada para la conexión de host.

Si el sitio no contiene zonas satélite, se presupone la selección de la zona principal y el cuadro de selección de zonas no aparece.

Conexiones y recursos

March 14, 2019

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 servicios de nube o los hipervisores compatibles. El almacenamiento y la red que seleccione forman los recursos necesarios para dicha conexión.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Los administradores de solo lectura pueden ver los detalles de conexiones y recursos. Debe ser un administrador total para realizar tareas de administración de conexiones y recursos. Para obtener más información, consulte Administración delegada.

Dónde encontrar información acerca de los tipos de conexión

Puede utilizar las plataformas de virtualización admitidas para alojar y administrar máquinas en el entorno de Citrix Virtual Apps o Citrix Virtual Desktops. El artículo Requisitos del sistema enumera los tipos respaldados. Puede utilizar las soluciones admitidas de implementación en la nube para alojar componentes de producto y aprovisionar máquinas virtuales. Estas soluciones agrupan recursos de procesamiento para construir nubes privadas, públicas o híbridas de Infraestructura como servicio (IaaS).

Para obtener más información, consulte las siguientes fuentes de información.

- **Microsoft Azure Resource Manager:**
  - Artículo Entornos de virtualización para el Administrador de recursos de Azure.
  - Documentación de Microsoft.
- **Amazon Web Services (AWS):**
  - Citrix XenDesktop en Amazon Web Services.
  - Documentación de AWS.
  - Al crear una conexión en Studio, debe proporcionar la clave API y la 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.
  - Configure una conexión de host de AWS para utilizar roles de IAM introduciendo **role_based_auth** como valor para los campos “clave de acceso” y “clave secreta”. Asimismo, se requiere un rol de IAM que defina la directiva y los permisos requeridos por Citrix al agregarse a las instancias de Delivery Controllers o Cloud Connectors alojadas de AWS.
  - El archivo de credenciales para la cuenta raíz de AWS, (que se puede obtener de la consola de AWS), no está en el mismo formato que los archivos de credenciales descargados para los usuarios estándar de AWS. Por lo tanto, Studio no puede usar el archivo para rellenar los campos de la clave API y la clave secreta. Compruebe que está utilizando archivos de credenciales IAM de AWS.
  - De forma predeterminada, las máquinas AWS no se conservan después de las operaciones de apagado (por ejemplo, reinicios). Esto no presenta problemas para la mayoría de las

© 1999-2019 Citrix Systems, Inc. All rights reserved.

implementaciones. Sin embargo, si quiere conservar la máquina (y su ID de instancia) en dichas operaciones:

1. Modifique la conexión.
2. En la página **Avanzado**, escriba lo siguiente en el campo "Opciones de conexión": `CreateNewInstanceOnReset=false`

- **Citrix XenServer:**
  - Entornos de virtualización de XenServer.
  - Documentación de Citrix 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.
- **Microsoft Azure (Classic):**
  - Este tipo de host está obsoleto.
  - Artículo Entornos de virtualización de Microsoft Azure.
  - Documentación de Microsoft.
- **CloudPlatform:**
  - Este tipo de host está obsoleto.
  - Documentación de CloudPlatform.
  - Al crear una conexión en Studio, debe proporcionar la clave API y la clave secreta. Puede exportar el archivo de claves que contiene esos valores desde CloudPlatform y, a continuación, importarlos en Studio.

Almacenamiento de host

Se admite un producto de almacenamiento si puede ser administrado por un hipervisor compatible. La asistencia de Citrix ayudará a los proveedores de los productos de almacenamiento a resolver problemas, y documentará esos problemas en Knowledge Center según sea necesario.

Cuando se aprovisionan máquinas, los datos se clasifican por tipo:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Datos de sistema operativo (SO), que incluye las imágenes maestras.
- Datos temporales, que incluyen todos los datos no persistentes escritos en las máquinas aprovisionadas por MCS, archivos de paginación de Windows, datos de los perfiles de usuario y todos los datos que se sincronicen con ShareFile. Estos datos se descartan cada vez que la máquina se reinicia.
- Datos personales guardados en los Personal vDisks.

Si se ofrece un almacenamiento por separado para cada tipo de datos se puede reducir la carga y mejorar el rendimiento de IOPS en cada dispositivo de almacenamiento, lo que hace un uso óptimo de los recursos del host. También habilita el almacenamiento apropiado para los distintos tipos de datos, ya que la persistencia y resistencia son más importantes para algunos tipos de datos que para otros.

El almacenamiento puede ser compartido (ubicado centralmente, separado de los hosts y utilizado por todos los hosts) o local, en un hipervisor. Por ejemplo, el almacenamiento compartido central puede ser uno o varios volúmenes de almacenamiento en clúster de servidores Windows Server 2012 (con o sin almacenamiento conectado), o un dispositivo de un proveedor de almacenamiento. El almacenamiento central también puede ofrecer sus propias optimizaciones, tales como rutas de control del almacenamiento del hipervisor y acceso directo a través de plugins asociados.

El almacenamiento local de los datos temporales evita que haya que atravesar la red para acceder al almacenamiento compartido. Esto también reduce la carga (IOPS) en el dispositivo de almacenamiento compartido. El almacenamiento compartido puede ser más costoso, por lo que el almacenamiento de datos local puede reducir el gasto. Estas ventajas deben tenerse en cuenta frente a la disponibilidad de almacenamiento suficiente en los servidores de hipervisor.

Cuando se crea una conexión, se elige uno de los dos métodos de administración del almacenamiento: el almacenamiento compartido por los hipervisores, o el almacenamiento local en cada hipervisor.

Cuando se usa el almacenamiento local en uno o varios hosts de 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 respaldo y una administración centralizadas. Ese almacenamiento guarda los discos de SO y los discos Personal vDisk.

Cuando se selecciona este método, se puede elegir si usar almacenamiento local (en servidores de la misma agrupación de hipervisores) para datos de máquina temporales que no requieren la persistencia o la resistencia requerida por los datos guardados en el almacenamiento compartido. Esto se

© 1999-2019 Citrix Systems, Inc. All rights reserved.

denomina *caché de datos temporales*. El disco local ayuda a reducir el tráfico hacia el almacenamiento de SO principal. Este disco se borra cada vez que se reinicia la máquina. Se accede al disco a través de una memoria caché de escritura. Tenga en cuenta que, si usa almacenamiento local para datos temporales, el VDA aprovisionado queda asociado a un host de hipervisor específico; si ese host falla, la VM no podrá iniciarse.

Excepción: Si usa volúmenes de almacenamiento en clúster o CSV (Clustered Storage Volumes), Microsoft System Center Virtual Machine Manager no permite la creación de discos caché de datos temporales en el almacenamiento local.

Cuando se crea una conexión, si se habilita la opción para almacenar datos temporales localmente, se pueden habilitar y configurar valores no predeterminados para el tamaño de la memoria y del disco de caché de cada VM cuando se crea un catálogo de máquinas que usa esa conexión. No obstante, los valores predeterminados se ajustan al tipo de conexión y son suficientes en la mayoría de los casos. Para obtener más información, consulte Crear catálogos de máquinas.

El hipervisor también puede ofrecer tecnologías de optimización a través de la caché local de lectura de las imágenes de los discos. Por ejemplo, XenServer ofrece IntelliCache. Esto también puede reducir el tráfico de red hacia el almacenamiento central.

Almacenamiento local en el hipervisor

El método de almacenamiento local en el hipervisor almacena datos localmente en el hipervisor. Con este método, las imágenes maestras y otros datos del SO se transfieren a todos los hipervisores utilizados en el sitio, tanto para la creación inicial de las máquinas como para las actualizaciones de las imágenes. Esto da como resultado un tráfico importante en la red de administración. La transferencia de imágenes consume también mucho tiempo y las imágenes no llegan a todos los hosts al mismo tiempo.

Cuando se selecciona este método, se puede elegir si se quiere usar el almacenamiento compartido para los discos Personal vDisk, para ofrecer resistencia y respaldo para los sistemas de recuperación antes desastres y copia de seguridad.

Crear una conexión y recursos

Si quiere, puede crear la primera conexión cuando crea el sitio. El asistente para la creación de sitios contiene las páginas relacionadas con la conexión, como se describe más abajo: Conexión, Administración del almacenamiento, Selección del almacenamiento y Red.

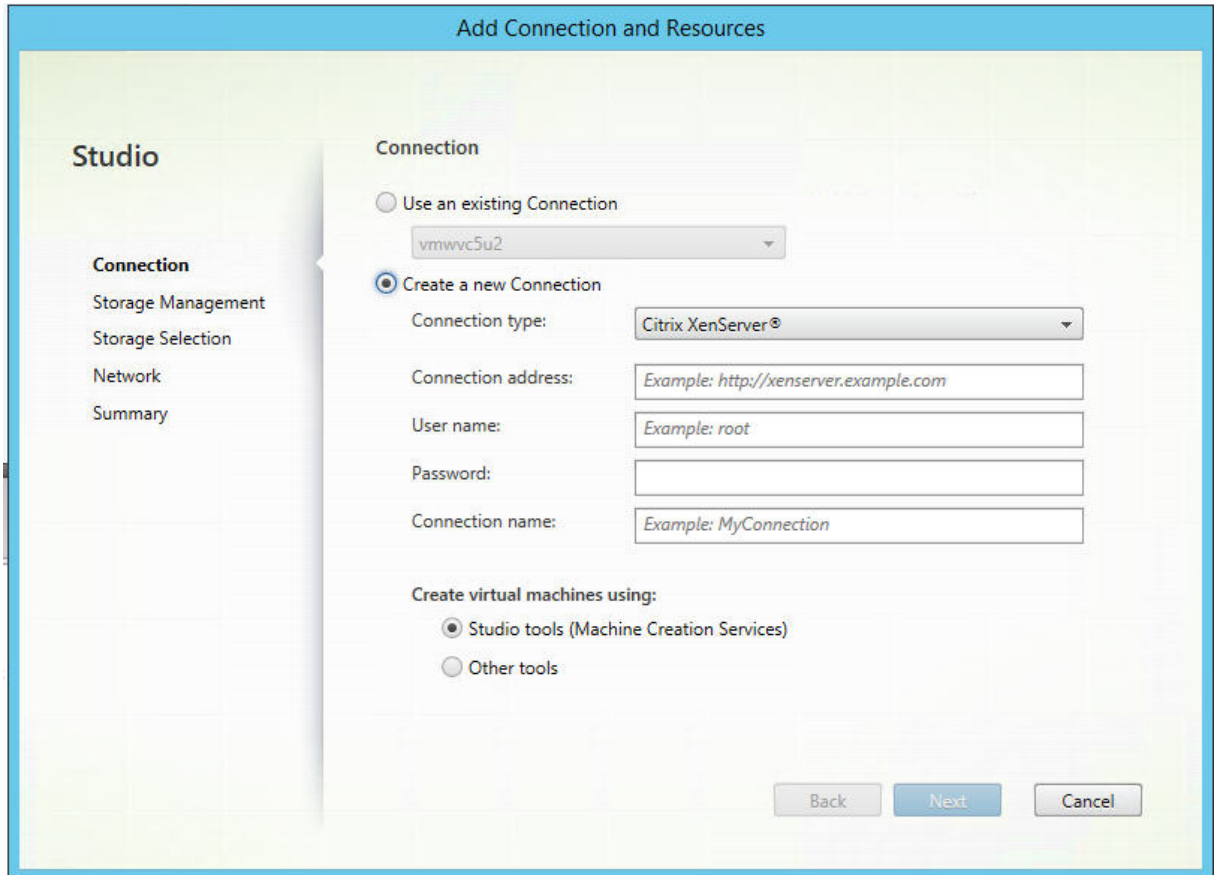
Si crea una conexión después de crear un sitio, empiece en el paso 1.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> **Importante:**
>
> Los recursos de host (almacenamiento y red) deben estar disponibles antes de crear la conexión.

1. Seleccione **Configuración > Alojamiento** en el panel de navegación de Studio.
2. Seleccione **Agregar conexiones y recursos** en el panel Acciones.
3. El asistente lo guiará por las páginas siguientes (el contenido específico de las páginas depende del tipo de conexión seleccionado). Después de completar cada página, haga clic en **Siguiente** hasta llegar a la página **Resumen**.

Conexión



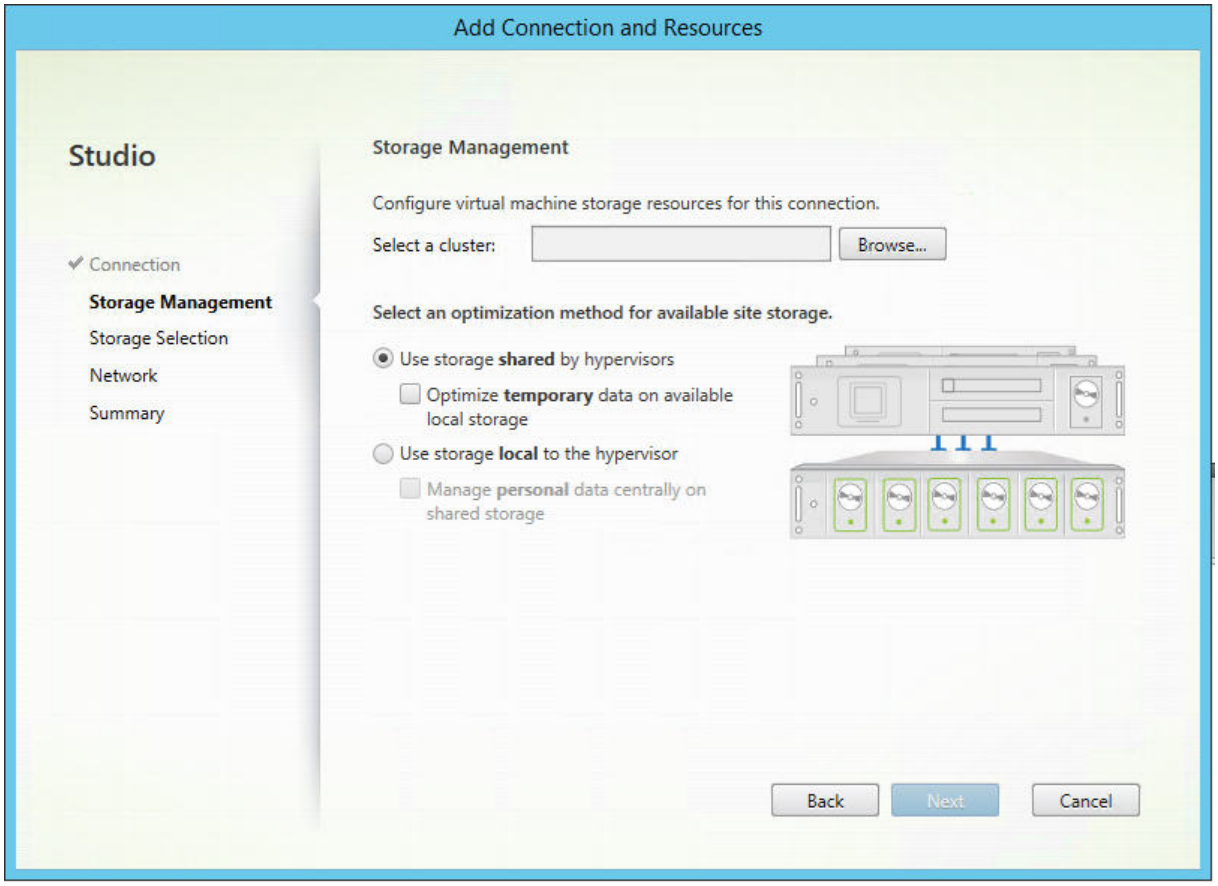
En la página **Conexión**:

- Para crear una nueva conexión, seleccione **Crear una nueva conexión**. Para crear una conexión basada en la misma configuración de host que una conexión existente, seleccione **Usar una conexión existente** y, a continuación, seleccione la conexión correspondiente.
- Seleccione el hipervisor o servicio de nube que está usando en el campo **Tipo de conexión**.
- Los campos de dirección de la conexión y credenciales difieren en función del tipo de conexión seleccionado. Introduzca la información requerida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Escriba un nombre para la conexión. Este nombre aparecerá en Studio.
- Elija la herramienta que usará para crear máquinas virtuales: herramientas de Studio (tales como Machine Creation Services o Citrix Provisioning) u otras herramientas.

Administración del almacenamiento



Para obtener más información sobre los tipos y métodos de administración de almacenamiento, consulte Almacenamiento de host.

Si está configurando una conexión con un host de Hyper-V o VMware, busque y seleccione el nombre del clúster. Otros tipos de conexión no requieren un nombre de clúster.

Seleccione un método de administración del almacenamiento: puede ser almacenamiento compartido por los hipervisores o almacenamiento local en cada hipervisor.

- Si elige el almacenamiento compartido por los hipervisores indique si quiere conservar los datos temporales en almacenamiento local disponible. (Puede especificar valores no predeterminados para el tamaño del almacenamiento en los catálogos de máquinas que usen esta conexión.) **Excepción:** Si usa volúmenes de almacenamiento en clúster o CSV (Clustered Storage Volumes), Microsoft System Center Virtual Machine Manager no permite crear discos

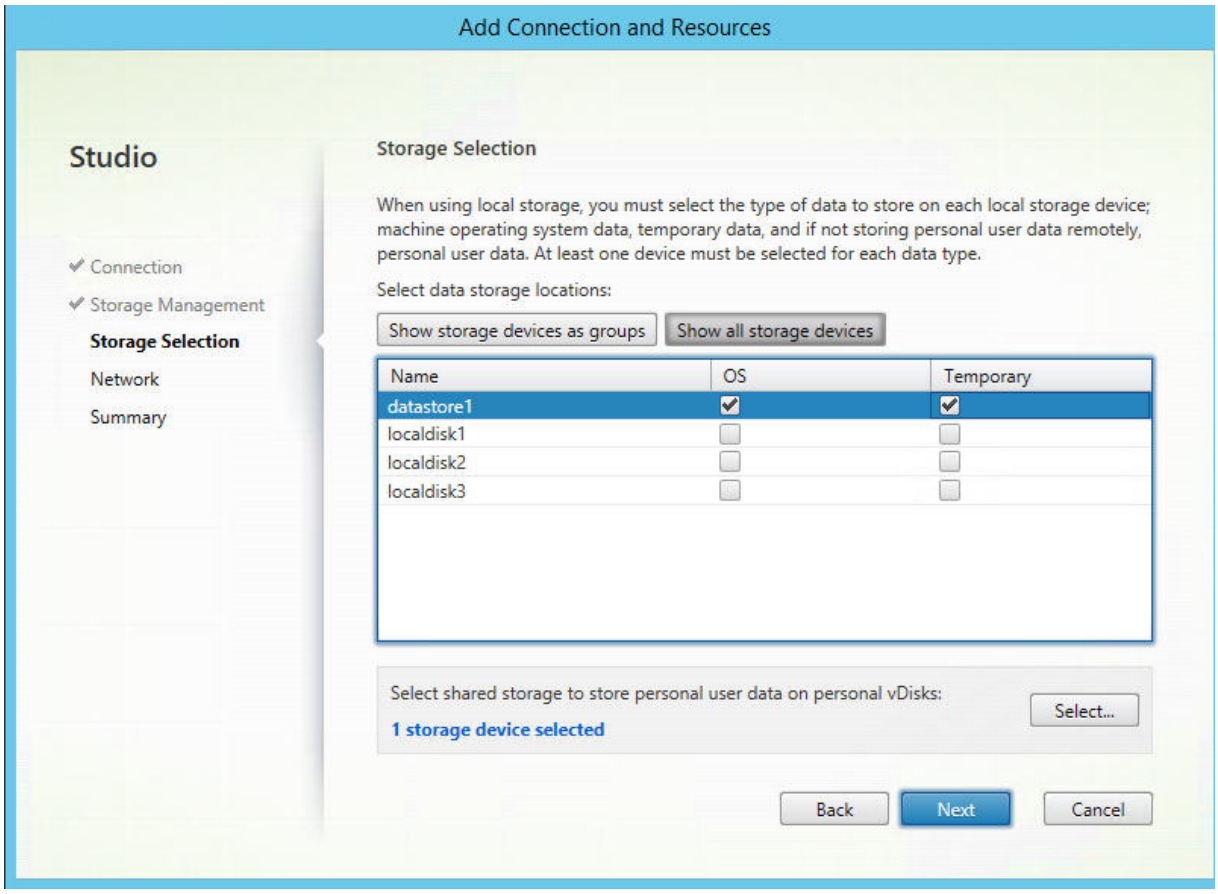
© 1999-2019 Citrix Systems, Inc. All rights reserved.

de caché de datos temporales en el almacenamiento local, por lo que el intento de configurar esa administración de almacenamiento en Studio fallará.

- Si elige usar el almacenamiento local en cada hipervisor, indique si quiere administrar los datos personales (Personal vDisk) en el almacenamiento compartido.

Si usa almacenamiento compartido en un hipervisor 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. Es necesario seleccionar al menos un dispositivo de almacenamiento para cada tipo de datos respaldado antes de pasar a la página siguiente del asistente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

La parte inferior de la página **Selección del almacenamiento** contiene opciones adicionales de configuración si se seleccionó alguna de las opciones siguientes en la página anterior.

- Si eligió almacenamiento compartido por los hipervisores y marcó la casilla **Optimizar datos temporales en el almacenamiento local disponible**, puede seleccionar los dispositivos de almacenamiento local (ubicados en la misma agrupación de hipervisores) que quiere usar para los datos temporales.
- Si eligió almacenamiento local en el hipervisor, y marcó la casilla **Administrar datos personales de forma centralizada en almacenamiento compartido**, puede seleccionar qué dispositivos compartidos quiere usar para los datos personales (datos de Personal vDisk).

Se mostrará la cantidad de dispositivos de almacenamiento seleccionados en ese momento (en el gráfico anterior, "1 storage device selected"). Cuando se pasa el puntero sobre ese texto, aparecen los nombres de los dispositivos seleccionados (a menos que no haya ninguno configurado).

1. Haga clic en **Seleccionar** para cambiar los dispositivos de almacenamiento que quiere usar.
2. En el cuadro de diálogo **Seleccionar almacenamiento**, seleccione o deje sin seleccionar las casillas de cada dispositivos de almacenamiento, y haga clic en **Aceptar**.

Red

En la página **Red**, introduzca un nombre para los recursos; este es el nombre que aparece en Studio para identificar la combinación de almacenamiento y red asociada con la conexión.

Seleccione una o varias redes que usarán las VM.

Resumen

En la página **Resumen**, revise sus selecciones. Cuando haya terminado, haga clic en **Finalizar**.

Recuerde: Si eligió guardar los datos temporales localmente, puede configurar valores no predeterminados para el almacenamiento de datos temporales cuando cree el catálogo de máquinas que contendrá las máquinas que usen esta conexión. Consulte Creación de catálogos de máquinas.

Modificar parámetros de conexión

No haga uso de este procedimiento para cambiar el nombre de una conexión o para crear una nueva conexión. Esas son operaciones diferentes. Cambie la dirección solo si la máquina host actual tiene una nueva dirección. Si introduce la dirección de una máquina distinta se romperán los catálogos de máquinas de la conexión.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 nueva.

1. Seleccione **Configuración > Alojamiento** en el panel de navegación de Studio.
2. Seleccione la conexión y, a continuación, seleccione **Modificar conexión** en el panel Acciones.
3. Siga las instrucciones que se indican a continuación para conocer los parámetros disponibles cuando se modifica una conexión.
4. Cuando haya terminado, haga clic en **Aplicar** para aplicar los cambios que haya hecho y deje la ventana abierta, o haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

Página **Propiedades de la conexión**:

- Para cambiar la dirección de conexión y las credenciales, seleccione **Modificar configuración** y, a continuación, escriba la nueva información.
- Si quiere especificar los servidores de alta disponibilidad para una conexión de XenServer, seleccione **Modificar servidores HA**. 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.

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, por lo general, no se deberían cambiar.
- En las opciones **Acciones simultáneas (de cualquier tipo)** y **Actualizaciones de inventario de Personal vDisk simultáneas**, se especifican dos valores: el número máximo absoluto que se puede dar de forma simultánea en esta conexión y un porcentaje máximo de todas las máquinas que utilizan esta conexión. Debe especificar tanto valores absolutos como porcentajes; el límite real aplicado es el menor de los valores.

  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 de porcentaje.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- 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. Por ejemplo:

  De forma predeterminada, las máquinas AWS no se conservan después de las operaciones de apagado (por ejemplo, reinicios). Esto no presenta problemas para la mayoría de las implementaciones. Sin embargo, si quiere conservar la máquina (y su ID de instancia) en dichas operaciones:

  1. Modifique la conexión.
  2. En la página **Avanzado**, escriba lo siguiente en el campo "Opciones de conexión": `CreateNewInstanceOnReset=false`

Activar o desactivar el modo de mantenimiento de una conexión

Si activa el modo de mantenimiento de una conexión, impide que cualquier otra acción de energía nueva afecte a las máquinas almacenadas en la conexión. Los usuarios no se pueden conectar a una máquina mientras está en modo de mantenimiento. Si los usuarios ya están conectados, los cambios del modo de mantenimiento se efectúan cuando se cierra la sesión.

1. Seleccione **Configuración > Alojamiento** en el panel de navegación de Studio.
2. Seleccione la conexión. Para activar el modo de mantenimiento, seleccione **Activar modo de mantenimiento** en el panel Acciones. Para desactivar el modo de mantenimiento, seleccione **Desactivar modo de mantenimiento**.

También puede activar o desactivar el modo de mantenimiento en máquinas individuales. Además, puede activar o desactivar el modo de mantenimiento en las máquinas de los catálogos o grupos de entrega.

Eliminar una conexión

> **Precaución:**
>
> La eliminación de una conexión puede provocar la eliminación de una gran cantidad de máquinas y la pérdida de datos. Compruebe que se haya hecho copia de seguridad de los datos de usuario en las máquinas afectadas, si fueran útiles.

Antes de eliminar una conexión, compruebe que:

- Todos los usuarios hayan cerrado la sesión en las máquinas almacenadas en la conexión.
- No existan sesiones de usuario desconectadas en ejecución.
- El modo de mantenimiento está activo para máquinas agrupadas y dedicadas.
- Todas las máquinas de los catálogos de máquinas que usa la conexión están apagadas.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Un catálogo de máquinas se vuelve inutilizable cuando se elimina una conexión a la que se hace referencia en ese catálogo. Si se hace referencia a esta conexión en un catálogo, tiene la opción de eliminar el catálogo. Antes de eliminar un catálogo, compruebe que no haya otras conexiones que lo estén utilizando.

1. Seleccione **Configuración > Alojamiento** en el panel de navegación de Studio.
2. Seleccione la conexión y, a continuación, seleccione **Eliminar conexión** en el panel Acciones.
3. Si esta conexión contiene máquinas almacenadas, se le preguntará si las máquinas deben eliminarse. Si debieran eliminarse, especifique qué medidas deben tomarse con las cuentas de equipo de Active Directory asociadas.

Cambiar de nombre o probar una conexión

1. Seleccione **Configuración > Alojamiento** en el panel de navegación de Studio.
2. Seleccione la conexión y luego seleccione **Cambiar nombre de la conexión** o **Probar conexión** en el panel Acciones.

Ver detalles de máquinas en una conexión

1. Seleccione **Configuración > Alojamiento** en el panel de navegación de Studio.
2. Seleccione la conexión y, a continuación, seleccione **Ver máquinas** en el panel Acciones.

El panel superior ofrece una lista de las máquinas a las que se accede a través de la conexión. Seleccione una máquina para ver información detallada sobre ella en el panel inferior. También se proporcionan detalles de sesión para las sesiones abiertas.

Utilice la función de búsqueda para encontrar máquinas rápidamente. Seleccione una búsqueda guardada en la lista que aparece en la parte superior de la ventana o cree una búsqueda nueva. Puede realizar la búsqueda con todo o parte del nombre de la máquina o puede crear una expresión y usarla para una búsqueda avanzada. Para crear una expresión, haga clic en **Expandir** y, a continuación, seleccione los elementos de las listas de propiedades y operadores.

Administrar máquinas en una conexión

1. Seleccione **Configuración > Alojamiento** en el panel de navegación de Studio.
2. Seleccione una conexión y, a continuación, seleccione **Ver máquinas** en el panel Acciones.
3. Seleccione una de las siguientes opciones en el panel Acciones. Es posible que algunas acciones no estén disponibles, según el estado de la máquina y el tipo de host de la conexión.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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.)
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. Solo puede eliminar una máquina cuando no hay ningún usuario conectado a ella (active el modo de mantenimiento para impedir temporalmente la conexión de usuarios durante el proceso de quitarla).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Acción	Descripción
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. Solo puede eliminar una máquina cuando no hay ningún usuario conectado a ella (active el modo de mantenimiento para impedir temporalmente la conexión de usuarios durante el proceso de quitarla).

Para acciones que implican el apagado de una máquina, si la máquina no se apaga en 10 minutos, se desconecta. Si Windows intenta instalar actualizaciones durante el cierre, existe el riesgo de que el equipo se apague antes de que se completen las actualizaciones.

Modificar la opción de almacenamiento

Puede mostrar el estado de los servidores que se usan para almacenar datos de sistema operativo, datos temporales y datos personales (PvD) para las VM que usan esa conexión. También puede especificar qué servidores usar para el almacenamiento de cada tipo de datos.

1. Seleccione Configuración > Alojamiento en el panel de navegación de Studio.
2. Seleccione la conexión y, a continuación, seleccione Modificar almacenamiento en el panel “Acciones”.
3. En el panel izquierdo, seleccione el tipo de datos: sistema operativo, Personal vDisk, o datos temporales.
4. Seleccione o deje sin seleccionar las casillas de los dispositivos de almacenamiento para el tipo de datos seleccionado.
5. Haga clic en 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 nuevas máquinas.
- **Reemplazado:** El almacenamiento se está usando solo para máquinas existentes. No se agregarán nuevas máquinas a este almacenamiento.
- **No utilizado:** El almacenamiento no se está utilizando para crear máquinas.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 nuevas máquinas.

Eliminar, cambiar el nombre o probar recursos

1. Seleccione **Configuración > Alojamiento** en el panel de navegación de Studio.
2. Seleccione el recurso y, a continuación, seleccione la entrada correspondiente en el panel Acciones: **Eliminar recursos**, **Cambiar nombre de recursos**, o **Probar recursos**.

Temporizadores de conexión

Puede usar configuraciones de directiva para configurar tres temporizadores de conexión:

- **Temporizador de duración máxima de conexión:** Determina la duración máxima de una conexión sin interrupciones entre un dispositivo de usuario y un escritorio virtual. Use las configuraciones de directiva **Temporizador de conexión de sesión** e **Intervalo de temporizador de conexión de sesiones**.
- **Temporizador de conexión inactiva:** Este parámetro determina la cantidad de tiempo que se mantendrá la conexión sin interrupciones entre un dispositivo de usuario y un escritorio virtual, si el usuario no realiza entradas. Use las configuraciones de directiva **Temporizador de sesión inactiva** e **Intervalo de temporizador de sesiones inactivas**.
- **Temporizador de desconexión:** Este parámetro determina la cantidad de tiempo que un escritorio virtual desconectado y bloqueado puede permanecer bloqueado antes de que se cierre la sesión. Use las configuraciones de directiva **Temporizador de sesión desconectada** e **Intervalo de temporizador de sesiones desconectadas**.

Al actualizar estos parámetros, compruebe que son coherentes en toda la implementación.

Consulte la documentación de configuraciones de directivas para obtener información.

Caché de host local

December 11, 2018

Para que la base de datos del sitio de Citrix Virtual Apps and Desktops esté siempre disponible, Citrix recomienda empezar con una implementación de SQL Server con tolerancia a fallos que resulta de las prácticas recomendadas para la alta disponibilidad de Microsoft. (Para ver las funcionalidades de alta disponibilidad de SQL Server que se admiten, consulte Bases de datos.) Sin embargo, las interrupciones y los problemas de red pueden tener como resultado que los usuarios no puedan conectarse a sus aplicaciones o escritorios.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

La función Caché de host local (LHC) permite que las operaciones de intermediación (broker) de las conexiones en un sitio continúen cuando se produce una interrupción. Se produce una interrupción cuando se interrumpe la conexión entre un Delivery Controller y la base de datos del sitio en un entorno local de Citrix.

A partir XenApp y XenDesktop 7.16, la Concesión de conexiones (una característica de alta disponibilidad en versiones anteriores) se eliminó de XenApp y XenDesktop, y ya no está disponible.

Contenido de datos

La Caché de host local incluye la siguiente información, que es un subconjunto de la información contenida en la base de datos principal:

- Identidades de los usuarios y los grupos que tienen derechos específicamente asignados a recursos publicados en el sitio.
- Identidades de los usuarios que actualmente usan, o que han utilizado recientemente, recursos publicados en el sitio.
- Identidades de las máquinas VDA (incluidas las máquinas de acceso con Remote PC) configuradas en el sitio.
- Identidades (nombres y direcciones IP) de las máquinas cliente de Citrix Receiver que se utilizan activamente para conectarse a los recursos publicados.

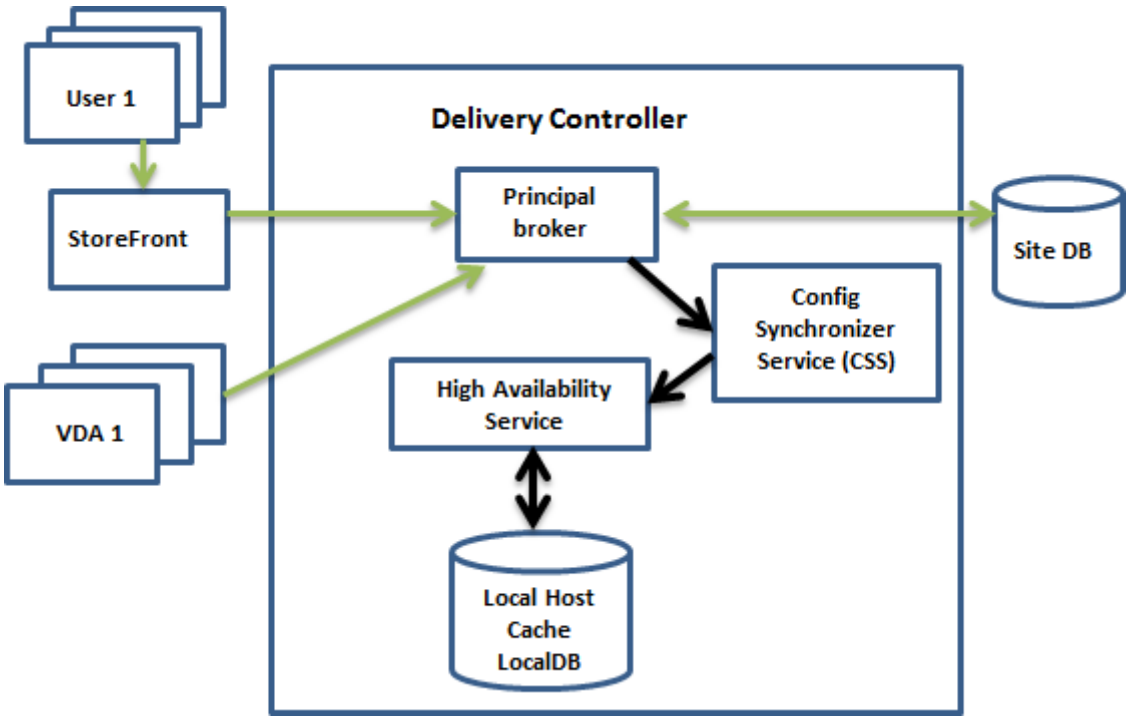
También contiene información para las conexiones actualmente activas que se establecieron mientras la base de datos principal no estaba disponible:

- Resultados de todos los análisis de máquinas de punto final del cliente realizados por Citrix Receiver.
- Identidades de las máquinas de la infraestructura (tales como NetScaler Gateway y servidores 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

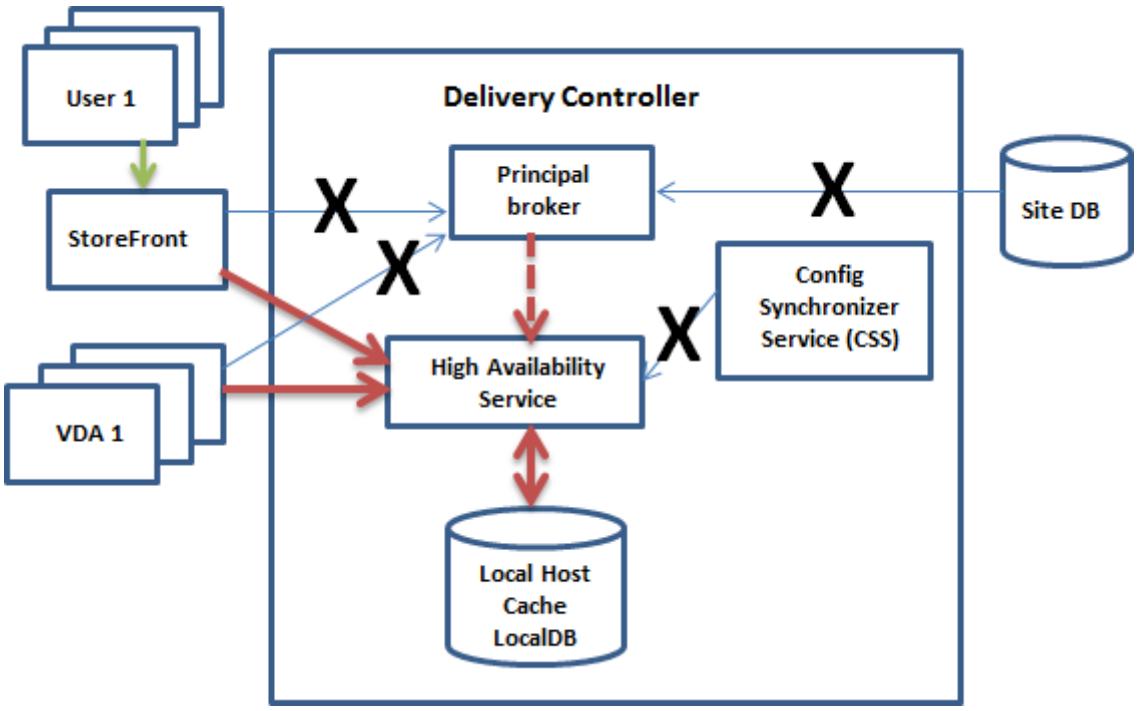


Durante el funcionamiento habitual:

- El *broker principal* (Citrix Broker Service) en un Controller acepta las solicitudes de conexión provenientes de StoreFront, y se comunica con la base de datos del sitio para conectar usuarios a los agentes VDA que están registrados en el Controller.
- Se comprueba periódicamente (un minuto después de la comprobación anterior) si se han realizado cambios en la configuración del broker principal. Esos cambios pueden haberse iniciado con acciones de PowerShell, de Studio (como modificar una propiedad del grupo de entrega) o del sistema (como las asignaciones de máquinas).
- Si se ha realizado algún cambio desde la última comprobación, el servicio Citrix Config Synchronizer Service (CSS) sincroniza (copia) información al servicio Citrix High Availability Service ubicado en el Controller. (En parte de la documentación, el servicio High Availability Service se denomina broker secundario.) Se copian todos los datos de configuración del broker, no solo los elementos que han cambiado desde la comprobación anterior. El servicio High Availability Service importa los datos en una base de datos LocalDB de Microsoft SQL Server Express ubicada en el Controller. El servicio CSS comprueba que la información de la base de datos LocalDB coincide con la información que hay en la base de datos del sitio. La base de datos LocalDB se crea con cada sincronización.
- Si no se han producido cambios desde la última comprobación, no se copian los datos.

En el siguiente gráfico, se muestran los cambios que se realizan en las rutas de comunicación si se interrumpe la conexión entre el broker principal y la base de datos del sitio:

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Cuando empieza una interrupción:

- El broker principal ya no puede comunicarse con la base de datos del sitio y deja de escuchar para obtener información de StoreFront y VDA (marcado con una X en el gráfico). El broker principal indica al servicio High Availability Service que empiece a escuchar y a procesar solicitudes de conexión (marcado con una línea discontinua de color rojo en el gráfico). El servicio High Availability Service descarta todas las llamadas provenientes del CSS.
- Cuando empieza la interrupción, el servicio High Availability Service no dispone de datos actuales de registro de agentes VDA, pero, en cuanto un VDA se comunica con él, comienza un proceso de re-registro. Durante este proceso, el servicio High Availability Service también obtiene información de sesión actualizada acerca de ese VDA.
- Mientras el servicio High Availability Service gestiona las conexiones, el broker principal sigue supervisando la conexión a la base de datos del sitio. Cuando se restaura la conexión, el broker principal indica al High Availability Service que deje de escuchar para obtener la información de conexión. A continuación, el broker principal reanuda la intermediación. La próxima vez que el VDA se comunica con el broker principal, comienza un proceso de re-registro. El servicio High Availability Service elimina toda información de registro de VDA que haya quedado de la interrupción anterior, y vuelve a actualizar la base de datos LocalDB con los cambios de configuración que ha recibido del servicio CSS.

La transición entre el modo normal y de interrupción no afecta a las sesiones existentes; solo afecta al inicio de sesiones nuevas.

En el caso improbable de que se inicie una interrupción durante una sincronización, la importación de ese momento se descarta y se utiliza la última configuración conocida.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

El registro de eventos proporciona información sobre sincronizaciones e interrupciones. Consulte la siguiente sección “Supervisar” para obtener más información.

También puede empezar intencionadamente una interrupción; consulte la siguiente sección “Forzar una interrupción” para obtener más información sobre cómo y por qué hacerlo.

Sitios con varios Controllers

Entre otras de sus tareas, CSS proporciona constantemente al servicio High Availability Service información sobre todos los Controllers de la zona. (Si su entorno no contiene varias zonas, esta acción afecta a todos los Controllers del sitio.) Con esta información, cada High Availability Service obtiene datos de todos los demás servicios High Availability Service de su nivel.

Los servicios High Availability Service se comunican entre sí por un canal independiente. Utilizan una lista alfabética de nombres de dominio completo (FQDN) de las máquinas que están ejecutando para determinar (elegir) al High Availability Service que estará a cargo de intermediar las operaciones de la zona si se produce una interrupción. Durante la interrupción, todos los VDA vuelven a registrarse en el High Availability Service que se haya elegido. Los servicios High Availability Service de la zona que no hayan sido elegidos rechazarán las solicitudes entrantes de conexión y de registro que les envíen los agentes VDA.

Si un High Availability Service falla durante una interrupción, se elige otro High Availability Service para tomar el control, y los VDA se volverán a registrar en el High Availability Service recién elegido.

Durante una interrupción, si se reinicia un Controller:

- Si ese Controller no es el broker principal elegido, el reinicio no tiene repercusión.
- Si ese Controller es el broker principal elegido, se elegirá otro Controller, por lo que los VDA deberán volver a registrarse. Después de que el Controller reiniciado se encienda, se hace cargo automáticamente de la intermediación, por lo que los VDA deben volver a registrarse. En este caso, el rendimiento puede verse afectado durante los nuevos registros.

Si apaga un Controller durante las operaciones normales y lo enciende durante una interrupción, la función Caché de host local no se puede utilizar en ese Controller si este se elige como broker principal.

El registro de eventos proporciona información sobre las opciones elegidas. Consulte la sección siguiente “Supervisión”.

Requisitos y consideraciones de diseño

No hay límites de tiempo impuestos para el funcionamiento en modo de interrupción. Sin embargo, debe restaurar el sitio a su funcionamiento normal lo más rápidamente posible.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Lo que no está disponible durante una interrupción y otras diferencias

- No puede usar Studio ni ejecutar cmdlets de PowerShell.
- Host Service no puede proporcionar credenciales de hipervisor. Todas las máquinas están en el estado de energía desconocido (unknown) y no se pueden emitir operaciones de administración de energía. No obstante, las máquinas virtuales del host que estén encendidas se pueden utilizar para las solicitudes de conexión.
- Una máquina asignada solo se puede usar si la asignación se dio durante el funcionamiento normal. No se pueden realizar asignaciones nuevas durante una interrupción.
- No se puede configurar ni inscribir automáticamente las máquinas de acceso con Remote PC. En cambio, las máquinas que se inscribieron y configuraron durante el funcionamiento normal se pueden usar.
- Si los recursos están en zonas diferentes, es posible que los usuarios de aplicaciones y escritorios alojados en servidor superen la cantidad de sesiones indicadas en el límite configurado de sesiones.
- Los usuarios solo pueden iniciar aplicaciones y escritorios desde los VDA registrados en la zona que contiene el High Availability Service actualmente activo o elegido. Durante una interrupción, no se admiten inicios entre zonas (desde un High Availability Service de una zona en un VDA de otra zona).

La función “Caché de host local” se admite para aplicaciones y escritorios alojados en servidores y escritorios estáticos (asignados).

De forma predeterminada, los escritorios VDA con la energía administrada que formen parte de grupos de entrega agrupados (creados con MCS o Citrix Provisioning) que tengan habilitada la propiedad “ShutdownDesktopsAfterUse” se colocan en el modo de mantenimiento cuando ocurre una interrupción. Puede cambiar este comportamiento predeterminado y permitir que esos escritorios se utilicen durante una interrupción. Sin embargo, no podrá confiar en la administración de energía durante la interrupción. (La administración de energía se reanuda una vez reanudadas las operaciones normales.) Además, esos escritorios podrían contener datos del usuario anterior, porque no ha sido reiniciados.

Para reemplazar el comportamiento predeterminado, debe habilitarlo en todo el sitio y para cada grupo de entrega afectado. Ejecute los siguientes cmdlets de PowerShell.

```
Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true Set-
BrokerDesktopGroup -Name ”name”-ReuseMachinesWithoutShutdownInOutage $true
```

Habilitar esta característica en el sitio y los grupos de entrega no afecta al funcionamiento de la propiedad configurada “ShutdownDesktopsAfterUse” durante las operaciones normales.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Consideraciones sobre tamaño de RAM

El servicio LocalDB puede usar aproximadamente 1,2 GB de RAM (1 GB máximo para la caché de la base de datos, más 200 MB para ejecutar LocalDB de SQL Server Express). El servicio High Availability Service puede usar hasta 1 GB de RAM si la interrupción es duradera y se producen muchos inicios de sesión (por ejemplo, 12 horas con 10 000 usuarios). Estos requisitos de memoria son adicionales a los requisitos de memoria RAM habituales para el Controller. Por lo tanto, es posible que necesite aumentar la cantidad total de RAM.

Tenga en cuenta que, si usa una base de datos de SQL Server Express como la base de datos del sitio, el servidor tendrá dos procesos sqlserver.exe.

Consideraciones sobre la configuración de sockets y núcleo de CPU

La configuración de la CPU de un Controller, especialmente la cantidad de núcleos disponibles para la base de datos LocalDB de SQL Server Express, afecta directamente al rendimiento que tendrá la Caché de host local, incluso más que la asignación de memoria. Este consumo de recursos de CPU solo se ha observado durante el periodo de interrupción cuando la base de datos no está disponible y el servicio High Availability Service está activo.

A pesar de que LocalDB pueda usar varios núcleos (hasta 4), está limitada a solamente un socket. Agregar más sockets no mejorará el rendimiento (por ejemplo, tener 4 sockets con 1 núcleo cada uno). En vez de ello, Citrix recomienda usar varios sockets con varios núcleos. En las pruebas llevadas a cabo por Citrix, una configuración de 2x3 (2 sockets, 3 núcleos) proporciona un mejor rendimiento que las configuraciones 4x1 y 6x1.

Consideraciones sobre almacenamiento

LocalDB aumenta de tamaño a medida que los usuarios acceden a los recursos durante una interrupción. Por ejemplo, durante una prueba de inicio y cierre de sesión en la que se ejecutan 10 inicios de sesión por segundo, la base de datos aumentó de tamaño 1 MB cada 2 o 3 minutos. Cuando se reanuda el funcionamiento normal, la base de datos local se vuelve a crear y el espacio se devuelve. No obstante, debe haber suficiente espacio en la unidad donde está instalada LocalDB para permitir el aumento del tamaño de la base de datos durante una interrupción. La Caché de host local también conlleva E/S adicional durante una interrupción: aproximadamente 3 MB de escrituras por segundo, con varios cientos de miles de lecturas.

Consideraciones sobre rendimiento

Durante una interrupción, un solo High Availability Service se encarga de todas las conexiones, por lo que, en los sitios (o las zonas) con carga equilibrada entre varios Controllers durante el

© 1999-2019 Citrix Systems, Inc. All rights reserved.

funcionamiento normal, es posible que el High Availability Service elegido deba gestionar muchas más solicitudes durante una interrupción que en una situación normal. Por lo tanto, la necesidad de CPU será mucho mayor. Cada High Availability Service del sitio (zona) debe ser capaz de gestionar la carga adicional que impone LocalDB y todos los VDA afectados porque el High Availability Service elegido durante una interrupción podría cambiar.

Límites de VDI:

- En una implementación de VDI de zona única, se puede controlar hasta 10 000 agentes VDA durante una interrupción.
- En una implementación de VDI de varias zonas, se puede controlar hasta 10 000 agentes VDA por zona durante una interrupción, hasta un máximo de 40 000 agentes VDA en el sitio. Por ejemplo, cada uno de los siguientes sitios puede controlarse de forma eficaz durante una interrupción:
  - Un sitio de cuatro zonas, cada zona con 10 000 agentes VDA.
  - Un sitio con siete zonas, una zona con 10 000 agentes VDA y seis zonas con 5 000 agentes VDA.

Durante una interrupción, la administración de carga dentro del sitio puede verse afectada. Es posible que se superen los patrones de carga (especialmente, las reglas de recuento de sesiones).

Mientras todos los VDA vuelven a registrarse en un High Availability Service, este puede no disponer de información completa sobre las sesiones actuales. Por lo tanto, si un usuario solicita conectarse durante ese intervalo, puede que se cree una nueva sesión aunque la reconexión a una sesión existente fuera posible. Este intervalo (mientras el "nuevo" High Availability Service obtiene la información de sesión de todos los VDA durante el proceso de re-registro) no se puede evitar. Tenga en cuenta que las sesiones que están conectadas cuando se inicia una interrupción no se verán afectadas durante ese intervalo de transición, pero las sesiones nuevas y las reconexiones sí pueden verse afectadas.

Este intervalo se da siempre que los VDA deben volver a registrarse:

- Comienza una interrupción: Al migrar desde un broker principal a un High Availability Service.
- Fallo del servicio High Availability Service durante una interrupción: Al migrar desde un servicio High Availability Service que falló al servicio High Availability Service recién elegido.
- Recuperación de una interrupción: Cuando se reanudan las operaciones normales y el broker principal retoma el control.

Puede reducir el intervalo si disminuye el valor de Registro HeartbeatPeriodMs del protocolo del broker de Citrix (el valor predeterminado es 600 000 ms, que equivale a 10 minutos). Este valor de latido es el doble del intervalo que usa el VDA para los pings, por lo que el valor predeterminado da como resultado un ping cada 5 minutos.

Por ejemplo, este comando cambia el latido a cinco minutos (300 000 milisegundos), lo que resulta en un ping cada 2 minutos y medio:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name HeartbeatPeriodMs
 -PropertyType DWORD -Value 300000
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Tenga cuidado al cambiar el valor de latido. Aumentar la frecuencia resulta en una mayor carga en los Controllers durante los modos de funcionamiento normal y el de interrupción.

El intervalo no se puede eliminar por completo, independientemente de lo rápido que se registren los VDA.

El tiempo que tarda la sincronización entre servicios High Availability Service aumenta con la cantidad de objetos (como agentes VDA, aplicaciones, grupos). Por ejemplo, sincronizar 5000 VDA podría llevar diez minutos o más. Consulte Supervisión para obtener información sobre las entradas de sincronización en el registro de eventos.

Diferencias con versiones de XenApp 6.x

Aunque esta implementación de Caché de host local comparte el nombre con la funcionalidad Caché de host local de XenApp 6.x y versiones anteriores de XenApp, existen entre ellas diferencias importantes. Esta implementación es más sólida e inmune al daño. Los requisitos de mantenimiento se han minimizado; por ejemplo, se ha eliminado la necesidad de comandos dsmaint periódicos. Técnicamente, esta implementación de Caché de host local es completamente diferente.

Administración de la Caché de host local

Para que la "Caché de host local" funcione correctamente, la directiva de ejecución de PowerShell en cada Controller debe establecerse en RemoteSigned, Unrestricted o Bypass.

LocalDB de SQL Server Express

La base de datos LocalDB de Microsoft SQL Server Express que usa la Caché de host local se instala automáticamente al instalar un Controller o actualizarlo desde una versión anterior a 7.9. No se necesita mantenimiento de administrador para la LocalDB. Only the High Availability Service communicates with this database. No puede usar cmdlets de PowerShell para realizar ningún cambio en esta base de datos. La LocalDB no se puede compartir entre los Controllers.

La base de datos LocalDB de SQL Server Express se instala independientemente de si la Caché de host local está habilitada.

Para impedir la instalación, instale o actualice el Controller con el comando XenDesktopServerSetup.exe e incluya la opción `/exclude "Local Host Cache Storage (LocalDB)"`. No obstante, tenga en cuenta que la función "Caché de host local" no funcionará sin la base de datos, y no se puede usar otra base de datos con el servicio High Availability Service.

Instalar esta base de datos LocalDB no influye en si instala SQL Server Express para usarla como la base de datos del sitio.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configuración predeterminada después de instalar y actualizar Citrix Virtual Apps o Citrix Virtual Desktops

La Caché de host local se habilita durante una nueva instalación de Citrix Virtual Apps and Desktops (7.16 como versión mínima). Después de una actualización (a la versión 7.16 o posterior), la Caché de host local se habilita si hay menos de 10 000 agentes VDA en toda la implementación.

Habilitar o inhabilitar la Caché de host local

- Para habilitar la Caché de host local, escriba:

  ```
  Set-BrokerSite -LocalHostCacheEnabled $true
  ```

  Para saber si la Caché de host local está habilitada, escriba:

  ```
  Get-BrokerSite
  ```

  Compruebe que la propiedad LocalHostCacheEnabled es True.

- Para inhabilitar la Caché de host local, escriba:

  ```
  Set-BrokerSite -LocalHostCacheEnabled $false
  ```

Recuerde: A partir de XenApp y XenDesktop 7.16, la concesión de conexiones (la característica que precedió a la Caché de host local desde la versión 7.6) se ha eliminado del producto y ya no está disponible.

Forzar una interrupción

Puede que le convenga forzar una interrupción de la base de datos.

- Si la red tiene altibajos repetidos. Forzar una interrupción hasta que se resuelvan los problemas de red impide una transición fluida entre los modos normal y de interrupción.
- Para probar un plan de recuperación ante desastres.
- Al cambiar o mantener el servidor de la base de datos del sitio.

Para forzar una interrupción, modifique el Registro de cada servidor que contiene un Delivery Controller. En HKLM\Software\Citrix\DesktopServer\LHC, establezca **OutageModeForced** en **1**. Esto indica al broker que introduzca el modo de interrupción independientemente del estado de la base de datos. (Establecer este valor en 0 saca al servidor del modo de interrupción.)

Supervisar

Los registros de eventos indican cuándo tienen lugar las sincronizaciones y las interrupciones.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Config Synchronizer Service:

Durante el funcionamiento normal, pueden ocurrir los siguientes eventos cuando CSS copia, exporta la configuración del broker y la importa a la LocalDB mediante High Availability Service.

- 503: Se ha encontrado un cambio en la configuración del broker principal, por lo que se inicia un proceso de importación.
- 504: La configuración del broker se ha copiado, exportado y, a continuación, importado a la LocalDB.
- 505: Ha fallado una importación a la LocalDB; consulte más adelante para obtener más información.
- 507: Se ha abandonado una importación debido a una interrupción pendiente. Si se inicia una interrupción durante una sincronización, la importación de ese momento se descarta y se utiliza la última configuración conocida.

High Availability Service (Servicio de alta disponibilidad):

- 3502: Se ha producido una interrupción y el servicio High Availability Service está llevando a cabo operaciones de intermediación.
- 3503: Se ha resuelto una interrupción y se ha reanudado el funcionamiento normal.
- 3504: Indica el servicio High Availability Service elegido, además de otros servicios que hayan participado en la elección.

Solucionar problemas

Existen varias herramientas de solución de problemas disponibles cuando falla una importación de sincronización a la LocalDB y se publica un evento 505.

Seguimiento CDF: Contiene opciones para los módulos ConfigSyncServer y BrokerLHC. Esas opciones, junto con otros módulos de broker, identificarán probablemente el problema.

Informe: Puede generar y proporcionar un informe que detalle el punto del error. Esta funcionalidad de informe afecta a la velocidad de sincronización, por lo que Citrix recomienda inhabilitarla cuando no se use.

Para habilitar y generar un informe de seguimiento de CSS, escriba:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -PropertyType DWORD -Value 1
```

El informe HTML se publica en C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerCor

Una vez generado el informe, inhabilite la funcionalidad de informes:

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -Value 0
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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`.

IP virtual y bucle invertido virtual

January 29, 2019

Esas características solo son válidas para máquinas de servidor Windows respaldadas. No se aplican a las máquinas con SO de escritorio Windows.

La función de dirección IP virtual de Microsoft proporciona una dirección IP exclusiva a una aplicación publicada, asignada dinámicamente para cada sesión. La función de bucle invertido virtual permite configurar aplicaciones que dependen de la comunicación con el host local (127.0.0.1 de forma predeterminada) para utilizar una dirección de bucle invertido virtual exclusiva en el rango del host local (127.*).

Algunas aplicaciones, como CRM y Computer Telephony Integration (CTI), utilizan una dirección IP para el direccionamiento, las licencias, la identificación y otros fines, y por lo tanto, requieren una dirección IP exclusiva o una dirección de bucle invertido en las sesiones. Otras aplicaciones pueden enlazar con un puerto estático, por lo que al intentar iniciar instancias adicionales de una aplicación en un entorno multiusuario, se producirá un error porque el puerto ya está en uso. Para que estas aplicaciones funcionen correctamente en un entorno Citrix Virtual Apps, se necesita una dirección IP exclusiva para cada dispositivo.

Las funciones de IP virtual y bucle invertido virtual son funciones independientes. Puede usar solo una de ellas o ambas.

Sinopsis de acciones de administrador:

- Para utilizar la dirección IP virtual de Microsoft, habilite y configure esta función en el servidor Windows. (No se necesitan configuraciones de directivas de Citrix).
- Para usar el bucle virtual de Citrix, configure dos parámetros en una directiva de Citrix.

IP virtual

Cuando la función IP virtual está habilitada y configurada en el servidor Windows, cada una de las aplicaciones configuradas que se ejecutan en una sesión parece tener una dirección exclusiva. Los usuarios acceden a dichas aplicaciones en un servidor Citrix Virtual Apps del mismo modo que acceden a cualquier otra aplicación publicada. Un proceso requiere IP virtual en cualquiera de los siguientes casos:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- El proceso utiliza un número de puerto TCP integrado en el código.
- El proceso utiliza Windows Sockets y requiere una dirección IP exclusiva o un número de puerto TCP específico.

Para determinar si una aplicación necesita utilizar direcciones IP virtuales:

1. Obtenga la herramienta TCPView de Microsoft. Esta herramienta muestra todas las aplicaciones que enlazan puertos y direcciones IP específicas.
2. Inhabilite la función de resolución de direcciones IP de forma que vea las direcciones en lugar de los nombres de host.
3. Ejecute la aplicación y con ayuda de TCPView consulte qué direcciones IP y puertos abre la aplicación y qué nombres de proceso abren estos puertos.
4. Configure los procesos que abren la dirección IP del servidor, 0.0.0.0 ó 127.0.0.1.
5. Para asegurarse de que la aplicación no abre la misma dirección IP en otro puerto, ejecute otra instancia de la aplicación.

Funcionamiento de la virtualización de IP de Escritorio remoto (RD) de Microsoft

- El uso de direcciones IP virtuales debe estar habilitado en el servidor de Microsoft.

  Por ejemplo, en un entorno de Windows Server 2008 R2, 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 usando el servidor DHCP (Dynamic Host Configuration Protocol) para cada sesión o cada programa. Consulte la documentación de Microsoft para obtener instrucciones.

- Después de habilitar la función, al comenzar una sesión, el servidor solicita al servidor DHCP las direcciones IP asignadas dinámicamente.

- La función de Virtualización de IP de Escritorio remoto asigna direcciones IP a las conexiones a escritorios remotos por sesión y por programa. Si se asignan direcciones IP para varios programas, éstos comparten una dirección IP por sesión.

- Después de asignar una dirección a una sesión, la sesión utiliza la dirección virtual en lugar de la dirección IP principal del sistema, siempre que se efectúan las siguientes llamadas: bind, closesocket, connect, WSAConnect, WSAAccept, getpeername, getsockname, sendto, WSASendTo, WSASocketW, gethostbyaddr, getnameinfo, getaddrinfo

Con la función de virtualización de IP de Microsoft en la configuración de host de sesiones de Escritorio remoto, las aplicaciones se vinculan con direcciones IP específicas mediante la introducción de un componente de “filtro” entre la aplicación y las llamadas de función de Winsock. La aplicación solo ve entonces la dirección IP que debe usar. Cualquier intento de la aplicación de escuchar comunicaciones TCP o UDP se vincula inmediatamente a su dirección IP virtual asignada (o dirección de

© 1999-2019 Citrix Systems, Inc. All rights reserved.

bucle invertido) y cualquier conexión de origen abierta por la aplicación se origina desde la dirección IP vinculada a la aplicación.

En funciones que devuelven una dirección, tales como GetAddrInfo() (que está controlada por una directiva de Windows), si se solicita la dirección IP local del host, la IP virtual examina la dirección IP devuelta y la cambia a la dirección IP virtual de la sesión. Las aplicaciones que intentan obtener la dirección IP del servidor local a través de dichas funciones de nombre solo ven la dirección IP virtual exclusiva asignada a dicha sesión. Esta dirección IP se utiliza con frecuencia en las posteriores llamadas de socket (tales como bind o connect). Para obtener más información acerca de las directivas de Windows, consulte Virtualización de IP de RDS en Windows Server.

A menudo una aplicación solicita vincularse a un puerto para escuchar en la dirección 0.0.0.0. En ese caso, si además la aplicación utiliza un puerto estático, no podrá ejecutar más de una instancia de la aplicación. La función de dirección IP virtual también busca 0.0.0.0 en estos tipos de llamada y cambia la llamada para escuchar en la dirección IP virtual específica, lo que permite que varias aplicaciones puedan escuchar en el mismo puerto en el mismo equipo, puesto que todas escuchan en diferentes direcciones. La llamada solo se cambia si se está en una sesión ICA y la función de dirección IP virtual está habilitada. Por ejemplo, si dos instancias de una aplicación que se ejecutan en distintas sesiones intentan vincularse a todas las interfaces (0.0.0.0) y un puerto específico, por ejemplo el 9000, se vinculan a VIPAddress1:9000 y VIPAddress2:9000, por lo que no existen conflictos.

Bucle invertido virtual

La habilitación de la configuración de directiva de Bucle invertido de IP virtual de Citrix permite que cada sesión disponga de su propia dirección de bucle invertido para las comunicaciones. Cuando una aplicación usa la dirección de host local (predeterminada = 127.0.0.1) en una llamada de Winsock, la función de bucle invertido virtual sencillamente sustituye 127.0.0.1 por 127.X.X.X, donde X.X.X es una representación del ID de sesión + 1. Por ejemplo, un ID de sesión de 7 es 127.0.0.8. En el caso improbable de que un ID de sesión fuera superior al cuarto octeto (más de 255), la dirección pasaría al octeto siguiente (127.0.1.0) hasta el máximo de 127.255.255.255.

Un proceso requiere el bucle invertido virtual en los siguientes casos:

- El proceso usa la dirección de bucle invertido de Windows Sockets del host local (127.0.0.1)
- El proceso utiliza un número de puerto TCP integrado en el código.

Use la
configuración de directiva de bucle invertido para aplicaciones que usan una dirección de bucle invertido para la comunicación entre procesos. No se requiere ninguna configuración adicional. La función de bucle invertido virtual no depende de la dirección IP virtual, de modo que no es necesario configurar el servidor de Microsoft.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Respaldo para bucle 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 desactivado 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 Respaldo para bucle invertido de IP virtual.

Funciones relacionadas

Se pueden usar los siguientes parámetros del Registro del sistema para garantizar que se da preferencia al bucle invertido sobre la IP virtual; esto se denomina bucle invertido preferido. Sin embargo, hay que actuar con precaución:

- Utilice el bucle invertido preferido solo cuando tanto IP virtual como Bucle invertido virtual están habilitados; en caso contrario, podría obtener resultados inesperados.
- Si modifica el Registro de forma incorrecta, pueden producirse problemas graves, que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Ejecute regedit en los servidores donde residen las aplicaciones.

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP
- Nombre: PreferLoopback, Tipo: REG_DWORD, Datos: 1
- Nombre: PreferLoopbackProcesses, Tipo: REG_MULTI_SZ, Datos: <lista de procesos>

Delivery Controllers

December 4, 2018

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **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 ofrecen la capacidad de administrar más usuarios y más solicitudes de aplicaciones y escritorios, además de mejorar la capacidad general de respuesta.

Cada Controller se comunica directamente con la base de datos del sitio. En un sitio con más de una zona, los Controllers de cada zona se comunican con la base de datos del sitio de la zona principal.

> **Importante:**
>
> No cambie el nombre de equipo ni la pertenencia al dominio de un Controller una vez configurado el sitio.

Cómo se registran los agentes VDA en Controllers

Para poder utilizar un VDA, este debe registrarse (establecer comunicación) con un Delivery Controller del sitio. Para obtener información sobre el registro de VDA, consulte Registro de VDA en Controllers.

Agregar, quitar o mover Controllers

Para agregar, quitar o mover un Controller, debe tener los permisos del rol de servidor y del rol de base de datos. Se ofrece una lista de esos permisos en el artículo *Bases de datos*.

No se admite la instalación de Controller en un nodo de clúster de SQL o de instalación duplicada (mirroring) de SQL.

Si la implementación usa la creación de reflejo de la base de datos:

- Antes de agregar, quitar o mover un Controller, compruebe que la base de datos principal y la reflejada se estén ejecutando. Además, si está usando scripts con SQL Server Management Studio, habilite el modo SQLCMD antes de ejecutar los scripts.
- Para verificar el reflejo después de agregar, quitar o mover un Controller, ejecute el cmdlet de PowerShell Get-configdbconnection para asegurarse de que el asociado de conmutación por error se ha definido en la cadena de conexión con la base de datos reflejada.

Después de agregar, quitar o mover un Controller:

- Si la actualización automática está habilitada, los VDA recibirán 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Controller a otro sitio, actualice la configuración de directiva o la clave del Registro en ambos sitios.

Agregar un Controller

Puede agregar Controllers al crear un sitio o más adelante. No puede agregar Controllers instalados con una versión anterior de este software a un sitio que se haya creado con esta versión.

1. Ejecute el instalador en un servidor con un sistema operativo compatible. Instale el componente Delivery Controller y los demás componentes principales que quiera. Complete el asistente de instalación.
2. Si aún no ha creado ningún sitio, inicie Studio; se le pedirá que cree un sitio. En la página Bases de datos del asistente para la creación de sitios, haga clic en el botón Seleccionar y, a continuación, agregue la dirección del servidor donde instaló el Controller adicional.

   Si va a generar scripts para inicializar bases de datos, agregue los Controllers antes de generarlos.
3. Si ya ha creado un sitio, indique en Studio el servidor donde instaló el Controller adicional. Haga clic en **Ampliar la implementación** e introduzca la dirección del sitio.

Quitar un Controller

Quitar un Controller de un sitio no desinstala el software de Citrix ni cualquier otro componente: solo se quita el Controller de la base de datos de forma que ya no se pueda usar para hacer de intermediario (broker) de conexiones ni 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 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. En caso de que ya no sea necesario, el inicio de sesión se debe quitar manualmente. Para hacerlo, se necesita el permiso del rol de servidor securityadmin.

> **Importante:**
>
> No quite el Controller de Active Directory hasta que lo haya quitado del sitio.

1. Compruebe que el Controller está ejecutándose de forma que Studio se cargue en menos de una hora. Una vez que Studio carga el Controller que quiere quitar, apague el Controller cuando lo pida el sistema.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

2. Seleccione **Configuración > Controllers** en el panel de navegación de Studio. A continuación, seleccione el Controller que quiere quitar.
3. Seleccione **Quitar Controller** en el panel Acciones. Si no dispone de los roles y permisos adecuados para la base de datos, se le ofrece la opción de generar un script que permite al administrador de bases de datos quitar el Controller por usted.
4. Es posible que necesite quitar la cuenta de la máquina del Controller del servidor de la base de datos. Antes de hacerlo, compruebe que no hay ningún otro servicio que esté usando la cuenta.

Después de usar Studio para quitar un Controller, el tráfico hacia ese Controller puede permanecer activo durante un corto período de tiempo para garantizar la correcta finalización de las tareas actuales. Si desea forzar la eliminación de un Controller en un período de tiempo muy corto, Citrix recomienda apagar el servidor donde se instaló o quitar ese servidor de Active Directory. A continuación, reinicie el resto de Controllers del sitio para asegurarse de que no hay más comunicaciones con el Controller que ha quitado.

Mover un Controller a otra zona

Si el sitio contiene más de una zona, puede mover un Controller a otra zona. Consulte el artículo *Zonas* para obtener información sobre cómo puede esto afectar al registro de VDA y otras operaciones.

1. Seleccione **Configuración > Controllers** en el panel de navegación de Studio. A continuación, seleccione el Controller que quiere mover.
2. Seleccione **Mover** en el panel Acciones.
3. Especifique la zona a la que quiere mover el Controller.

Mover un Controller a otro sitio

No puede mover un Controller a un sitio creado con una versión anterior del software.

1. En el sitio donde el Controller se encuentra actualmente (el que será el sitio antiguo), seleccione **Configuración > Controllers** en el panel de navegación de Studio y, a continuación, seleccione el Controller que quiera mover.
2. Seleccione **Quitar Controller** en el panel Acciones. Si no dispone de los roles y permisos adecuados para la base de datos, se le ofrece la opción de generar un script que permita a alguien con esos permisos (como un administrador de bases de datos) quitar el Controller por usted. Un sitio requiere como mínimo un Controller; esto significa que no puede quitar el último de la lista de Studio.
3. En el Controller que está moviendo, abra Studio, restablezca los servicios cuando el sistema se lo solicite, seleccione **Incorporarse a un sitio existente** e introduzca la dirección del sitio nuevo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 sitio porque MCS no respalda 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 con el sitio donde fueron creados.

Hay dos formas de mover un VDA a otro sitio: mediante el instalador o mediante directivas de Citrix.

Instalador

Ejecute el instalador y agregue un Controller, especificando el FQDN (entrada DNS) de un Controller en el sitio 2.

Especifique los Controllers en el instalador solo si la configuración de directiva de Controllers no se utiliza.

Editor de directivas de grupo

En el siguiente ejemplo se mueven varios VDA entre sitios.

1. Cree una directiva en el Sitio 1 que contenga la siguiente configuración y, a continuación, filtre la directiva al nivel de grupo de entrega para iniciar una migración de VDA entre sitios, por fases.
    - Contiene los nombres de dominio completo o FQDN (entradas de DNS) de uno o más Controllers del sitio 2.
    - Habilitar actualización automática de Controller: defínala como inhabilitada.
2. Cada VDA en el grupo de entrega recibe un aviso sobre la nueva directiva en los siguientes 90 minutos. El VDA ignora la lista de Controllers que recibe (porque la actualización automática está inhabilitada). 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. Puesto que el Controller con el que se registró el VDA en el sitio 1 no está en la lista enviada por el Controller del sitio 2, el VDA vuelve a registrarse y selecciona un Controller de la lista de Controllers del sitio 2. A partir de entonces, el VDA se actualiza automáticamente con la información del sitio 2.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Registro de VDA

March 8, 2019

Introducción

Para poder utilizar un VDA, este debe registrarse en (o establecer comunicación con) uno o varios Controllers o Cloud Connectors del sitio. (En una implementación local de Citrix Virtual Apps and Desktops, los VDA se registran en los Controllers. En una implementación de servicio de Citrix Virtual Apps and Desktops, los VDA se registran en Cloud Connectors.) El VDA busca un Controller o un Connector en una lista llamada *ListofDDCs*. En un VDA, la lista ListOfDDCs consta de entradas DNS que le indican los Controllers o Cloud Connectors del sitio. Para conseguir un equilibrio de carga, el VDA distribuye automáticamente las conexiones entre todos los Controllers o Cloud Connectors de la lista.

¿Por qué es tan importante que el VDA se registre?

- Desde el punto de vista de la seguridad, el registro es una operación confidencial. Se establece una conexión entre el Controller o Cloud Connector y el VDA. Para una operación confidencial, el comportamiento esperado es rechazar la conexión si algo no se cumple a la perfección. Se establecen dos canales independientes de comunicación: del VDA al Controller o Cloud Connector y del Controller o Cloud Connector al VDA. La conexión utiliza Kerberos, de modo que los problemas de sincronización horaria y los problemas de pertenencia a dominios son obstáculos que impiden la conexión. Kerberos utiliza nombres principales de servicio (SPN), por lo que no se puede usar IP ni nombre de host con carga equilibrada.
- Si un VDA no tiene 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 en un sitio), 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 la lista ListOfDDCs, la lista *ListOfSIDs* (identificadores de seguridad) indica qué máquinas de la lista ListOfDDCs son de confianza. La 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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. Esto se denomina registro inicial. Durante ese registro inicial, se crea una memoria caché persistente en el VDA. Durante los registros subsiguientes, el VDA obtiene la lista de Controllers o Cloud Connectors desde esa memoria caché local, a menos que se detecte un cambio de configuración.

La forma más fácil de recuperar esa lista en los registros subsiguientes es mediante la función de actualización automática. De forma predeterminada, la actualización automática está habilitada. Para obtener más información, consulte Actualización automática.

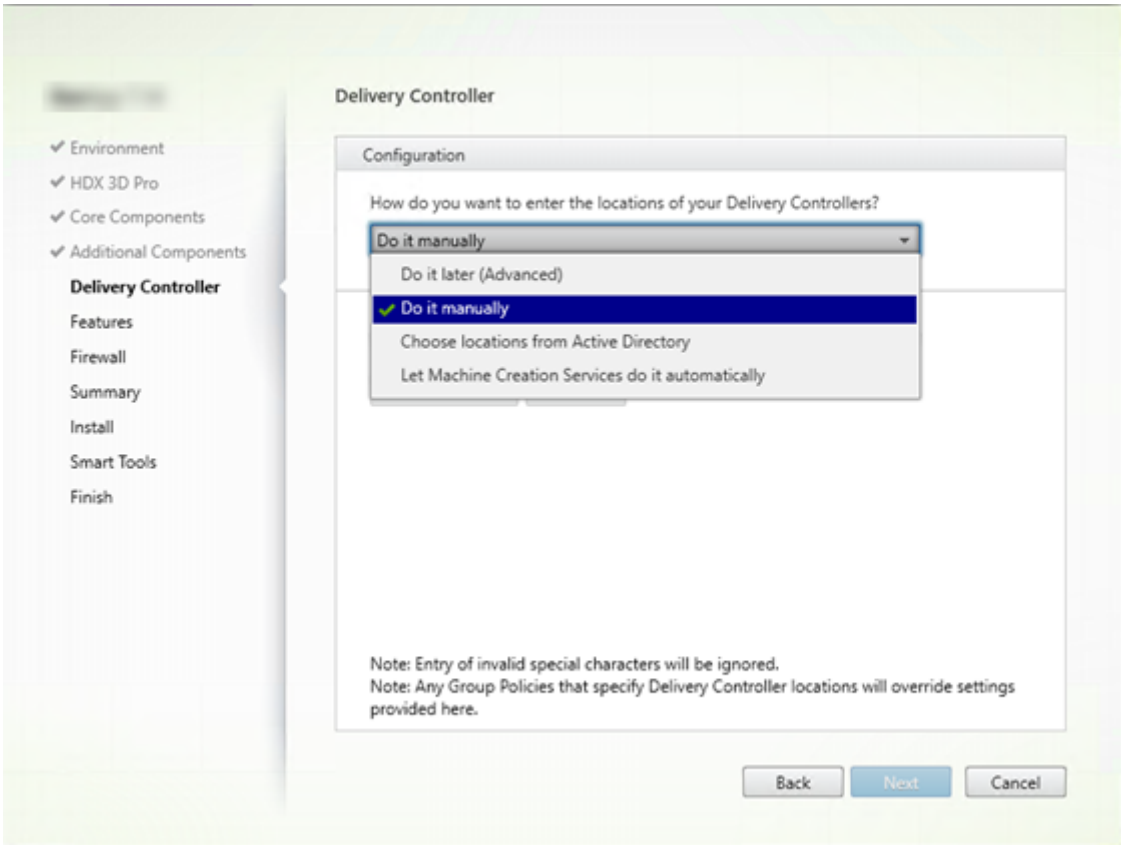
Existen varios métodos para configurar direcciones de Controller o Cloud Connector en un VDA.

- Método basado en directivas (LGPO o GPO)
- Método basado en el Registro (manual, GPP, direcciones especificadas durante la instalación de VDA)
- Método basado en unidades organizativas de Active Directory (detección de OU antiguas)
- Método basado en MCS (personality.ini)

El método de registro inicial se indica cuando se instala un VDA. (Si se inhabilita la actualización automática, el método seleccionado durante la instalación del VDA también se utilizará para los registros posteriores.)

En la siguiente imagen, se muestra la página **Delivery Controller** del Asistente de instalación de VDA.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Método basado en directivas (LGPO o GPO)

Citrix recomienda usar GPO para el registro inicial del VDA. Tiene la prioridad más alta. (Aunque la actualización automática se haya indicado como la máxima prioridad, solo se usa después del registro inicial.) El registro basado en directivas ofrece las ventajas de las directivas de grupo centralizadas para la configuración.

Para especificar este método, complete los dos siguientes pasos:

- En la página **Delivery Controller** del Asistente de instalación de VDA, seleccione **Hacerlo más tarde (Avanzado)**. El asistente le recordará varias veces que indique direcciones de Controller, incluso aunque no las indique durante la instalación del VDA. (Se lo recuerda porque el registro del VDA es sumamente importante.)
- Habilite o inhabilite el registro del VDA basado en directivas mediante la directiva de Citrix desde Virtual Delivery Agent > Parámetros > Controllers. (Si la seguridad es su prioridad principal, use la configuración: Virtual Delivery Agent > Parámetros > Identificadores SID de Controller.)

Esta configuración se almacena en HKLM\Software\Policies\Citrix\VirtualDesktopAgent (ListOfDDCs).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 Controllers adicionales, 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.

Por regla general, esta información se almacena en el valor del registro ListOfDDCs, en la clave de registro HKLM\Software\Citrix\VirtualDesktopAgent or 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 del Registro HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent contiene tanto la clave ListOfDDCs como la clave FarmGUID, la lista ListOfDDCs se utiliza para la detección de Controllers o Cloud Connectors. FarmGUID está presente si la OU de un sitio se especificó durante la instalación del VDA. (Puede usarlo en implementaciones antiguas.)

Si lo prefiere, puede actualizar la clave del registro de 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**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Use el script `Set-ADControllerDiscovery.ps1` (disponible en cada Controller). Además, configure la entrada del registro FarmGuid en cada VDA para que apunte a la OU correspondiente. Esta configuración puede configurarse mediante la directiva de grupo.

Para obtener más información, consulte Detección basada en unidades organizativas de Active Directory.

Método basado en MCS

Si solo va a usar MCS para aprovisionar las VM, puede indicar a MCS que configure la lista de Controllers o Cloud Connectors. Esta característica funciona con la actualización automática: MCS inserta la lista de Controllers o Cloud Connectors en el archivo Personality.ini durante el aprovisionamiento inicial (al crear el catálogo de máquinas). La actualización automática mantiene la lista actualizada.

No se recomienda este método para entornos de gran tamaño. Puede usar este método si:

- Dispone de un entorno pequeño
- No mueve agentes VDA de un sitio a otro
- Solo usa MCS para aprovisionar las VM
- No quiere usar la directiva de grupo

Para especificar este método, en la página **Delivery Controller** del Asistente de instalación de VDA, seleccione **Dejar que Machine Creation Services lo haga**.

Recomendaciones

Como práctica recomendada:

- Use el método del registro basado en la directiva de grupo para el registro inicial.
- Use la actualización automática (habilitada de forma predeterminada) para mantener actualizada su lista de Controllers.
- En una implementación de varias zonas, use la directiva de grupo para la configuración inicial (con al menos dos Controllers o Cloud Connectors). Apunte los agentes VDA a los Controllers o Cloud Connectors locales de la zona. Utilice la actualización automática para mantenerlos actualizados. La actualización automática optimiza automáticamente la lista ListOfDDCs para agentes VDA en las zonas satélite.
- Incluya más de un Controller en la clave de Registro ListOfDDCs, separados por un espacio para evitar problemas de registro si un Controller no está disponible.

  Ejemplo:

  DDC7x.xd.local DDC7xHA.xd.local

© 1999-2019 Citrix Systems, Inc. All rights reserved.

32 bits: HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\ListOfDDCs

HKEY_LOCAL_MACHINE \Software\Citrix\VirtualDesktopAgent\ListOfDDCs (REG_SZ)

- Compruebe que todos los valores enumerados en ListOfDDCs se asignen a un nombre de dominio completo y válido para evitar retrasos en el registro de inicios.

Actualización automática

Introducida desde XenApp y XenDesktop 7.6, la actualización automática está habilitada de forma predeterminada. Es el método más eficaz para mantener actualizados los registros de VDA. A pesar de que la actualización automática no se utilice para el registro inicial, el software de la actualización automática descarga y almacena la lista ListOfDDCs en una caché persistente en el VDA cuando se produce el registro inicial. Esto se lleva a cabo para cada VDA. (Esta memoria caché también contiene información de directivas de máquina que garantizan que las configuraciones de directiva se conserven después de reiniciar.)

Se respalda la actualización automática cuando se utiliza MCS o Citrix Provisioning para aprovisionar las máquinas, salvo para la caché del servidor Citrix Provisioning (que no es un caso frecuente porque no hay almacenamiento persistente para la caché de actualización automática).

Para especificar este método:

- Habilite o inhabilite la actualización automática a través de una directiva de Citrix que contiene la configuración: Virtual Delivery Agent > Parámetros > Habilitar actualización automática de Controllers. Este parámetro está habilitado 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).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- 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 respaldo. 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 respaldada.

```
Get-WmiObject -Namespace "Root\Citrix\DesktopInformation" -Class "Citrix_VirtualDeskt
" -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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Excepción a la prioridad de actualización automática

Aunque normalmente la actualización automática tiene la prioridad más alta de todos los métodos de registro de VDA y anula la configuración de los demás métodos, existe una excepción. Los elementos NonAutoListOfDDCs en la memoria caché especifican el método inicial de configuración de VDA. La actualización automática supervisa esta información. Si cambia el método de registro inicial, el proceso de registro omite la actualización automática y usa el siguiente método de configuración de prioridad más alta. Esto puede ser útil cuando se mueve un VDA a otro sitio (por ejemplo, durante la recuperación ante desastres).

Consideraciones sobre la configuración

Tenga en cuenta lo siguiente al configurar los elementos que pueden afectar el registro de VDA.

Direcciones de Controller o Cloud Connector

Independientemente del método que utilice para especificar Controllers o Cloud Connectors, Citrix recomienda usar una dirección FQDN. Una dirección IP no se considera una configuración de confianza, porque es más fácil interceptar una IP que un registro DNS. Si rellena manualmente la lista ListOfSIDs, puede usar una IP en una lista ListOfDDCs. Aun así, se recomienda el FQDN.

Equilibrio de carga

Como se ha indicado anteriormente, el VDA distribuye automáticamente las conexiones entre todos los Controllers o Cloud Connectors de la lista ListOfDDCs. La funcionalidad de equilibrio de carga y conmutación por error se ha integrado en el protocolo Citrix Brokering Protocol (CBP). Si especifica varios Controllers o Cloud Connectors en la configuración, el registro conmuta por error automáticamente entre ellos, si fuera necesario. Con la actualización automática, la conmutación por error automática se produce automáticamente para todos los VDA.

Por motivos de seguridad, no puede usar ningún equilibrador de carga de red, como Citrix ADC. En el registro del VDA, se utiliza la autenticación mutua de Kerberos, donde el cliente (VDA) debe demostrar su identidad al servicio (Controller). No obstante, el Controller o Cloud Connector también debe demostrar su identidad al VDA. Eso significa que el VDA y el Controller o Cloud Connector actúan como cliente y servidor al mismo tiempo. Como se ha indicado al principio de este artículo, hay dos canales de comunicación: VDA -> Controller/Cloud Connector y Controller/Cloud Connector -> 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”

© 1999-2019 Citrix Systems, Inc. All rights reserved.

quiere comunicarse; esa 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 usando Kerberos

La actualización automática reemplaza CNAME

La función de actualización automática sustituye a la función CNAME (alias de DNS) desde versiones de XenApp y XenDesktop anteriores a 7.x. La función CNAME se inhabilitó a partir de XenApp y XenDesktop 7. Utilice la actualización automática en lugar de CNAME. (Si le es necesario usar CNAME, consulte CTX137960. Para que el alias de DNS funcione de manera coherente, no use la actualización automática y CNAME al mismo tiempo.)

Grupos de Controllers o Cloud Connectors

En ciertos casos, puede que le interese procesar a los Controllers o Cloud Connectors por grupos, donde un grupo es el preferente y el otro se utiliza para una conmutación por error si fallan todos los Controllers o Cloud Connectors del primer grupo. Recuerde que los Controllers o Cloud Connectors se seleccionan aleatoriamente de la lista; por tanto, agruparlos puede fomentar la preferencia de un grupo sobre otro.

Estos grupos están diseñados para ser utilizados dentro de un único sitio (no en múltiples sitios).

Use paréntesis para especificar grupos de Controllers o Cloud Connectors. Por ejemplo, con cuatro Controllers (dos primarios y dos de respaldo), 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 realizar para usar la función **Grupos de registro**. Debe prohibir la directiva de Citrix Studio **Habilitar la actualización automática de Controller**

ListOfSIDs

La lista de Controllers con los que un VDA puede contactar para el registro se llama ListOfDDCs. 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 usar un seguimiento CDF para leer la lista ListOfSIDs.

Por lo general, no es necesario modificar manualmente la lista ListOfSIDs. Sin embargo, existen varias excepciones a ello. Las dos primeras excepciones ya no son válidas, porque están disponibles tecnologías más recientes.

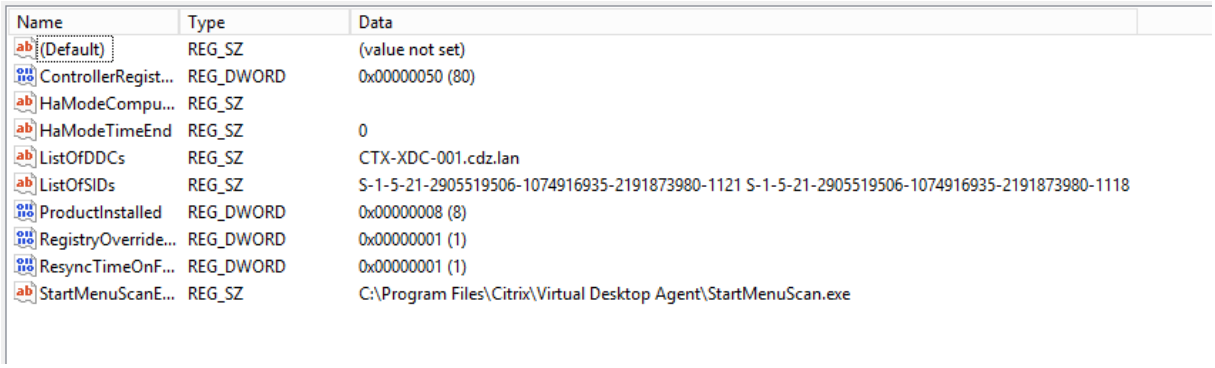
- **Separar roles para los Controllers:** Antes de que se introdujeran las zonas en XenApp y XenDesktop 7.7, la lista ListOfSIDs se configuraba manualmente cuando solo se utilizaba un subconjunto de los Controllers para el registro. Por ejemplo: si se utilizaba XDC-001 y XDC-002 como brokers XML, y XDC-003 y XDC-004 para el registro de VDA, se especificaban todos los Controllers en la lista ListOfSIDs, y XDC-003 y XDC-004 se indicaban en la lista ListOfDDCs. Ésta no es una configuración típica ni recomendada, y no debe utilizarse en entornos más recientes. En su lugar, use las zonas.
- **Reducir la carga de Active Directory:** Antes de que se introdujera la función de actualización automática en XenApp y XenDesktop 7.6, la lista ListOfSIDs se utilizaba para reducir la carga de los controladores de dominio. Al rellenarse previamente la lista ListOfSIDs, no se podía 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 le es necesario modificar la lista ListOfSIDs, cree una clave de registro denominada 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).

© 1999-2019 Citrix Systems, Inc. All rights reserved.



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

Solucionar problemas en el registro de VDA

Como se ha indicado anteriormente, un VDA debe registrarse en un Delivery Controller para que se le tenga en cuenta al iniciar sesiones con broker. Los VDA no registrados pueden derivar en una 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 podido obtener información acerca de una máquina (posiblemente porque nunca se ha registrado en un Delivery Controller), puede optar por agregarla de todos modos.

  Con el nivel funcional de un catálogo, decide qué funciones de producto están disponibles para las máquinas del catálogo. Para poder usar las funciones introducidas en las nuevas versiones de producto, es posible que necesite un nuevo VDA. Establecer un nivel funcional permite que todas las funcionalidades introducidas en esa versión (y versiones posteriores, si el nivel funcional no cambia) estén disponibles para las máquinas del catálogo. Sin embargo, las máquinas de ese catálogo que tengan una versión anterior de VDA no podrán registrarse.

- **Identificación de problemas después de crear los grupos de entrega:** Después de crear un grupo de entrega, Studio muestra información sobre las máquinas asociadas a ese grupo. El panel de detalles de un grupo de entrega indica la cantidad de máquinas que deberían estar registradas pero no se han registrado. En otras palabras, una o varias máquinas que están activadas y no están en modo de mantenimiento, pero no están actualmente registradas en el Controller. Al ver una máquina que “no está registrada pero debería estarlo”, consulte la ficha

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Solución de problemas del panel “Detalles”, porque ahí se ofrecen las posibles causas y las acciones correctivas recomendadas.

Más información sobre la solución de problemas de registro de VDA

- Para obtener más información acerca de niveles funcionales, consulte la sección Versiones de VDA y niveles funcionales.
- Para obtener más información sobre la solución de problemas de registro de VDA, consulte CTX136668.
- También puede usar Citrix Health Assistant para solucionar problemas de inicio de sesiones y registro de VDA. Para obtener más información, consulte CTX207624.

Sesiones

December 11, 2018

El mantenimiento de la actividad de las sesiones es fundamental para ofrecer la mejor experiencia de uso. La pérdida de conectividad debido a redes poco fiables, a una latencia de red muy variable y a limitaciones del alcance de los dispositivos inalámbricos puede provocar frustración en el usuario. Poder cambiar rápidamente de una estación de trabajo a otra y acceder al mismo conjunto de aplicaciones cada vez que se inicie sesión es prioritario para muchos empleados móviles, como sería el caso de los empleados de un hospital.

Las funciones que se describen en este artículo optimizan la fiabilidad de las sesiones y reducen las molestias, los periodos de inactividad y la pérdida de productividad; con estas funciones, los usuarios móviles pueden trasladarse de unos equipos a otros fácil y rápidamente.

Además, puede cerrar la sesión o desconectar a un usuario, así como configurar el preinicio y la persistencia de sesiones. Para obtener más información, consulte Administrar grupos de entrega.

Fiabilidad de la sesión

La fiabilidad de la sesión mantiene las sesiones activas y en la pantalla de los usuarios cuando se interrumpe la conexión de red. Los usuarios siguen viendo la aplicación que están utilizando hasta que vuelve la conexión.

Esta función es especialmente útil para usuarios móviles con conexiones inalámbricas. Pensemos, por ejemplo, en un usuario con una conexión inalámbrica que se encuentra viajando en un tren y entra en un túnel, y pierde por un momento la conectividad. Por lo general, la sesión se desconecta y desaparece de la pantalla del usuario y después debe volver a conectarse. Con la función Fiabilidad de

© 1999-2019 Citrix Systems, Inc. All rights reserved.

la sesión, la sesión permanece activa en la máquina. Para indicar que se ha perdido la conectividad, la pantalla del usuario se congela y el cursor se convierte en un reloj de arena giratorio hasta que se recupera la conectividad al salir del túnel. El usuario sigue teniendo acceso a la presentación en pantalla durante la interrupción y puede reanudar la interacción con la aplicación después de restablecerse la conexión de red. La función Fiabilidad de la sesión vuelve a conectar a los usuarios sin pedirles que repitan la autenticación.

Los usuarios de la aplicación Citrix Workspace no pueden anular la configuración de Controller.

Puede usar la función de fiabilidad de la sesión con Transport Layer Security (TLS). TLS cifra solo los datos enviados entre el dispositivo de usuario y Citrix Gateway.

Habilite y configure la fiabilidad de la sesión con las siguientes configuraciones de directiva:

- La configuración de directiva Conexiones de fiabilidad de la sesión permite o impide la fiabilidad de la sesión.
- La configuración de directiva Tiempo de espera de fiabilidad de la sesión tiene un tiempo predeterminado de 180 segundos, o tres minutos. Aunque puede ampliar la cantidad de tiempo que Fiabilidad de la sesión mantiene abierta una sesión, esta función está diseñada para la comodidad del usuario, por lo que no pedirá a éste que repita la autenticación. Si se alarga la cantidad de tiempo que una sesión se mantiene abierta, se incrementa el riesgo de que un usuario se distraiga, se aleje del dispositivo y con ello facilite a usuarios no autorizados el acceso a la sesión.
- Las conexiones entrantes de fiabilidad de la sesión utilizan el puerto 2598 a menos que usted cambie el número de puerto definido en la configuración de directiva Número de puerto para fiabilidad de la sesión.
- Si no desea que los usuarios se reconecten con sesiones interrumpidas sin tener que repetir la autenticación, use la función Reconexión automática de clientes. Puede definir la configuración de directiva Autenticación para reconexión automática de clientes para 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

En sesiones de aplicación, la aplicación Citrix Workspace trata de reconectarse a la sesión hasta que lo logra o el usuario cancela el intento de reconexión.

En sesiones de escritorio, la aplicación Citrix Workspace intenta reconectarse a la sesión durante un período de tiempo especificado a menos que lo logre o el usuario cancele el intento de reconexión. De forma predeterminada, este período es de cinco minutos. Para cambiar este período de tiempo, modifique el Registro en el dispositivo de usuario:

HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;<seconds>

donde <*seconds*> es la cantidad de segundos después de los que no hay más intentos para volver a conectarse a la sesión.

Habilite y configure la Reconexión automática de clientes con las siguientes configuraciones de directiva:

- **Reconexión automática de clientes:** Habilita o inhabilita la reconexión automática de la aplicación Citrix Workspace cuando una sesión se ve interrumpida.
- **Autenticación para reconexión automática de clientes:** Habilita o inhabilita el requisito de autenticación del usuario después de la reconexión automática.
- **Registro de reconexión automática de clientes:** Habilita o inhabilita el registro de sucesos de reconexión en el registro de sucesos. El registro de sucesos está inhabilitado de forma predeterminada. Si está habilitado, los registros de sistema del servidor capturan información sobre sucesos de reconexión automática correctos y fallidos. Cada servidor almacena información sobre los sucesos de reconexión en su propio registro de sistema; el sitio no proporciona los registros combinados de sucesos de reconexión en todos los servidores.

Reconexión automática de clientes incorpora un mecanismo de autenticación basado en credenciales de usuario cifradas. Cuando un usuario inicia una primera sesión, el servidor cifra y guarda en memoria las credenciales de usuario, y crea y envía a la aplicación Citrix Workspace una cookie que contiene la clave de cifrado. La aplicación Citrix Workspace envía la clave al servidor para la reconexión. El servidor descifra las credenciales y las envía al inicio de sesión de Windows para su autenticación. Cuando caducan las cookies, los usuarios deben repetir la autenticación para volver a conectarse a las sesiones.

Las cookies no se usan si se habilita la configuración Autenticación para reconexión automática de clientes. En este caso, en su lugar, los usuarios ven un cuadro de diálogo que les solicita sus credenciales cuando la aplicación Citrix Workspace intenta reconectarse automáticamente.

Para lograr la máxima protección de las credenciales y las sesiones del usuario, utilice el cifrado para todas las comunicaciones entre los clientes y el sitio.

Inhabilite la función Reconexión automática de clientes en la aplicación Citrix Workspace para Windows mediante el archivo icaclient.adm. Para obtener más información, consulte la documentación correspondiente a su versión de la aplicación Citrix Workspace para Windows.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Las configuraciones de las conexiones también influyen en la función de reconexión automática de clientes:

- De forma predeterminada, la reconexión automática de clientes se habilita a través de las configuraciones de directiva en el nivel del sitio, como se describe anteriormente. No es necesario repetir la autenticación de los usuarios. Sin embargo, si la conexión ICA TCP del servidor está configurada para restablecer sesiones con un vínculo de comunicación interrumpido, la reconexión automática no se produce. La reconexión automática de clientes sólo funciona si el servidor desconecta sesiones cuando existe alguna conexión interrumpida o que ha superado el tiempo de espera. En este contexto, la conexión ICA TCP hace referencia a un puerto virtual del servidor (en lugar de una conexión de red real) que se utiliza para las sesiones en redes TCP/IP.
- De manera predeterminada, la conexión ICA TCP de un servidor está configurada para desconectar sesiones cuya conexión se haya interrumpido o haya superado el tiempo de espera. Las sesiones desconectadas permanecen intactas en la memoria del sistema y la aplicación Citrix Workspace puede volver a conectarse a ellas.
- La conexión se puede configurar para restablecer o cerrar sesiones cuya conexión se haya interrumpido o haya superado el tiempo de espera. Si una sesión se restablece, los intentos de reconexión inician una nueva sesión; es decir, en lugar de restaurar al usuario a la posición en que se encontraba la aplicación que estaba utilizando, la aplicación se reinicia.
- Si el servidor está configurado para restablecer sesiones, la reconexión automática de clientes crea una sesión nueva. En este proceso, el usuario debe introducir sus credenciales para iniciar sesión en el servidor.
- Es posible que la reconexión automática no se lleve a cabo si la aplicación Citrix Workspace o el plugin envían una información de autenticación incorrecta; por ejemplo, durante un ataque o si el servidor determina que ha transcurrido demasiado tiempo desde que se detectó la interrupción de la conexión.

ICA Keep-Alive

La habilitación de ICA Keep-Alive impide que las conexiones interrumpidas se desconecten. Cuando esta función está habilitada, si el servidor detecta que no hay actividad (por ejemplo, no hay cambios en el reloj, no hay movimientos del puntero ni actualizaciones de pantalla), esta función impide que Servicios de Escritorio remoto desconecte la sesión. El servidor envía paquetes de Keep-Alive cada pocos segundos a fin de detectar si la sesión está activa. Si la sesión ya no está activa, el servidor la marca como desconectada.

> **Importante:**
>
> La función ICA Keep-Alive solo funciona si no se usa la función Fiabilidad de la sesión. Fiabilidad de la sesión tiene su propio mecanismo para impedir que las conexiones interrumpidas se desconecten. Configure ICA Keep-Alive únicamente para las conexiones que no usen Fiabilidad de

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> la sesión.

Los parámetros de ICA Keep-Alive sobrescriben los parámetros de Keep-Alive configurados en la directiva de grupo de Microsoft Windows.

Habilite y configure ICA Keep-Alive con las siguientes configuraciones de directiva:

- **Tiempo de espera de ICA Keep Alive:** Especifica el intervalo de envío de mensajes de ICA Keep-Alive (de 1 a 3600 segundos). No seleccione esta opción si desea que su software de supervisión de red cierre las conexiones inactivas en los entornos en los que las conexiones interrumpidas son tan poco frecuentes que permitir que los usuarios se vuelvan a conectar a las sesiones no es relevante.

  El intervalo predeterminado es 60 segundos: los paquetes de ICA Keep-Alive se envían a los dispositivos de usuario cada 60 segundos. Si un dispositivo del usuario no responde en 60 segundos, el estado de las sesiones ICA cambia a "Desconectado".

- **ICA Keep Alive:** Envía o impide el envío de mensajes de ICA Keep-Alive.

Control del espacio de trabajo

Con el control del espacio de trabajo, los escritorios y las aplicaciones permanecen disponibles para el usuario cuando éste pasa de un dispositivo a otro. Esta capacidad para moverse entre dispositivos permite que un usuario pueda acceder a todos sus escritorios o aplicaciones abiertas, desde cualquier lugar, simplemente iniciando una sesión, sin tener que reiniciar dichos escritorios y aplicaciones cuando cambia de dispositivo. Por ejemplo, el control del espacio de trabajo puede ser muy útil para los trabajadores de un hospital, que se desplazan rápidamente entre estaciones de trabajo y necesitan acceder al mismo conjunto de aplicaciones cada vez que inician una sesión. Si configura las opciones de control del espacio de trabajo con este propósito, estos trabajadores pueden desconectarse de varias aplicaciones en un dispositivo cliente y reconectarse a las mismas en un dispositivo cliente distinto.

El control del espacio de trabajo afecta a las siguientes actividades:

- **Inicio de sesión:** De manera predeterminada, el control del espacio de trabajo permite a los usuarios reconectarse automáticamente a todos los escritorios y las aplicaciones que estén ejecutándose simplemente iniciando una sesión, sin tener que volver a abrirlos manualmente. Mediante el control del espacio de trabajo, los usuarios pueden abrir aplicaciones y escritorios desconectados, así como otros que estén activos en otro dispositivo cliente. Cuando el usuario se desconecta de una aplicación o de un escritorio, estos siguen ejecutándose en el servidor. Si hay usuarios móviles que necesitan mantener en ejecución ciertas aplicaciones o escritorios en un dispositivo cliente, mientras se reconectan con un subconjunto de sus aplicaciones y escritorios en otro dispositivo cliente distinto, puede configurar el comportamiento de reconex-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

ión durante el inicio de sesión para que se abran solo los escritorios y aplicaciones de los que se haya desconectado el usuario anteriormente.

- **Reconexión:** Después de iniciar una sesión en el servidor, los usuarios pueden reconectarse a todos sus escritorios o aplicaciones en cualquier momento haciendo clic en Reconectar. De manera predeterminada, la función Reconectar abre los escritorios y aplicaciones desconectados, además de los que estén ejecutándose en ese momento en otro dispositivo cliente. Puede configurar la función Reconectar para que abra solo los escritorios y aplicaciones de los que se desconectó el usuario anteriormente.
- **Cierre de sesión:** En el caso de usuarios que abren aplicaciones o escritorios mediante StoreFront, puede configurar el comando Cerrar sesión para que el usuario cierre su sesión en StoreFront y en todas las sesiones activas conjuntamente, o bien para que solo cierre la sesión en StoreFront.
- **Desconexión:** Los usuarios se pueden desconectar de todos los escritorios y aplicaciones a la vez, sin necesidad de desconectarse de cada uno de ellos individualmente.

El control del espacio de trabajo solamente está disponible para los usuarios de la aplicación Citrix Workspace que acceden a escritorios y aplicaciones a través de una conexión de Citrix StoreFront. De manera predeterminada, el control del espacio de trabajo está inhabilitado para las sesiones de escritorio virtual, pero está habilitado para las aplicaciones alojadas en servidores. El uso compartido de sesiones no se produce de manera predeterminada entre los escritorios publicados y las aplicaciones publicadas que se ejecutan en esos escritorios.

Las directivas de usuario, asignaciones de unidad cliente y configuraciones de impresora cambian según sea necesario al cambiar el usuario de dispositivo cliente. Las directivas y asignaciones se aplican según el dispositivo cliente donde el usuario haya iniciado sesión. Por ejemplo, si un trabajador cierra sesión en un dispositivo cliente en el área de Urgencias del hospital y luego inicia una sesión en una estación de trabajo del Laboratorio de rayos X, las directivas, las asignaciones de impresora y las asignaciones de unidades del cliente adecuadas para la sesión en el Laboratorio de rayos X entran en efecto en el momento en que se inicia esa nueva sesión.

Puede personalizar qué impresoras se muestran a los usuarios cuando éstos cambian de ubicación. También puede controlar si los usuarios pueden imprimir en impresoras locales, cuánto ancho de banda pueden consumir cuando se conectan de forma remota, así como otros aspectos de la impresión.

Si desea más información sobre cómo habilitar y configurar el control del espacio de trabajo para los usuarios, consulte la documentación de StoreFront.

Movilidad de sesión

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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

sesión y las aplicaciones están disponibles en ambos dispositivos. Las aplicaciones se mueven, independientemente del dispositivo o de si las sesiones actuales existen. En muchos casos, las impresoras y otros recursos asignados a la aplicación también se mueven.

Aunque este comportamiento predeterminado ofrece muchas ventajas, es posible que no sea el mejor para todos los casos. Puede impedir la movilidad de sesión mediante el SDK de PowerShell.

Ejemplo 1. Un miembro del personal médico usa dos dispositivos: uno para completar un formulario del seguro en un equipo de escritorio y otro para consultar información sobre un paciente en una tableta.

- Si la movilidad de sesión está habilitada, ambas aplicaciones aparecerán en ambos dispositivos (una aplicación iniciada en un dispositivo es visible en todos los dispositivos en uso). Es posible que este comportamiento no cumpla los requisitos de seguridad.
- Si se inhabilita la movilidad de sesión, el registro del paciente no aparecerá en el equipo de escritorio y el formulario del seguro no aparecerá en la tableta.

Ejemplo 2. Un director de producción inicia una aplicación en su equipo de oficina. La ubicación y el nombre del dispositivo determinan qué impresoras y otros recursos están disponibles para esa sesión. Más tarde en la misma jornada laboral, el director va a una oficina situada en el edificio contiguo con el objetivo de asistir a una reunión para la que necesitará usar una impresora.

- Si la movilidad de sesión está habilitada, posiblemente el director de producción no podrá acceder a las impresoras de la sala de la reunión porque las aplicaciones que inició antes, en su oficina, resultaron en la asignación de impresoras y otros recursos cercanos a esa ubicación.
- Si la movilidad de sesión está inhabilitada, cuando inicie sesión en otra máquina (con las mismas credenciales), se iniciará una nueva sesión y las impresoras y los recursos cercanos estarán disponibles.

Configuración de movilidad de sesión

Para configurar la movilidad de sesión, use los siguientes cmdlets de la regla de directiva de derechos con la propiedad “SessionReconnection”. Opcionalmente, también puede especificar la propiedad “LeasingBehavior”.

Para sesiones de escritorio:

```
Set-BrokerEntitlementPolicyRule \<Delivery-Group-name> -SessionReconnection
 \<value> -LeasingBehavior Allowed|Disallowed
```

Para sesiones de aplicación:

```
Set-BrokerAppEntitlementPolicyRule \<Delivery-Group-name> -SessionReconnection
 \<value> -LeasingBehavior Allowed|Disallowed
```

Donde <*value*> puede ser una de las siguientes opciones:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **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 utilizando el control del espacio de trabajo para moverlas explícitamente.) Una sesión activa conectada desde otro dispositivo cliente no se utiliza nunca; en su lugar, se inicia una nueva sesión.
- **SameEndpointOnly:** El usuario obtiene una sesión única para cada dispositivo que use. Esto inhabilita completamente la movilidad. Los usuarios solo pueden volver a conectarse al mismo dispositivo que usaron anteriormente en la sesión.

La propiedad "LeasingBehavior" se describe más adelante.

Efectos de otras opciones de configuración:

La inhabilitación de la movilidad de sesión se ve afectada por el límite para aplicaciones "Permitir una sola instancia de aplicación por usuario" en las propiedades de aplicación, en el grupo de entrega.

- Si inhabilita la movilidad de sesión, inhabilite el límite para aplicaciones "Permitir una sola instancia de aplicación por usuario".
- Si habilita el límite para aplicaciones "Permitir una sola instancia de aplicación por usuario", no configure uno de los dos valores que permiten sesiones nuevas en dispositivos nuevos.

Intervalo de inicio de sesión

Si una máquina virtual que contiene un escritorio VDA se cierra antes de que se complete el proceso de inicio de sesión, se puede asignar más tiempo al proceso. El valor predeterminado para 7.6 y versiones posteriores es de 180 segundos, mientras que el predeterminado para versiones de 7.0 a 7.5 es de 90 segundos.

En la máquina (o la imagen maestra utilizada en un catálogo de máquinas), defina la siguiente clave de Registro:

Clave: HKLM\SOFTWARE\Citrix\PortICA

- Valor: AutoLogonTimeout
- Tipo: DWORD
- Especifique un número decimal en segundos que vaya de 0 a 3600.

Si cambia una imagen maestra, actualice el catálogo.

Esta configuración se aplica solo a las máquinas virtuales con agentes VDA de escritorio (estaciones de trabajo). Microsoft controla el tiempo de espera de inicio de sesión en las máquinas con servidores VDA.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Usar búsquedas en Studio

January 29, 2019

Utilice la función de búsqueda para ver información sobre máquinas, sesiones, catálogos de máquinas, aplicaciones o grupos de entrega específicos.

1. Seleccione **Buscar** en el panel de navegación de Studio.

   No se puede buscar dentro de las fichas Catálogos de máquinas o Grupos de entrega desde el cuadro de búsqueda. Use el nodo Buscar en el panel de navegación.

   Para mostrar criterios de búsqueda adicionales en la pantalla, haga clic en el signo más, junto a los campos desplegables de búsqueda. Quite criterios de búsqueda haciendo clic en el botón de menos.

2. Escriba el nombre o use la lista desplegable para seleccionar otra opción de búsqueda para el elemento que quiere buscar.

3. También puede guardar la búsqueda si selecciona **Guardar como**. La búsqueda aparece en la lista **Búsquedas guardadas**.

Si lo prefiere, también puede hacer clic en el icono **Expandir búsqueda** (doble corchete angular hacia abajo) para mostrar un menú de propiedades de búsqueda. Puede realizar una búsqueda avanzada creando una expresión a partir de las propiedades del menú.

Sugerencias para mejorar la búsqueda:

- Para mostrar las características adicionales a incluir en la pantalla en la que puede buscar y ordenar, haga clic con el botón secundario en cualquier columna y seleccione **Seleccionar columnas**.
- Para buscar un dispositivo de usuario conectado a una máquina, use **Cliente (IP)** y **Es** y escriba la dirección IP del dispositivo.
- Para buscar sesiones activas, use **Estado de la sesión**, **Es** y **Conectado**.
- Para enumerar todas las máquinas de un grupo de entrega, seleccione **Grupos de entrega** en el panel de navegación, seleccione el grupo pertinente y, a continuación, seleccione **Ver máquinas** en el panel Acciones.

Etiquetas

March 8, 2019

> Nota:
>
> Cuando se utilizan grupos de aplicaciones con Citrix Virtual Apps and Desktops Service, la fun-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> ción de restricción por etiqueta no está disponible por el momento.

Introducción

Las etiquetas son cadenas que identifican elementos como, por ejemplo, máquinas, aplicaciones, escritorios, grupos de entrega, grupos de aplicaciones y directivas. Después de crear una etiqueta y agregarla a un elemento, puede adaptar determinadas operaciones para que solo se apliquen a los elementos que tengan esa etiqueta concreta.

- Personalizar las pantallas de búsquedas en Studio.

  Por ejemplo, si quiere que solo se muestren las aplicaciones que se hayan optimizado de cara a evaluadores, cree una etiqueta llamada “evaluar” y agréguela (aplíquela) a esas aplicaciones. Entonces, podrá filtrar la búsqueda de Studio con la etiqueta “evaluar”.

- Publicar aplicaciones de un grupo de aplicaciones o escritorios concretos de un grupo de entrega, teniendo en cuenta solo un subconjunto de las máquinas en los grupos de entrega seleccionados. Esto se denomina una *restricción de etiqueta*.

  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 máquinas adicionales. La restricción de etiqueta puede entenderse como una subdivisión (o partición) de las máquinas de un grupo de entrega. Su funcionalidad es similar (pero no idéntica) a los grupos de trabajo en las versiones de XenApp anteriores a 7.x.

  Usar un grupo de aplicaciones o escritorios con una restricción de etiqueta puede ser útil para aislar un subconjunto de las máquinas de un grupo de entrega y solucionar los problemas que presentan.

  Consulte los siguientes apartados para obtener información más detallada y ejemplos de restricciones de etiqueta.

- Programar reinicios periódicos para un subconjunto de las máquinas de un grupo de entrega.

  Una restricción de etiqueta en las máquinas permite utilizar los nuevos cmdlets de PowerShell para configurar varias programaciones de reinicios para subconjuntos de máquinas en un grupo de entrega. Para obtener más información, consulte Administrar grupos de entrega.

- Personalizar la aplicación (asignación) de las directivas de Citrix a 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

continuación, aplicar una directiva de Citrix a ese grupo. Para obtener más información, consulte el artículo Crear directivas y esta entrada de blog. (La interfaz de Studio para agregar una etiqueta a una máquina ha cambiado desde que se publicó la entrada del blog.)

Puede aplicar etiquetas a:

- Máquinas
- Aplicaciones
- Grupos de entrega
- Grupos de aplicaciones

Puede configurar una restricción de etiqueta al crear o modificar lo siguiente en Studio:

- Un escritorio en un grupo de entrega compartido
- Un grupo de aplicaciones

Restricciones de etiqueta para un grupo de escritorios o aplicaciones

Una restricción de etiqueta implica varios pasos:

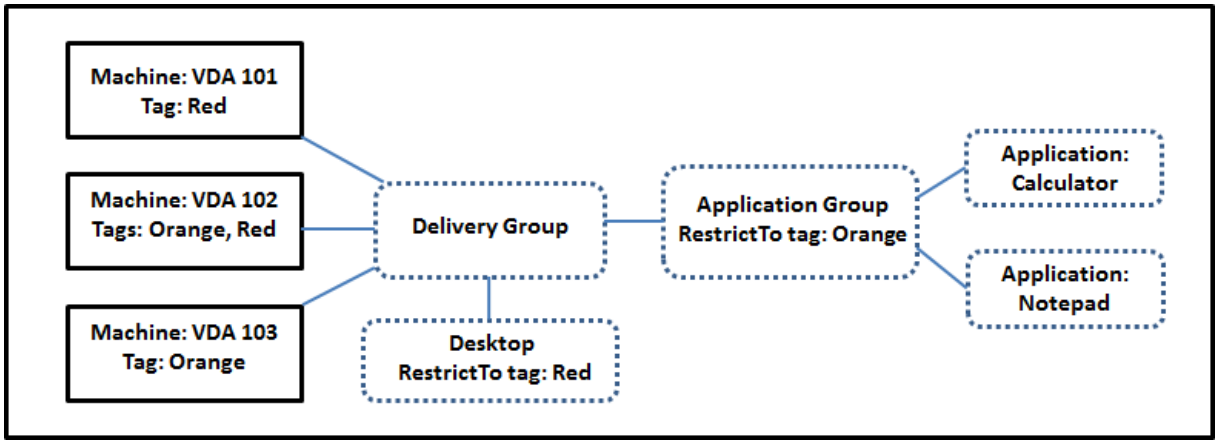
- Crear la etiqueta y, a continuación, agregarla (aplicarla) a las máquinas.
- Crear o modificar un grupo con la restricción de etiqueta (en otras palabras, "restringir inicios a máquinas con la etiqueta x").

La restricción de etiqueta amplía el proceso de selección de máquinas del broker. 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 de etiqueta para limitar las máquinas que se tendrán en cuenta para ciertos inicios de aplicaciones y escritorios. El sitio tiene un grupo de entrega compartido, un escritorio publicado, y un grupo de aplicaciones configurado con dos aplicaciones.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



- 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”, por lo que ese escritorio solo se puede iniciar en las máquinas de ese grupo de entrega que tengan la etiqueta “Rojo”: VDA 101 y 102.
- El grupo de aplicaciones se creó con la restricción de etiqueta “Naranja”, por lo que cada una de sus aplicaciones (Calculadora y Bloc de notas) solo se pueden iniciar en las máquinas de ese grupo de entrega que tengan la etiqueta “Naranja”: VDA 102 y 103.

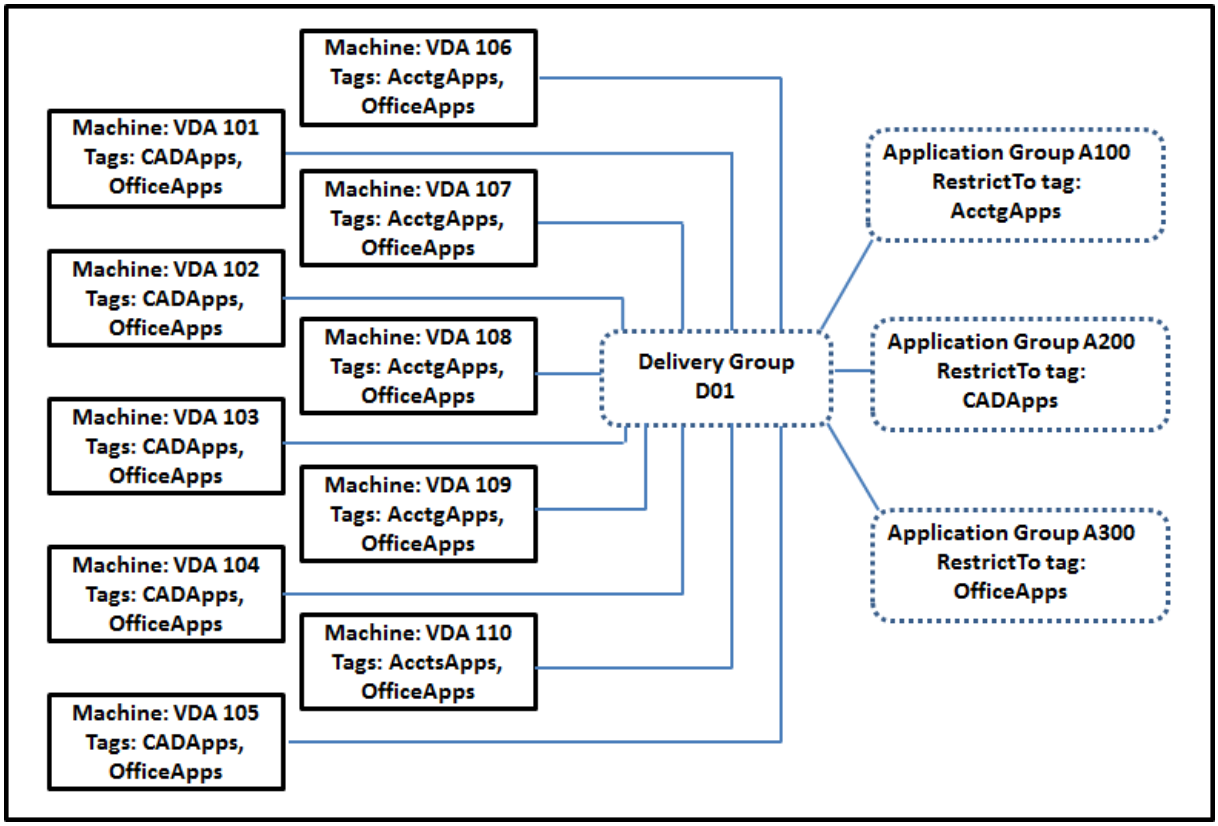
Ahora bien, la máquina VDA 102 tiene ambas etiquetas (Rojo y Naranja); por lo tanto, puede considerarse para iniciar las aplicaciones y el escritorio.

Ejemplo 2: distribución más sencilla

En este ejemplo, existen varios grupos de aplicaciones que se han creado con restricciones de etiqueta. Por eso, se pueden entregar más aplicaciones con menos máquinas de las que se necesitarían si solo se usaran grupos de entrega.

(Ejemplo 2: Cómo configurar, describe los pasos a seguir para crear, aplicar las etiquetas y configurar las restricciones de etiqueta de este ejemplo.)

© 1999-2019 Citrix Systems, Inc. All rights reserved.



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 de etiqueta cuando cree cada grupo de aplicaciones:

- Los usuarios de Contabilidad del grupo pueden acceder a las aplicaciones que necesitan en cinco máquinas (VDA de 101 a 105)
- Los diseñadores de CAD del grupo pueden acceder a las aplicaciones que necesitan en cinco máquinas (VDA de 106 a 110)
- Los usuarios del grupo que necesitan las aplicaciones de Office pueden acceder a las aplicaciones Office en diez máquinas (VDA de 101 a 110)

Solo se utilizan diez 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 de etiqueta

Las etiquetas se crean y se agregan (se aplican), se modifican y se eliminan de los elementos seleccionados mediante la acción **Administrar etiquetas** en Studio.

(Excepción: Las etiquetas que se utilizan para las asignaciones de directiva se crean, se modifican y se eliminan mediante la acción **Administrar etiquetas** en Studio; sin embargo, las etiquetas se aplican

© 1999-2019 Citrix Systems, Inc. All rights reserved.

(asignan) en el momento de crear la directiva. Ver Crear directivas para más detalles).

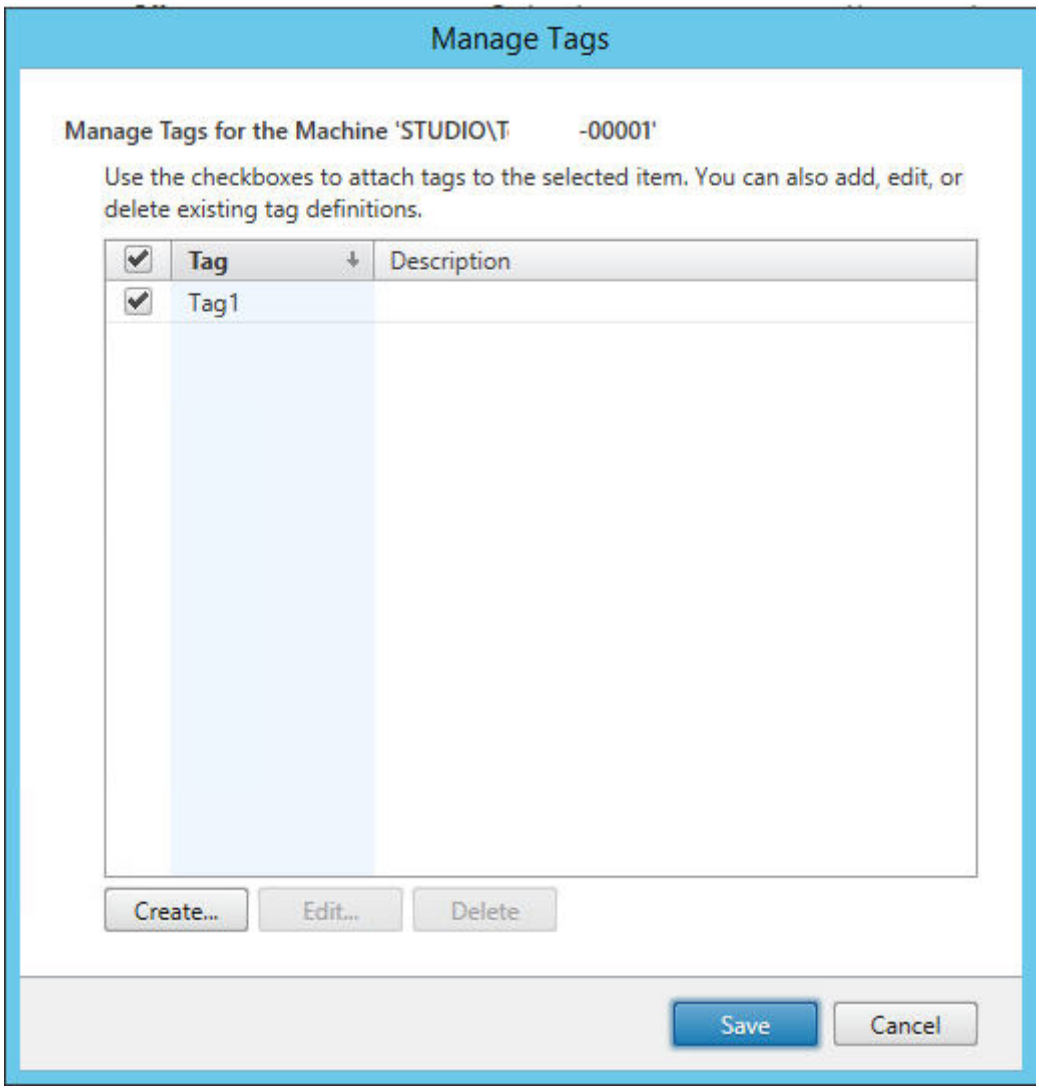
Las restricciones de etiqueta se configuran cuando crea o modifica los escritorios de los grupos de entrega, y cuando crea y modifica grupos de aplicaciones.

Uso del cuadro de diálogo Administrar etiquetas en Studio

En Studio, seleccione los elementos a los que quiere aplicar una etiqueta (una o varias máquinas o aplicaciones, un escritorio, un grupo de entrega o un grupo de aplicaciones) y, a continuación, seleccione **Administrar etiquetas** en el panel Acciones. El cuadro de diálogo Administrar etiquetas muestra todas las etiquetas que se han creado en el sitio, no solo las correspondientes a los elementos seleccionados.

- La casilla de verificación que contiene una marca indica que la etiqueta ya se ha agregado a los elementos seleccionados. (En la captura de pantalla siguiente, la 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Puede llevar a cabo las siguientes 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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**. Escriba un nuevo nombre y/o descripción. Solo puede modificar una etiqueta a la vez.

- **Para eliminar una o varias etiquetas:**

  Seleccione las etiquetas y, a continuación, haga clic en **Eliminar**. El cuadro de diálogo "Eliminar etiqueta" indica la cantidad de elementos que usan en ese momento las etiquetas seleccionadas (por ejemplo, "2 máquinas"). Haga clic en un elemento para ver más información. Por ejemplo, hacer clic en "2 máquinas" mostrará los nombres de las dos máquinas que tienen aplicada la etiqueta. Confirme si quiere eliminar las etiquetas.

  No puede usar Studio para eliminar una etiqueta que se usa como una restricción. Primero, debe modificar el grupo de aplicaciones y quitar la restricción de etiqueta o seleccionar otra etiqueta.

Cuando haya terminado en el cuadro de diálogo Administrar etiquetas, haga clic en **Guardar**.

> **Sugerencia:**
>
> Para ver si una máquina tiene etiquetas aplicadas: Seleccione **Grupos de entrega** en el panel de navegación. Seleccione un grupo de entrega en el panel central y, a continuación, seleccione **Ver máquinas** en el panel Acciones. Seleccione una máquina en el panel central y, a continuación, seleccione la ficha Etiquetas en el panel inferior Detalles.

Administración de restricciones de etiqueta

Configurar una restricción de etiqueta 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Para crear y aplicar la etiqueta:**

  Cree la etiqueta y, a continuación, agréguela (aplíquela) a las máquinas que se verán afectadas por la restricción de etiqueta mediante las acciones de **Administrar etiquetas** descritas anteriormente.

- **Para agregar una restricción de etiqueta a un grupo de aplicaciones:**

  Cree o modifique el grupo de aplicaciones. En la página Grupos de entrega, seleccione la opción **Restringir inicios a máquinas con la etiqueta** y, a continuación, seleccione la etiqueta en el menú desplegable.

- **Para cambiar o quitar una restricción de etiqueta de un grupo de aplicaciones:**

  Modifique el grupo. En la página Grupos de entrega, seleccione otra etiqueta en el menú desplegable o quite la restricción de etiqueta totalmente desmarcando **Restringir inicios a máquinas con la etiqueta**.

- **Para agregar una restricción de etiqueta a un escritorio:**

  Cree o edite 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 desplegable.

- **Para cambiar o quitar la restricción de etiqueta de un grupo de entrega:**

  Modifique el grupo. En la página Escritorios, haga clic en **Modificar**. En el cuadro de diálogo, seleccione otra etiqueta en el menú desplegable o quite la restricción de etiqueta totalmente desmarcando **Restringir inicios a máquinas con la etiqueta**.

Precauciones al trabajar con etiquetas

Una etiqueta que se aplica a un elemento se puede usar para distintos fines, por lo tanto, tenga en cuenta que agregar, quitar y eliminar una etiqueta puede tener efectos no deseados. Puede utilizar una etiqueta para ordenar máquinas en el campo de búsqueda de Studio. Puede usar la misma etiqueta como una restricción cuando configure un grupo de aplicaciones o un escritorio, lo que provocará que se tengan en cuenta para inicios solo aquellas máquinas de los grupos de entrega especificados que tengan esa etiqueta.

Si intenta agregar una etiqueta a una o varias máquinas después de que la etiqueta se haya configurado como una restricción de etiqueta para un escritorio o un grupo de aplicaciones, Studio le advertirá que agregar esa etiqueta puede hacer que las máquinas estén disponibles para iniciar aplicaciones o escritorios adicionales. Si es su objetivo, continúe. Si no, puede cancelar la operación.

Por ejemplo, supongamos que crea un grupo de aplicaciones con la restricción de la 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, Studio mostrará un

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 una etiqueta se está utilizando en un grupo de aplicaciones para restringir inicios, Studio le advierte que no puede eliminar la etiqueta hasta que la haya quitado como una restricción modificando el grupo. (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 en ese momento como una restricción para inicios de escritorio. Después de modificar el grupo de aplicaciones o escritorios en el grupo de entrega para quitar la restricción de etiqueta, puede eliminar la etiqueta.

Es posible que no todas las máquinas tengan el mismo conjunto de aplicaciones. Un usuario puede pertenecer a más de un grupo de aplicaciones, cada uno con una restricción de etiqueta diferente y conjuntos de máquinas diferentes o iguales 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 de etiqueta	Cualquier máquina
Un grupo de aplicaciones con una restricción de etiqueta A	Máquinas que tienen aplicada la etiqueta A
Dos grupos de aplicaciones: uno con una restricción de etiqueta A y otro con una restricción de etiqueta B	Máquinas que tienen las etiquetas A y B; si no hay ninguna disponible, máquinas que tienen la etiqueta A o B
Dos grupos de aplicaciones: uno con una restricción de etiqueta A y otro sin restricción de etiqueta	Máquinas que tienen la etiqueta A; si no hay ninguna disponible, cualquier máquina

Si ha utilizado una restricción de etiqueta en una programación de reinicios, los cambios que realice que afecten a las aplicaciones o las restricciones de etiqueta afectarán al próximo ciclo de reinicios. Lo que no afecta a los ciclos de reinicios en vigor mientras se realizan los cambios.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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.

Cómo crear etiquetas y aplicarlas a las máquinas:

1. En Studio, seleccione el grupo de entrega D01 y, a continuación, seleccione **Ver máquinas** en el panel Acciones.
2. Seleccione las máquinas VDA de la 101 a la 105 y, a continuación, seleccione **Administrar etiquetas** en el panel Acciones.
3. En el cuadro de diálogo Administrar etiquetas, haga clic en **Crear** 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. Sin salir del 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) y, a continuación, cierre el cuadro de diálogo.
6. Seleccione el grupo de entrega D01 y, a continuación, seleccione **Ver máquinas** en el panel Acciones.
7. Seleccione las máquinas VDA de la 106 a la 110 y, a continuación, seleccione **Administrar etiquetas** en el panel Acciones.
8. En el cuadro de diálogo Administrar etiquetas, haga clic en **Crear** y, a continuación, 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.

Cómo crear los grupos de aplicaciones con restricciones de etiqueta:

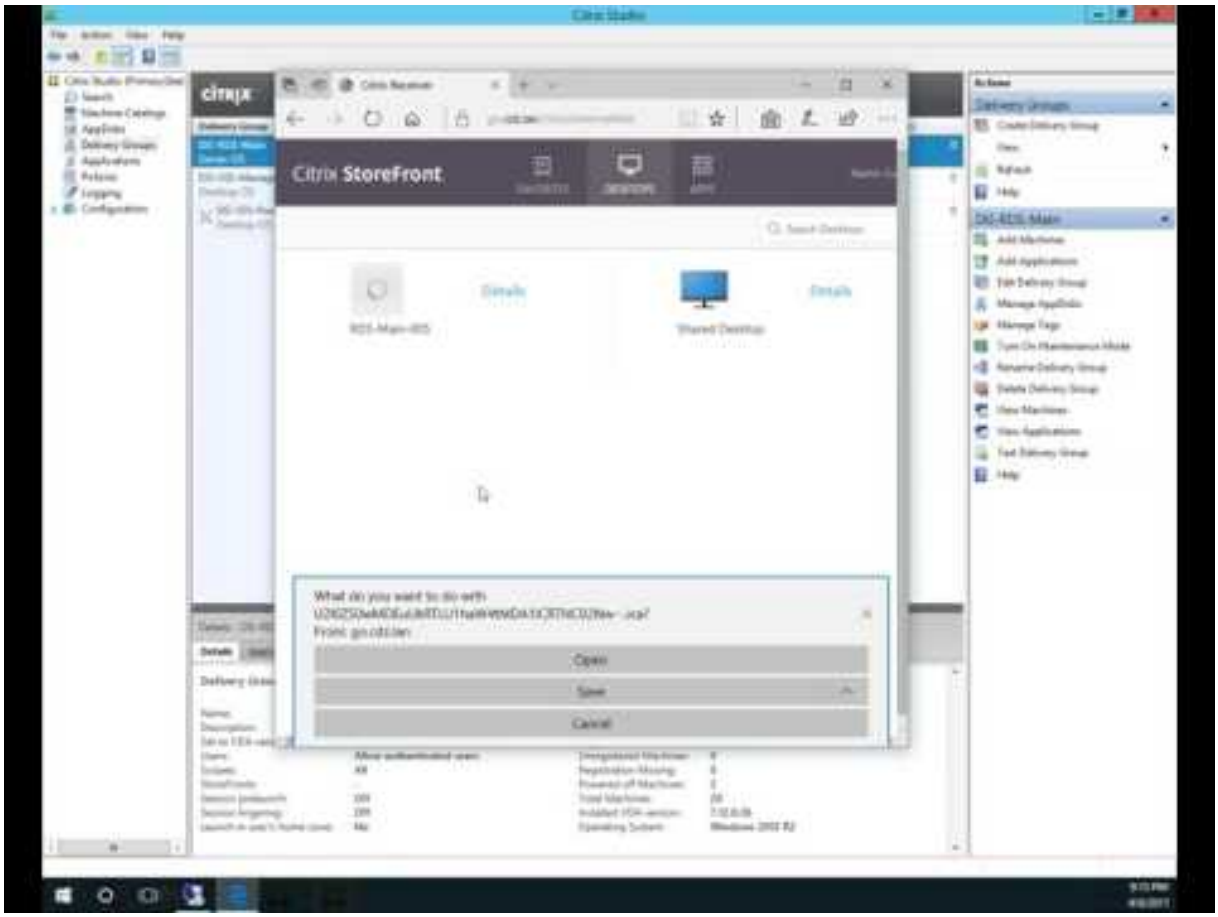
1. En Studio, seleccione **Aplicaciones** en el panel de navegación y, a continuación, seleccione **Crear grupo de aplicaciones** en el panel Acciones. Se iniciará el asistente Crear grupo de aplicaciones.
2. En la página **Grupos de entrega** del asistente, seleccione el grupo de entrega D01. Seleccione la opción **Restringir inicios a máquinas con la etiqueta** y, a continuación, seleccione la etiqueta "AcctgApps" de la lista desplegable.
3. Complete el asistente, especificando a los usuarios de contabilidad y las aplicaciones de contabilidad. (Cuando agregue la aplicación, seleccione el origen "Desde el menú Inicio", que buscará la aplicación en las máquinas que tienen la etiqueta "AcctgApps".) En la página **Resumen**, especifique un nombre para el grupo A100.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 los pasos para crear un grupo de aplicaciones A300, en que especifique las máquinas que tienen la etiqueta “OfficeApps”, además de sus usuarios y aplicaciones pertinentes.

Más información

La entrada de blog How to assign desktops to specific servers también tiene un enlace al siguiente vídeo.



Compatibilidad con IPv4/IPv6

January 29, 2019

Esta versión es compatible con solo IPv4, con solo IPv6, así como con implementaciones de doble pila que usan redes IPv4 e IPv6 superpuestas.

Las comunicaciones de IPv6 se controlan con dos configuraciones de directiva de Citrix relacionadas con las conexiones del Virtual Delivery Agent (VDA):

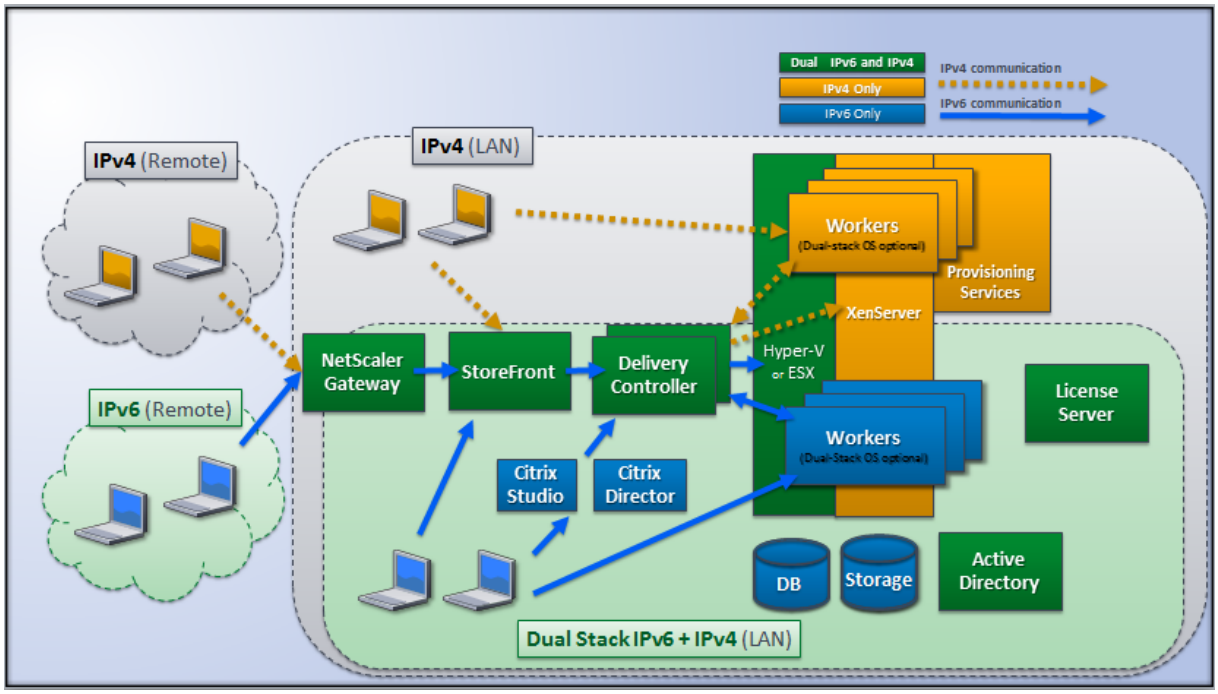
© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Una configuración principal que aplica el uso de IPv6: Usar solo registro de Controller con IPv6.
- Una configuración dependiente que define una máscara de red IPv6: Máscara de red IPv6 para registro de Controller.

Cuando la configuración de directiva Usar solo registro de Controller con IPv6 está habilitada, el VDA se registra con un Delivery Controller para las conexiones entrantes usando una dirección IPv6.

Implementación de doble pila IPv4/IPv6

La siguiente figura ilustra una implementación de doble pila de IPv4/IPv6. En este caso, un trabajador es un VDA instalado en un hipervisor o en un sistema físico, y se utiliza principalmente para habilitar las conexiones de aplicaciones y escritorios. Los componentes que dan respaldo a ambos protocolos, IPv4 y IPv6, se ejecutan en los sistemas operativos que usan software de tunelización o protocolo doble.



Estos productos, componentes y funciones de Citrix solo respaldan IPv4:

- Citrix Provisioning
- XenServer
- Los VDA no controlados por la configuración de directiva **Usar solo registro de Controller con IPv6**
- Versiones de XenApp anteriores a 7.5, versiones de XenDesktop anteriores a 7 y Director

En esta implementación:

- Si un grupo de usuarios usa una red IPv6 de manera habitual y el administrador desea que use el tráfico IPv6, publicará escritorios y aplicaciones con IPv6 para esos usuarios a partir de una

© 1999-2019 Citrix Systems, Inc. All rights reserved.

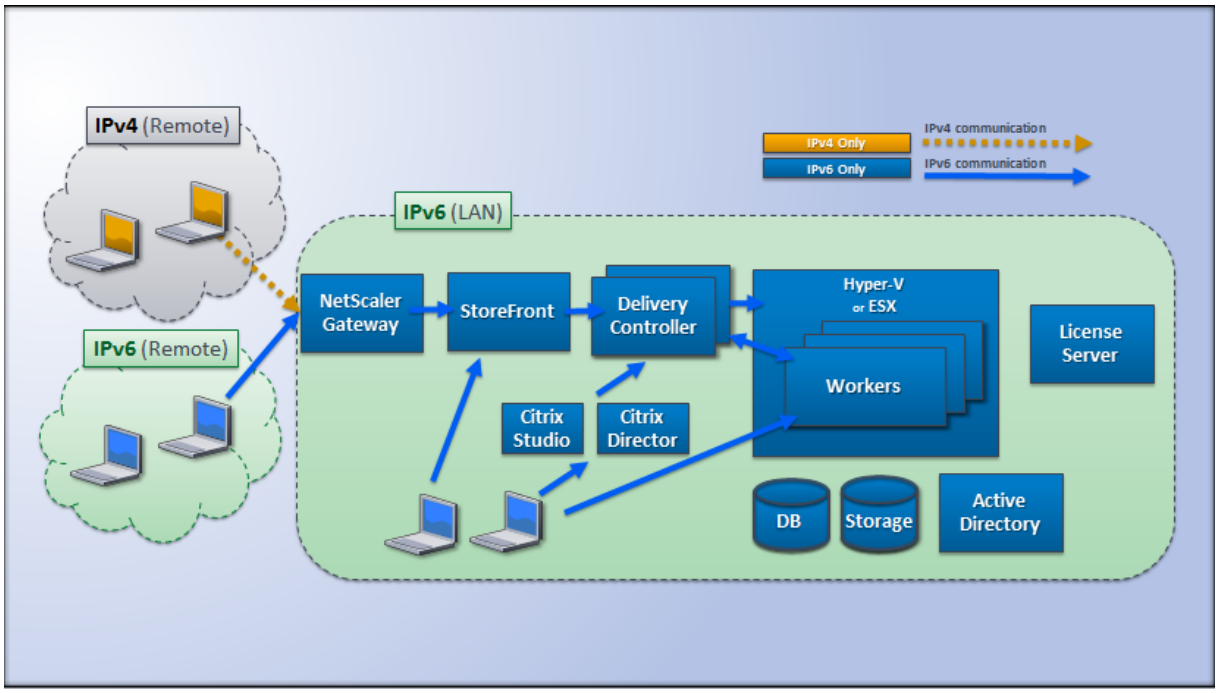
imagen de trabajo o de una unidad organizativa (OU) que tiene la configuración de directiva principal de IPv6 habilitada (es decir, la configuración Usar solo registro de Controller con IPv6 está habilitada).

- Si un grupo de usuarios usa una red IPv4 de manera habitual, el administrador publicará los escritorios y las aplicaciones con IPv4 para esos usuarios a partir de una imagen de trabajo o unidad organizativa que tiene la configuración de directiva de IPv6 inhabilitada (es decir, Usar solo registro de Controller con IPv6 está inhabilitada), que es el valor predeterminado.

Implementación de solo IPv6

En la siguiente imagen se ilustra una implementación de solo IPv6. En este caso:

- Los componentes se están ejecutando en sistemas operativos configurados para dar respaldo a una red IPv6.
- La configuración de directiva principal de Citrix (Usar solo registro de Controller con IPv6) está habilitada para todos los VDA, por lo que deben registrarse con el Controller mediante una dirección IPv6.



Configuraciones de directiva para IPv6

Hay dos configuraciones de directiva de Citrix que afectan al respaldo de implementaciones puras de IPv6 o implementaciones de doble pila IPv4/IPv6. Defina las siguientes configuraciones de directiva relacionadas con las conexiones:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Usar solo registro de Controller con IPv6:** Controla el formato de dirección que utiliza Virtual Delivery Agent (VDA) para registrarse en el Delivery Controller. Valor predeterminado = inhabilitado
  - Cuando el VDA se comunica con el Controller, utiliza una sola dirección IPv6 seleccionada según las siguientes prioridades: dirección IP global, Unique Local Address (ULA), dirección local de enlace (solo si no hay otras direcciones IPv6 disponibles).
  - Cuando está inhabilitada, el VDA se registra y se comunica con el Controller mediante la dirección IPv4 de la máquina.
- **Máscara de red IPv6 para registro de Controller:** Una máquina puede tener varias direcciones IPv6; esta configuración de directiva permite a los administradores restringir el VDA a una sola subred preferida (en lugar de una dirección IP global, si hay alguna registrada). Esta configuración especifica la red en la que se registrará VDA. El VDA se registra solo en la primera dirección que coincide con la máscara de red. Esta configuración solo es válida si la configuración de directiva Usar solo registro de Controller con IPv6 está habilitada. Valor predeterminado = Cadena vacía

Importante:

> El uso de IPv4 o IPv6 por parte de un VDA está determinado únicamente por estas configuraciones de directiva. En otras palabras, para usar direcciones IPv6, el VDA debe estar controlado por una directiva de Citrix que contenga la configuración **Usar solo registro de Controller con IPv6** habilitada.

Consideraciones sobre la implementación

Si el entorno contiene redes IPv4 e IPv6, necesitará configuraciones diferentes de grupos de entrega, uno para los clientes que solo pueden acceder a IPv4 y otro para los clientes que pueden acceder a la red IPv6. Considere la posibilidad de usar nombres, asignaciones de grupo de Active Directory o filtros de SmartAccess para diferenciar a los usuarios.

Es posible que la reconexión a una sesión falle si la conexión se inicia en una red IPv6 y, a continuación, se intenta la reconexión a partir de un cliente interno que solo tiene acceso de IPv4.

Perfiles de usuario

January 29, 2019

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para responder a las distintas necesidades de los usuarios, puede aplicar, mediante las directivas de Citrix Virtual Apps and Desktops, un comportamiento de perfil diferente a las máquinas de cada grupo de entrega. Por ejemplo, un grupo de entrega puede requerir perfiles obligatorios de Citrix, cuya plantilla está almacenada en una ubicación de red, mientras que otro grupo de entrega puede requerir perfiles móviles de Citrix almacenados en otra ubicación con varias carpetas redirigidas.

- Si otros administradores de su organización son responsables de las directivas de Citrix Virtual Apps and Desktops, colabore con ellos para asegurarse de que establecen directivas relacionadas con los perfiles en todos los grupos de entrega.
- Las directivas de Profile Management también se pueden establecer en las Directivas de grupo, en el archivo .ini de Profile Management, y localmente, en máquinas virtuales individuales. Todas estas formas de definir el comportamiento de perfil se leen en el orden siguiente:

  1. Directiva de grupo (archivos .adm o .admx)
  2. Directivas de Citrix Virtual Apps and Desktops en el nodo Directiva
  3. Directivas locales en la máquina virtual a la que el usuario se conecta
  4. Archivo .ini de Profile Management

  Por ejemplo, si configura la misma directiva en la Directiva de grupo y en el nodo Directiva, el sistema lee la configuración de directiva en la Directiva de grupo y omite la configuración de directiva de Citrix Virtual Apps and Desktops.

Independientemente de la solución de administración de perfiles que elija, los administradores de Director pueden acceder a la información de diagnóstico y solucionar problemas de perfiles de usuario. Para obtener más información, consulte la documentación de Director.

Si usa la función Personal vDisk, los perfiles de usuario de Citrix se almacenan en los discos Personal vDisk de los escritorios virtuales de forma predeterminada. No borre la copia de ningún perfil en el almacén de usuarios mientras aún quede una copia en el disco Personal vDisk. Si lo hace, se producirá un error de Profile Management y provocará el uso de un perfil temporal para los inicios de sesión en el escritorio virtual.

Configuración automática

Este tipo de escritorio se detecta automáticamente en función de la instalación de Virtual Delivery Agent y, además de las opciones de configuración seleccionadas en Studio, configura los parámetros predeterminados de Profile Management según corresponda.

En la tabla siguiente se muestran las directivas que ajusta Profile Management. Esta función conserva las configuraciones de directiva no predeterminadas, no las sobrescribe. Consulte la documentación de Profile Management para obtener información sobre cada directiva. Los tipos de máquinas que crean perfiles afectan a las directivas que se ajustan. Los factores principales son si las máquinas son

© 1999-2019 Citrix Systems, Inc. All rights reserved.

persistentes o aprovisionadas y si están compartidas por varios usuarios o son máquinas dedicadas a un solo usuario.

Los sistemas persistentes tienen un tipo de almacenamiento local, cuyo contenido se conserva (persiste) cuando el sistema se apaga. Los sistemas persistentes pueden emplear tecnología de almacenamiento como las redes de área de almacenamiento SAN (Storage Area Network) para proveer de imitaciones de discos locales. En cambio, los sistemas aprovisionados se crean "en el momento" a partir de un disco base y algún tipo de disco de identidad. El almacenamiento local es imitado por un disco RAM o disco de red, y éste último es normalmente suministrado por una red SAN con un enlace de alta velocidad. La tecnología de aprovisionamiento suele ser Citrix Provisioning o Machine Creation Services (o un producto equivalente de terceros). Algunas veces los sistemas aprovisionados tienen un almacenamiento local persistente, que puede consistir en discos virtuales personales (Personal vDisk); estos se clasifican como persistentes.

Juntos, estos dos factores definen los siguientes tipos de máquinas:

- **Persistentes y dedicadas**. Por ejemplo, máquinas con SO de escritorio con una asignación estática y un disco Personal vDisk, creadas con Machine Creation Services; escritorios con discos Personal vDisk creados con VDI-in-a-Box; estaciones de trabajo físicas y equipos portátiles.
- **Persistentes y compartidas**. Por ejemplo, máquinas con SO de servidor creadas con los servicios Machine Creation Services.
- **Aprovisionadas y dedicadas:** Por ejemplo, máquinas de SO de escritorio con una asignación estática pero sin Personal vDisk, creadas con Citrix Provisioning.
- **Aprovisionadas y compartidas:** Por ejemplo, máquinas de SO de escritorio con una asignación aleatoria, creadas con Citrix Provisioning; escritorios sin discos Personal vDisk creados con VDI-in-a-Box.

Se sugieren las siguientes configuraciones de directiva de Profile Management para los distintos tipos de máquina. En la mayoría de los casos funcionan correctamente, aunque puede cambiarlas según sea necesario en su entorno.

Importante:

> Eliminar perfiles guardados en caché local al cerrar la sesión,
> Streaming de perfiles y
> Guardar siempre en caché se aplican obligatoriamente mediante la función de configuración automática. Ajuste el resto de las directivas manualmente.

Máquinas persistentes

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Directiva	Persistentes y dedicadas	Persistentes y compartidas
Eliminar perfiles guardados en caché local al cerrar la sesión	Inhabilitada	Habilitada
Streaming de perfiles	Inhabilitada	Habilitada
Guardar siempre en caché	Habilitada (nota 1)	Inhabilitada (nota 2)
Reescritura activa	Inhabilitada	Inhabilitada (nota 3)
Procesar inicios de sesión de administradores locales	Habilitada	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)	Habilitada
Streaming de perfiles	Habilitada	Habilitada
Guardar siempre en caché	Inhabilitada (nota 6)	Inhabilitada
Reescritura activa	Habilitada	Habilitada
Procesar inicios de sesión de administradores locales	Habilitada	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 varios servidores Citrix Virtual Apps. En ese caso, habilite esta directiva.
4. Inhabilite Procesar inicios de sesión de administradores locales excepto para escritorios alojados compartidos. En ese caso, habilite esta directiva.
5. Inhabilite Eliminar perfiles guardados en caché local al cerrar la sesión. Esto conserva los per-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

files 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 varios servidores Citrix Virtual Apps and Desktops. En ese caso, inhabilite esta directiva.

Redirección de carpetas

La redirección de carpetas permite almacenar datos de usuario en recursos compartidos de red, distintos de la ubicación donde se guardan los perfiles. Esto reduce el tamaño y el tiempo de carga del perfil pero podría afectar al ancho de banda de la red. Para la redirección de carpetas no se requiere el empleo de perfiles de usuario de Citrix. Puede optar por administrar los perfiles de usuario usted mismo y aplicar la redirección de carpetas.

Configure la redirección de carpetas con las directivas de Citrix en Studio.

- Asegúrese de que las ubicaciones de red usadas para almacenar el contenido de las carpetas redirigidas estén disponibles y tengan los permisos correctos. Se validan las propiedades de ubicación.
- Las carpetas redirigidas se configuran en la red y su contenido se crea desde los escritorios virtuales de los usuarios al iniciar sesión.

Configure la redirección de carpetas con las directivas de Citrix o con los objetos de directiva de grupo de Active Directory, pero no ambos a la vez. Si configura la redirección de carpetas usando ambos motores de directivas, puede que obtenga resultados impredecibles.

Redirección de carpetas avanzada

En las implementaciones con varios sistemas operativos (SO), puede ser conveniente que una porción de un perfil de usuario esté compartida por cada SO. El resto del perfil no está compartido y solo lo utiliza un sistema operativo. Para garantizar una experiencia de usuario consistente en todos los sistemas operativos, necesita una configuración diferente para cada sistema operativo. En esto consiste la redirección de carpetas avanzada. Por ejemplo, es posible que haya diferentes versiones de una aplicación que se ejecuta en dos sistemas operativos que necesiten leer o editar un archivo compartido. En este caso, puede decidir redirigir dicho archivo a una única ubicación de red donde ambas

© 1999-2019 Citrix Systems, Inc. All rights reserved.

versiones de la aplicación puedan acceder a él. O, 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. Esto separa la carpeta Menú Inicio y su contenido en cada sistema operativo, lo que garantiza una experiencia consistente para los usuarios.

Si la implementación requiere una redirección de carpetas avanzada, es necesario comprender la estructura de los datos de perfil de los usuarios y determinar qué partes de ella se pueden compartir entre distintos sistemas operativos. Esto es importante porque si la redirección de carpetas no se aplica correctamente, su comportamiento puede ser impredecible.

Para redirigir las carpetas en implementaciones avanzadas:

- Use un grupo de entrega distinto para cada sistema operativo.
- Es necesario conocer dónde guardan las aplicaciones virtuales, incluidas las ejecutadas en escritorios virtuales, los datos y los parámetros del usuario, y conocer cómo están organizados esos datos.
- En el caso de datos de perfil compartidos que se pueden mover de manera segura (porque están organizados idénticamente en cada SO), redirija las carpetas contenedoras en cada grupo de entrega.
- En el caso de datos de perfil no compartidos que no se pueden mover, redirija la carpeta contenedora solo en uno de los grupos de entrega, normalmente el grupo correspondiente al SO utilizado con más frecuencia, o el grupo donde los datos sean más importantes. De manera alternativa, en el caso de datos no compartidos que no se pueden mover entre sistemas operativos, puede redirigir las carpetas contenedoras de ambos sistemas a ubicaciones de red distintas.

Ejemplo de implementación avanzada

Esta implementación contiene aplicaciones (incluidas las versiones de Microsoft Outlook y de Internet Explorer) que se ejecutan en escritorios Windows 8, así como aplicaciones (incluidas otras versiones de Outlook y de Internet Explorer) entregadas por Windows Server 2008. Para lograr esto, se han configurado dos grupos de entrega, uno para cada sistema operativo. Los usuarios quieren acceder al mismo conjunto de Contactos y Favoritos en ambas versiones de esas dos aplicaciones.

Importante: Las decisiones y las sugerencias siguientes son válidas para los sistemas operativos y la implementación descrita. 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Folder (Carpeta)	¿Redirigida en Windows 8?	¿Redirigida en Windows Server 2008?
Mis documentos	Sí	Sí
Datos de programa	No	No
Contactos	Sí	Sí
Escritorio	Sí	No
Descargas	No	No
Favoritos	Sí	Sí
Vínculos	Sí	No
Mi música	Sí	Sí
Mis imágenes	Sí	Sí
Mis vídeos	Sí	Sí
Búsquedas	Sí	No
Juegos guardados	No	No
Menú Inicio	Sí	No

- Para las carpetas redirigidas compartidas:
  - Después de analizar la estructura de los datos guardados por las distintas versiones de Outlook y de Internet Explorer, se decide que es posible compartir las carpetas Contactos y Favoritos
  - Se sabe que las carpetas Mis documentos, Mi música, Mis imágenes y Mis vídeos tienen una estructura estándar en todos los sistemas operativos, por lo tanto se pueden guardar en la misma ubicación de red para cada grupo de entrega
- Para las carpetas redirigidas no compartidas:
  - Se decide no redirigir las carpetas Escritorio, Vínculos, Búsquedas ni Menú Inicio del grupo de entrega de Windows Server porque los datos incluidos en estas carpetas están organizados de manera diferente en cada sistema operativo. Por lo tanto, no se pueden compartir.
  - Para garantizar un comportamiento predecible de estos datos no compartidos, se decide aplicar la redirección solamente en el grupo de entrega de Windows 8. Se elige éste, en lugar del grupo de entrega de Windows Server, porque los usuarios utilizarán Windows 8 con más frecuencia en su trabajo del día a día, mientras que solo ocasionalmente necesitarán acceder a las aplicaciones entregadas por el servidor. Además, en este caso, los datos no compartidos son más relevantes para el entorno de escritorio que para un entorno de aplicaciones. Por ejemplo, los accesos directos de escritorio se guardan en la

© 1999-2019 Citrix Systems, Inc. All rights reserved.

carpeta Escritorio y pueden ser útiles si se originan desde una máquina Windows 8, pero no desde una máquina Windows Server.

- Para las carpetas no redirigidas:
  - No conviene que los servidores se llenen de archivos descargados por los usuarios, por lo que se decide no redirigir la carpeta Descargas
  - Los datos de las distintas aplicaciones pueden provocar problemas de compatibilidad y de rendimiento, por lo que se decide no redirigir la carpeta Datos de programa

Para obtener más información sobre la redirección de carpetas, consulte http://technet.microsoft.com/en-us/library/cc766489%28v=ws.10%29.aspx.

Redirección de carpetas y exclusiones

En Citrix Profile Management (pero no en Studio), hay una mejora del rendimiento que permite impedir que las carpetas se procesen, aplicando exclusiones. Si usa esta función, no excluya ninguna de las carpetas redirigidas. Las funciones de redirección de carpetas y exclusión funcionan juntas, de modo que si se asegura de que ninguna de las carpetas redirigidas está excluida, Profile Management puede moverlas de vuelta a la estructura de carpetas del perfil, conservando la integridad de los datos, si más adelante decide no redirigir dichas carpetas. Para obtener más información acerca de las exclusiones, consulte Para incluir y excluir elementos.

Recopilar seguimientos de Citrix Diagnostic Facility (CDF) durante el inicio del sistema

December 4, 2018

La utilidad CDFControl es un controlador o consumidor de seguimiento de eventos que sirve para capturar los mensajes de seguimiento de Citrix Diagnostic Facility (CDF) mostrados por varios proveedores de seguimiento de Citrix. Está diseñado para solucionar problemas complejos relacionados con Citrix, analizar la compatibilidad de filtros y recopilar datos de rendimiento. Para descargar la utilidad CDFControl, consulte CTX111961.

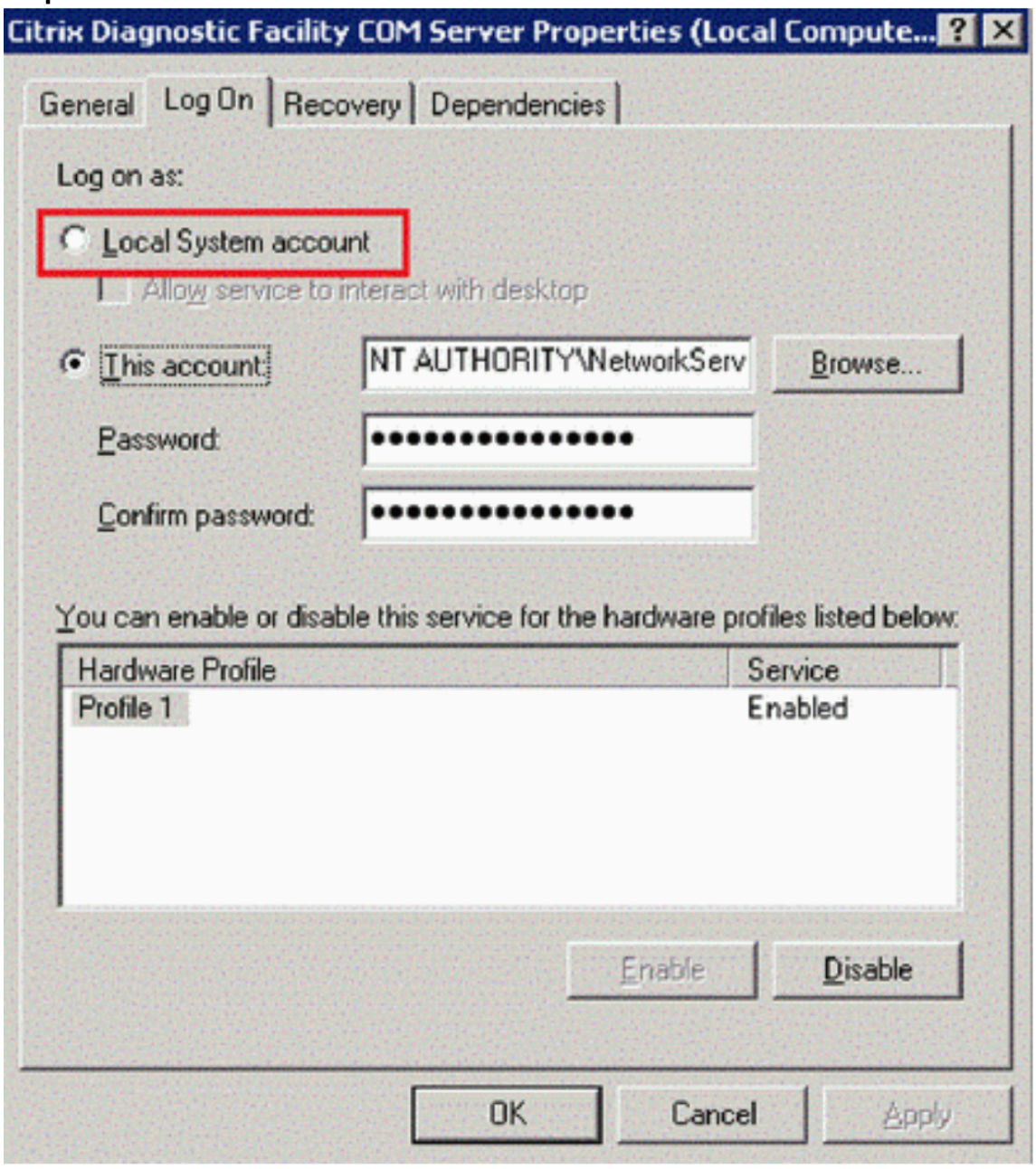
Use la cuenta del sistema local

Para usar la cuenta del sistema local para el servicio del servidor COM de Citrix Diagnostic Facility, complete los siguientes pasos:

1. Haga clic en **Ejecutar** desde el menú **Inicio**.
2. Introduzca `services.msc` en el cuadro de diálogo y haga clic en **OK**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

3. Seleccione el servicio **Servidor COM de Citrix Diagnostics Facility** y elija **Propiedades**.
4. Haga clic en la pestaña **Iniciar sesión** y habilite la cuenta **Sistema local**. Luego haga clic en **Aceptar**.



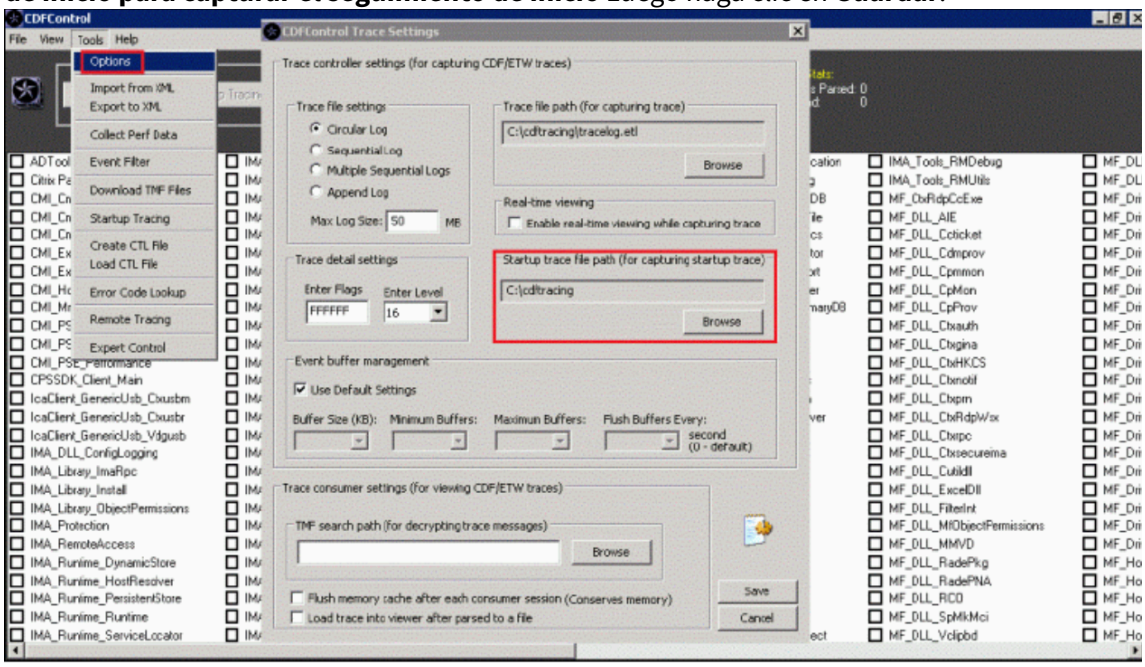
5. Reinicie el servicio.
6. Si el servicio Citrix Telemetry se está ejecutando, detenga el servicio y configure el tipo de **Inicio** como **Inhabilitado**.

Recopilar un seguimiento al iniciar el sistema

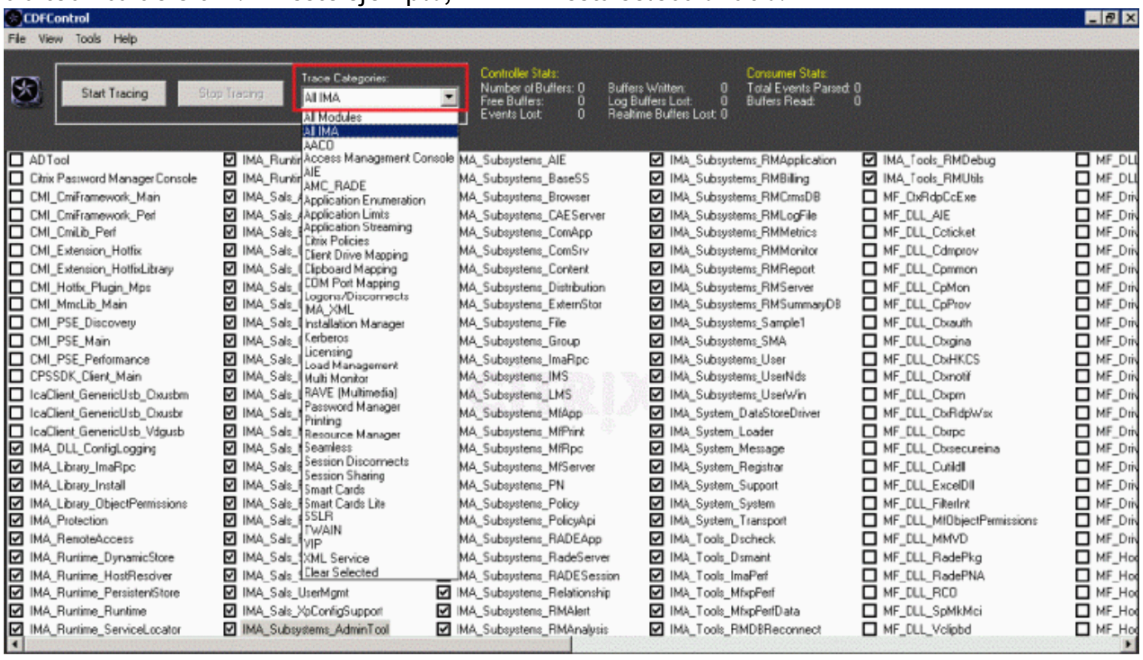
Para recopilar un seguimiento de CDF al iniciar del sistema, consulte el procedimiento:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

1. Inicie **CDFControl** y seleccione **Opciones** del menú **Herramientas**.
2. Especifique la ruta del archivo de seguimiento en la sección **Ruta de archivo de seguimiento de inicio para capturar el seguimiento de inicio** Luego haga clic en **Guardar**.



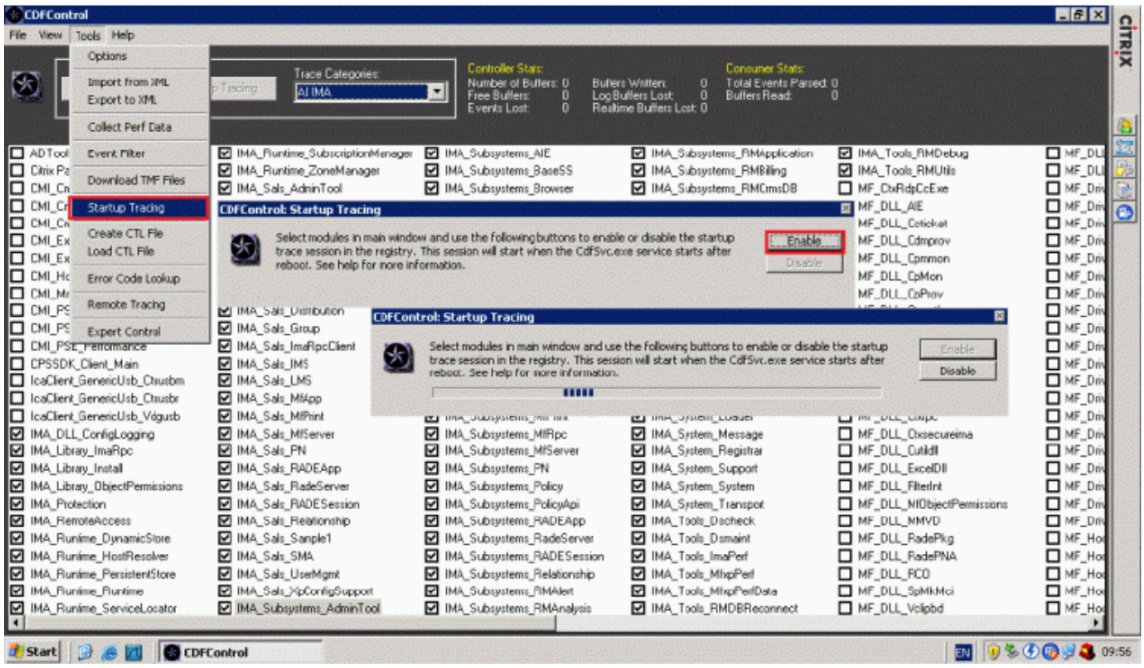
3. Seleccione las **Categorías de seguimiento** según las recomendaciones del servicio de asistencia técnica de Citrix. En este ejemplo, **ALL IMA** está seleccionado.



4. Con privilegios de administrador, seleccione **Seguimiento de inicio** y haga clic en **Habilitar** desde el menú **Herramientas**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> Nota:
>
> Después de seleccionar **Habilitar**, la barra animada comienza a desplazarse. Esto no afecta al procedimiento. Continúe con el paso 5.



5. Cierra la **utilidad CDFControl** y reinicie el sistema después de habilitar el **Seguimiento de inicio**.
6. Inicie la utilidad **CDF Control**. Después de que el sistema se reinicie y aparezca el error, inhabilite la opción **Seguimiento de inicio** con el botón **Inhabilitar**.

   Inhabilite la opción **Seguimiento de inicio** seleccionando Seguimiento de inicio desde el menú **Herramientas** y haciendo clic en **Inhabilitar**, como se describe en los pasos 4 y 5.
7. Interrumpa el servicio del servidor **COM de Citrix Diagnostics Facility**.
8. Recopile el archivo de registros de seguimiento (.etl) para analizarlo en la ruta del archivo especificado siguiendo los pasos 1 y 2.
9. Inicie el servicio del servidor **COM de Citrix Diagnostics Facility**.

Citrix Insight Services

March 8, 2019

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 corre-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

girlos, 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).

Las funciones que ofrece Citrix Insight Services aumentan y evolucionan cada vez, y ahora forman parte de Citrix Smart Tools. Citrix Smart Tools permite automatizar las tareas de implementación, las comprobaciones de estado y la administración de energía. Para obtener información sobre las tecnologías, consulte la documentación de Citrix Smart Tools.

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.citrix.com/about/legal/privacy.html

Esta versión de Citrix Virtual Apps and Desktops admite las siguientes herramientas y tecnologías.

- Análisis sobre la instalación y la actualización de Citrix Virtual Apps and Desktops
- Customer Experience Improvement Program (CEIP) de Citrix
- Citrix Smart Check
- 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 esta configuración con la clave de Registro HKLM\Software\Citrix\DesktopStudio\GAEnabled. El valor 1 habilita la recopilación y la carga, mientras que el valor 0 inhabilita la recopilación y la carga.

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. Para obtener más información, consulte https://more.citrix.com/XD-INSTALLER.

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- 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 **Configuración** en el panel de navegación de Studio. A continuación, seleccione la ficha **Asistencia para productos** y siga las instrucciones.

Cuando se actualiza una implementación de Citrix Virtual Apps and Desktops:

- Si actualiza desde una versión que no respaldaba CEIP, se le preguntará si desea participar.
- Si actualiza desde una versión que respaldaba CEIP y la participación en el programa ya estaba habilitada, CEIP se habilitará en el sitio actualizado.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Si actualiza desde una versión que respaldaba CEIP y la participación en el programa no estaba habilitada, CEIP se inhabilitará en el sitio actualizado.
- Si actualiza desde una versión que respaldaba CEIP, pero no se conoce si la participación estaba o no habilitada, se le preguntará si desea 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 VDA para Windows. 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 Smart Check

Puede habilitar Smart Check (que forma parte de Smart Tools) cuando instala un Delivery Controller.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Smart Check permite realizar comprobaciones de estado periódicas en su entorno Citrix. Smart Check ayuda a buscar problemas y solucionarlos antes de que los usuarios se vean afectados. Con Smart Check, puede:

- Programar y ejecutar una amplia variedad de controles de estado en su sitio.
- Conocer cualquier problema potencial de estado que afecte a su sitio.
- Buscar las correcciones y las actualizaciones recomendadas para los Delivery Controllers y los catálogos de máquinas que haya en su sitio.
- Cargar los diagnósticos del sitio y compartirlos con la asistencia de Citrix para que los analicen.
- Ver informes completos sobre el estado de su sitio.

La opción para habilitar el acceso a Citrix Smart Tools (y participar en Call Home, si no está ya habilitado) está marcada de forma predeterminada. Haga clic en **Conectar**. Se abre una ventana de explorador Web y va automáticamente a la página web de Smart Services, donde puede introducir sus **credenciales de cuenta de Citrix Cloud**. (Si no dispone de una cuenta de Citrix Cloud, simplemente introduzca las credenciales de cuenta de Citrix y se creará automáticamente una nueva cuenta de Citrix Cloud.) Después de autenticarse, se instala silenciosamente un certificado en el directorio Smart Tools Agent.

Para usar las tecnologías de Smart Tools, consulte la documentación de Citrix Smart Tools.

> Nota:
>
> Si habilita Smart Check al instalar un Controller, puede desactivarlo más tarde desinstalando Smart Check Agent. Para obtener más información, consulte Quitar el agente.

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 seguimientos de Citrix Diagnostic Facility que pueden ser útiles

© 1999-2019 Citrix Systems, Inc. All rights reserved.

para solucionar errores comunes como, por ejemplo, los registros de VDA e inicios de aplicaciones o escritorios. Esta tecnología se conoce como seguimiento permanente (Always-On Tracing o AOT). Los registros AOT se guardan en el disco en C:Users CitrixTelemetryServiceAppDataLocalCitrixAot.

Call Home no recopilará ningún otro seguimiento de eventos de Windows (Event Tracing for Windows, ETW), ni tampoco se puede configurar para hacerlo.

Call Home también recopila información adicional, como:

- Entradas de Registro creadas por Citrix Virtual Apps and Desktops en HKEY_LOCAL_MACHINE\SOFTWARE\Cit
- Información de WMI (Windows Management Instrumentation) 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

La información de seguimiento se comprime tras recopilarse. El servicio Citrix Telemetry Service conserva un máximo de 10 MB de la información de seguimiento 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 seguimientos 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> Nota:
>
> Si habilita Call Home al instalar un componente, puede inhabilitarlo más tarde. Para obtener más información, consulte Inhabilitar Call Home.

Requisitos previos

- La máquina debe estar ejecutando PowerShell 3.0 o posterior.
- La máquina debe estar ejecutando el servicio 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 del Controller: Cuando instala o actualiza un Controller desde la interfaz gráfica, se le pregunta si quiere participar en Call Home y conectarse a Citrix Smart Tools. Existen tres opciones:

- Conectar con Citrix Smart Tools, lo que incluye la funcionalidad Call Home vía Smart Tools Agent. Esta es la opción predeterminada y recomendada. Si elige esta opción, se configura el agente Smart Tools. (El agente Smart Tools se instala independientemente de si se selecciona esta opción.)
- Participar solo en Call Home, pero no conectar con Smart Tools. Si elige esta opción, el agente Smart Tools se instala, pero no se configura. La funcionalidad Call Home se proporciona a través de Citrix Telemetry Service y Citrix Insight Services.
- No conectar con Smart Tools ni participar en Call Home.

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, la página le preguntará solo sobre Smart Tools. Si ya está inscrito en Call Home y el agente Smart Tools ya está instalado, no aparecerá la página del asistente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para obtener más información acerca de Smart Tools, consulte la documentación de Smart Tools.

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.

```
$cred = Get-Credential
Enable-CitrixCallHome -Credential $cred
```

Para confirmar que las cargas programadas se han habilitado, escriba **Get-CitrixCallHome**. Este comando debe devolver 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. Este comando debe devolver IsEnabled=True y IsMasterImage=True.

Creación de una programación personalizada: Cree una programación semanal o diaria para recopilaciones y cargas de diagnósticos.

```
$timespan = New-TimeSpan -Hours <hours> -Minutes <minutes>
Set-CitrixCallHomeSchedule -TimeOfDay $timespan -DayOfWeek <day> -
   UploadFrequency {
 Daily|Weekly }
```

Ejemplos:

El cmdlet siguiente crea una programación para crear un paquete con los datos y cargarlos a las 23:20 de la noche. 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
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para confirmar la programación, introduzca `Get-CitrixCallHomeSchedule`. En el ejemplo anterior, la acción debería devolver `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 23:20 de la noche 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 debería devolver `StartTime=22:20:00, DayOfWeek=Wednesday, Upload Frequency=Weekly`.

Inhabilitar Call Home

Puede inhabilitar Call Home usando 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`. La acción debería devolver `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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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.

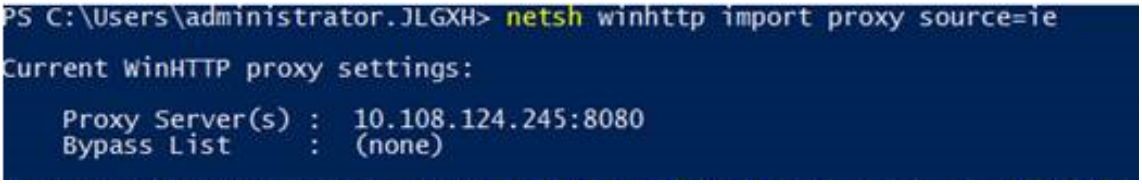
```
Enable-CitrixTrace -Listen '{ "trace" :{ "enabled" :false, "persistDirectory"
: "C:\Users\Public" ," maxSizeBytes" :1000000, "sliceDurationSeconds" :300 } }
'
```

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

4. Reinicie el servicio de telemetría.

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 usando el sitio Web de CIS:

1. Inicie una sesión en Citrix Insight Services usando 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. Posteriormente, use el cmdlet `Send-CitrixCallHomeBundle` para cargar 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

carga en el registro de eventos del sistema. La solicitud de carga puede rechazarse si el servicio ya está ejecutando 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 <String>] [<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 guardará 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.
- **SRNumbwe:** 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'
  - 'localdata'

© 1999-2019 Citrix Systems, Inc. All rights reserved.

  - '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 VDA de Citrix Provisioning, notificados a las 2:30 para el caso de asistencia de Citrix Support número 123456. Además de los datos de Call Home, se incorporará el archivo "c:\Diagnostics\ExtraData.zip" al paquete que se carga.

```
1 C:\PS>Start-CitrixCallHomeUpload -InputPath "c:\Diagnostics\ExtraData.
     zip" -Description "Registration failures with Citrix Provisioning
     VDAs" -IncidentTime "14:30" -SRNumber 123456 -Name "
     RegistrationFailure-021812016" -Collect "{
2  'wmi':{
3  'enabled':false }
4   }
5  " -UploadHeader "{
6  'key1':'value1' }
7  " -AppendHeaders "{
8  'key2':'value2' }
9  "
```

El siguiente cmdlet guarda los datos de Call Home relacionados con el caso de asistencia técnica de Citrix Support número 223344, notificado a las 8:15 de la mañana. Los datos se guardan en el archivo mydata.zip en un recurso compartido de red. Además de los datos de Call Home, se incorporará el archivo "c:\Diagnostics\ExtraData.zip" al paquete guardado.

```
1 C:\PS>Start-CitrixCallHomeUpload -OutputPath \mynetwork\myshare\mydata.
     zip -InputPath "c:\Diagnostics\ExtraData.zip" -Description "
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

```
    Diagnostics for incident number 223344" -IncidentTime "8:15" -
    SRNumber 223344
```

El cmdlet siguiente carga el paquete de los datos que guardó previamente.

```
1 $cred=Get-Credential
2 C:\PS>Send-CitrixCallHomeBundle  -Credential $cred -Path \mynetwork\
    myshare\mydata.zip
```

Citrix Scout

March 8, 2019

Introducción

Citrix Scout recopila diagnósticos que pueden usarse para el mantenimiento proactivo de la implementación de Citrix Virtual Apps and Desktops. Citrix ofrece un análisis integral y automatizado a través de Citrix Insight Services. También puede usar Citrix Scout para solucionar problemas por su cuenta o siguiendo las instrucciones de la Asistencia de Citrix. 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 tres procedimientos principales:

- **Recopilar:** Se recopilan diagnósticos una vez en las máquinas que seleccione en el sitio. A continuación, puede cargar en Citrix el archivo que contiene la información recopilada, o bien, puede 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. Entonces, Scout recopila otros diagnósticos y carga en Citrix el archivo que contiene el rastreo y la información recopilada, o bien, guarda el archivo localmente.
- **Programar:** Se programan recopilaciones diarias o semanales de diagnósticos en un tiempo especificado y en las máquinas que seleccione. El archivo que contiene cada recopilación se carga automáticamente en Citrix.

La interfaz gráfica que se describe en este artículo es la forma principal de usar Citrix Scout. De forma alternativa, puede utilizar la interfaz de PowerShell para configurar recopilaciones puntuales, programarlas o cargarlas. Consulte Call Home.

Dónde ejecutar Scout:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- En una implementación local de Citrix Virtual Apps and Desktops, ejecute Citrix Scout desde un Delivery Controller para capturar diagnósticos de uno o varios Delivery Controllers y de agentes Virtual Delivery Agent (VDA). También puede ejecutar Scout desde un VDA para recopilar diagnósticos locales.
- En un entorno de Citrix Cloud donde se usa el servicio Citrix Virtual Apps and Desktops, ejecute Citrix Scout desde un VDA para recopilar datos de diagnóstico local.

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 rastreos 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).

Los datos capturados incluyen:

- Entradas de Registro creadas por Citrix Virtual Apps and Desktops en HKEY_LOCAL_MACHINE\SOFTWARE\CIT
- Información de WMI (Windows Management Instrumentation) en el espacio de nombres de Citrix.
- Procesos que se están ejecutando.
- Volcados de errores de procesos de Citrix que están almacenados en %PROGRAM DATA%\Citrix\CDF

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, el servicio Citrix Telemetry Service conserva la información de rastreo más reciente comprimida, durante un tiempo límite máximo de ocho días.
- A partir de Citrix Virtual Apps y Desktops 7 1808, los seguimientos de AOT se guardan en el disco local de forma predeterminada. (En versiones anteriores, los seguimientos se guardaban en la memoria). Ruta predeterminada = C:\Users\CitrixTelemetryService\AppData\Local\CitrixAOT.
- A partir de Citrix Virtual Apps and Desktops 7 1811, los seguimientos de 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, utilizando el cmdlet `Enable-CitrixTrace` o la cadena de Registro de DefaultListen HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Telemetry.
- Los seguimientos se adjuntan al archivo hasta que el archivo 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Consideraciones y requisitos

Permisos

- 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.
- Use **Ejecutar como administrador** al iniciar Citrix Scout.

Para cada máquina desde la que recopile diagnósticos:

- 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 el servicio Citrix Telemetry Service.
- Si quiere programar la recopilación de diagnósticos, la máquina debe ejecutar una versión de Scout que se incluye en Citrix Virtual Apps and Desktops (o XenApp y XenDesktop de 7.14 a 7.18).

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 comprobar que se cumplen estos requisitos.

Pruebas de verificación

Antes del inicio de una recopilación de diagnóstico, se ejecutan automáticamente pruebas en cada máquina seleccionada. Estas pruebas tienen por finalidad comprobar que se cumplen los requisitos mencionados. 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. (Esto puede incluir 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **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 el servicio de telemetría de Citrix** Asegúrese de que el servicio de telemetría Citrix Telemetry Service está instalado e iniciado en la máquina.
- **No se puede obtener la programación** Actualice la máquina a XenApp y XenDesktop 7.14 (mínimo).

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 versión posterior respaldada), la versión anterior de Scout se reemplaza por la versión actual.

Función	Scout 2.23	Scout 3.0
Respaldo para Citrix Virtual Apps and Desktops (además de XenApp y XenDesktop de 7.14 a 7.18)	Sí	Sí
Respaldo para XenDesktop 5.x, 7.1 a 7.13	Sí	No
Respaldo para XenApp 6.x, 7.5 a 7.13	Sí	No
Entregado con el producto	7.1 a 7.13	A partir de 7.14
Se puede descargar desde un artículo CTX	Sí	No
Captura de rastreos CDF	Sí	Sí
Captura de 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)

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Función	Scout 2.23	Scout 3.0
Permitir que los datos de diagnóstico se envíen a Citrix	Sí	Sí
Permitir que los datos de diagnóstico se guarden localmente	Sí	Sí
Respaldo para credenciales de Citrix Cloud	No	Sí
Respaldo para credenciales de Citrix	Sí	Sí
Respaldo de servidor proxy para cargas	Sí	Sí
Ajustar programaciones	N/D	Sí
Respaldo para script	Línea de comandos (solo para el Controller local)	PowerShell mediante los cmdlets de Call Home (es decir, cualquier máquina con telemetría instalada)

Instalar

De forma predeterminada, Scout se instala automáticamente como parte de Citrix Telemetry Service cuando se instala un VDA o un Controller.

Si omite el servicio 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 la ISO de Citrix Virtual Apps and Desktops.

Autorización de carga

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

- Si se autentica con una cuenta de Citrix, el proceso de emisión de token no se ve. Simplemente, introduce sus credenciales de cuenta. Una vez que Citrix valida las credenciales, se le permite continuar en el asistente de Citrix Scout.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Si se autentica con una cuenta de Citrix Cloud, debe hacer clic en un enlace para acceder a Citrix Cloud mediante HTTPS con su explorador Web predeterminado. Después de introducir sus credenciales de Citrix Cloud, se muestra el token. Copie el token y luego péguelo en Citrix Scout. Entonces, se le permite continuar en el asistente de Citrix Scout.

El token se almacena localmente en la máquina que ejecuta Citrix Scout. Si quiere usar este token la próxima vez que seleccione **Recopilar** o **Rastrear y reproducir**, marque la casilla **Guardar el token y omitir este paso en el futuro**.

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

Usar un proxy para cargas

Si quiere utilizar un proxy para cargar recopilaciones en Citrix, puede configurar Citrix Scout para que use los parámetros de proxy configurados para las propiedades de Internet del explorador, o bien, puede especificar la dirección IP y el número de puerto del servidor proxy.

Agregar máquinas manualmente

Después de que Scout forme una lista de los Controllers y los agentes VDA que haya detectado, puede agregar manualmente otras máquinas que se utilicen en la implementación de Citrix Virtual Apps and Desktops (por ejemplo, servidores StoreFront y servidores 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 máquinas adicionales, si fuera necesario. 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 lo tienen.

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 las máquinas adicionales agregadas manualmente.

Scout recuerda las máquinas agregadas manualmente hasta que las elimine. Después de agregar las máquinas, si cierra y luego vuelve 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 StoreFront. Sin embargo, se recopila toda la información restante de rastreo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Recopilar diagnósticos

El procedimiento de recopilación comprende: 1) la selección de máquinas, 2) el inicio de la recopilación de datos de diagnóstico y 3) la carga del archivo que contiene la recopilación en Citrix (también se puede guardar localmente).

1. Inicie Citrix Scout. Desde el menú de inicio de la máquina: **Citrix > Citrix Scout**. En la página de inicio, haga clic en **Recopilar**.
2. Seleccione las máquinas. La página **Seleccionar máquinas** ofrece una lista de todos los agentes VDA y los Controllers del sitio. Puede filtrar la lista por el nombre de la máquina. Marque la casilla de verificación situada junto a cada máquina de la que quiera recopilar datos de diagnóstico y, a continuación, haga clic en **Continuar**.

   Scout inicia automáticamente pruebas en cada máquina que haya seleccionado 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 de 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.

   (Para agregar manualmente otras máquinas, por ejemplo, servidores Citrix Provisioning o StoreFront, consulte Agregar máquinas manualmente.)

   Cuando las pruebas de verificación se completen, haga clic en **Continuar**.
3. Recopile diagnósticos de máquinas. En el resumen, se ofrece una lista de todas las máquinas desde donde se recopilarán los diagnósticos (las máquinas seleccionadas que han superado las pruebas de verificación). Haga clic en **Empezar a recopilar**.

   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**.
   - Si la recopilación de una máquina se realiza correctamente y quiere volver a recopilar datos de diagnóstico de ella, haga clic en **Recopilar otra vez** en la columna “Acción” de la

© 1999-2019 Citrix Systems, Inc. All rights reserved.

máquina. La recopilación más reciente sobrescribe la anterior.
- Si se produce un error en una recopilación, haga 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 en ese botón y confirma la solicitud del sistema, se pierde la recopilación.

Cuando la recopilación se complete, haga clic en **Continuar**.

4. Guarde o cargue la recopilación. Elija si quiere cargar el archivo que contiene el diagnóstico recopilado en Citrix o guardarlo en la máquina local.

   Si elige cargar el archivo ahora, continúe al 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 más adelante en Citrix; consulte CTX136396 para Citrix Insight Services o Respaldo para Smart Tools.

   Haga clic en **Hecho** 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 especifique un proxy opcional. Revise Autorización de carga para obtener más información de este proceso.

   - Si aún no se ha autenticado por Citrix Scout, continúe con este paso.
   - Si ya se ha autenticado por Citrix Scout, el token de autorización almacenado se utiliza de forma predeterminada. Si le parece bien, elija esta opción y haga clic en **Continuar**. No se le solicitan credenciales para esta recopilación; continúe al paso 6.
   - Si se ha autenticado antes, pero quiere volver a autorizar la carga y volver a tener un token recién emitido, 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 Citrix Scout para que use los parámetros de proxy configurados para las propiedades de Internet del explorador, o bien, puede especificar 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 iniciará con una página de Citrix Cloud donde se mostrará el token. Copie el token y luego péguelo en la página de Citrix Scout.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Para una cuenta de Citrix, introduzca las credenciales.

Cuando haya terminado, haga clic en **Continuar**.

6. Facilite información sobre la carga. Introduzca los datos de carga:

   - El campo de nombre contiene el nombre predeterminado para el archivo que contendrá los diagnósticos recopilados. Este nombre debería bastar 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 de descripción opcional, 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 **Hecho** para volver a la página de inicio de Citrix Scout.

Rastrear y reproducir

El procedimiento de rastreo y reproducción comprende: 1) la selección de máquinas, 2) el inicio del rastreo en esas máquinas, 3) la reproducción de los problemas en esas máquinas, 4) la recopilación de diagnósticos y 5) la carga del archivo que contiene el rastreo y la recopilación en Citrix (también puede guardarlo localmente).

Este procedimiento es similar al procedimiento de recopilación estándar. No obstante, permite iniciar un rastreo en las máquinas y, a continuación, recrear los problemas ocurridos en esas máquinas. Todas las recopilaciones de diagnóstico incluyen información de rastreo AOT; este procedimiento agrega rastreos CDF para facilitar la solución de problemas.

1. Inicie Citrix Scout. Desde el menú de inicio de la máquina: **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 y, a continuación, haga clic en **Continuar**.

   Scout inicia pruebas en cada máquina que haya seleccionado para verificar que cumple los criterios que figuran en Pruebas de verificación. Si se produce un error en la verificación de una

© 1999-2019 Citrix Systems, Inc. All rights reserved.

máquina, aparece un mensaje en la columna de 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 rastreo ni diagnóstico en esa máquina.

(Para agregar manualmente otras máquinas, por ejemplo, servidores Citrix Provisioning o StoreFront, consulte Agregar máquinas manualmente.)

Cuando las pruebas de verificación se completen, haga clic en **Continuar**.

3. Rastreo. En el resumen, se ofrece una lista de todas las máquinas desde donde se recopilarán rastreos. Haga clic en **Empezar el 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 **Empezar a recopilar**. 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**.
   - Si la recopilación de una máquina se realiza correctamente y quiere volver a recopilar datos de diagnóstico de ella, haga clic en **Recopilar otra vez** en la columna “Acción” de la máquina. La recopilación más reciente sobrescribe la anterior.
   - Si se produce un error en una recopilación, haga 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 el botón **Atrás**. Si hace clic en ese botón y confirma la solicitud del sistema, se pierde la recopilación.

   Cuando la recopilación se complete, haga clic en **Continuar**.

5. Guarde o cargue la recopilación. Elija si quiere cargar el archivo que contiene el diagnóstico recopilado en Citrix o guardarlo en la máquina local.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Si elige cargar el archivo ahora, continúe al 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 o Citrix Smart Tools.

Haga clic en **Hecho** 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 especifique un proxy opcional. Revise Autorización de carga para obtener más información de este proceso.

   - Si aún no se ha autenticado por Citrix Scout, continúe con este paso.
   - Si ya se ha autenticado por Citrix Scout, el token de autorización almacenado se utiliza de forma predeterminada. Si le parece bien, elija esta opción y haga clic en **Continuar**. No se le solicitan credenciales para esta recopilación; continúe al paso 7.
   - Si se ha autenticado antes, pero quiere volver a autorizar la carga y volver a tener un token recién emitido, 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 Citrix Scout para que use los parámetros de proxy configurados para las propiedades de Internet del explorador, o bien, puede especificar 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 iniciará con una página de Citrix Cloud donde se mostrará 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 para el archivo que contendrá los diagnósticos recopilados. Este nombre debería bastar 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.)

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Si lo prefiere, puede especificar un número de caso de asistencia de Citrix de 8 dígitos.
- En el campo de descripción opcional, 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 **Hecho** para volver a la página de inicio de Citrix Scout.

Programar recopilaciones

El procedimiento de programación comprende: 1) seleccionar las máquinas y 2) establecer o cancelar 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 Citrix Scout. Desde el menú de inicio de la máquina: **Citrix > Citrix Scout**. En la página de inicio, haga clic en **Programar**.
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.

   Cuando instaló agentes VDA y Controllers desde la interfaz gráfica, se le ofreció la posibilidad de participar en Call Home. Para obtener más información, consulte Citrix Call Home. (Call Home incluye una funcionalidad de programación equivalente a Scout.) Scout muestra esos parámetros de forma predeterminada. Puede usar esta versión de Scout para iniciar recopilaciones programadas por primera vez, o bien, para cambiar una programación previamente configurada.

   Tenga en cuenta que, aunque haya habilitado o inhabilitado Call Home para cada máquina, al configurar una programación en Scout, se utilizan los mismos comandos, y éstos afectan a todas las máquinas que seleccione.

   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 pruebas en cada máquina que haya seleccionado 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 de estado y la casilla de verificación de la máquina se desmarca. Puede:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- 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 rastreo ni diagnóstico en esa máquina.

(Para agregar manualmente otras máquinas, por ejemplo, servidores Citrix Provisioning o StoreFront, consulte Agregar máquinas manualmente.)

Cuando las pruebas de verificación se completen, haga clic en **Continuar**.

En la página de resumen, se ofrece una lista de las máquinas a las que se aplicarán las programaciones. Haga clic en **Continuar**.

3. Configure la programación. Indique si quiere que se recopilen datos de diagnóstico. Recuerde: La programación afecta a todas las máquinas seleccionadas.

   - Para configurar una programación semanal para las máquinas seleccionadas, haga clic en **Semanalmente**. Elija el día de la semana e introduzca la hora del día (reloj de 24 horas) cuando comenzará la recopilación de datos de diagnóstico.
   - Para configurar una programación diaria para las máquinas seleccionadas, haga clic en **Diariamente**. Elija la hora del día (reloj de 24 horas) cuando comenzará la recopilación de datos de diagnóstico.
   - 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 especifique un proxy opcional. 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 Citrix Scout para que use los parámetros de proxy configurados para las propiedades de Internet del explorador, o bien, puede especificar 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 iniciará con una página de Citrix Cloud donde se mostrará 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**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Revise la programación configurada. Haga clic en **Hecho** para volver a la página de inicio de Citrix Scout.

Cuando se produzca cada recopilación programada, la recopilación y la carga se registrarán en entradas del registro de aplicación Windows de cada máquina seleccionada.

Supervisar

November 29, 2018

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.

Registros de configuración

El registro de configuración (Configuration Logging) es una función que permite a los administradores realizar un seguimiento 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 seguimiento 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 fallidas de escritorio
- Máquinas fallidas de servidor

Para obtener más información sobre cómo habilitar y configurar la función Registro de configuración, consulte el artículo Registro de configuración. Los artículos de Director describen cómo ver la información registrada de esa herramienta.

Registros de eventos

Los servicios dentro de Citrix Virtual Apps and Desktops registran los eventos que ocurren. Los registros de eventos se pueden usar para supervisar y solucionar problemas de las operaciones.

Para obtener más información, consulte Registros de eventos. Los artículos referidos a funcionalidades individuales también pueden contener información de eventos.

Registros de configuración

January 29, 2019

La característica Registros de configuración (Configuration Logging) captura, en una base de datos, los cambios de configuración y las actividades de administración realizados en un sitio. Puede usar el contenido registrado para:

- Diagnosticar y solucionar problemas después de realizar cambios de configuración; el registro proporciona un trazado de los pasos seguidos.
- Ayudar en la administración de cambios y en el seguimiento de las configuraciones
- Realizar informes de actividades administrativas

Puede establecerlas 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 durante la fase de 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).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 respaldo 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 respaldan los registros de configuración no tienen ningún nodo Registros en Studio.

Habilitar o inhabilitar los Registros de configuración y el registro obligatorio

De forma predeterminada, Registros de configuración (Configuration Logging) está habilitado, pero la captura obligatoria está inhabilitada.

1. Seleccione **Registros** en el panel de navegación de Studio.
2. Seleccione **Preferencias** en el panel "Acciones". El cuadro de diálogo Registros de configuración contiene información sobre las bases de datos e indica si los registros de configuración y el registro obligatorio están habilitados o inhabilitados.
3. Seleccione la acción pertinente:

   Para habilitar Registros de configuración, seleccione **Habilitar**. Esta es la opción predeterminada. Si no se puede escribir en la base de datos, los datos de registros se descartan, aunque la operación sigue teniendo lugar.

   Para inhabilitar Registros de configuración, seleccione **Inhabilitar**. Si la captura de registros estuvo habilitada previamente, los registros existentes se conservan y se pueden seguir consultando con el SDK de PowerShell.

   Para habilitar la captura obligatoria de registros, seleccione **Impedir cambios en la configuración si la base de datos no está disponible**. No se permitirá ningún cambio de configuración o de tipo administrativo que normalmente se registraría, a menos que pueda registrarse en la base de datos de registros de configuración. Puede habilitar el registro obligatorio solo cuando Registros de configuración está habilitado; es decir, cuando **Habilitar** está seleccionado. Si el servicio de registros de configuración (Configuration Logging Service) falla y no se usa la alta

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 usando una versión respaldada de SQL Server.
2. Seleccione **Registros** en el panel de navegación de Studio.
3. Seleccione **Preferencias** en el panel "Acciones".
4. En el cuadro de diálogo "Preferencias de registros", seleccione **Cambiar base de datos de registros**.
5. En el cuadro de diálogo Cambiar base de datos de registros, especifique la ubicación del servidor que contiene el nuevo servidor de base de datos. Consulte Formatos de direcciones de bases de datos para conocer los formatos válidos.
6. Para permitir que Studio cree la base de datos, haga clic en **Aceptar**. Cuando se le solicite, haga clic en **Aceptar** y la base de datos se creará automáticamente. Studio intenta acceder a la base de datos usando 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 opera-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

ciones 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:

- Ordenar los elementos en pantalla por el encabezado de la columna.
- Filtrar los elementos en pantalla especificando un intervalo de un día o escribiendo un texto en el cuadro **Buscar**. Para volver a la versión estándar de la presentación de los registros, borre el texto del cuadro **Buscar**.

Generar informes

Puede generar informes CSV y HTML que contengan los datos de los registros de configuración.

- El informe CSV es un volcado de todos los datos de registros correspondientes a un intervalo de tiempo específico. Los datos jerárquicos en la base de datos se vuelcan sin estructura en una sola tabla CSV. Ningún aspecto de los datos tiene prioridad en la tabla. No se utiliza ningún tipo de formato y no se supone ningún tipo de legibilidad humana. El archivo (denominado MyReport) contiene datos en formato universalmente consumible. Los archivos CSV se usan a menudo para archivos históricos o como fuentes de datos para alguna herramienta de gestión de datos o de creación de informes como Microsoft Excel.
- El informe HTML presenta los datos de registros correspondientes a un intervalo de tiempo, en un formato legible para las personas. Proporciona una vista estructurada y explorable donde se pueden consultar los cambios. Un informe HTML consta de dos archivos, llamados Resumen y Detalles. El archivo de Resumen consiste en una lista de las operaciones de alto nivel: cuándo ocurrió cada operación, quién la realizó y el resultado de la misma. 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para generar un informe de registros de configuración, seleccione **Registros** en el panel de navegación de Studio y, a continuación, seleccione **Crear informe personalizado** en el panel "Acciones".

- Seleccione el intervalo de fechas del informe.
- Seleccione el formato del informe: CSV, HTML o ambos.
- Busque la ubicación donde quiere guardar el informe.

Eliminar contenido de los registros de configuración

Para eliminar el registro de configuración, debe tener ciertos permisos de Administración delegada y permisos para la base de datos de SQL Server.

- **Administración delegada:** Debe tener un rol de administración delegada que le permita leer la configuración de la implementación. El rol Administrador total tiene ese permiso. Si se trata de un rol personalizado, éste debe tener seleccionados Solo lectura o Administrar en la categoría Otros permisos.

  Para crear una copia de respaldo de los datos de registros de configuración (Configuration Logging) antes de eliminarlos, el rol personalizado también debe tener seleccionados Solo lectura o Administrar en la categoría de Permisos para registros.

- **Base de datos SQL Server:** Debe tener unas credenciales de inicio de sesión de SQL Server con permiso para eliminar registros de la base de datos. Hay dos formas de hacerlo:

  - Usar unas credenciales para la base de datos SQL Server con un rol sysadmin de servidor, que permite realizar cualquier actividad en el servidor de la base de datos. De forma alternativa, los roles serveradmin o setupadmin de servidor permiten realizar operaciones de eliminación.
  - Si la implementación requiere seguridad adicional, use unas credenciales de base de datos que no sean de sysadmin asignadas a un usuario de la base de datos que tenga permisos para eliminar registros de la misma.

    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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Para eliminar los registros de configuración:

1. Seleccione **Registros** en el panel de navegación de Studio.
2. Seleccione **Eliminar registros** en el panel "Acciones".
3. Verá la opción para crear una copia de respaldo de los registros antes de eliminarlos. Si decide crear una copia de seguridad, vaya a la ubicación donde se guarda la copia archivada. La copia de seguridad se crea como un archivo CSV.

Una vez eliminados los registros de configuración, la eliminación de los registros es la primera actividad que se anotará en el nuevo registro vacío. Esa entrada proporciona información acerca de quién y cuándo eliminó los registros.

Registros de eventos

October 3, 2018

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 características concretas para obtener más información sobre los eventos.

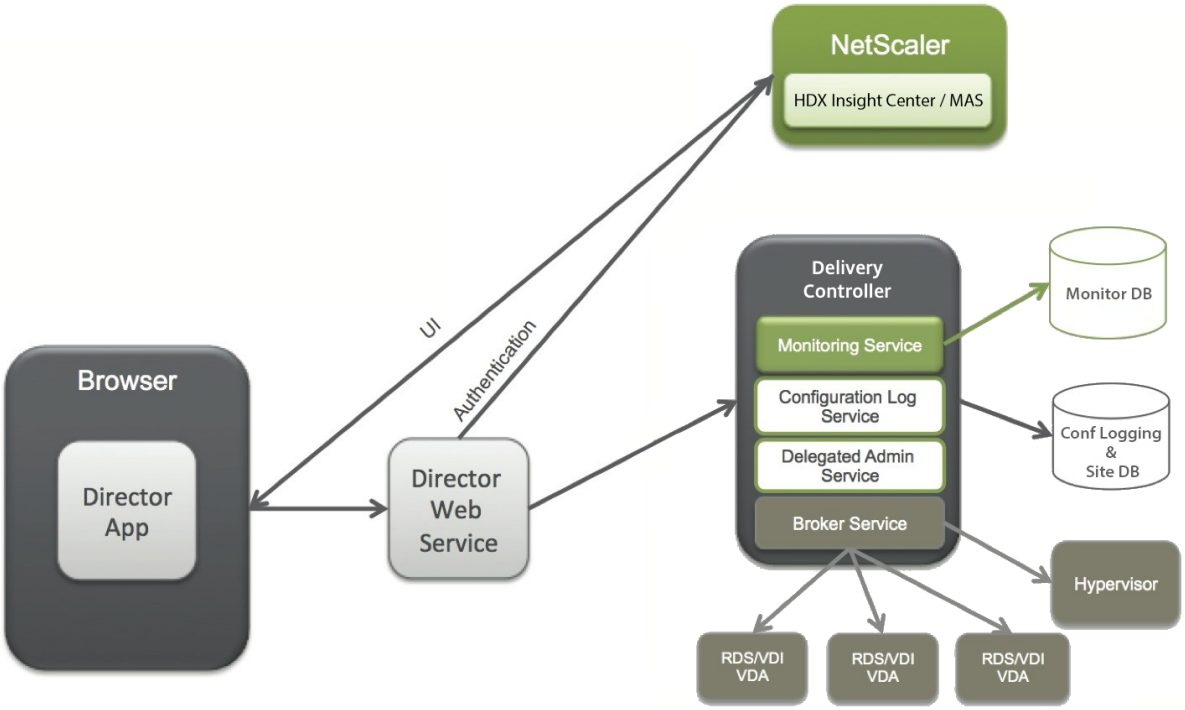
- Eventos de Citrix Broker Service
- Eventos del Citrix FMA Service SDK
- Eventos de Citrix Configuration Service
- Eventos de Citrix Delegated Administration Service

Director

March 8, 2019

Director es una consola para supervisar y solucionar problemas de Citrix Virtual Apps and Desktops.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



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 características de Analytics incluyen la administración de rendimiento para garantizar el estado y la capacidad de la implementación y el análisis de red y tendencias históricas, con tecnología de NetScaler MAS, con el fin de identificar posibles cuellos de botella debido a problemas de red en el entorno de Citrix Virtual Apps y Desktops.
- Datos históricos almacenados en la base de datos de supervisión para acceder a la base de datos de registros de configuración.
- Datos ICA desde NetScaler Gateway usando NetScaler MAS.
  - 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.
- Datos de Personal vDisk que permiten la supervisión en tiempo de ejecución y muestran la asignación base. Esto da a los equipos de asistencia la capacidad de restablecer los discos Personal vDisk (esta opción solo se utiliza como último recurso).
  - La herramienta de línea de comandos de CtxPvdDiag.exe se usa para recopilar la información de registros de usuarios en un solo archivo para la solución de problemas.

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 característica permite ver

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 Matriz de compatibilidad de funciones.

> Nota:
>
> Con la divulgación sobre las vulnerabilidades del canal lateral de ejecución especulativa Meltdown y Spectre, Citrix recomienda que instale las revisiones de mitigación relevantes. Tenga en cuenta que esas revisiones pueden afectar al rendimiento de SQL Server. Para obtener más información, consulte el artículo de asistencia de Microsoft: Protect SQL Server from attacks on Spectre and Meltdown side-channel vulnerabilities. Citrix recomienda probar la escalabilidad y planificar las cargas de trabajo antes de implementar esas revisiones en sus entornos de producción.

Director se instala de forma predeterminada como un sitio Web en el Delivery Controller. Para obtener información sobre requisitos previos y otros datos, consulte la documentación de Requisitos del sistema para esta versión. Para obtener información específica sobre la instalación y la configuración de Director, consulte Instalar y configurar Director.

Iniciar sesión en Director

El sitio Web de Director está ubicado en https o `http://<Server FQDN>/Director`.

Si uno de los sitios en la implementación de varios sitios está inactivo, el inicio de sesión de Director tarda un poco más porque intenta conectarse con el sitio que está inactivo.

Usar Director con la autenticación por tarjeta inteligente PIV

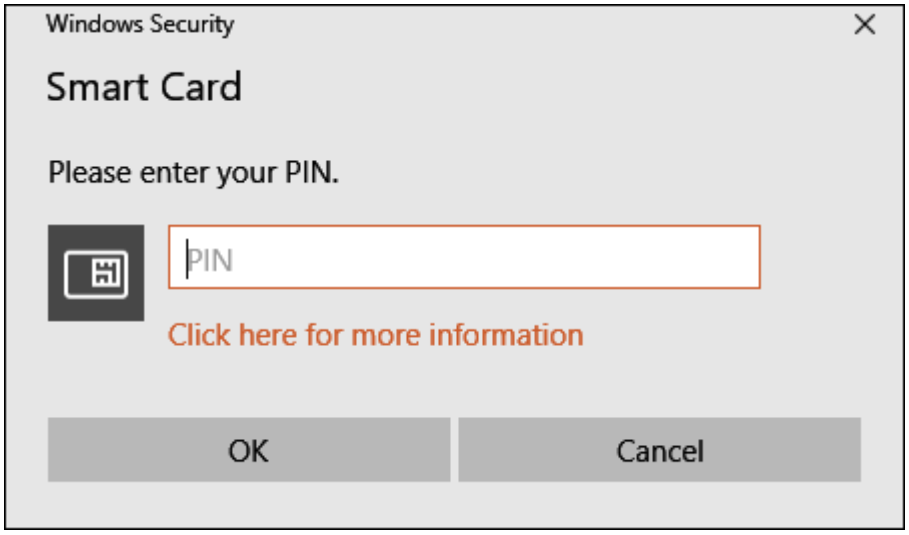
Ahora Director admite la autenticación con tarjetas inteligentes basadas en PIV (Personal Identity Verification) para iniciar sesión. Esta función es útil para organizaciones y agencias gubernamentales que usan la autenticación basada en tarjetas inteligentes para controlar el acceso.
La autenticación con tarjeta inteligente requiere una configuración específica en el servidor 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 utilizando una tarjeta inteligente:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

1. Inserte su tarjeta inteligente en el lector de tarjetas inteligentes.
2. Abra un explorador Web y vaya a la URL de Director, `https://<directorfqdn>/Director`.
3. Seleccione un certificado de usuario válido de la lista que se muestra.
4. Escriba su token de tarjeta inteligente.



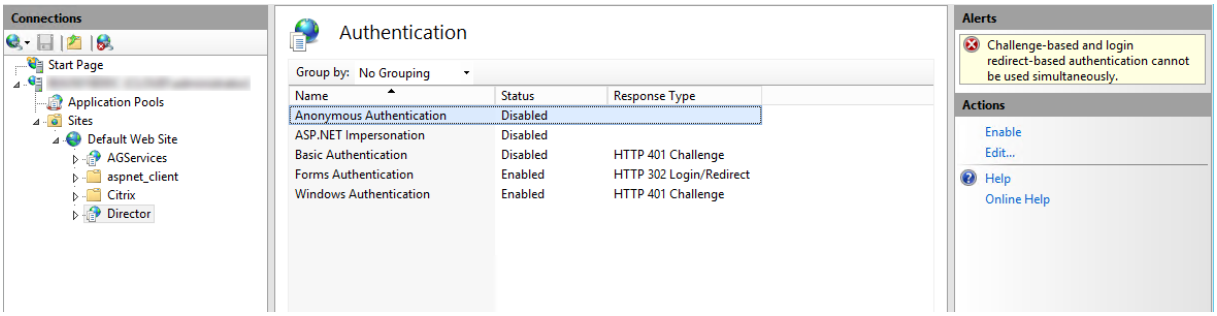
5. Después de autenticarse, puede acceder a Director sin tener que suministrar credenciales adicionales en la página de inicio de sesión de Director.

Usar Director con la autenticación integrada de Windows

Con la autenticación de Windows integrada (IWA), los usuarios unidos a un dominio obtienen acceso directo a Director sin tener que volver a escribir sus credenciales en la página de inicio de sesión de Director. A continuación, se presentan los requisitos previos para utilizar Director y la autenticación integrada de Windows:

- Habilite la autenticación de Windows integrada en el sitio Web de IIS que aloja Director. Al instalar Director, se habilitan formularios de autenticación anónima. Para combinar Director con la autenticación integrada de Windows, inhabilite la autenticación anónima y habilite la autenticación de Windows. Los formularios de autenticación deben permanecer establecidos en Habilitados para la autenticación de usuarios sin dominio.
  1. Inicie el Administrador de IIS.
  2. Vaya a **Sitios** > **Sitio Web predeterminado** > **Director**.
  3. Seleccione **Autenticación**.
  4. Haga clic con el botón secundario en **Autenticación anónima** y seleccione **Inhabilitar**.
  5. Haga clic con el botón secundario en **Autenticación de Windows** y seleccione **Habilitar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



- Configure el permiso de delegación de Active Directory para la máquina de Director. Esto solo es necesario si Director y el Delivery Controller están instalados en máquinas independientes.
    1. En la máquina de Active Directory, abra la consola de administración de Active Directory.
    2. Una vez abierta la consola de administración de Active Directory, vaya a **Nombre de dominio** > **Equipos**. Seleccione la máquina de Director.
    3. Haga clic con el botón secundario y seleccione **Propiedades**.
    4. En Propiedades, seleccione la ficha **Delegación**.
    5. Seleccione la opción **Confiar en este equipo para delegar en cualquier servicio (solo Kerberos)**.
- El explorador Web que se utilice para acceder a Director debe admitir la autenticación de Windows integrada. Esto puede requerir pasos de configuración adicionales en Firefox y Chrome. Para obtener más información, consulte la documentación del explorador.
- El servicio Monitoring Service debe ejecutar Microsoft .NET Framework 4.5.1 o una versión posterior admitida que conste en los Requisitos del sistema para Director. Para obtener más información, consulte Requisitos del sistema.

En Director, si un usuario cierra sesión o se agota el tiempo de espera de esa sesión, aparece la página de inicio de sesión. Desde la página de inicio de sesión, el usuario puede establecer el tipo de autenticación en **Inicio de sesión automático** o **Credenciales del usuario**.

Vistas de interfaz

Director proporciona diferentes vistas de la interfaz que se adaptan a administradores específicos. Los permisos del producto definen lo que se muestra y los comandos disponibles.

Por ejemplo, los administradores de asistencia técnica ven una interfaz adaptada a las tareas de asistencia técnica. Director permite a los administradores de asistencia técnica buscar al usuario que informa de un problema y muestra las actividades asociadas al usuario, tales como el estado de las aplicaciones y los procesos de ese usuario. Pueden resolver problemas rápidamente al realizar acciones como finalizar una aplicación o un proceso que no responden, las operaciones de remedo en la máquina del usuario, reiniciar la máquina o restablecer el perfil de usuario.

En cambio, los administradores totales pueden ver y administrar todo el sitio, y pueden ejecutar comandos para varios usuarios y máquinas. El panel de mandos ofrece información general de los as-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

pectos clave de la implementación, tales como el estado de las sesiones, los inicios de sesión de los usuarios y la infraestructura del sitio. La información se actualiza cada minuto. En caso de problemas, aparecen automáticamente los detalles sobre la cantidad y el tipo de fallos que se han producido.

Para obtener más información sobre los diversos roles y sus permisos en Director, consulte Administración delegada y Director

Recopilación de datos de uso por parte de Google Analytics

Después de instalar Director, el servicio de Director usa Google Analytics para recopilar datos de uso anónimos. Se recopilan estadísticas e información sobre el uso de las páginas "Tendencias" y los análisis sobre las llamadas de OData API. La recopilación de datos de análisis cumple con la directiva de privacidad de Citrix. La recopilación de datos se habilita de forma predeterminada cuando se instala Director.

Para dejar de participar en la recopilación de datos de Google Analytics, modifique la clave de Registro como se describe a continuación en la máquina donde está instalado Director. Si la clave de Registro aún no existe, créela y establézcala en el valor pertinente. Actualice la instancia de Director después de cambiar el valor de la clave de Registro.
Precaución: El uso incorrecto del Editor del Registro puede causar problemas graves que pueden requerir la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Citrix recomienda hacer una copia de seguridad del Registro de Windows antes de modificarlo.

Ubicación: HKEY_LOCAL_MACHINE\Software\Citrix\Director

Nombre: DisableGoogleAnalytics

Valor: 0 = habilitado (de forma predeterminada), 1 = inhabilitado

Puede usar el siguiente cmdlet de PowerShell para inhabilitar la recopilación de datos por parte de Google Analytics:

New-ItemProperty -Path HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Director -Name DisableGoogleAnalytics -PropertyType DWORD -Value 1

Instalar y configurar

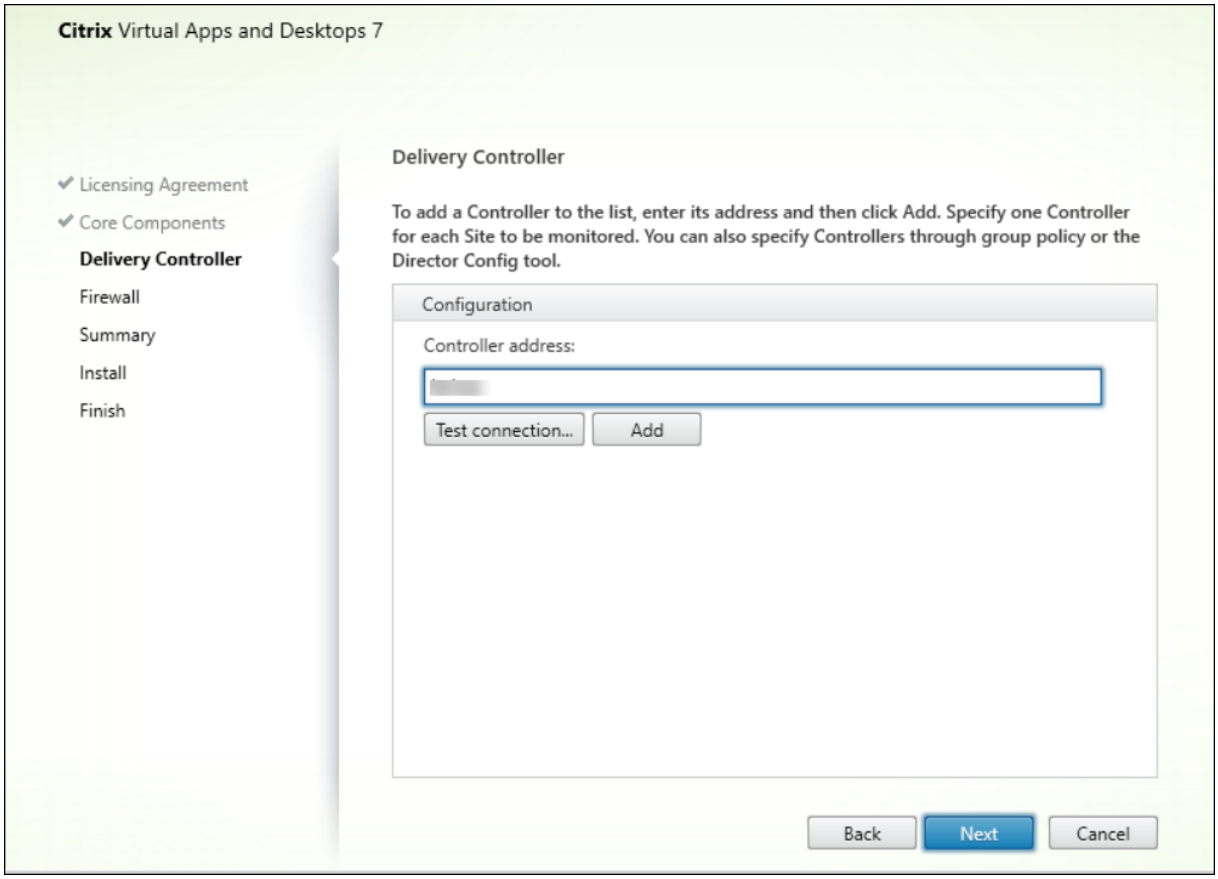
December 14, 2018

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 la ISO del instalador administra implementaciones típicas. 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.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

> Nota:
>
> Haga clic en **Agregar** para agregar el Controller que quiera supervisar.

Director se comunica con el Controller especificado de forma predeterminada. Especifique solo una dirección de un Controller para cada sitio que desea 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, asegúrese de sincronizar los relojes del sistema en todos los servidores donde estén instalados los Controllers, Director y otros componentes principales. De lo contrario, los sitios podrían no mostrarse correctamente en Director.

> Importante:
>
> Para proteger los nombres de usuario y las contraseñas enviados como texto sin formato a través de la red, Citrix recomienda permitir las conexiones de Director solo con HTTPS (no con HTTP). Algunas herramientas pueden leer nombres y contraseñas de texto sin formato en paquetes de red HTTP (sin cifrar), lo que puede crear un riesgo de seguridad para los usuarios.

Configurar permisos

Para iniciar sesión en Director, los administradores con permisos para Director deben ser usuarios del dominio de Active Directory y deben contar con los siguientes derechos:

- Derechos de lectura en todos los bosques de AD en los que se realizarán búsquedas (consulte Configuración avanzada).
- Roles configurados de administrador delegado (consulte Administración delegada y Director).
- Para remedar usuarios, los administradores deben configurarse mediante una directiva de grupo de Microsoft para la Asistencia remota de Windows. Además:
  - Durante la instalación de VDA, compruebe que la función Asistencia remota de Windows está habilitada en todos los dispositivos de usuario (seleccionada de forma predeterminada).

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- 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.

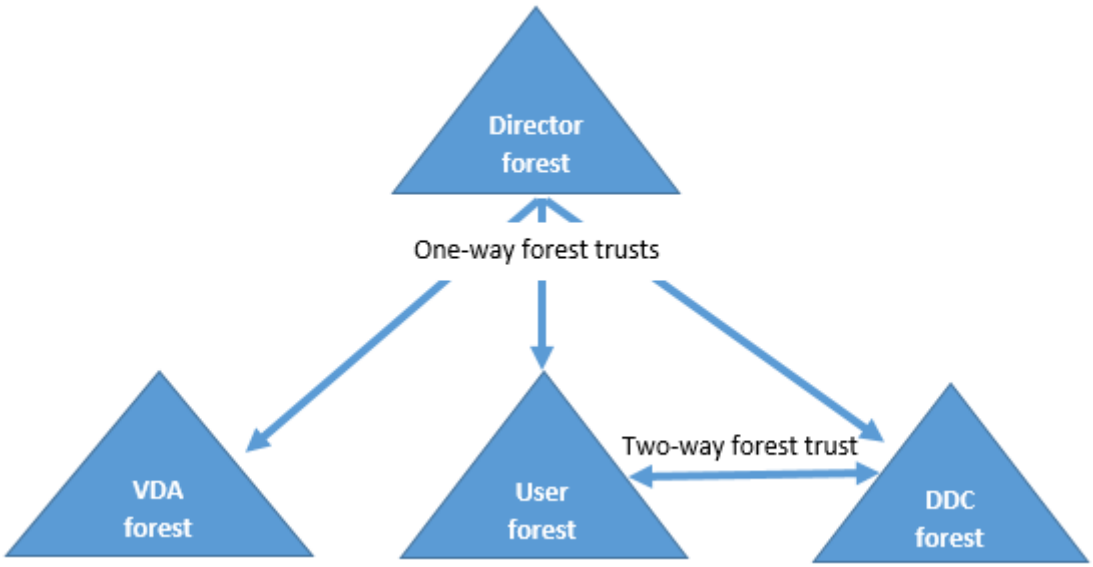
Configuración avanzada

January 29, 2019

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

La configuración avanzada necesaria para que Director respalde varios bosques se controla a través de parámetros definidos en el Administrador de Internet Information Services (IIS).

> Importante:
>
> Cuando cambie un parámetro en IIS, el servicio de Director se reiniciará automáticamente y cerrará las sesiones de los usuarios.

Para configurar parámetros avanzados mediante IIS:

1. Abra la consola del Administrador de Internet Information Services (IIS).
2. Vaya al sitio Web de Director en el sitio Web predeterminado.
3. Haga doble clic en **Configuración de aplicaciones**.
4. Haga doble clic en un parámetro para modificarlo.
5. Haga clic en **Agregar** para agregar un parámetro nuevo.

Director utiliza Active Directory para buscar usuarios y para consultar información adicional sobre usuarios y máquinas. De forma predeterminada, Director busca el dominio o el bosque en el que:

- La cuenta del administrador es miembro.
- El servidor Web de Director es miembro (en caso de que sea diferente).

Director intenta realizar búsquedas en el nivel del bosque mediante el catálogo global de Active Directory. Si no tiene permisos para realizar búsquedas en los bosques, la búsqueda se realiza en el dominio solamente.

Para buscar datos en otros dominios o bosques de Active Directory, debe establecer explícitamente los dominios o bosques en los que realizar las búsquedas. Configure este parámetro Aplicaciones para el sitio Web de Director en el Administrador de IIS:

```
1 Connector.ActiveDirectory.Domains = (user),(server)
```

Los atributos de valor user y server representan los dominios del usuario de Director (el administrador) y el servidor de Director respectivamente.

Para habilitar búsquedas desde un dominio o bosque adicionales, agregue el nombre del dominio a la lista, tal y como se muestra en el ejemplo:

```
1 Connector.ActiveDirectory.Domains = (user),(server),\<domain1\>,\<
    domain2\>
```

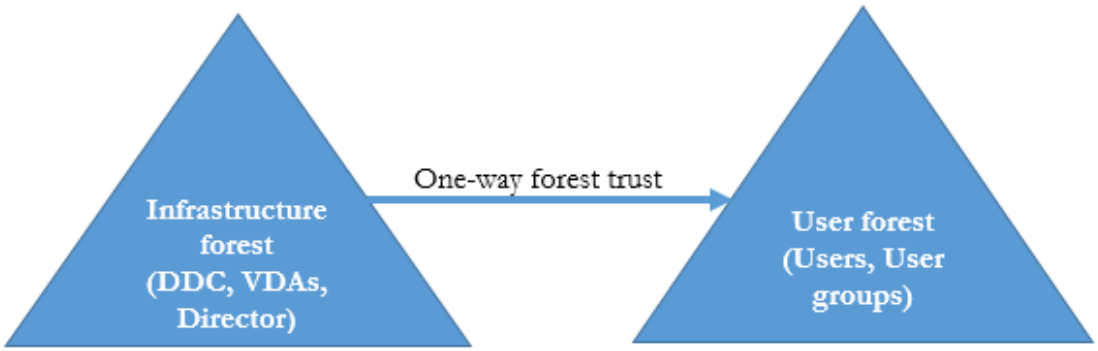
Para cada dominio de la lista, Director intenta realizar búsquedas en el nivel del bosque. Si no tiene permisos para realizar búsquedas en los bosques, la búsqueda se realiza en el dominio solamente.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurar grupo local de dominio

La mayoría de los proveedores de servicios Citrix (Citrix Service Providers) tienen configuraciones similares de entornos, compuestos de agentes VDA, Delivery Controllers y Director en lo que se llama el "bosque de infraestructura", mientras que los registros de usuarios o grupos pertenecen al "bosque del cliente". Existe una relación de confianza saliente unidireccional que se extiende desde el bosque de infraestructura al bosque del cliente.

Por regla general, los administradores CSP crean un grupo local de dominio en el bosque de infraestructura, y agregan a los usuarios o los grupos de usuarios que haya en el bosque del cliente a este grupo local de dominio.



Director da respaldo a una configuración 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 Connector.
       ActiveDirectory

   DomainLocalGroupSearchDomains= \<domain1\>,\<domain2\>
   ```

   Donde <domain1><domain2> son los nombres de los bosques donde reside el grupo local de dominio.

2. Asigne el grupo local de dominio a los grupos de entrega en Citrix Studio.
3. Reinicie IIS y vuelva a iniciar sesión en Director para que los cambios surtan efecto. Ahora, Director puede supervisar y mostrar las sesiones de estos usuarios.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Agregar sitios a Director

Si Director ya está instalado, configúrelo para que funcione con varios sitios. Para ello, utilice la consola del Administrador de IIS en cada servidor de Director para actualizar la lista de direcciones de servidor en la configuración de la aplicación.

Agregue la dirección de un Controller de cada sitio al siguiente parámetro:

```
Service.AutoDiscoveryAddresses = SiteAController,SiteBController
```

donde SiteAController y SiteBController son las direcciones de los Delivery Controllers de dos sitios diferentes.

Inhabilitar la visibilidad de las aplicaciones en ejecución en el Administrador de actividades

De forma predeterminada, el Administrador de actividades de Director muestra una lista de todas las aplicaciones que haya en ejecución en la sesión del usuario. Esta información pueden verla todos los administradores que tengan acceso a la función del Administrador de actividades de Director. Para los roles de administrador delegado, esto incluye los roles de administrador total, administrador de grupo 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, se pueden generar problemas graves que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

1. En el VDA, modifique la clave de Registro ubicada en HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskM
   De forma predeterminada, el valor de la clave es 1. Cambie el valor a 0 para que la información no se recopile del VDA y, por tanto, no se muestre en el Administrador de actividades.
2. En el servidor que tiene Director instalado, modifique el parámetro que controla la visibilidad de las aplicaciones en ejecución. De forma predeterminada, el valor es true, lo que permite la visibilidad de las aplicaciones en ejecución en la ficha Aplicaciones. Cambie el valor a false, lo que inhabilita la visibilidad. Esta opción solo afecta al Administrador de actividades de Director, no al VDA.
   Modifique el valor del parámetro siguiente:
   UI.TaskManager.EnableApplications = false

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> Importante:
>
> Para inhabilitar la vista de las aplicaciones en ejecución, Citrix recomienda realizar ambos cambios para que los datos no se muestren en el Administrador de actividades.

Configurar la autenticación con tarjetas inteligentes PIV

March 14, 2019

Este artículo contiene la configuración requerida en el servidor Director y en Active Directory para habilitar la función de la autenticación con tarjetas inteligentes.

> Nota:
>
> La autenticación con tarjetas inteligentes solo se admite para usuarios del mismo dominio de Active Directory.

Configurar el servidor de Director

Realice los siguientes pasos de configuración en el servidor de Director:

1. Instale y active la Autenticación de asignaciones de certificado de cliente. Siga las instrucciones indicadas en **Client Certificate Mapping authentication using Active Directory**, en el documento Client Certificate Mapping Authentication de Microsoft.
2. Inhabilite la autenticación mediante formularios en el sitio de Director.

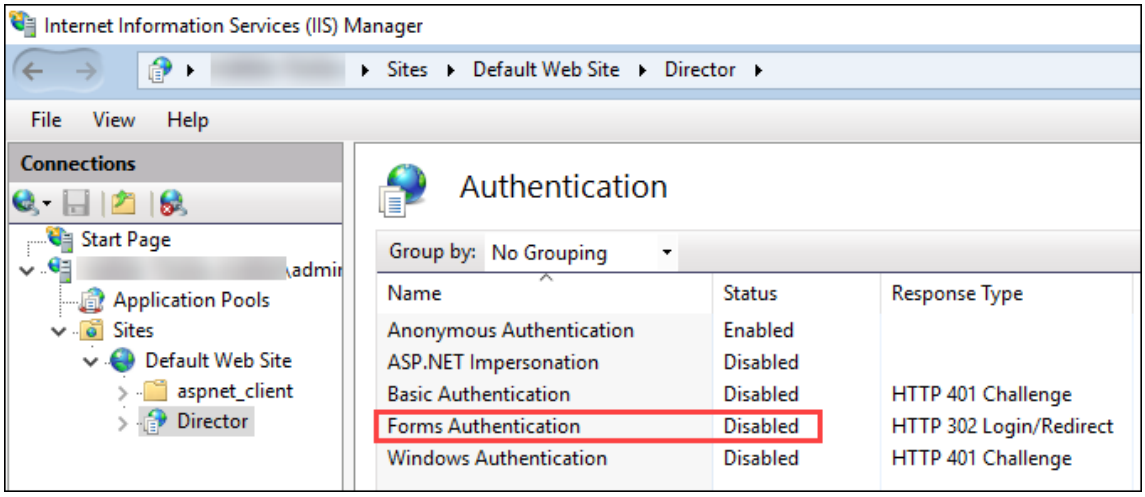
   Inicie el Administrador de IIS.

   Vaya a **Sitios** > **Sitio Web predeterminado** > **Director**.

   Seleccione **Autenticación**.

   Haga clic con el botón secundario en **Autenticación mediante formularios** y seleccione **Deshabilitar**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



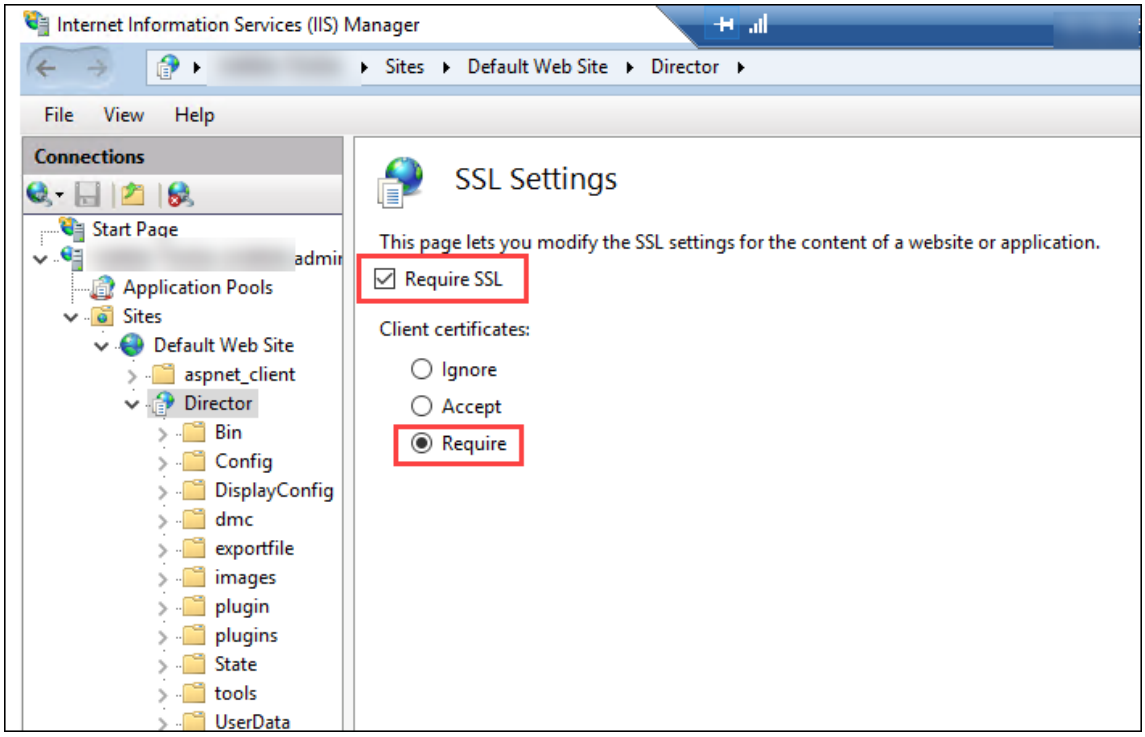
3. Configure la URL de Director para el protocolo HTTPS (más seguro que HTTP) para la autenticación de certificado del cliente.

   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) usando un editor de texto.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Debajo del elemento principal **<system.webServer>**, agregue el siguiente fragmento como primer elemento secundario:

```
<defaultDocument>
   <files>
       <add value="LogOn.aspx">
   <files>
<defaultDocument>
```

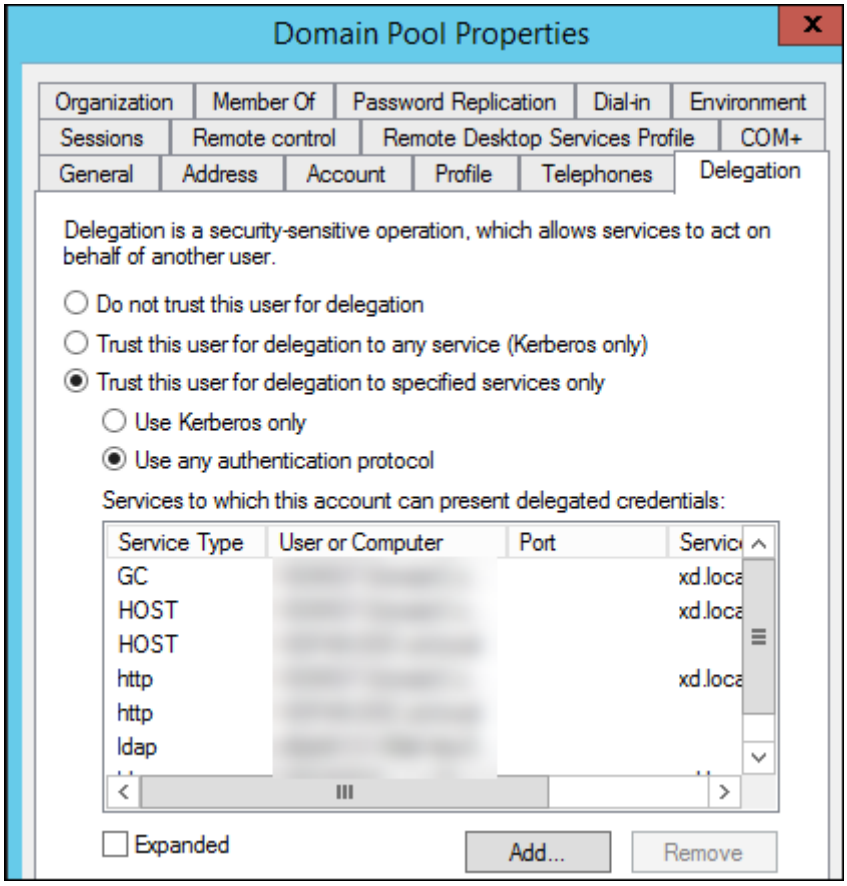
Configurar Active Directory

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 MSDN Microsoft.

Asigne la cuenta de servicio recién creada al grupo de aplicaciones de Director. La siguiente imagen muestra el cuadro de diálogo de propiedades de una cuenta de servicio de ejemplo, Domain Pool.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



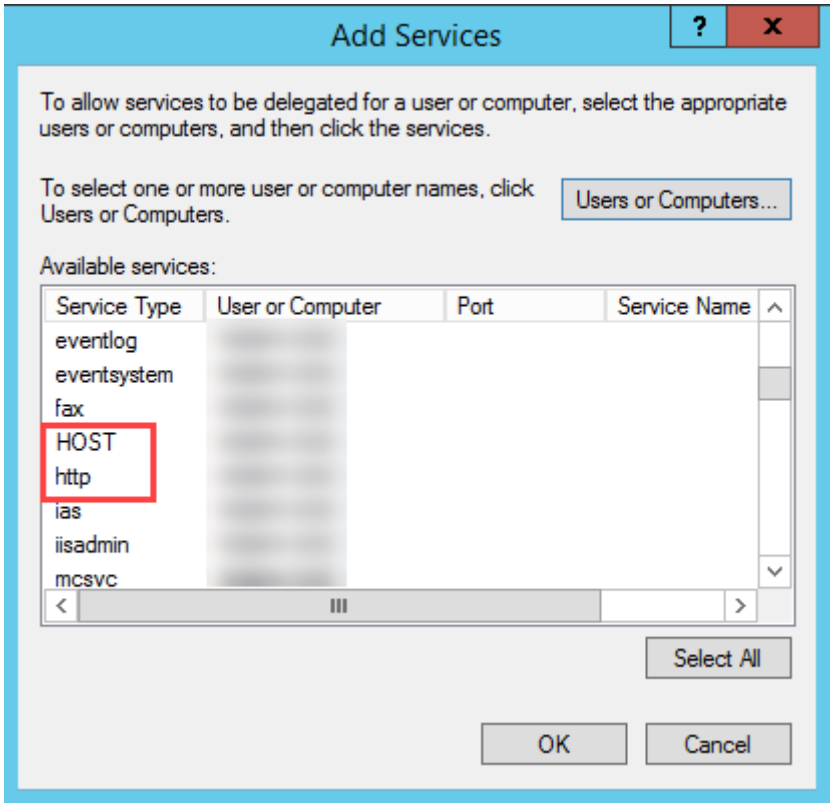
Configure los siguientes servicios para esta cuenta:

- Delivery Controller: HOST, http
- Director: HOST, http
- Active Directory: GC, LDAP

Para ello:

1. En el cuadro de diálogo de propiedades de la cuenta de usuario, haga clic en **Agregar**.
2. En el diálogo **Agregar servicios**, haga clic en “Usuarios o equipos”.
3. Seleccione el nombre de host del Delivery Controller.
4. En la lista **Servicios disponibles**, seleccione “HOST” y “http” en **Tipo de servicio**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



De forma similar, agregue “Tipos de servicio” para los hosts de **Director** y **Active Directory**.

Configurar el explorador Firefox

Para usar el explorador Firefox, instale el controlador PIV disponible en OpenSC 0.17.0. Para obtener instrucciones de instalación y configuración, consulte Installing OpenSC PKCS#11 Module in Firefox, Step by Step.
Para obtener información sobre el uso de la función de autenticación basada en tarjetas inteligentes en Director, consulte el apartado Usar Director con la autenticación por tarjeta inteligente basada en PIV en el artículo “Director”.

Configurar el análisis de red

December 14, 2018

> Nota:
>
> La disponibilidad de esta función depende de la licencia de la organización y los permisos de administrador.

Director se integra en Citrix ADM para ofrecer análisis de la red y administración del rendimiento:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- El análisis de red utiliza informes de HDX Insight desde Citrix ADM para proporcionar una visión en contexto de los escritorios y las aplicaciones en la red. Con esta función, Director ofrece análisis avanzados del tráfico ICA en la implementación.
- La función de administración del rendimiento (Performance Management) proporciona la retención del historial y los informes de tendencias. Con la retención del historial de datos frente a la evaluación en tiempo real, puede crear informes de tendencias que incluyen las tendencias de capacidad y estado.

Después de habilitar esta función en Director, los informes de HDX Insight le proporcionan información adicional:

- La ficha Red en la página Tendencias muestra los efectos de la latencia y el ancho de banda para las aplicaciones, los escritorios y los usuarios de toda la implementación.
- La página Detalles del usuario muestra la información de latencia y ancho de banda específica de la sesión de un usuario en particular.

Limitaciones:

- En la vista Tendencias, los datos de inicio de sesión de conexiones HDX no se recopilan para los VDA anteriores a 7. Para los VDA anteriores, los datos gráficos se muestran como 0.

Para habilitar el análisis de red, debe instalar y configurar Citrix ADM en Director. Director requiere Citrix ADM 11.1 compilación 49.16 o posterior. MAS es un dispositivo virtual que se ejecuta en un servidor Citrix XenServer. Con el análisis de red, Director se comunica con la implementación y recopila la información relacionada con ella.

Para obtener más información, consulte la documentación de Citrix ADM.

> Nota:
>
> Citrix NetScaler Insight Center ha alcanzado la fecha de su ciclo Fin de Mantenimiento el 15 de mayo de 2018. Consulte Tabla de productos Citrix. Integre Director en Citrix ADM para el análisis de red. Para migrar NetScaler Insight Center a Citrix ADM, consulte Migrar desde NetScaler Insight Center a Citrix ADM.

1. En el servidor donde está instalado Director, localice la herramienta de línea de comandos DirectorConfig en C:\inetpub\wwwroot\Director\tools y ejecútela con el parámetro /configNetScaler desde un símbolo del sistema.
2. Cuando se le solicite, introduzca el nombre de la máquina de Citrix ADM (el nombre de dominio completo o la dirección IP), el nombre de usuario, la contraseña, el tipo de conexión (se prefiere el tipo HTTPS al HTTP) y elija la integración en Citrix ADM.
3. Para comprobar los cambios, cierre la sesión y vuelva a iniciarla.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Administración delegada y Director

December 4, 2018

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 documento principal de Administración delegada.

Los permisos administrativos determinan la interfaz de Director que ven los administradores y las tareas que estos pueden realizar. Los permisos determinan:

- Las vistas a las que los administradores pueden acceder, denominadas conjuntamente como una vista.
- Los escritorios, las máquinas y las sesiones que el administrador puede ver y con las que puede interactuar.
- Los comandos que el administrador puede ejecutar, como el remedo de la sesión de un usuario o habilitar el modo de mantenimiento.

Los roles y permisos integrados también determinan cómo los administradores usan Director:

Rol de administrador	Los permisos en Director
Administrador total	Cuenta con acceso completo a todas las vistas y puede ejecutar todos los comandos, incluidos remedar la sesión de un usuario, habilitar el modo de mantenimiento y exportar los datos de tendencias.
Administrador de grupo de entrega	Cuenta con acceso completo a todas las vistas y puede ejecutar todos los comandos, incluidos remedar la sesión de un usuario, habilitar el modo de mantenimiento y exportar los datos de tendencias.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Rol de administrador	Los permisos en Director
Administrador de solo lectura	Puede acceder a todas las vistas y ver todos los objetos en los ámbitos especificados, así como información global. Puede descargar informes de canales HDX y puede exportar datos de tendencias mediante la opción de exportación en la vista Tendencias. No puede ejecutar ningún otro comando ni cambiar nada en las vistas.
Administrador de asistencia técnica	Puede acceder únicamente a las vistas del Servicio de asistencia y de los Detalles del usuario y solo puede ver los objetos que le han sido delegados para que los administre. Puede remedar la sesión de un usuario y ejecutar comandos para ese usuario. Puede realizar operaciones en modo de mantenimiento. Puede utilizar las opciones de control de energía para las máquinas con sistema operativo de escritorio. 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 de servidor.
Administrador de catálogo 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:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

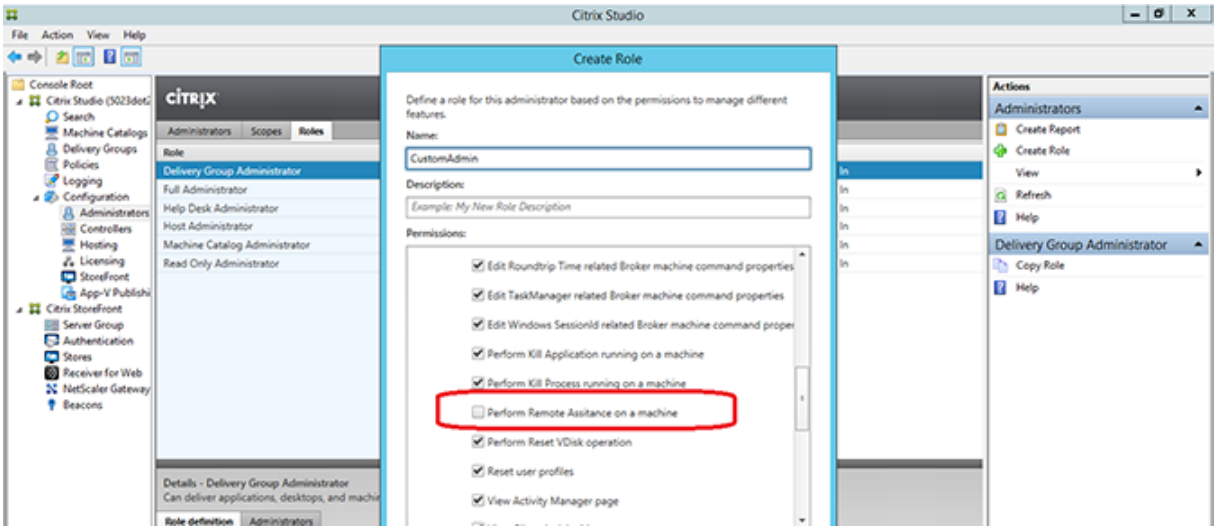
- Permiso de Delivery Controller para iniciar sesión en Director; al menos el acceso de solo lectura en el nodo Administrador
- Permisos para que los grupos de entrega vean los datos relacionados con esos grupos de entrega en Director; al menos el acceso de solo lectura

También puede crear un rol personalizado mediante la copia de un rol existente e incluir permisos adicionales para vistas diferentes. Por ejemplo, puede copiar el rol del servicio de asistencia e incluir permisos para ver las páginas Panel de mandos o Filtros.

Seleccione los permisos de Director para el rol personalizado, incluidos:

- Terminar aplicación ejecutada en una máquina
- Terminar proceso ejecutado en una máquina
- Asistencia remota en una máquina
- Restablecer disco virtual
- Restablecer perfiles de usuario
- Ver página Detalles de cliente
- Ver página Panel de mandos
- Ver página Filtros
- Ver página Detalles de la máquina
- Ver página Tendencias
- Ver página Detalles del usuario

En este ejemplo, el Remedo (Asistencia remota en una máquina) está desactivado.



Un permiso puede depender de otros para que se pueda aplicar en la interfaz de usuario. Por ejemplo, seleccionar el permiso **Terminar aplicación ejecutada en una máquina** habilita la funcionalidad **Finalizar aplicación** solo en aquellos paneles a los que tiene permiso el rol. Se pueden seleccionar los siguientes permisos de panel:

- Ver página Filtros

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- 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.

Proteger la implementación de Director

December 14, 2018

En este artículo se muestran las áreas que pueden afectar a la seguridad del sistema durante la implementación y la configuración de Director.

Configurar Microsoft Internet Information Services (IIS)

Director puede configurarse con una configuración restringida de IIS. Esta no es la configuración predeterminada de IIS.

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

Director requiere los siguientes verbos de HTTP en Filtro de solicitudes. Puede prohibir los verbos que no se encuentren en la lista.

- GET
- POST

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- HEAD

Director no requiere:

- Filtros de ISAPI
- Extensiones ISAPI
- Programas CGI
- Programas FastCGI

> Importante:
>
> - Director requiere Plena confianza. No configure el nivel de confianza de .NET con un nivel Alto o inferior.
> - Director mantiene un grupo de aplicaciones separado. Para modificar los parámetros de Director, seleccione el sitio de Director y modifíquelos.

Configurar derechos de usuario

Cuando se instala Director, sus grupos de aplicaciones reciben el derecho de Iniciar sesión como un servicio, y los privilegios siguientes: Ajustar las cuotas de la memoria para un proceso, Generar auditorías de seguridad y Reemplazar un símbolo (token) de nivel de proceso. Este es el comportamiento normal de instalación cuando se crean los grupos de aplicaciones.

No es necesario que cambie estos derechos de usuario. Estos privilegios no se usan en Director y están inhabilitados automáticamente.

Comunicaciones de Director

En un entorno de producción, Citrix recomienda el uso del protocolo IPsec o los protocolos HTTPS para proteger la transferencia de los datos entre Director y los servidores. IPsec es un conjunto de extensiones estándar para el protocolo de Internet. Proporciona comunicaciones autenticadas y cifradas con integridad de datos y protección contra reproducción. Como IPsec es un conjunto de protocolos de capa de red, los protocolos con niveles más elevados pueden utilizarlo sin realizar ninguna modificación. HTTPS utiliza el protocolo Transport Layer Security (TLS) para brindar un cifrado de datos avanzado.

> Nota:
>
> - Citrix recomienda no habilitar conexiones a Director que no sean seguras en un entorno de producción.
> - Para proteger las comunicaciones desde Director, se requiere una configuración aparte para cada conexión.
> - No se recomienda usar el protocolo SSL. En su lugar, use el protocolo TLS, que es más se-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> guro.
> - Debe proteger las comunicaciones con Citrix ADC mediante TLS, no IPsec.

Para proteger las comunicaciones entre Director y los servidores Citrix Virtual Apps and Desktops (para supervisión e informes), consulte Data Access Security.

Para proteger las comunicaciones entre Director y Citrix ADC (para Citrix Insight), consulte Configurar el análisis de red.

Para proteger las comunicaciones entre Director y el servidor de licencias, consulte Proteger License Administration Console.

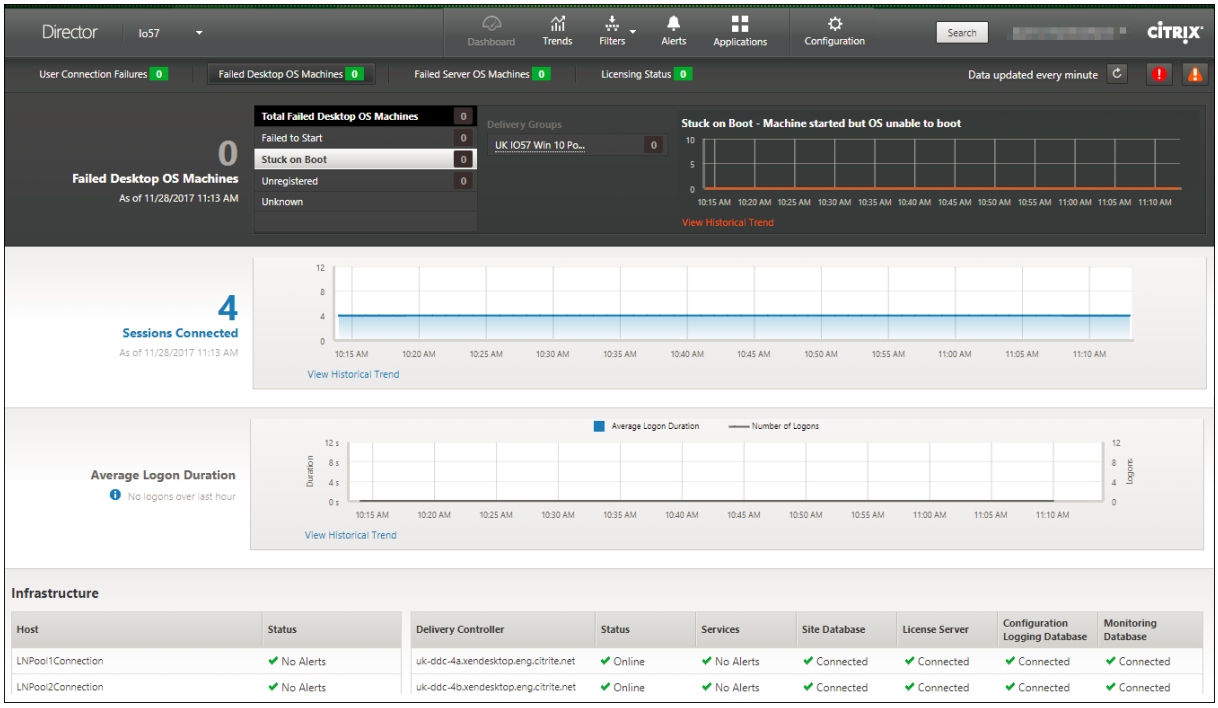
Separar la seguridad de Director

Si implementa aplicaciones Web en el mismo dominio Web (nombre de dominio y puerto) que Director, cualquier posible problema de seguridad de esas aplicaciones Web podrían afectar a su vez a la seguridad de la implementación de Director. Cuando se necesita un mayor nivel de seguridad es necesario separarlos: Citrix recomienda implementar Director en un dominio Web aparte.

Análisis de sitios

December 14, 2018

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.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

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.

Panel	Descripción
Fallos de conexión de usuario	Fallos de conexión en los últimos 60 minutos. Haga clic en las categorías junto al número total para ver las mediciones para ese tipo de fallo. En la tabla adyacente, esa cantidad se desglosa por grupos de entrega. Los fallos de conexión incluyen fallos provocados por haberse alcanzado el límite de las aplicaciones. Para obtener más información acerca de los límites para aplicaciones, consulte Aplicaciones.
Máquinas fallidas de SO de escritorio o Máquinas fallidas de SO de servidor	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 de servidor, 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Panel	Descripción
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 información más detallada, vaya a XenServer Current Release y consulte la sección “XenCenter Performance Alerts” en “Citrix XenServer Administrator’s Guide”.

> 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 (documentadas a continuación):

- Controlar los estados de energía de la máquina del usuario

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Acción	Descripción
Ver datos para un periodo 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.

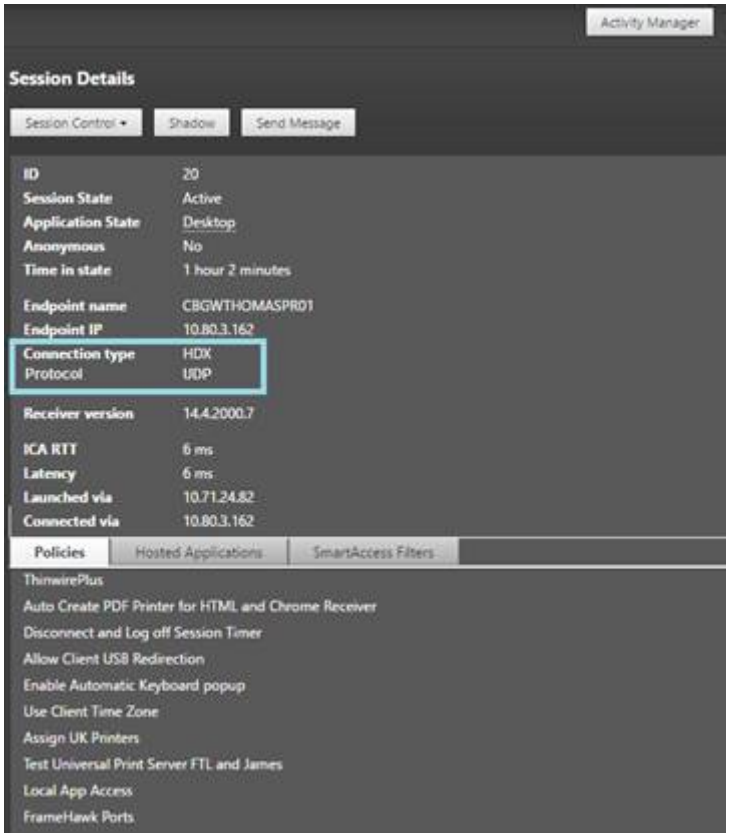
Limitación de reglas de asignación de escritorios:
Citrix Studio permite la asignación de varias reglas de asignación de escritorios (DAR) para distintos usuarios o grupos de usuarios a un solo VDA en el grupo de entrega. StoreFront muestra el escritorio asignado con el **nombre simplificado** correspondiente que se haya especificado en las reglas de asignación de escritorios 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 usando 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



- 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**.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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.ExportPdfDrilldownL	5000
Excel	100 000	UI.ExportExcelDrilldownLimit	100 000
CSV	100 000 (10 000 000 en la ficha **Sesiones**)	UI.ExportCsvDrilldownL	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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 darse por problemas de red o por un consumo alto de recursos por parte de Monitor Service o en el servidor de Director.

La duración predeterminada del tiempo de espera es de 100 segundos. Para aumentar el tiempo de espera del servicio Director, establezca el valor del campo **Connector.DataServiceContext.Timeout** en la Configuración de aplicaciones de Director, en Internet Information Services (IIS):

1. Abra la consola del Administrador IIS.
2. Vaya al sitio Web de Director en el sitio Web predeterminado.
3. Haga doble clic en **Configuración de aplicaciones**.
4. Modifique el valor **Connector.DataServiceContext.Timeout**.

- **Se agotó el tiempo de espera del Monitor**

Este error puede darse por problemas de red o por un consumo alto de recursos por parte de Monitor Service o en SQL Server.

Para aumentar la duración del tiempo de espera de Monitor Service, ejecute los siguientes comandos de PowerShell en el Delivery Controller:

```
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 está respaldado:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 revisiones hotfix

Para ver las revisiones hotfix instaladas 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 las máquinas con sistema operativo de escritorio, pero es posible que no estén disponibles para máquinas con sistema operativo de servidor.

> 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Comando	Función
Apagar	Realiza un apagado ordenado (suave) 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

1. Seleccione la máquina en, por ejemplo, la vista Detalles del usuario o un grupo de máquinas en la vista Filtros.
2. Seleccione **Modo de mantenimiento** y active esta opción.

Si un usuario intenta conectarse a un escritorio asignado mientras éste se encuentra en el modo de mantenimiento, aparecerá un mensaje indicándole que el escritorio no se encuentra disponible por el momento. No se pueden establecer nuevas conexiones hasta que se inhabilite el modo de mantenimiento.

Análisis de aplicaciones

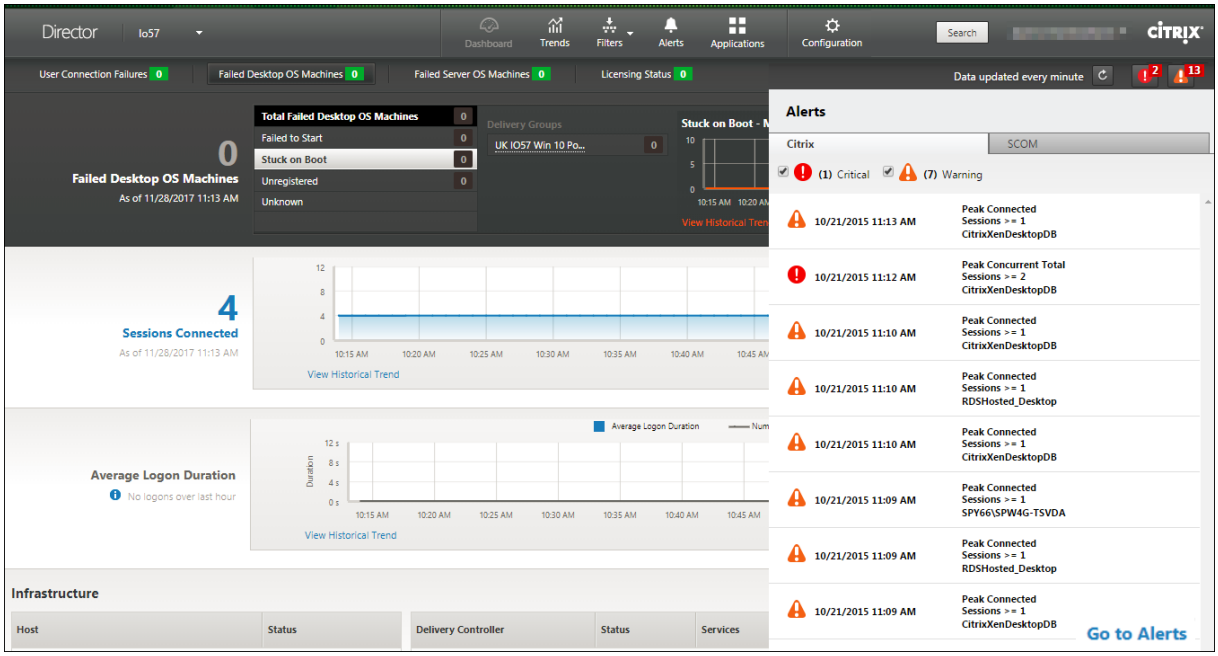
La ficha **Aplicaciones** muestra datos de análisis de aplicaciones en una vista única y consolidada, con el fin de ayudar a analizar y gestionar de forma eficiente el rendimiento de las aplicaciones. Puede obtener información valiosa sobre el estado y el uso de todas las aplicaciones publicadas en el sitio. Muestra diferentes métricas, como los resultados del sondeo, la cantidad de instancias por aplicación y los fallos y errores asociados a las aplicaciones publicadas. Para obtener más información, consulte la sección Análisis de aplicaciones en **Solucionar problemas de aplicaciones**.

Alertas y notificaciones

March 8, 2019

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

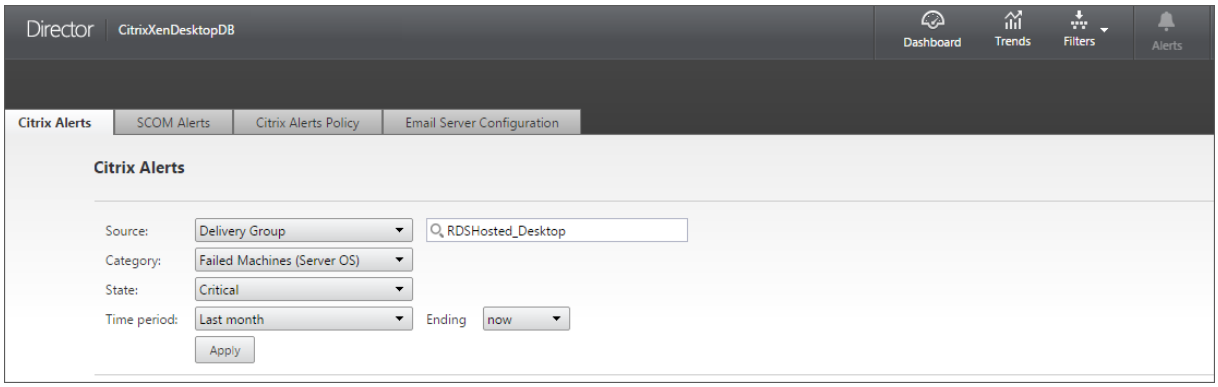


Una alerta de advertencia (un triángulo ámbar) indica que se ha alcanzado o superado el umbral de advertencia de una condición.

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 de servidor 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.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

Alertas de Citrix

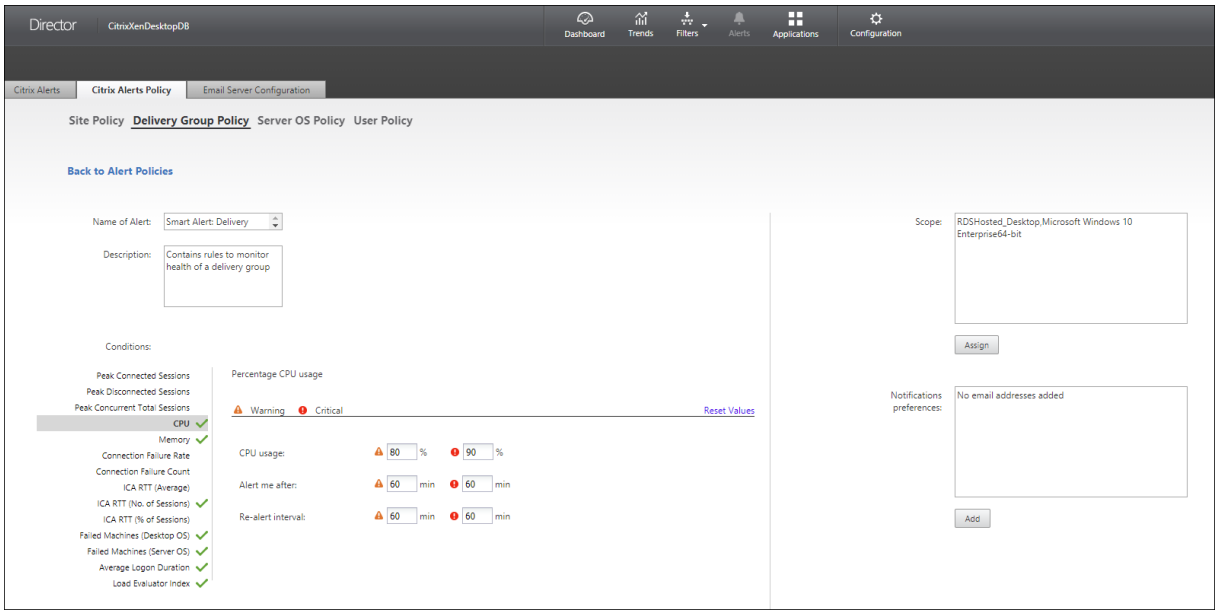
Estas alertas son avisos que se supervisan en Director y que se originan en componentes de Citrix. Puede configurar las alertas de Citrix desde Director, en **Alertas** > **Directiva de alertas de Citrix**. Durante la configuración, puede definir las notificaciones que se enviarán por correo electrónico a usuarios y grupos cuando las alertas superen los umbrales que haya configurado. También puede configurar notificaciones como webhooks de Octoblu o capturas de SNMP. Para obtener más información sobre la configuración de alertas de Citrix, consulte Crear directivas de alertas.

Directivas de alertas inteligentes

Dispone de un conjunto de directivas de alertas integradas con valores de umbral predefinidos para el ámbito Grupos de entrega y el ámbito VDA de servidor. 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 de servidor definido en el sitio. Además, estas alertas integradas se agregan automáticamente a un nuevo grupo de entrega o a un VDA de SO de servidor.

En caso de que actualice Director y el sitio, se transfieren las directivas de alertas provenientes de la instancia anterior de Director. Las directivas de alertas integradas se crean solo si no existen reglas de alertas correspondientes en la base de datos de supervisión.

Para conocer los valores de umbral que tienen las directivas de alertas integradas, consulte la sección Condiciones para directivas de alertas.



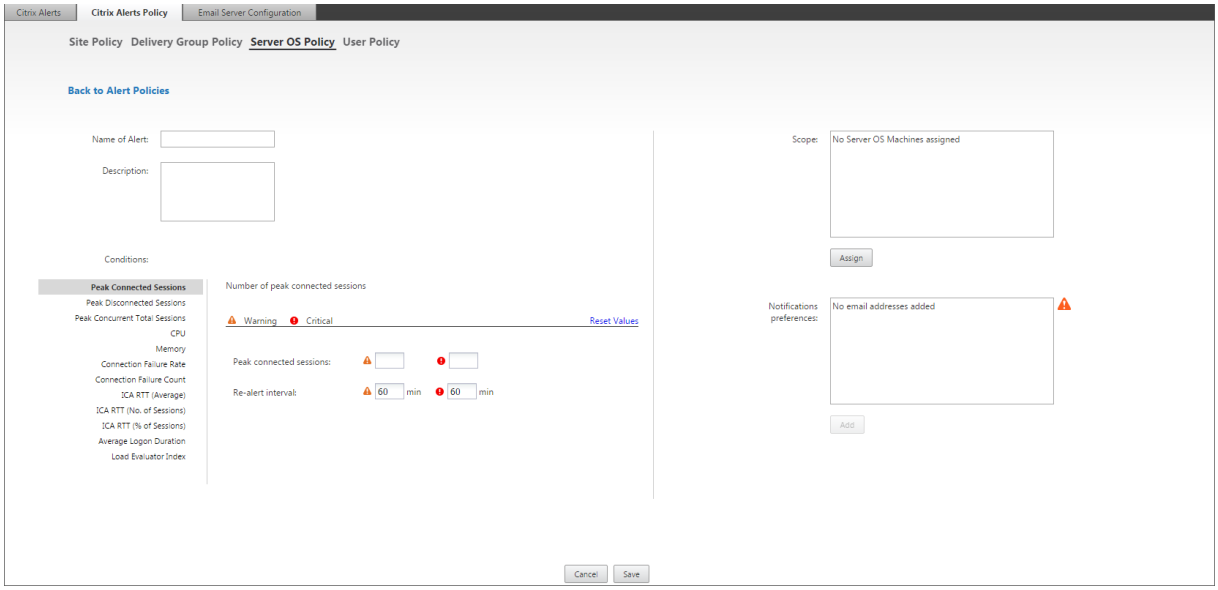
© 1999-2019 Citrix Systems, Inc. All rights reserved.

Alertas de SCOM

Las alertas de SCOM muestran información de alertas de Microsoft System Center 2012 Operations Manager (SCOM). Con ellas, se ofrece información más detallada acerca del estado y el rendimiento del centro de datos desde Director. Para obtener más información, consulte Configurar la integración de SCOM.

La cantidad de alertas que aparecen junto a los iconos de alertas antes de expandir la barra lateral es la suma de las alertas de SCOM y Citrix.

Crear directivas de alertas



Para crear una nueva directiva de alertas (por ejemplo, para que se genere una alerta cuando se cumple un conjunto concreto de criterios referentes al recuento de sesiones):

1. Vaya a **Alertas** > **Directiva de alertas de Citrix** y seleccione, por ejemplo, la directiva de SO de servidor.
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,

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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.
7. Haga clic en **Guardar**.

Para obtener más información acerca de la configuración de webhooks de Octoblu, consulte Configurar directivas de alertas con webhooks de Octoblu.

Para obtener más información sobre la configuración de capturas de SNMP, consulte Configurar directivas de alertas con capturas de SNMP.

Crear una directiva con 20 o más grupos de entrega definidos en el ámbito puede llevar aproximadamente 30 segundos en completar la configuración. Aparece un cursor giratorio durante este tiempo.

Crear más de 50 directivas para un máximo de 20 grupos de entrega distintos (1000 grupos de entrega de destino en total) puede hacer que aumente el tiempo de respuesta (más de 5 segundos).

Mover una máquina que contiene sesiones activas desde un grupo de entrega a otro puede provocar alertas de grupo de entrega erróneas, al estar definidas mediante parámetros de máquina.

Condiciones para directivas de alertas

A continuación, dispone de las categorías de alertas, las acciones recomendadas para mitigar la alerta y las condiciones de directiva integrada, si están definidas. Las directivas de alertas integradas se definen para alertar cada 60 minutos.

Pico de sesiones conectadas

- En Director, consulte la vista “Tendencias de sesiones” para ver la cantidad máxima de sesiones conectadas.
- Compruebe que haya capacidad suficiente para admitir la carga de las sesiones.
- Agregue más máquinas, si fuera necesario.

Pico de sesiones desconectadas

- En Director, consulte la vista “Tendencias de sesiones” para ver la cantidad máxima de sesiones desconectadas.
- Compruebe que haya capacidad suficiente para admitir la carga de las sesiones.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Agregue más máquinas, si fuera necesario.
- Cierre sesiones desconectadas, si fiera 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 fiera necesario.

Porcentaje de uso de CPU

- Identifique los procesos o los recursos que consumen la CPU.
- 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 de servidor
- **Valores de umbral:** Advertencia (80%), Crítico (90%)

Memoria

Porcentaje de uso de memoria.

- Identifique los procesos o los recursos que consumen la memoria.
- 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> 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 de servidor
- **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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 de servidor
  - **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 escritorio)

Cantidad de máquinas fallidas de SO de escritorio. Los errores pueden ocurrir por diversos motivos, como se muestra en las vistas Panel de mandos y Filtros de Director.

- Ejecute diagnósticos de Citrix Scout para determinar la causa principal. Para obtener más información, consulte Solucionar problemas de usuarios.

  Condiciones para directivas inteligentes:

  - **Ámbito:** Grupo de entrega
  - **Valores de umbral:** Advertencia (1), Crítico (2)

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Máquinas fallidas (SO de servidor)

Cantidad de máquinas fallidas de SO de servidor. 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 de servidor
  - **Valores de umbral:** Advertencia (1), Crítico (2)

Promedio de duración de inicio de sesión

Duración media de los inicios de sesión que se han producido durante la última hora.

- Consulte el panel de mandos de Director para obtener métricas actualizadas sobre la duración de los inicios de sesión. Si una gran cantidad de usuarios intenta iniciar sesión en un corto período de tiempo, el tiempo que tardan los inicios de sesión puede alargarse.
- Consulte la línea base y desglose 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 de servidor
  - **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 máquinas con sistema operativo de servidor que tengan 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 de servidor
  - **Valores de umbral:** Advertencia (80%), Crítico (90%)

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Supervisar alertas de hipervisor

Director muestra alertas para supervisar el estado del hipervisor. Las alertas de Citrix Hypervisor y VMware vSphere ayudan a supervisar los parámetros y estados del hipervisor. El estado de conexión al hipervisor también se supervisa, y se genera una alerta si el clúster o el grupo de hosts se reinicia o no está disponible.

Para recibir las alertas de hipervisor, compruebe que se haya creado una conexión de alojamiento en Citrix Studio. Para obtener más información, consulte Conexiones y recursos. Solo se supervisan estas conexiones para las alertas de hipervisor. En la tabla siguiente se describen los distintos parámetros y estados de las alertas de hipervisor.

Alerta	Hipervisores compatibles	Desencadenada por	Condición	Configuración
Uso de CPU	Citrix Hypervisor, VMware vSphere	Hipervisor	Se alcanza o supera el umbral de alerta que tiene el consumo de CPU.	Los umbrales de alerta deben configurarse en el hipervisor.
Uso de memoria	Citrix Hypervisor, VMware vSphere	Hipervisor	Se alcanza o supera el umbral de alerta que tiene el consumo de memoria.	Los umbrales de alerta deben configurarse en el hipervisor.
Uso de la red	Citrix Hypervisor, VMware vSphere	Hipervisor	Se alcanza o supera el umbral de alerta que tiene el uso de la red.	Los umbrales de alerta deben configurarse en el hipervisor.
Uso del disco	VMware vSphere	Hipervisor	Se alcanza o supera el umbral de alerta que tiene el uso del disco.	Los umbrales de alerta deben configurarse en el hipervisor.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Alerta	Hipervisores compatibles	Desencadenada por	Condición	Configuración
Conexión de host o estado de energía	VMware vSphere	Hipervisor	El host del hipervisor se ha reiniciado o no está disponible.	Las alertas están preintegradas en VMware vSphere. No se necesita ninguna configuración adicional.
Conexión de hipervisor no disponible.	Citrix Hypervisor, VMware vSphere	Delivery Controller	La conexión con el hipervisor (grupo o clúster) se pierde, se apaga o se reinicia. Esta alerta se genera cada hora mientras la conexión no esté disponible.	Las alertas están preintegradas en el Delivery Controller. No se necesita ninguna configuración adicional.

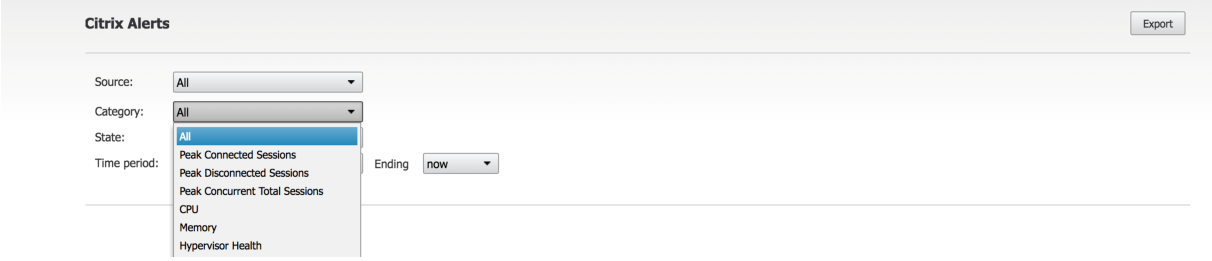
> Nota:
>
> Para obtener más información sobre la configuración de alertas, consulte Alertas de Citrix XenCenter o Alertas de VMware vCenter.

La preferencia de notificación por correo electrónico se puede configurar en **Directiva de alertas de Citrix > Directiva de sitio > Estado del hipervisor**. Las condiciones de umbral para las directivas de alertas del hipervisor se pueden configurar, modificar, inhabilitar o eliminar únicamente desde el hipervisor, no desde Director. Sin embargo, en Director se pueden modificar las preferencias de correo electrónico y se puede descartar una alerta.

> Importante:
>
> - Las alertas activadas por el hipervisor se obtienen y se muestran en Director. Sin embargo, los cambios en el ciclo de vida o el estado de las alertas del hipervisor no se reflejan en Director.
> - Las alertas que están en estado correcto o descartadas o inhabilitadas en la consola del hipervisor seguirán apareciendo en Director y deberán descartarse explícitamente.

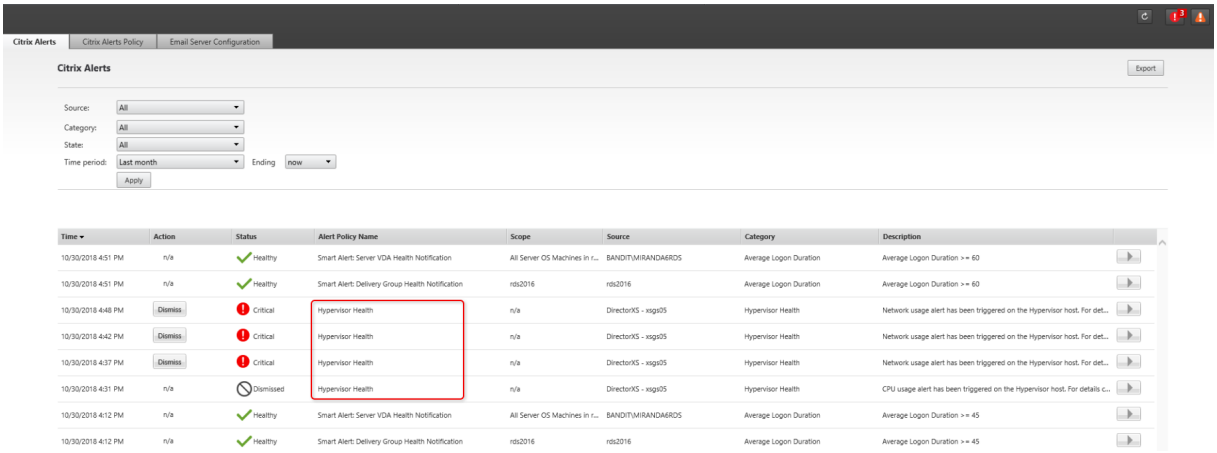
© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Las alertas que se descartan en Director no se descartan automáticamente en la consola del hipervisor.



Se ha agregado una nueva categoría de alerta denominada **Estado del hipervisor** para habilitar el filtrado únicamente de las alertas del hipervisor. Estas alertas se muestran una vez que se alcanzan o superan los umbrales. Las alertas del hipervisor pueden ser:

- Crítico: Se ha alcanzado o superado el umbral crítico de la directiva de alertas del hipervisor.
- Advertencia: Se ha alcanzado o superado el umbral de advertencia de la directiva de alertas del hipervisor.
- Descartado: La alerta ya no se muestra como activa.



Esta función requiere Delivery Controller 7 1811 o posterior. Si está utilizando una versión anterior de Director con la versión 7 1811 o más reciente del sitio, solo se muestra el recuento de alertas del hipervisor. Para ver las alertas, debe actualizar Director.

Configurar directivas de alertas con webhooks de Octoblu

> Nota:
>
> El 29 de noviembre de 2017, Citrix cerró su servicio gratuito Octoblu.com en Citrix Cloud. En consecuencia, le recomendamos que deje de integrar Octoblu en Director. Para obtener más información sobre el anuncio de Citrix para cerrar su servicio de Octoblu.com, consulte el blog The Future of Octoblu y Citrix Workspace IoT.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Configurar directivas de alertas con webhooks de Octoblu para iniciar los servicios IoT. Esta característica requiere Delivery Controllers 7.11 o posterior.

Los servicios IoT donde podrían utilizarse alertas son, por ejemplo, el envío de notificaciones SMS al personal de asistencia o la integración con las plataformas personalizadas de solución de incidentes para ayudar en el seguimiento de las notificaciones.

Puede configurar una directiva de alertas con una respuesta HTTP o un POST HTTP mediante cmdlets de PowerShell. Se han ampliado para dar respaldo a 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 de Octoblu 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>
```

Para obtener más información sobre la configuración de directivas de alertas con PowerShell, consulte Director 7.7: Managing and Configuring Alerts and Notifications Using PowerShell en “Advanced Concepts”.

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>,

```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

```
10 "Timestamp": <Time in UTC when notification was generated>,
11
12 "PolicyName": <Name of the Alert policy>,
13
14 "Description": <Description of the Alert policy>,
15
16 "Scope" : <Scope of the Alert policy>,
17
18 "NotificationState": <Notification state critical, warning, healthy or
      dismissed>,
19
20 "Site" : <Site name> }
```

Configurar directivas de alertas con capturas de SNMP

Cuando se activa una alerta configurada con una captura de SNMP, se reenvía el mensaje correspondiente de captura de SNMP al agente de escucha de red configurado para el procesamiento posterior de la alerta. Las alertas de Citrix admiten capturas de SNMP a partir de la versión 2. Actualmente, el mensaje de captura se puede reenviar a un solo agente de escucha.

> Nota:
>
> Esta función requiere Delivery Controllers 7.12 o posterior.

Para configurar capturas de SNMP, utilice los siguientes cmdlets de PowerShell:

- Obtenga la configuración actual del servidor de SNMP:

```
1 Get-MonitorNotificationSnmpServerConfiguration
```

- Establezca la configuración del servidor para SNMP versión 2:

```
1 Set-MonitorNotificationSnmpServerConfiguration -ServerName <
      Server IP> -PortNumber <Port ID> -SnmpSender <Sender name> -
      CommunityString public -Protocol V2
```

- Establezca la configuración del servidor para SNMP versión 3:

```
1 $authpass = "<authentication password>" | ConvertTo-SecureString
      -AsPlainText -Force
2 $privpass = "<Privacy password>" | ConvertTo-SecureString -
      AsPlainText -Force
3 Set-MonitorNotificationSnmpServerConfiguration -ServerName <
      Server IP> -PortNumber <Port ID> -SnmpSender <Sender name> -
      EngineId <Engine Id> -AuthPassword $authpass -PrivPassword
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

```
    $privpass -PrivPasswordProtocol <Privacy password protocol> -
    AuthPasswordProtocol <Authentication password protocol> -
    Protocol V3
```

- Habilite la captura de SNMP para una directiva de alertas existente:

```
Set-MonitorNotificationPolicy -IsSnmpEnabled $true -Uid <Policy
    ID>
```

- Cree una nueva directiva de alertas con la configuración de capturas de SNMP:

```
$policy = New-MonitorNotificationPolicy -Name <Policy name> -
    IsSnmpEnabled $true -Description <Policy description> -Enabled
     $true
```

La estructura de los OID en los mensajes de captura de SNMP provenientes de Director es:
1.3.6.1.4.1.3845.100.1.<UID>
Aquí, el **<UID>** se genera en serie para cada directiva de alertas definida en Director. Por tanto, los OID son únicos para cada entorno de usuario.

- Use **1.3.6.1.4.1.3845.100.1** para filtrar todos los mensajes de captura provenientes de Director.
- Use **1.3.6.1.4.1.3845.100.1.<UID>** para filtrar y gestionar mensajes de captura para alertas concretas.

Utilice el siguiente cmdlet para obtener los UID de las directivas de alertas definidas en su entorno:

```
Get-MonitorNotificationPolicy
```

Puede reenviar capturas de SNMP a SCOM. Para ello, configure SCOM con el Delivery Controller para escuchar los mensajes de captura.

Configurar la integración de alertas de SCOM

La integración de SCOM con Director permite ver la información de alertas provenientes de SCOM en el panel de mandos y en otras vistas de alto nivel de Director.

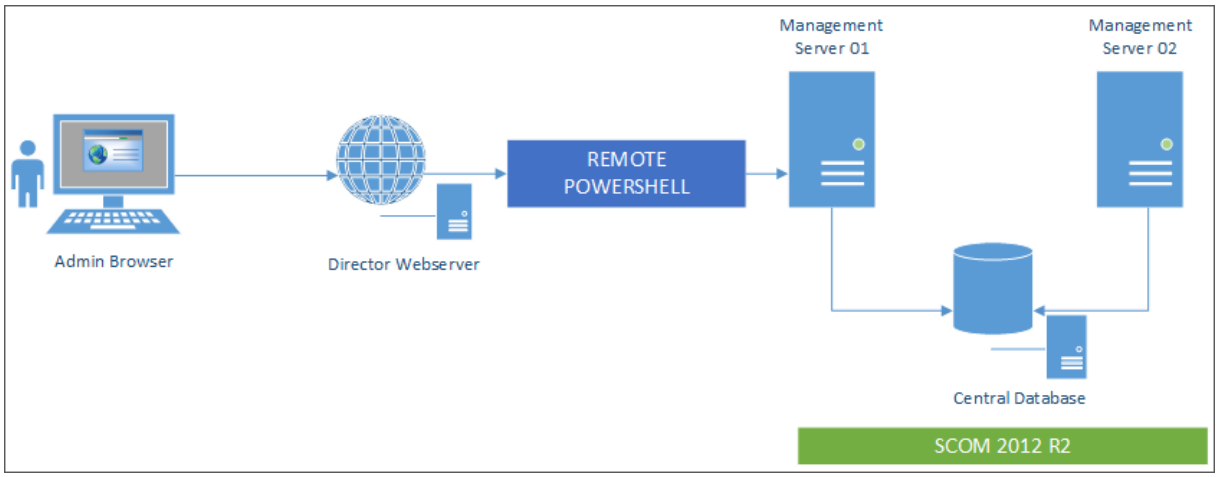
Las alertas de SCOM se muestran junto a las alertas de Citrix. Puede acceder y consultar los detalles de las alertas de SCOM. Para ello, vaya a la ficha SCOM, situada en la barra lateral.

Puede ver el historial de alertas que datan, como máximo, del mes anterior. Asimismo, puede ordenar, filtrar y exportar la información filtrada a informes en formatos CSV, Excel y PDF. Para obtener más información, consulte Exportar informes.

La integración de SCOM usa PowerShell 3.0 (o una versión posterior) de forma remota para consultar datos del servidor de administración de SCOM y mantiene una conexión persistente en el espacio

© 1999-2019 Citrix Systems, Inc. All rights reserved.

de ejecución de la sesión de usuario en Director. Director y el servidor SCOM deben tener la misma versión de PowerShell.



Los requisitos para la integración de SCOM son:

- Windows Server 2012 R2
- System Center 2012 R2 Operations Manager
- PowerShell 3.0 o una versión posterior (las versiones de PowerShell en Director y en el servidor SCOM deben coincidir)
- CPU de cuatro núcleos con 16 GB de RAM (recomendado)
- Debe configurarse un servidor de administración principal para SCOM en el archivo web.config de Director. Puede hacerlo mediante la herramienta DirectorConfig.

> Nota:
>
> - Citrix recomienda que la cuenta de administrador de Director se configure como rol de Operador de SCOM, para que los administradores puedan obtener información completa de alertas en Director. Si no es posible, se puede configurar una cuenta de administrador de SCOM en el archivo web.config mediante la herramienta DirectorConfig.
> - Para un rendimiento óptimo, Citrix recomienda no configurar más de 10 administradores de Director por servidor de administración de SCOM.

En el servidor de Director:

1. Escriba **Enable-PSRemoting** para habilitar la comunicación remota de PowerShell.
2. Agregue el servidor de administración de SCOM a la lista TrustedHosts. Abra un símbolo del sistema de PowerShell y ejecute los siguientes comandos:
   - Obtenga la lista actual de TrustedHosts

     Get-Item WSMAN:\localhost\Client\TrustedHosts
   - Agregue el nombre de dominio completo (FQDN) del servidor de administración de SCOM a la lista TrustedHosts. <Old Values> representa el conjunto de entradas existentes devuelto

© 1999-2019 Citrix Systems, Inc. All rights reserved.

por el cmdlet Get-Item.

Set-Item WSMAN:\localhost\Client\TrustedHosts -Value "<FQDN del servidor de administración de SCOM>,<Old Values>"

3. Configure SCOM mediante la herramienta DirectorConfig.

   C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configscom

En el servidor de administración de SCOM:

1. Asigne administradores de Director al rol de administrador de SCOM.
   a) Abra la consola de administración de SCOM y vaya a **Administración** > **Seguridad** > **Funciones de usuario**.
   b) En "Funciones de usuario", puede crear un rol de usuario o modificar uno existente. Existen cuatro categorías de roles de operador de SCOM que definen la clase de acceso a los datos de SCOM. Por ejemplo, un rol de Solo lectura no verá el panel Administración y no podrá detectar ni administrar reglas, máquinas o cuentas. Un rol de Operador de SCOM es un rol de administrador total.

      > Nota:
      >
      > Las operaciones siguientes no están disponibles si se asigna un rol que no sea Operador al administrador de Director:
      >
      > - Si hay varios servidores de administración configurados y el servidor de administración principal no está disponible, el administrador de Director no podrá conectarse a servidores de administración secundarios. El servidor de administración principal es aquel que está configurado en el archivo web.config de Director, y es el mismo que se ha especificado en el paso 3 anterior con la herramienta DirectorConfig. Los servidores de administración secundarios son servidores de administración del mismo nivel que el servidor principal.
      > - Al filtrar alertas, el administrador de Director no puede buscar por el origen de las alertas. Eso requiere un nivel de permiso de operador.

   c) Para modificar un Rol de usuario, haga clic con el botón secundario en el rol y, a continuación, haga clic en las **Propiedades**.
   d) En el cuadro de diálogo "Propiedades de función de usuario", puede agregar o quitar administradores de Director que tengan la función de usuario especificada.
2. Agregue administradores de Director al grupo Usuarios de administración remota en el servidor de administración de SCOM. Esto permite a los administradores de Director establecer una conexión remota con PowerShell.
3. Escriba **Enable-PSRemoting** para habilitar la comunicación remota de PowerShell.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

4. Establezca los límites de las propiedades de WS-Management:

   a) Modifique MaxConcurrentUsers:

      En la interfaz de línea de comandos:

      ```
      winrm set winrm/config/winrs @{ MaxConcurrentUsers = ”20”}
      ```

      En PowerShell:

      ```
      Set-Item WSMan:\localhost\Shell\MaxConcurrentUsers 20
      ```

   b) Modifique MaxShellsPerUser:

      En la interfaz de línea de comandos:

      ```
      winrm set winrm/config/winrs @{ MaxShellsPerUser=”20”}
      ```

      En PowerShell:

   ```
   Set-Item WSMan:\localhost\Shell\MaxShellsPerUser 20
   ```

   a) Modifique MaxMemoryPerShellMB:

      En la interfaz de línea de comandos:

      ```
      winrm set winrm/config/winrs @{ MaxMemoryPerShellMB=”1024”}
      ```

      En PowerShell:

   ```
   Set-Item WSMan:\localhost\Shell\MaxMemoryPerShellMB 1024
   ```

5. Para que la integración de SCOM funcione en entornos de dominios mixtos, configure la siguiente entrada del Registro.

Ruta: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Clave: LocalAccountTokenFilterPolicy

Tipo: DWORD

Valor: 1

Precaución: Si modifica el Registro de forma incorrecta, podrían generarse problemas graves que pueden provocar la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Una vez configurada la integración de SCOM, es posible que aparezca el mensaje “No se pueden obtener las alertas recientes de SCOM. Revise los registros de eventos del servidor de Director para obtener más información”. Los registros de eventos del servidor ayudarán a identificar y corregir el problema. Las causas pueden ser:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Pérdida de conectividad de red a la máquina de SCOM o Director.
- El servicio de System Center Operations Manager no está disponible o está demasiado ocupado para responder.
- Error de autorización debido a un cambio en los permisos del usuario configurado.
- Un error en Director al procesar datos de SCOM.
- Las versiones de PowerShell en Director y en el servidor SCOM no coinciden.

Filtrar datos para solucionar fallos

January 29, 2019

Cuando haga clic en números en el panel de mandos o seleccione un filtro predefinido desde el menú Filtros, la vista Filtros se abre y muestra los datos en función de la máquina seleccionada o del tipo de fallo.

Los filtros predefinidos no se pueden modificar, pero puede guardar un filtro predefinido como un filtro personalizado y, a continuación, modificarlo. Además, puede crear vistas con filtros personalizados de máquinas, conexiones, sesiones e instancias de aplicaciones en todos los grupos de entrega.

1. Seleccione una vista:
    - **Máquinas**. Seleccione máquinas de SO de escritorio o máquinas de SO de servidor. Estas vistas muestran la cantidad de máquinas configuradas. La ficha Máquinas con SO de servidor también incluye el índice del patrón de carga. Este índice indica la distribución de contadores de rendimiento, así como información sobre herramientas del recuento de sesiones si pasa el puntero sobre el vínculo.
    - **Sesiones**. También puede ver el recuento de sesiones desde la vista Sesiones. Use las mediciones del tiempo de inactividad para identificar las sesiones que estén inactivas más allá de un umbral de período de tiempo.
    - **Conexiones**. Filtre conexiones por distintos períodos de tiempo, incluidos los últimos 60 minutos, las últimas 24 horas o los últimos 7 días.
    - **Instancias de aplicaciones**. Esta vista muestra las propiedades de todas las instancias de aplicaciones que haya en los VDA de SO de escritorio y de servidor. Las métricas del tiempo de inactividad de la sesión están disponibles para las instancias de aplicaciones en los VDA de SO de servidor.
2. En **Filtrar por**, seleccione un criterio de filtro.
3. Utilice las fichas adicionales para cada vista, según sea necesario, para completar el filtro.
4. Seleccione columnas adicionales, según sea necesario, para solucionar problemas más complejos.
5. Guarde el filtro y cámbiele el nombre.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

6. Para acceder a los filtros desde múltiples servidores Director, almacene los filtros en una carpeta compartida accesible desde esos servidores:
    - Las cuentas del servidor Director deben tener permiso para modificar la carpeta compartida.
    - Los servidores Director deben configurarse con acceso a la carpeta compartida. Para ello, ejecute el **Administrador de IIS**. En Sitios > Sitio Web predeterminado > Director > Parámetros de la aplicación, modifique el parámetro **Service.UserSettingsPath** para reflejar la ruta UNC de la carpeta compartida.
7. Para abrir el filtro más adelante, en el menú **Filtros**, seleccione el tipo de filtro (Máquinas, Sesiones, Conexiones o Instancias de aplicación) 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 posterior.
9. Si es necesario, para las vistas **Máquinas** o **Conexiones**, use los controles de energía para todas las máquinas que seleccione en la lista filtrada. Para la vista Sesiones, utilice los controles de sesión u opciones para enviar mensajes.
10. En las vistas **Máquinas** y **Conexiones**, haga clic en **Motivo del fallo** de la máquina o conexión donde se ha producido el error para obtener una descripción detallada del error y las acciones recomendadas para solucionarlo. Los motivos de los errores y las acciones recomendadas para fallos de máquinas y conexiones están disponibles en Citrix Director 7.12 Failure Reasons Troubleshooting Guide.
11. En la vista **Máquinas**, haga clic en un enlace del nombre de la máquina para ir a la página correspondiente de **Detalles de la máquina**. Esta página muestra los datos de la máquina, ofrece controles de alimentación, y muestra gráficos de CPU, memoria, supervisión de disco y supervisión de GPU. Además, puede hacer clic en **Ver utilización histórica** para ver las tendencias de utilización de los recursos en la máquina. Para obtener más información, consulte Solucionar problemas de máquinas.
12. En la vista **Instancias de aplicaciones**, ordene o filtre en función del **Tiempo de inactividad** superior al período de tiempo del umbral. Seleccione las instancias de aplicaciones inactivas que quiere finalizar. Cerrar o desconectar una instancia de aplicación finaliza todas las instancias de aplicaciones activas que haya en la misma sesión. Para obtener más información, consulte Solucionar problemas de aplicaciones. La página de filtro “Instancias de aplicaciones” y las mediciones del tiempo de inactividad en la página de filtro “Sesiones” están disponibles si Director, los Delivery Controllers y los agentes VDA son de la versión 7.13 o posterior.

> Nota:
>
> Citrix Studio permite la asignación de varias reglas de asignación de escritorios (DAR) para dis-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> tintos usuarios o grupos de usuarios a un solo VDA en el grupo de entrega. StoreFront muestra el escritorio asignado con el nombre simplificado correspondiente que se haya especificado en las reglas de asignación de escritorios 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 usando 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

March 14, 2019

En la vista "Tendencias", verá la información histórica sobre tendencias de sesiones, fallos de conexión, fallos de máquinas, rendimiento de los inicios de sesión, evaluación de la carga, administración de capacidad, uso de máquinas, utilización de recursos y análisis de red para cada sitio. Para buscar esta información, haga clic en el menú **Tendencias**.

La función de consulta detallada de datos permite navegar entre los gráficos de tendencias, 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 qué o quién se ve afectado por las tendencias que se muestran.

Para cambiar el ámbito predeterminado de cada gráfico, aplique un filtro distinto a los datos.

Elija el período de tiempo del que quiere obtener información histórica sobre tendencias. La disponibilidad de un período de tiempo depende de la implementación de Director, como se indica a continuación:

- En los sitios con licencia Premium, están disponibles los informes de tendencias del último año (365 días) como máximo.
- En los sitios con licencia Advanced, están disponibles los informes de tendencias del último mes (31 días) como máximo.
- Informes de tendencias de hasta los últimos 7 días en sitios sin licencia Premium ni Advanced.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Nota:

- En todas las implementaciones de Director, la información de tendencias referentes a sesiones, fallos y rendimiento de inicios de sesión está representada en gráficos y tablas cuando el período de tiempo es "Último mes" (**hasta el día de hoy**) o menos. Cuando el período de tiempo es "Último mes" (con una fecha de finalización personalizada) o "Último año", la información de tendencias se representa en gráficos, pero no en tablas.
- Con los valores de la retención de limpieza de Monitor Service, se controla la disponibilidad de los datos de las tendencias. Los valores predeterminados están disponibles en Granularidad y retención de datos. Los clientes de los sitios con licencia Premium pueden cambiar la retención de la limpieza de datos a la cantidad de días de retención que quieran.
- Los siguientes parámetros en el Administrador de IIS controlan el rango de las fechas de finalización personalizadas disponibles para la selección. Estos parámetros se pueden personalizar. Sin embargo, la disponibilidad de los datos para las fechas seleccionadas depende del parámetro de retención de la limpieza para la métrica específica que mide.

Parámetro	Valores predeterminados
UI.TrendsLast2HoursRange	3
UI.TrendsLast24HoursRange	32
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.

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 escritorio" o en la ficha "Fallos de máquina de SO de servidor", 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

de las fases de inicio de sesión, tales como la duración de la intermediación y la hora de inicio de la VM.
Estos datos se refieren específicamente a inicios de sesión y no incluyen a usuarios que intentan reconectar con sesiones desconectadas.
La tabla debajo del gráfico muestra la duración de los inicios de sesión por cada sesión de usuario. Usted puede elegir las columnas que desea mostrar y ordenar el informe por cualquiera de las columnas.
Para obtener más información, consulte Diagnosticar problemas de inicio de sesión de los usuarios.

Ver tendencias de evaluación de carga: En la ficha "Índice de patrón de carga", dispone de un gráfico con información detallada sobre la carga que se distribuye entre las máquinas con sistema operativo de servidor. Las opciones de filtro para este gráfico incluyen: grupo de entrega o máquina con SO de servidor en un grupo de entrega, máquina con SO de servidor (disponible solo si se selecciona Máquina con SO de servidor en un grupo de entrega) y un intervalo.

Ver uso de aplicaciones alojadas: La disponibilidad de esta función depende de la licencia que tenga en su organización.
En la ficha "Administración de capacidad", seleccione la ficha "Uso de aplicaciones alojadas", el grupo de entrega y el período de tiempo para ver un gráfico con el uso simultáneo en las horas punta y una tabla que muestra el uso de las 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 usando, o han usado, la aplicación.

Ver el uso de SO de escritorio y de servidor: La vista "Tendencias" muestra el uso del SO de escritorio por sitio y por grupo de entrega. Cuando se selecciona un 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 de servidor por sitio, por máquina y por grupo de entrega. Cuando se selecciona un 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 de SO de escritorio" o "Máquinas de SO de servidor" para obtener una vista en tiempo real 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 escritorio: Muestra el estado actual de las máquinas de SO de escritorio (VDI) por disponibilidad, para el sitio entero o para un grupo de entrega específico.
Disponibilidad de SO de servidor: Muestra el estado actual de las máquinas de SO de servidor 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Ver uso de máquinas virtuales: Para una planificación más precisa, vaya a la ficha "Utilización de recursos" y seleccione máquinas de SO de escritorio o servidor 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 de promedio de CPU, promedio de memoria, promedio de E/S por segundo, latencia de disco y máximo de sesiones simultáneas. Puede explorar en profundidad una máquina para ver datos y gráficos sobre los 10 procesos principales que consumen la CPU. Asimismo, puede filtrar por grupo de entrega y período de tiempo. Los gráficos de CPU, consumo de memoria y pico de sesiones simultáneas están disponibles para las últimas 2 horas, 24 horas, 7 días, mes y año. Los gráficos del promedio de E/S por segundo y la latencia de disco están disponibles para las últimas 24 horas, el último mes y el último año.

> Nota:
>
> - La configuración de la directiva de Supervisión, Habilitar supervisión de procesos, debe estar establecida en "Permitida" para recopilar y mostrar datos en la tabla "10 procesos principales" de la página "Utilización histórica de máquinas". De forma predeterminada, la directiva está establecida en "Prohibida". De forma predeterminada, se recopilan los datos referentes al uso de recursos. Se pueden inhabilitar mediante la configuración de directiva Habilitar supervisión de recursos. La tabla situada bajo los gráficos muestra los datos de utilización de recursos por máquina.
> - El Promedio de E/S por segundo muestra los promedios diarios. Para indicar el pico de E/S por segundo, se calcula la mayor de las E/S medias para el intervalo de tiempo seleccionado. (Un promedio de E/S por segundo son las operaciones medias de E/S por segundo recopiladas durante una hora en el VDA.)

Ver datos de análisis de red: La disponibilidad de esta función depende de la licencia de la organización y los permisos de administrador. Esta característica requiere Delivery Controllers **7.11** o posterior.

Desde la ficha "Red", 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 aplicación: 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 escritorio con Windows Vista o posterior y los VDA de SO de servidor 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 de servidor.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Puede configurar la supervisión de los fallos de aplicación mediante las directivas de supervisión. Para obtener más información, consulte Configuraciones de directiva de Supervisión.

Ver resultados del sondeo de aplicaciones: En la ficha "Resultados del sondeo de aplicaciones", se muestran los resultados del sondeo de las aplicaciones que se han configurado para el sondeo en la página "Configuración". En esa página, se registra la fase del inicio durante el que ocurrió el fallo de la aplicación.

Esta función requiere agentes VDA y Delivery Controllers de la **versión 7.18** o posterior. Para obtener más información, consulte Sondeo de aplicaciones.

Crear informes personalizados: La ficha "Informes personalizados" ofrece una interfaz de usuario para generar informes personalizados que contienen datos históricos y en tiempo real obtenidos de la base de datos de supervisión en formato tabular.

Esta característica requiere Delivery Controllers **7.12** o posterior.

Desde la lista de las consultas de "Informe personalizado" previamente guardadas, puede hacer clic en **Ejecutar y descargar** para exportar un informe en formato CSV, y hacer clic en **Copiar OData** para copiar y compartir la consulta de OData correspondiente, o hacer clic en **Modificar** para modificarla. Puede crear una nueva consulta de informe personalizado basada en máquinas, conexiones, sesiones o instancias de aplicaciones. Especifique las condiciones de filtro, que pueden establecerse en función de campos como la máquina, el grupo de entrega o el período de tiempo. Especifique columnas adicionales necesarias en el informe personalizado. La vista previa muestra un ejemplo de los datos del informe. Si guarda la consulta del informe personalizado, esta se agrega a la lista de consultas guardadas.

Puede crear una nueva consulta de informe personalizado a partir de una consulta de OData copiada. Para ello, seleccione la opción de consulta de OData y pegue la consulta de OData copiada. Puede guardar la consulta resultante para ejecutarla más adelante.

> Nota:
>
> Los nombres de las columnas en el informe de vista previa y exportación que se generan mediante consultas de OData no están localizados, aparecen en inglés.

Los iconos de marcas del gráfico indican acciones o sucesos significativos para un intervalo de tiempo concreto. Pase el puntero sobre el marcador y haga clic en la lista de sucesos o acciones.

> Nota:
>
> - Los datos de inicio de sesión de conexiones HDX no se recopilan para versiones del VDA anteriores a 7. Para los VDA anteriores, los datos gráficos se muestran como 0.
> - Los grupos de entrega eliminados en Citrix Studio pueden seleccionarse en los filtros de tendencias de Director hasta que los datos relacionados con ellos se hayan limpiado y eliminado. Si se selecciona un grupo de entrega eliminado se muestran gráficos para los datos

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> disponibles durante el periodo de retención. Sin embargo, las tablas no mostrarán datos.
> - Al mover una máquina que contiene sesiones activas de un grupo de entrega a otro, las tablas de **Utilización de recursos e Índice de patrón de carga** del nuevo grupo de entrega muestran métricas consolidadas de ambos grupos de entrega, el antiguo y el nuevo.

Solucionar problemas de implementaciones

October 3, 2018

Como administrador de asistencia técnica, puede buscar al usuario que informa un problema y ver datos de las sesiones o las aplicaciones asociadas a ese usuario. Del mismo modo, puede buscar máquinas o dispositivos de punto final donde se han producido problemas. Los problemas se pueden resolver rápidamente supervisando las métricas relevantes y realizando las acciones correspondientes. Las acciones disponibles pueden ser: finalizar una aplicación o un proceso que no responde, remedar operaciones en la máquina del usuario, cerrar una sesión que no responde, reiniciar la máquina, colocar una máquina en el modo de mantenimiento o restablecer el perfil del usuario.

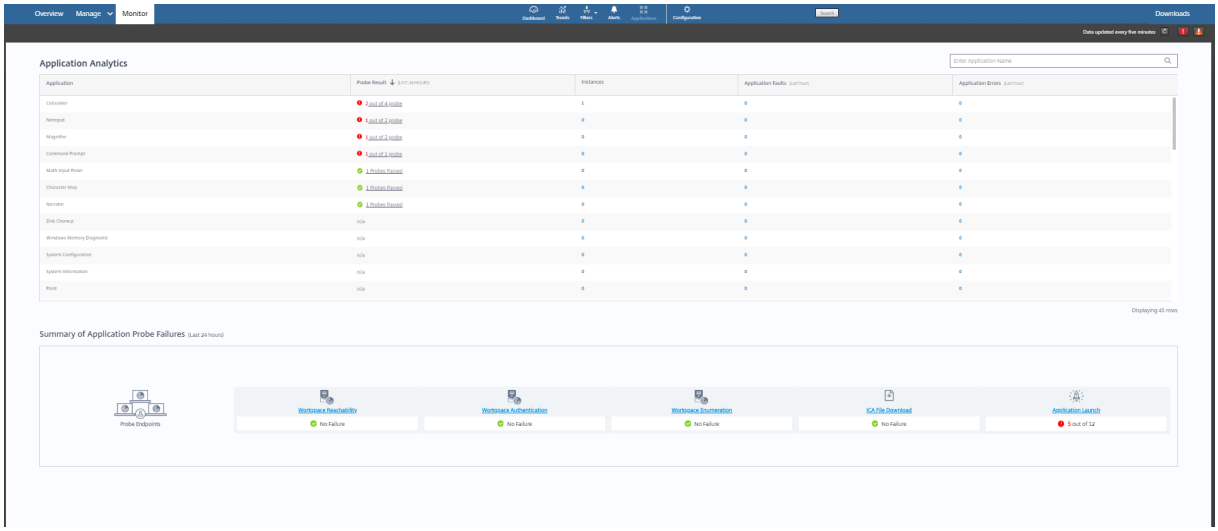
Solucionar problemas de aplicaciones

December 14, 2018

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



En la columna **Resultado del sondeo**, se muestra el resultado del sondeo de aplicaciones ejecutado en las últimas 24 horas. Haga clic en el enlace de resultados del sondeo para ver más datos en la página **Tendencias** > **Resultados del sondeo de aplicaciones**. Para obtener más información sobre cómo configurar los sondeos de aplicaciones, consulte Sondeo de aplicaciones.

La columna **Instancias** muestra el uso de las aplicaciones. Indica la cantidad de instancias de aplicación que se ejecutan en ese momento (instancias conectadas y desconectadas). Para solucionar problemas complejos, haga clic en el campo **Instancias** para ver la página de filtros de **Instancias de aplicación** correspondientes. En ella, puede seleccionar las instancias de aplicación que se van a cerrar o desconectar.

Puede supervisar el estado de las aplicaciones publicadas en el sitio con las columnas **Fallos de aplicación** y **Errores de aplicación**. Esas columnas muestran la cantidad total de fallos y errores que se han producido mientras se iniciaba la aplicación en cuestión durante la última hora. Haga clic en el campo **Fallos de aplicación** o **Errores de aplicación** para ver datos sobre los fallos y errores en la página **Tendencias** > **Fallos y errores de aplicación** que corresponde a la aplicación seleccionada.

La disponibilidad y la presentación de los fallos y los errores se define con las configuraciones de directiva de fallos de aplicación. Para obtener más información acerca de las directivas y cómo modificarlas, consulte Directivas para supervisar fallos de aplicación en “Configuraciones de directiva de Supervisión”.

Supervisar aplicaciones en tiempo real

Puede solucionar las aplicaciones y las sesiones con la ayuda de métricas de inactividad para identificar las instancias que llevan inactivas más de un límite de tiempo concreto.

Los casos típicos donde solucionar problemas de aplicaciones pertenecen al sector de la asistencia médica, donde los empleados comparten licencias de aplicación. Allí, debe finalizar las sesiones in-

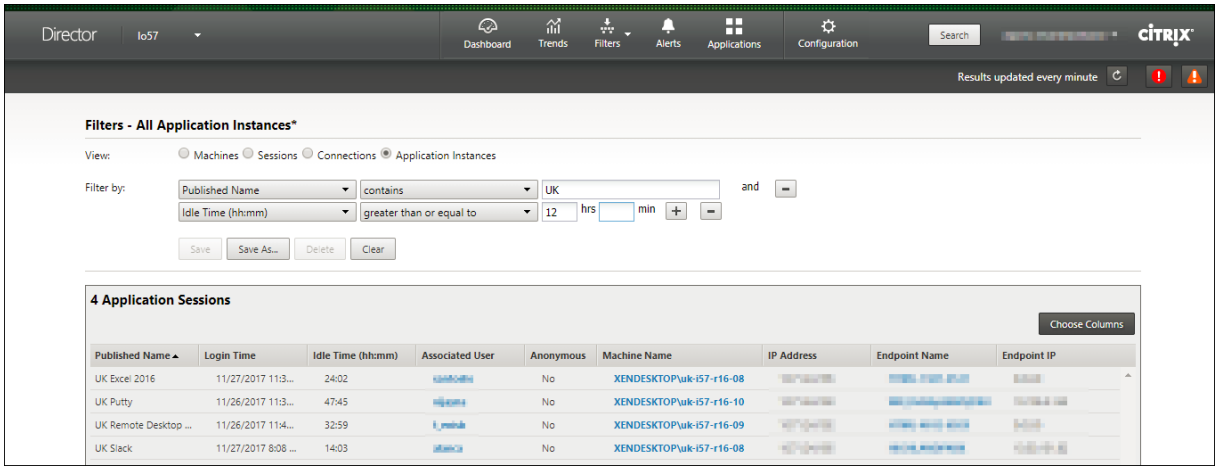
© 1999-2019 Citrix Systems, Inc. All rights reserved.

activas y las instancias de aplicaciones 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 de SO de servidor y SO de escritorio. Se muestran las métricas del tiempo de inactividad asociadas a las instancias de aplicación en los VDA de SO de servidor 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 más allá de un período de tiempo concreto con el objetivo de cerrarles o desconectarlas, según corresponda. Para ello, seleccione **Filtros > Instancias de aplicación**. A continuación, seleccione un filtro guardado previamente o elija **Todas las instancias de aplicación** y cree su propio filtro.



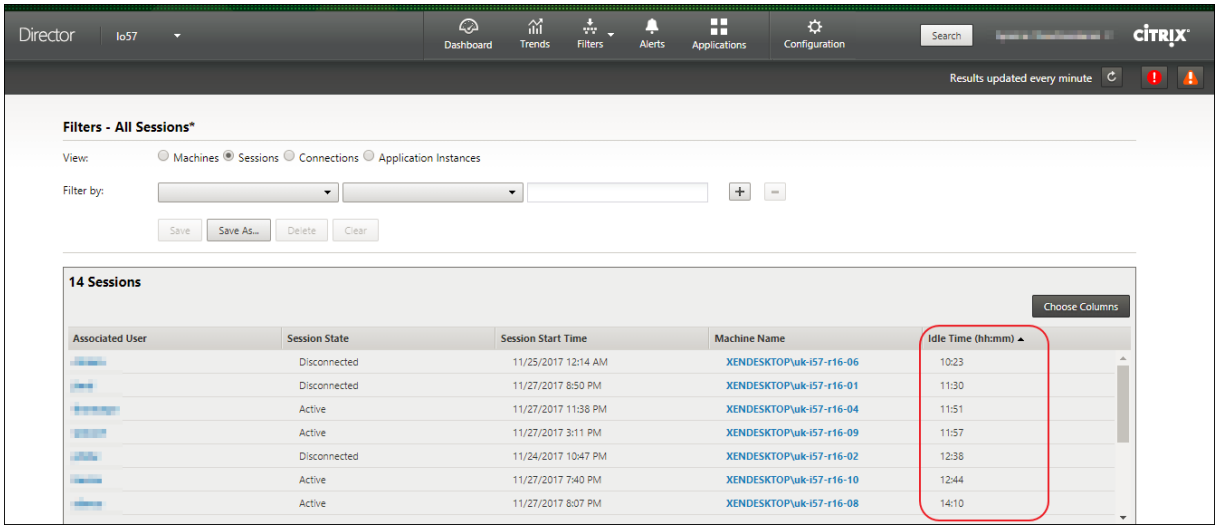
A continuación, se ofrece un filtro de ejemplo. Como criterio **Filtrar por**, elija **Nombre publicado** (de la aplicación) y **Tiempo de inactividad**. A continuación, establezca **Tiempo de inactividad** en **mayor o igual que** un límite de tiempo concreto y guarde el filtro si quiere volver a utilizarlo en el futuro. En la lista filtrada, seleccione las instancias de aplicación. Seleccione la opción para enviar mensajes o, desde la lista desplegable **Control de sesión**, elija **Cerrar sesión** o **Desconectar** para finalizar las instancias.

> Nota:
>
> Cerrar la sesión o desconectar una instancia de aplicación cierra o desconecta la sesión actual, lo que finaliza todas las instancias de aplicación que pertenezcan a la misma sesión.

Puede identificar las sesiones inactivas desde la página de filtro **Sesiones** si utiliza el estado de la sesión y la métrica del tiempo de inactividad de la sesión. Ordene por la columna **Tiempo de inactividad** o defina un filtro para identificar las sesiones que estén inactivas más allá de un límite de

© 1999-2019 Citrix Systems, Inc. All rights reserved.

tiempo específico. Se muestra el tiempo de inactividad de las sesiones en los VDA de SO de servidor 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 escritorio o
- se ha iniciado en un VDA que ejecuta la versión 7.12 o una versión anterior.

Supervisar fallos históricos de aplicaciones

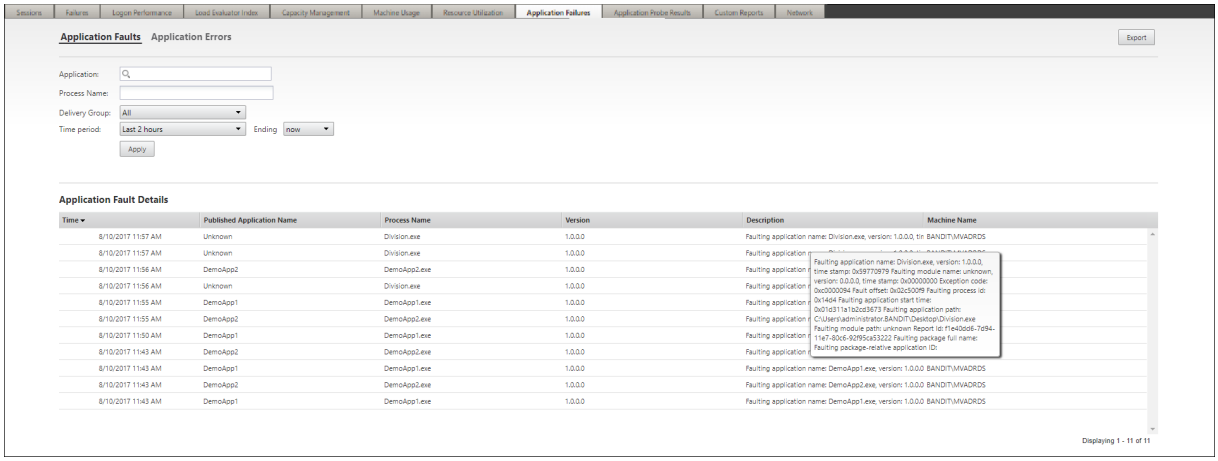
La ficha **Tendencias** > **Fallos y errores de aplicación** muestra los fallos y los errores asociados a las aplicaciones publicadas en los VDA.

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>
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.



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 del mismo. 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 deducir 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 de servidor. Puede modificar los parámetros de supervisión desde las directivas de grupo de supervisión (Habilitar supervisión de fallos de aplicación, Habilitar supervisión de fallos de aplicación en VDA de SO de escritorio 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Sondeo de aplicaciones

March 8, 2019

El sondeo de aplicaciones automatiza las comprobaciones de estado de las aplicaciones de Citrix Virtual Apps publicadas en un sitio. Los resultados del sondeo de aplicaciones están disponibles en Director.

Requisitos:

- Delivery Controller ejecuta la versión 7.18 o posterior.
- Las máquinas de punto final que ejecutan Probe Agents son máquinas de Windows con Citrix Receiver para Windows versión 4.8 o posterior, o la aplicación Citrix Workspace para Windows (anteriormente Citrix Receiver para Windows) versión 1808 o posterior. No se admite la aplicación Workspace para UWP.
- Director y StoreFront admiten la autenticación predeterminada basada en formularios.

Cuentas de usuario o permisos requeridos para ejecutar el sondeo de aplicaciones:

- Un usuario único de StoreFront para sondear aplicaciones en cada máquina de punto final. No es necesario que el usuario de StoreFront sea un administrador; los sondeos pueden ejecutarse en un contexto no administrativo.
- Cuentas de usuario con permisos de administrador de Windows para instalar y configurar Citrix Probe Agent en las máquinas de punto final
- Una cuenta de administrador total o un rol personalizado con los siguientes permisos. Si reutiliza cuentas de usuarios existentes para el sondeo de aplicaciones, podrían cerrarse las sesiones activas de esos usuarios.
  - Permisos de grupo de entrega:
    * Solo lectura
  - Permisos de Director:
    * Crear, modificar y eliminar la configuración del servidor de correo electrónico de alertas (si el servidor de correo electrónico aún no está configurado)
    * Crear, modificar y eliminar configuraciones de sondeo
    * Ver página Configuraciones
    * Ver página Tendencias

Configurar el sondeo de aplicaciones

Puede programar los sondeos de aplicaciones para que se ejecuten durante las horas de menor actividad en varios puntos geográficos. Unos resultados exhaustivos pueden ayudar a solucionar problemas relacionados con las aplicaciones aprovisionadas, las máquinas de host o las conexiones antes de que los usuarios los experimenten.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

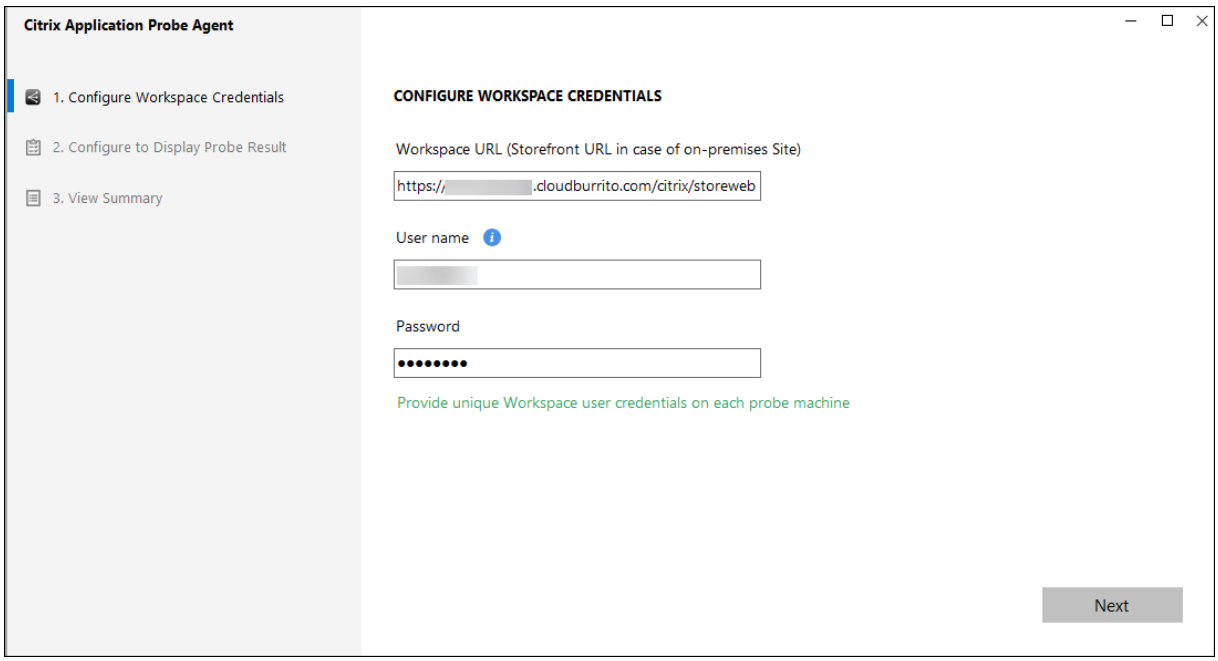
Paso 1: Instalar y configurar el Citrix Probe Agent

Citrix Probe Agent es un ejecutable de Windows que simula el inicio de la aplicación por parte del usuario a través de StoreFront. Prueba los inicios de las aplicaciones siguiendo las pautas configuradas en Director e informa de los resultados a Director.

1. Identifique las máquinas de punto final desde donde ejecutar el sondeo de aplicaciones.
2. Los usuarios con privilegios administrativos pueden instalar y configurar Citrix Probe Agent en la máquina de punto final. Descargue el ejecutable de Citrix Probe Agent disponible en https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html
3. Inicie el agente y configure sus credenciales de StoreFront y Receiver para Web. Configure un usuario único de StoreFront en cada máquina de punto final. Las credenciales se cifran y se almacenan de forma segura.

   > Nota:
   >
   > Para acceder al sitio que va a sondear desde fuera de la red, escriba la URL de inicio de sesión de Citrix Gateway en el campo de URL de StoreFront. Citrix Gateway enruta automáticamente la solicitud a la URL de StoreFront del sitio correspondiente. Esta función está disponible para Citrix Gateway 12.1 o posterior, y Delivery Controllers 1811 o posterior.

4. En la ficha **Configurar para mostrar el resultado del sondeo**, introduzca sus credenciales de Director.

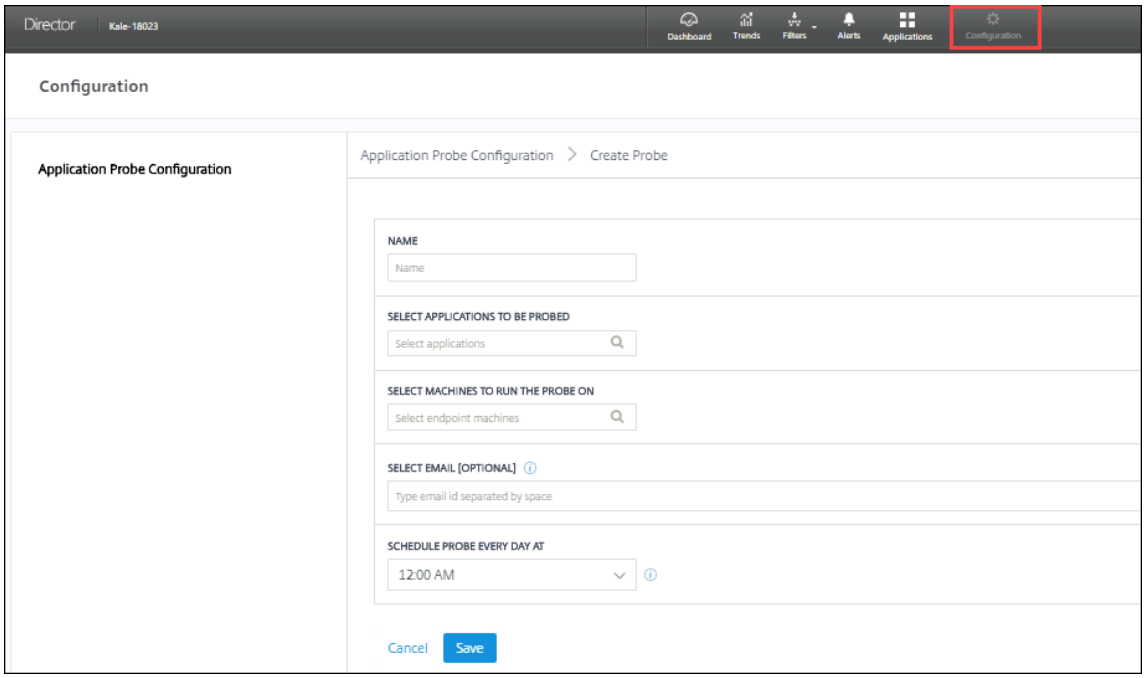


© 1999-2019 Citrix Systems, Inc. All rights reserved.

Paso 2: Configurar el sondeo de aplicaciones en Director

1. Vaya a **Configuración** > **Configuración del sondeo de aplicaciones**.
2. Cree un sondeo y elija:
   - las aplicaciones a sondear,
   - las máquinas de punto final en las que debe ejecutarse el sondeo,
   - las direcciones de correo electrónico a las que se enviarán los resultados de errores en el sondeo (configure su servidor de correo electrónico en **Alertas** > **Configuración del servidor de correo electrónico**), y
   - la hora a la que debe ejecutarse el sondeo (según la zona horaria local de la máquina de punto final).

   Una vez configurado en Director, el agente tarda 10 minutos en prepararse para comenzar el sondeo. Luego, ejecuta los sondeos configurados a partir de la hora siguiente.



Paso 3: Ejecutar el sondeo

El agente ejecuta el sondeo de aplicaciones según esté configurado cada sondeo (la configuración se obtiene de Director periódicamente). Inicia las aplicaciones seleccionadas en serie utilizando StoreFront. El agente informa de los resultados a Director a través de la base de datos de supervisión. Los fallos se informan en cinco etapas específicas:

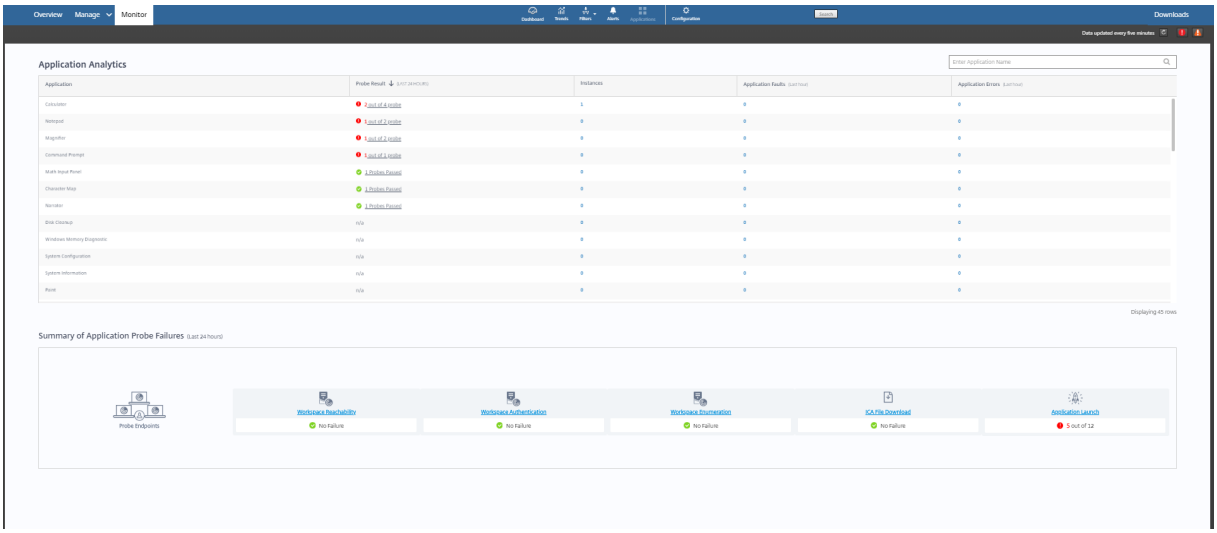
- **Accesibilidad de StoreFront:** No se puede acceder a la URL configurada en StoreFront.
- **Autenticación de StoreFront:** Las credenciales configuradas en StoreFront no son válidas.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

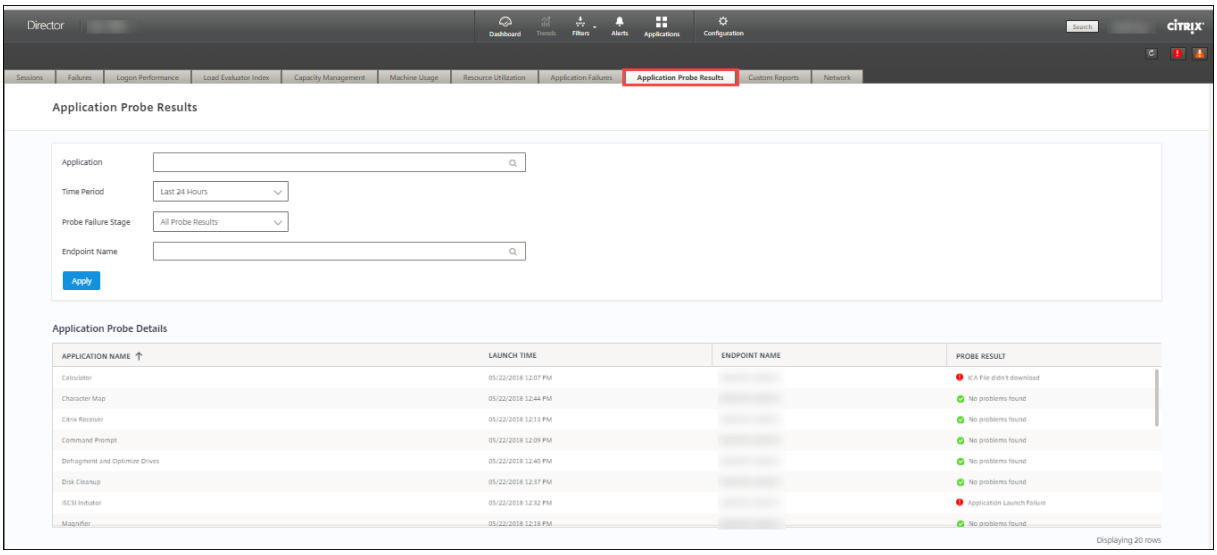
- **Enumeración de StoreFront:** La lista de aplicaciones en StoreFront no contiene la aplicación a sondear.
- **Descarga de ICA:** El archivo ICA no está disponible.
- **Inicio de aplicación:** La aplicación no se ha podido iniciar.

Paso 4: Consultar los resultados del sondeo

Los resultados del último sondeo se encuentran en la página **Aplicaciones**.



Haga clic en el enlace de resultados del sondeo para ver más datos en la página **Tendencias** > **Resultados del sondeo de aplicaciones**.



En esta página, están disponibles los resultados completos de los sondeos realizados durante las últimas 24 horas o los últimos 7 días. Puede ver la etapa en la que falló el sondeo. Asimismo, puede

© 1999-2019 Citrix Systems, Inc. All rights reserved.

filtrar la tabla para ver la aplicación específica, la etapa exacta del fallo del sondeo o la máquina de punto final concreta.

Solucionar problemas de máquinas

March 8, 2019

> Nota:
>
> Con la herramienta **Citrix Health Assistant**, puede solucionar problemas de configuración en agentes VDA no registrados. La herramienta automatiza una serie de comprobaciones de estado para identificar las posibles causas de problemas en el registro de los VDA, el inicio de sesión y la configuración de la redirección de zonas horarias. Dispone de las instrucciones de descarga y uso de la herramienta **Citrix Health Assistant** en el artículo Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch de Citrix Knowledge Center.

La vista **Filtros > Máquinas** en la consola de Director muestra las máquinas configuradas en el sitio. La ficha "Máquinas de SO de servidor" contiene el índice del patrón de carga. Este índice indica la distribución de contadores de rendimiento e información sobre el recuento de sesiones si pasa el puntero sobre el enlace.

Haga clic en la columna **Motivo del fallo** de la máquina donde se ha producido el fallo para obtener una descripción detallada de este y las acciones recomendadas para solucionarlo. Los motivos de los errores y las acciones recomendadas para fallos de máquinas y conexiones están disponibles en Citrix Director 7.12 Failure Reasons Troubleshooting Guide.

Haga clic en el enlace del nombre de máquina para ir a la página **Detalles de la máquina**.

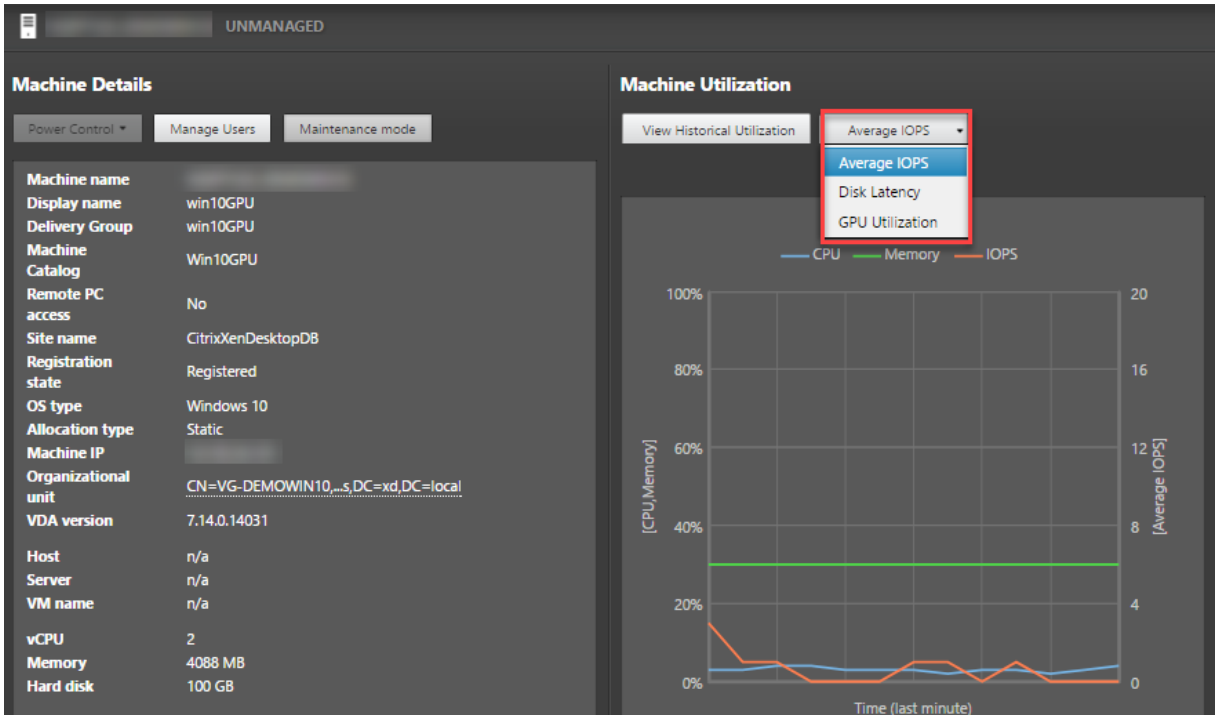
La página "Detalles de la máquina" muestra datos de la máquina, de la infraestructura y de las revisiones hotfix que se hayan aplicado a la máquina.

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



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 escritorio o servidor. Los gráficos de uso de la GPU están únicamente disponibles para los VDA que ejecutan Windows de 64 bits con GPU de NVIDIA Tesla M60 y que ejecutan la versión de controlador de pantalla 369.17 o posterior.

Los VDA deben tener HDX 3D Pro habilitado para proporcionar la aceleración de GPU. Para obtener más información, consulte Aceleración de GPU para sistemas operativos de escritorio Windows y Aceleración de GPU para sistemas operativos de servidor Windows.

Cuando el VDA accede a más de una GPU, el gráfico de uso muestra el promedio de las métricas de GPU recopiladas a partir de las GPU individuales. Las métricas de la GPU se recopilan del VDA entero, no de procesos individuales.

Usar recursos históricos en cada máquina

En el panel **Utilización de máquinas**, haga clic en **Ver utilización histórica** para ver el historial del uso de los recursos en la máquina seleccionada.

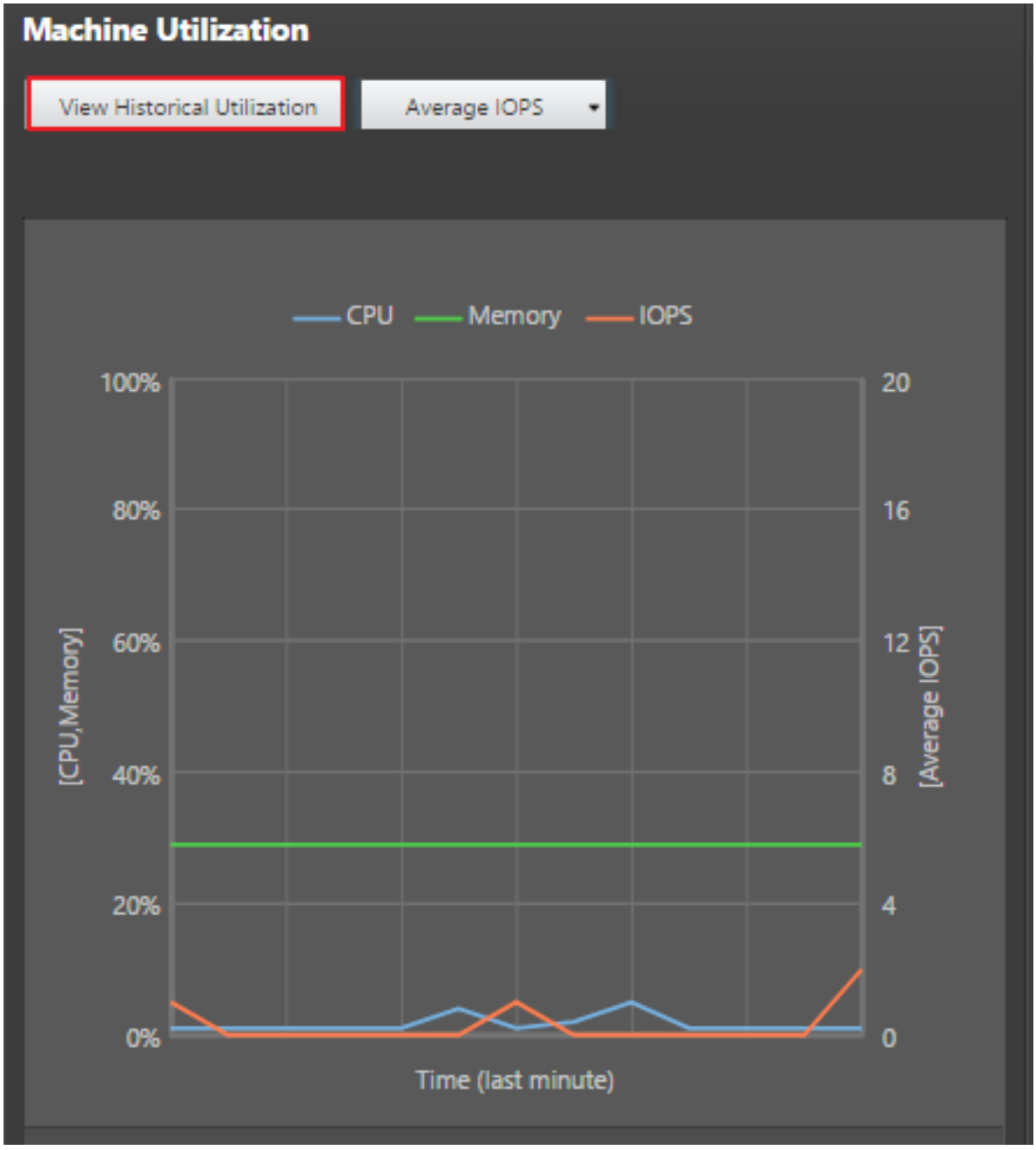
Los gráficos de utilización contienen contadores de rendimiento de la CPU, la memoria, el pico de sesiones simultáneas, el promedio de IOPS y la latencia de disco.

> Nota:
>
> La configuración de la directiva de supervisión **Habilitar supervisión de procesos** debe estar establecida en “Permitida” para recopilar y mostrar datos en la tabla “10 procesos principales”

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> 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**.



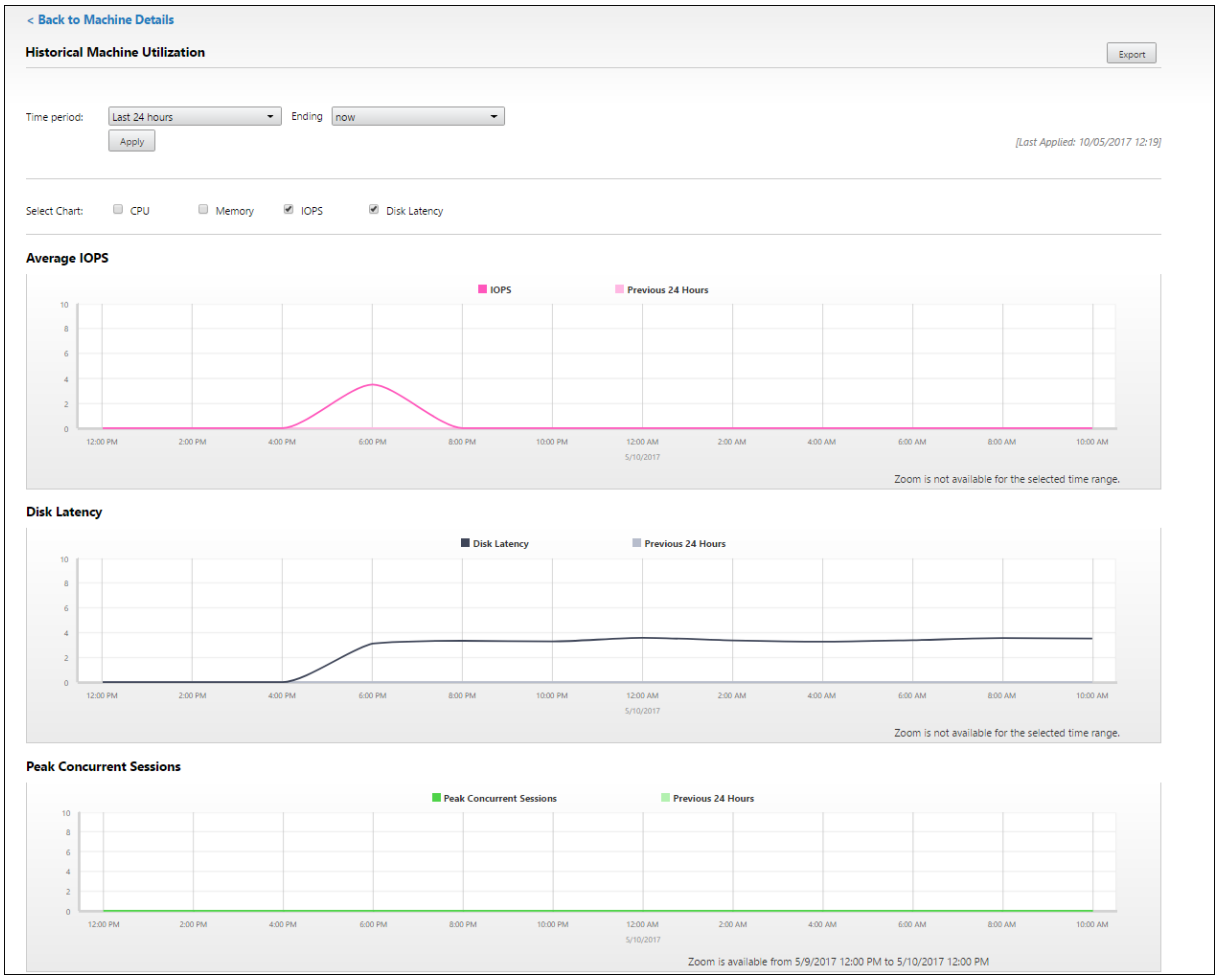
1. En el panel **Utilización de máquinas** de la vista **Detalles de la máquina**, seleccione **Ver utilización histórica**.
2. En la página **Utilización histórica de máquinas**, establezca el **Período de tiempo** para ver las

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 periodo 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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.

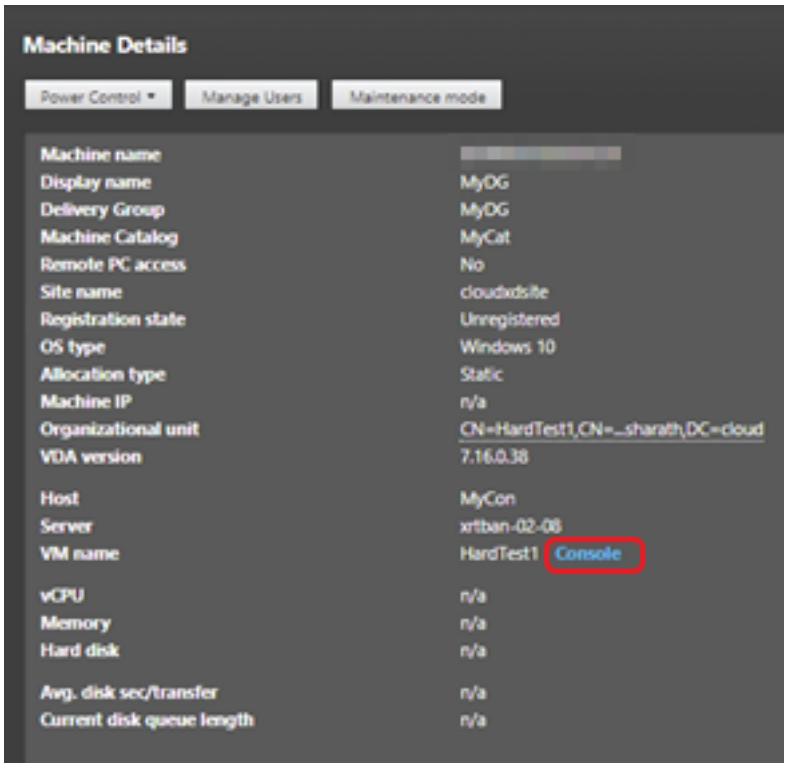
   > Nota:
   >
   > El ID de sesión aparece como "0000" para los procesos del sistema.

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.

Acceder a la consola de la máquina

Puede acceder a las consolas de las máquinas de sistema operativo de escritorio y servidor alojadas en XenServer 7.3 y posterior directamente desde Director. De esta manera, no necesita XenCenter para solucionar problemas en los VDA alojados en XenServer. Para que esta característica 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.



© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 utilizando noVNC, un cliente Web VNC. Ahora tiene acceso por teclado y mouse a la consola.

> Nota:
>
> - Esta característica no es compatible con Internet Explorer 11.
> - Si la posición del puntero en la consola no coincide con la posición del puntero en la máquina, consulte CTX230727 para conocer los pasos para solucionar el problema.
> - Director inicia el acceso a la consola en una nueva ficha; por eso, su explorador Web debe permitir las ventanas emergentes.
> - Por razones de seguridad, Citrix recomienda instalar certificados SSL en su explorador Web.

Estado de la licencia 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 de servidor.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 la licencia RDS para máquinas en período de gracia con una licencia válida, se muestra el mensaje **Licencia disponible** en color verde. Renueve la licencia antes de que

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> caduque.

Cuando se trata de mensajes de advertencia y de error, coloque el puntero sobre el icono de información para ver información adicional como se indica en la tabla siguiente.

Tipo de mensaje	Mensajes en Director
Error	Disponible para VDA 7.16 y posterior.
Error	No se permiten nuevas conexiones de RDS.
Error	La licencia de RDS ha excedido 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 de 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 de RDS configurado.
Advertencia	No se puede acceder al controlador de dominio o al servidor de licencias con el tipo de licencia de RDS de acceso de cliente por dispositivo.
Advertencia	Con el tipo de licencia de acceso de cliente por dispositivo, la licencia del dispositivo de cliente no se pudo determinar, ya que no se puede acceder al servidor de licencias para el nivel de SO que se requiere.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> Nota:
>
> Esta función solo se aplica a Microsoft RDS CAL (Licencia de acceso de cliente).

Solucionar problemas de usuarios

March 11, 2019

Use el **Servicio de asistencia** de Director (página **Administrador de actividades**) para ver información sobre el usuario:

- Compruebe la información acerca del inicio de sesión, la conexión y las aplicaciones del usuario.
- Remede la máquina del usuario.
- Grabe la sesión ICA.
- Solucione el problema con las acciones recomendadas en la tabla siguiente y, si es necesario, remita el problema al administrador que corresponda.

Sugerencias para solucionar problemas

Problema de usuario	Sugerencias
El inicio de sesión tarda mucho tiempo o falla de forma intermitente o repetidamente	Diagnosticar problemas de inicio de sesión de los usuarios
La aplicación es lenta o no responde	Resolver fallos de aplicación
La conexión falló	Restaurar conexiones de escritorios
La sesión es lenta o no responde	Restaurar sesiones
Grabar sesiones	Grabar sesiones
El vídeo es lento o de poca calidad	Ejecutar informes de 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”.

Sugerencias para la búsqueda

Cuando se introduce un nombre de usuario en el campo Buscar, Director busca usuarios en Active Directory en todos los sitios configurados para el respaldo de Director.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Cuando se escribe un nombre de máquina multiusuario en el campo Buscar, Director muestra los Detalles de la máquina para la máquina especificada.

Cuando se escribe un nombre de punto final en el campo Buscar, Director utiliza las sesiones sin autenticar (anónimas) y las sesiones autenticadas que están conectadas a un punto final específico, lo que permite resolver problemas en las sesiones no autenticadas. Asegúrese de que los nombres de los dispositivos de punto final son exclusivos para poder resolver problemas de sesiones no autenticadas.

Los resultados de la búsqueda incluyen también usuarios que no están utilizando máquinas en ese momento o no tienen asignada ninguna.

- Las búsquedas no distinguen el uso de mayúsculas y minúsculas.
- Las entradas parciales generan una lista de posibles coincidencias.
- Después de escribir unas pocas letras de un nombre que tiene dos partes (nombre de usuario, nombre y apellidos o nombre simplificado) separadas por un espacio, los resultados incluyen coincidencias para ambas cadenas. Por ejemplo, si escribe ju rod, los resultados pueden incluir cadenas como “Juan Rodríguez” o Rodrigo, Juárez.

Para volver a la página inicial, haga clic en el logotipo de Director.

Acceder a Citrix Insight Services

Puede acceder a Citrix Insight Services (CIS) desde la lista desplegable del usuario en Director para acceder a otras perspectivas de diagnóstico. Los datos disponibles en CIS proceden de orígenes como Call Home y Citrix Scout.

Cargar información de solución de problemas para la asistencia técnica de Citrix

Ejecute Citrix Scout desde un solo Delivery Controller o VDA para capturar puntos de datos clave y seguimientos 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 Citrix Scout, desde el menú Inicio o la pantalla Inicio, seleccione Citrix > Citrix Scout.

Para obtener información sobre el uso y la configuración de Citrix Scout, y para ver las preguntas frecuentes, consulte CTX130147.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Diagnosticar problemas de inicio de sesión de los usuarios

March 8, 2019

Use los datos de Duración de inicio de sesión para solucionar problemas de inicio de sesión.

La duración del inicio de sesión se mide solo para las conexiones iniciales a un escritorio o aplicación que usa HDX. Esta información no incluye a los usuarios que intentan conectarse con el protocolo de escritorio remoto (RDP) o que se vuelven a conectar desde sesiones desconectadas. Específicamente, la duración del inicio de sesión no se mide cuando un usuario se conecta inicialmente utilizando un protocolo que no es HDX y vuelve a conectarse usando HDX.

En la vista "Detalles del usuario", la duración se muestra como un valor numérico; debajo se muestra la hora en que se produjo el inicio de sesión y un gráfico de las fases de ese inicio.

A medida que los usuarios inician sesión en Citrix Virtual Apps and Desktops, Monitor Service supervisa las fases del proceso de inicio de sesión desde el momento en que el usuario se conecta desde Citrix Receiver al momento en que el escritorio está listo para usarse.

El número elevado de la parte izquierda es el tiempo total de inicio de sesión. Se calcula sumando el tiempo que se tarda en establecer la conexión y en obtener un escritorio desde Delivery Controller más el tiempo que se tarda en autenticarse e iniciar sesión en un escritorio virtual. La información de duración se presenta en segundos (o fracciones de segundos) en la hora local del explorador Web del administrador.

Requisitos previos

Deben cumplirse los siguientes requisitos previos para que aparezcan los datos de duración del inicio de sesión y los resultados detallados:

1. Instale **Citrix User Profile Manager** y **Citrix User Profile Manager WMI Plugin** en el VDA.
2. Compruebe que el servicio de Citrix Profile Management se esté ejecutando.
3. Para los sitios de XenApp y XenDesktop 7.15 y versiones anteriores, inhabilite la configuración de GPO llamada **No procesar la lista de ejecución antigua**.
4. El seguimiento del proceso de auditoría debe estar habilitado para obtener el desglose de la sesión interactiva.
5. Para obtener el desglose del GPO, aumente el tamaño de los registros de operaciones de las directivas de grupo.

> Nota:
>
> La duración del inicio de sesión solo se admite en el shell predeterminado de Windows (explorer.exe), no en los shells personalizados.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Pasos para solucionar problemas en el inicio de sesión de los usuarios

1. En la vista **Detalles del usuario**, puede resolver problemas del estado de inicio de sesión desde el panel “Duración de inicio de sesión”.
    - Si el usuario está iniciando una sesión, esta vista refleja dicho proceso.
    - Si el usuario tiene una sesión ya iniciada actualmente, el panel “Duración de inicio de sesión” muestra el tiempo que tardó el inicio de sesión del usuario.
2. Examine las fases del proceso de inicio de sesión.

Fases del proceso de inicio de sesión

Intermediación con broker

Cuánto tiempo se tardó en decidir qué escritorio asignar al usuario.

Inicio de la VM

Si la sesión requería el inicio de una máquina virtual, este es el tiempo que tardó en iniciarse la máquina.

Conexión HDX

Tiempo que se tardó en completar los pasos requeridos para configurar la conexión HDX desde el cliente a la máquina virtual.

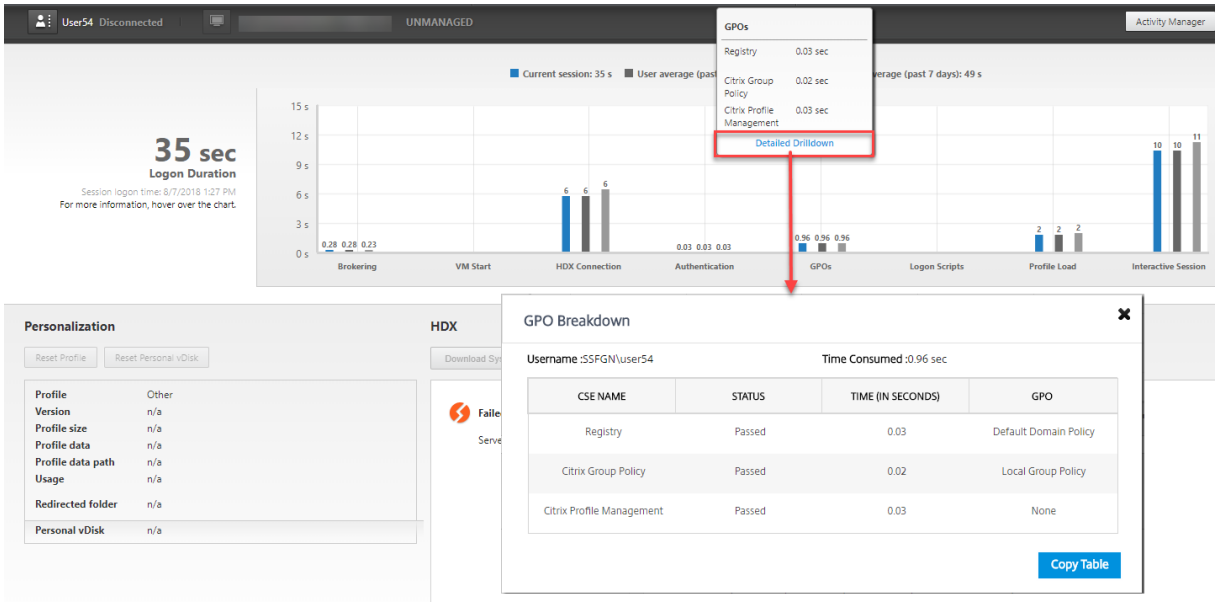
Autenticación

Tiempo que se tardó en completar la autenticación en la sesión remota.

Objetos de directiva de grupo (GPO)

Si había configuraciones de directiva de grupo habilitadas en las máquinas virtuales, este es el tiempo que se tardó en aplicar los objetos de directiva de grupo durante el inicio de sesión. El desglose del tiempo necesario para aplicar cada directiva por cada CSE (extensión del lado del cliente) está disponible como texto de ayuda cuando pasa el cursor sobre la barra de GPO.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Haga clic en **Desglose detallado** para ver una tabla con el estado de la directiva y el nombre del GPO correspondiente. Las duraciones del desglose representan solo el tiempo de procesamiento de CSE, no se suman al tiempo total de GPO. Puede copiar la tabla de detalles para resolver problemas o utilizarla en los informes. El tiempo de GPO para las directivas se obtiene de los registros del Visor de eventos. Los registros se pueden sobrescribir dependiendo de la memoria asignada para los registros de operaciones (el tamaño predeterminado es 4 MB). Para obtener más información sobre cómo aumentar el tamaño del registro para los registros de operaciones, consulte Configurar los registros de eventos.

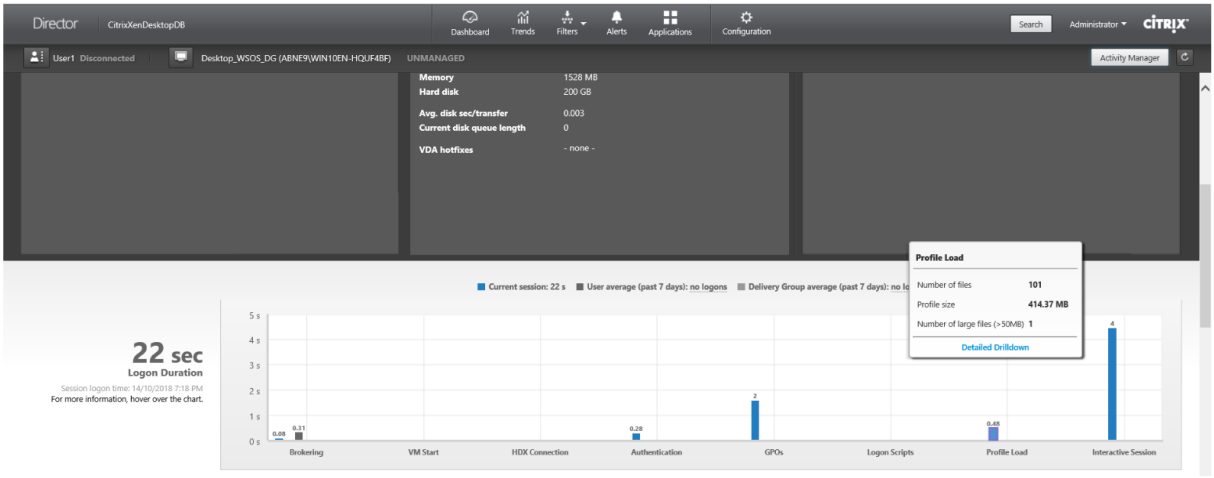
Scripts de inicio de sesión

Si había scripts de inicio de sesión configurados para la sesión, este es el tiempo que se tardó en ejecutarlos.

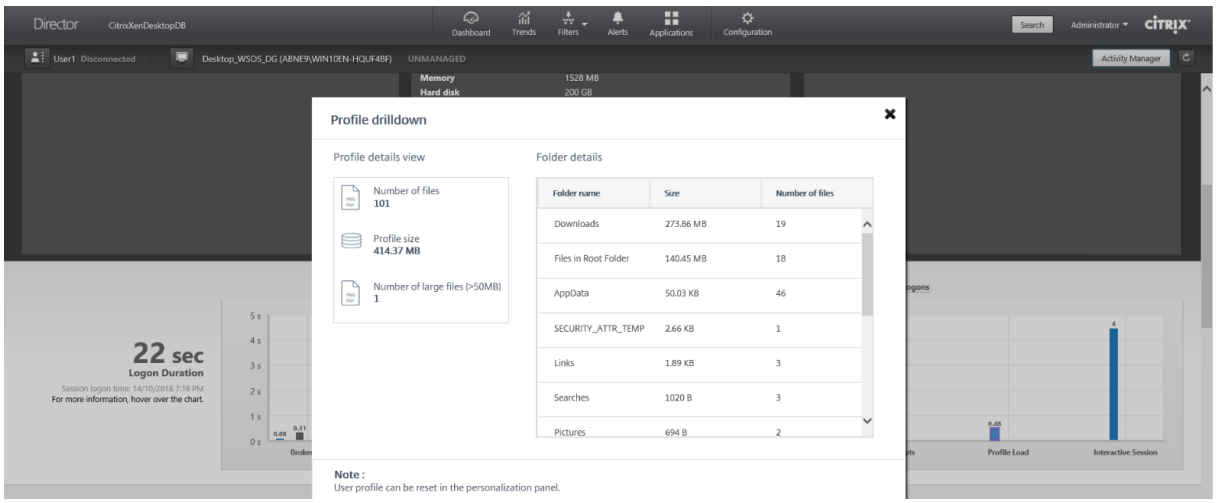
Carga de perfil

Si había parámetros de perfil configurados para el usuario o para la máquina virtual, este es el tiempo que tardó el perfil en cargarse. 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. Esta información adicional puede ayudar a solucionar problemas de cargas largas de perfiles.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Hacer clic en **Desglose detallado** para ver cada carpeta individual que hubiera en la carpeta raíz del perfil (por ejemplo, C:/Usuarios/nombre de usuario), su tamaño y la cantidad de archivos (incluidos los archivos dentro de las carpetas anidadas).



Con la información desglosada del perfil, puede resolver problemas de tiempos de carga largos para los perfiles. Puede:

- 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, se ven los nombres de todas las carpetas. Para ocultar los nombres de las carpetas, modifique los valores de Registro en la máquina VDA siguiendo estos pasos:

> Advertencia:
>
> Si se modifica el Registro o se le agregan valores de forma incorrecta, se pueden generar problemas graves que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Cit-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> rix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

1. En el VDA, agregue el nuevo valor de Registro **ProfileFoldersNameHidden** a HKEY_LOCAL_MACHINE\Softwar
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 PowerShell para aplicar el cambio de valor del Registro a varias máquinas. Para obtener más información sobre el uso de GPO para implementar cambios en el Registro, consulte el blog.

Información adicional

- En el desglose de perfil no se tienen en cuenta las carpetas redirigidas.
- Puede que los usuarios finales no vean los archivos ntuser.dat de la carpeta raíz. Sin embargo, están incluidos en el desglose de perfil y se muestran en la lista de archivos de la **Carpeta raíz**.
- Hay algunos archivos ocultos en la carpeta AppData que no se incluyen en el desglose de perfil.
- Es posible que el número de archivos y los datos de tamaño de perfil no coincidan con los datos del panel de Personalización, debido a ciertas limitaciones de Windows.

Esta función está disponible en Delivery Controller 7 1811 o posterior y VDA 1811 o posterior.

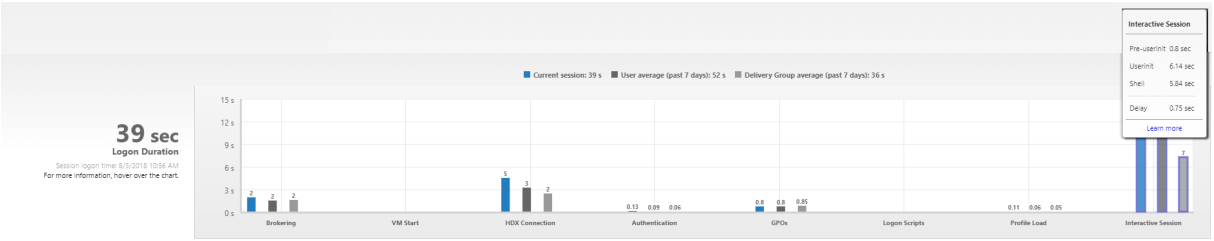
Sesión interactiva

Este es el tiempo que se tardó en entregar el control del mouse y el escritorio al usuario después de cargar el perfil de usuario. Suele ser la fase más larga de todas las fases de inicio de sesión y se calcula de este modo: **Duración de la sesión interactiva = Marca de hora del evento en el escritorio preparado (EventId 1000 en el VDA) - Marca de hora en el evento de perfil de usuario cargado (EventId 2 en el VDA)**. La fase Sesión interactiva está compuesta de tres subfases: Pre-userinit, Userinit y Shell. Al pasar el mouse sobre la sesión interactiva, se muestran las subfases, el tiempo empleado para cada una de ellas, el tiempo total de demora acumulada entre esas subfases y un enlace a la documentación. Esta función está disponible en Delivery Controller 7 1811 o posterior y VDA 1811 o posterior.
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:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

1. Cree un GPO y modifíquelo usando 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:** Este es el segmento de Sesión Interactiva que se superpone con los scripts y los objetos de directivas de grupo. Esta subfase se puede reducir optimizando los GPO y los scripts.
- **Sesión interactiva: Userinit:** Cuando un usuario inicia sesión en una máquina con Windows, Winlogon ejecuta userinit.exe. Userinit.exe ejecuta scripts de inicio de sesión, restablece las conexiones de red y luego inicia Explorer.exe, la interfaz de usuario de Windows. Esta subfase de Sesión interactiva representa la duración entre el inicio de Userinit.exe y el inicio de la interfaz de usuario para el escritorio o la aplicación virtual.
- **Sesión interactiva: Shell:** En la fase previa, Userinit comienza a inicializar la interfaz de usuario de Windows. La subfase Shell captura la duración entre la inicialización de la interfaz de usuario y la hora en que el usuario recibe el control del teclado y del mouse.
- **Demora:** Este es el tiempo de demora que se haya acumulado entre las subfases **Pre-userinit y Userinit** y las subfases **Userinit y Shell**.

El tiempo total de inicio de sesión no es exactamente la suma de esas fases. Por ejemplo, algunas fases se dan simultáneamente y, en otras fases, se llevan a cabo procesos adicionales que pueden llevar a una duración de inicio de sesión más larga que la suma de las fases.
El tiempo total del inicio de sesión no incluye el tiempo de inactividad de ICA; es decir, el tiempo transcurrido entre la descarga del archivo ICA y el inicio del archivo ICA para una aplicación.
Para habilitar la apertura automática del archivo ICA en el inicio de la aplicación, configure el navegador para que abra automáticamente el archivo ICA tras descargarlo. Para obtener más información, consulte CTX804493.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> 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.

Sugerencias para solucionar problemas

Para identificar valores poco habituales o inesperados en el gráfico, compare el tiempo tomado en cada fase de la sesión actual con los valores promedio para este usuario correspondientes a los últimos siete días, y los valores promedio para todos los usuarios del grupo de entrega, también correspondientes a los últimos siete días.

Si observa algún problema, remita la cuestión a otros administradores según sea necesario. Por ejemplo, si el inicio de la VM es lento, el problema puede estar en el hipervisor. En ese caso, contacte con el administrador del hipervisor. O bien, si la intermediación del broker es lenta, se puede remitir el problema al administrador del sitio para que compruebe el equilibrio de carga en el Delivery Controller.

Examine diferencias inusuales, como:

- Cuando falten barras de inicios de sesión (actuales)
- Discrepancias importantes entre los valores de duración actual y de duración promedio para un usuario. Las causas pueden ser:
  - Se ha instalado una nueva aplicación.
  - Se ha actualizado el sistema operativo.
  - Se realizaron cambios en la configuración.
  - El tamaño del perfil del usuario es muy grande. En este caso el valor de Carga del perfil puede ser alto.
- Discrepancias importantes entre los valores de inicios de sesión del usuario (duración actual y duración promedio) y el valor de duración promedio del grupo de entrega.

Si fuera necesario, haga clic en **Reiniciar** para observar el proceso de inicio de sesión del usuario y, así, solucionar problemas de intermediación con broker o inicio de VM.

Remedar usuarios

January 29, 2019

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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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 utilizando la Asistencia remota de Windows. Habilite la función Asistencia remota de Windows en la máquina del usuario durante la instalación del VDA. Para obtener más información, consulte la sección Habilitar o inhabilitar funciones en "Instalar agentes VDA".

1. Después de hacer clic en **Remedar**, se inicia la conexión de remedo y un cuadro de diálogo le pide que abra o guarde el archivo del incidente MSRC.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

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.

Envío de mensajes a los usuarios

October 3, 2018

Desde Director, puede enviar un mensaje a un usuario que está conectado a una o varias máquinas. Por ejemplo, puede usar esta característica para enviar notificaciones inmediatas acerca de acciones administrativas, tales como unas operaciones de mantenimiento de escritorios que están a punto de tener lugar, cierres de sesión y reinicios de máquinas y restablecimientos de perfiles.

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. Si la máquina del usuario está conectada, aparece el mensaje allí.

Si el mensaje no se envió correctamente, aparece un mensaje de error en Director. Solucione el problema de acuerdo con el mensaje de error. Cuando haya terminado, escriba el asunto y texto de mensaje de nuevo y haga clic en Intentar de nuevo.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Resolver fallos de aplicación

December 14, 2018

En la vista
Administrador de actividades, haga clic en la ficha
“Aplicaciones”. Puede ver todas las aplicaciones de todas las máquinas a las que el usuario tiene acceso, incluidas las aplicaciones locales y las alojadas para la máquina conectada actualmente, y el estado actual de cada una de ellas.

> Nota:
>
> Si la ficha”Aplicaciones” aparece atenuada, 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 escritorio o de servidor, 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 ha 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 fallarán.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Acción	Descripción
Reiniciar la máquina del usuario	Si se trata solo de máquinas con sistema operativo de escritorio, 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 de servidor, la opción de reinicio no está disponible. En vez de reiniciar, cierre la sesión del usuario y permita que el usuario inicie sesión de nuevo.
Colocar la máquina en modo de mantenimiento	Si la imagen de la máquina necesita mantenimiento (por ejemplo, instalar una revisión o actualización de software), colóquela en modo de mantenimiento. Desde la vista “Detalles de la máquina”, haga clic en “Detalles” y active el modo de mantenimiento. Remita la cuestión al administrador que corresponda.

Restaurar conexiones de escritorio

March 8, 2019

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Acción	Descripción
Reiniciar la máquina del usuario	Seleccione la máquina y haga clic en Reiniciar. Utilice esta opción si la máquina del usuario no responde o no puede conectarse a ella porque, por ejemplo, está utilizando una cantidad inusualmente alta de recursos de la CPU, lo que puede inutilizar la CPU.

Restaurar sesiones

March 8, 2019

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 responda 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 de servidor 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

usuario para supervisar más de cerca esta sesión.

> Nota:
>
> Si los dispositivos de usuario ejecutan agentes Virtual Delivery Agent (VDA) anteriores a XenDesktop 7, Director no puede mostrar información completa sobre la sesión; en vez de ello, se muestra un mensaje que indica que la información no está disponible. Estos mensajes pueden aparecer en la página
> Detalles del usuario y el
> Administrador de actividades.

Ejecutar informes de sistema de canales HDX

March 8, 2019

En la vista
"Detalles del usuario", puede consultar 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.

Los servicios de asistencia técnica de Citrix utilizan principalmente los informes del sistema de canales HDX para soluciones de problemas más complejas.

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 disco Personal vDisk

December 14, 2018

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Precaución: Al restablecer el disco, la configuración se revierte a los valores predeterminados de fábrica y todos los datos contenidos en él se eliminan, incluidas las aplicaciones. Los datos de perfil se conservan, a menos que se haya modificado el valor predeterminado de Personal vDisk (redirigir perfiles desde la unidad C:) o no se esté usando una solución externa para administrar perfiles.

Para restablecer el disco, la máquina que tiene el disco Personal vDisk debe estar ejecutándose; sin embargo, no es necesario que el usuario esté conectado en una sesión.

Esta opción está disponible solo para máquinas con sistema operativo de escritorio; está inhabilitada para las máquinas con sistema operativo de servidor.

1. En la vista Servicio de asistencia, elija la máquina de destino con sistema operativo de escritorio.
2. En esta vista o en el panel Personalización de la página Detalles del usuario, haga clic en Restablecer Personal vDisk.
3. Haga clic en Restablecer. Aparece un mensaje de advertencia para avisar al usuario de que su sesión se cerrará. Después de que la sesión del usuario se haya cerrado (en caso de que estuviera abierta), se reinicia la máquina.

Si el restablecimiento se realiza correctamente, el valor del campo Estado de Personal vDisk en el panel de Personalización de la página Detalles del usuario es En ejecución. Si el restablecimiento no se realiza correctamente, aparece una X de color rojo a la derecha del valor En ejecución. Cuando se sitúa el puntero sobre la X, aparece información sobre el fallo.

Restablecer un perfil de usuario

March 14, 2019

Precaución: Cuando se restablece un perfil, aunque las carpetas y los archivos del usuario se guarden y se copian al nuevo perfil, la mayor parte de los datos del perfil se eliminan (por ejemplo, el Registro se restablece y los parámetros de aplicaciones podrían eliminarse).

1. Desde Director, busque al usuario cuyo perfil quiere restablecer y seleccione la sesión de ese usuario.
2. Haga clic en **Restablecer perfil**.
3. Indique al usuario que cierre todas las sesiones.
4. Indique al usuario que vuelva a iniciar sesión. Las carpetas y archivos del perfil de usuario que se guardaron, se copian en el nuevo perfil.

> Importante:
>
> Si el usuario tiene perfiles en varias plataformas (por ejemplo, en Windows 8 y en Windows 7), indíquele que inicie sesión primero en el mismo escritorio o aplicación que notificó

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> como un problema. Esto garantiza el restablecimiento del perfil adecuado. Si el perfil es un perfil de usuario de Citrix, el perfil se habrá restablecido para cuando aparezca el escritorio del usuario. Si el perfil es un perfil móvil 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.

> Nota:
>
> En los pasos anteriores, se presupone que está usando Citrix Virtual Desktops (VDA de escritorio). Si está usando Citrix Virtual Desktops (VDA de servidor) necesitará tener una sesión iniciada para realizar el restablecimiento del perfil. El usuario tiene que cerrar la sesión y volver a iniciarla para completar el restablecimiento del perfil.

Si el perfil no se restablece correctamente (por ejemplo, el usuario no puede volver a iniciar la sesión en la máquina o faltan algunos archivos), debe restaurar manualmente el perfil original.

Las carpetas (y sus archivos) del perfil del usuario se guardan y se copian en el nuevo perfil. Se copian por este orden:

- Escritorio
- Cookies
- Favoritos
- Documentos
- Imágenes
- Música
- Vídeos

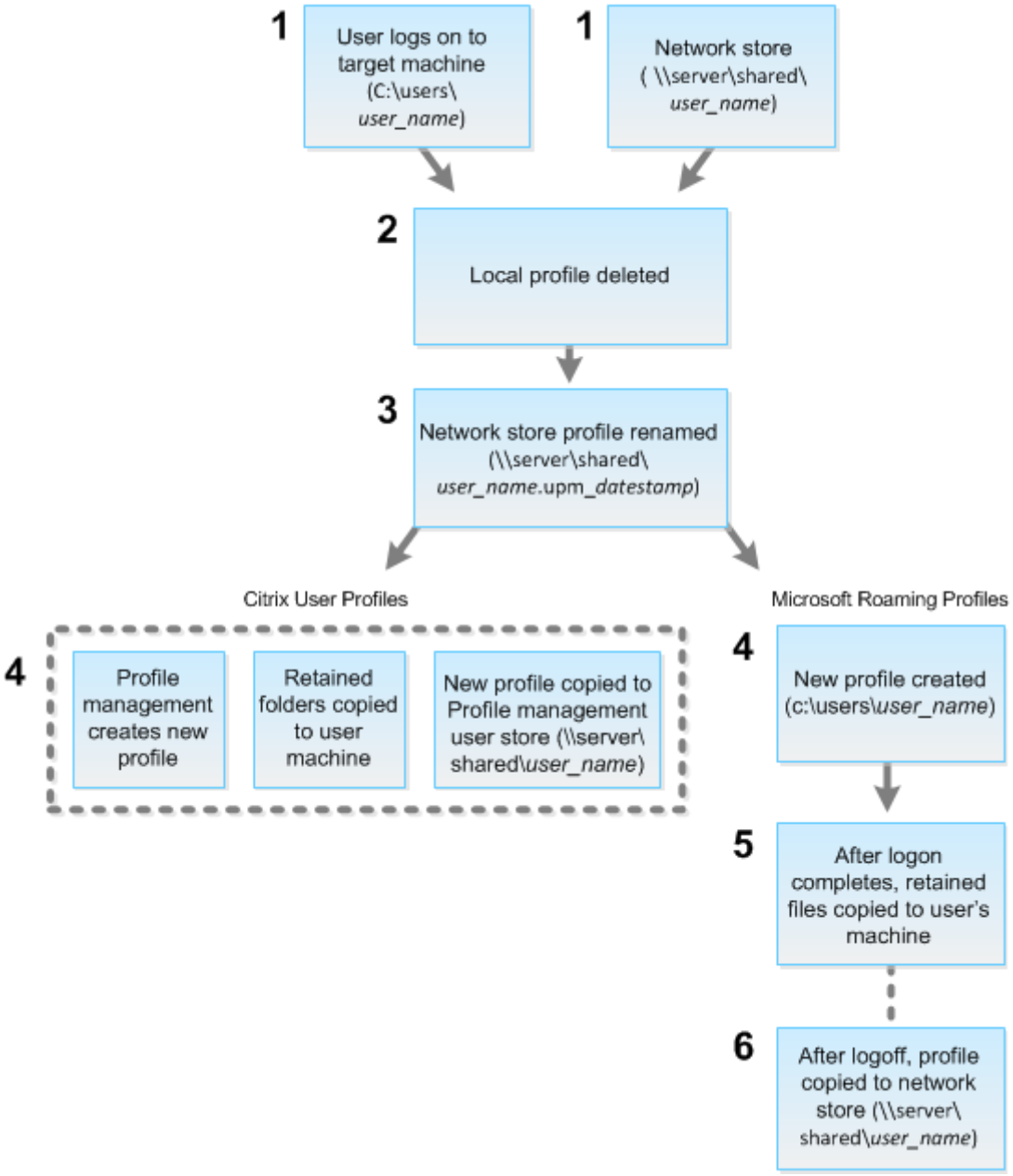
> Nota:
>
> En Windows 8 y versiones posteriores, las cookies no se copian cuando los perfiles se restablecen.

Cómo se procesan los perfiles restablecidos

Es posible restablecer cualquier perfil de usuario de Citrix o perfil móvil 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



El comando de restablecimiento emitido por Director especifica el tipo de perfil. Después, el servicio de Profile Management intenta restablecer un perfil de ese tipo y busca el recurso compartido de red (el almacén de usuarios). Si el usuario está procesado por Profile Management, pero recibe un comando de perfil móvil, 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 móvil de Microsoft.
    - Para los perfiles de usuario de Citrix, el nuevo perfil se crea usando las reglas de im-

© 1999-2019 Citrix Systems, Inc. All rights reserved.

portación de Profile Management, y las carpetas se copian de vuelta en el perfil de red, y el usuario puede iniciar una sesión como lo hace normalmente. Si se usa un perfil móvil para el restablecimiento, los parámetros de Registro en el perfil móvil se conservan en el perfil restablecido.

> Nota:
> Si es necesario, puede configurar Profile Management para que un perfil de plantilla sobrescriba el perfil móvil.

- Para los perfiles móviles de Microsoft, Windows crea un nuevo perfil y cuando el usuario inicia una sesión, las carpetas se copian de vuelta en el dispositivo de usuario. Cuando el usuario cierra la sesión de nuevo, el nuevo perfil se copia en el almacén de la red.

Para restablecer un perfil manualmente después de un error de restablecimiento

1. Indique al usuario que cierre todas las sesiones.
2. Elimine el perfil local si existe.
3. Busque la carpeta archivada en el recurso compartido de red que contiene la fecha y hora junto con el nombre de la carpeta, la carpeta con la extensión .upm_fechayhora.
4. Elimine el nombre del perfil actual; es decir, el que no tiene la extensión .upm_fechayhora.
5. Cambie el nombre de la carpeta archivada utilizando el nombre de perfil original; es decir, elimine la extensión de fecha y hora. Con ello, habrá devuelto el perfil a su estado original, prerestablecido.

Grabar sesiones

December 14, 2018

En Director, puede grabar sesiones ICA mediante los controles de la función Grabación de sesiones, desde las pantallas **Detalles del usuario** y **Detalles de la máquina**. Esta función está disponible para los clientes de los sitios con licencia **Premium**.

Para configurar la Grabación de sesiones en Director mediante la herramienta DirectorConfig, consulte la sección **Configurar Director para usar el Servidor de grabación de sesiones** en Crear y activar directivas de grabación.
Los controles de la Grabación de sesiones solo están disponibles en Director si el usuario que ha iniciado sesión tiene el permiso para modificar las directivas de la Grabación de sesiones. Este permiso puede establecerse en la consola de autorización de la Grabación de sesiones, como se describe en Crear y activar directivas de grabación.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

> Nota:
>
> Los cambios realizados en los parámetros de la Grabación de sesiones a través de Director o la Consola de directivas de grabación de sesiones surten efecto a partir de la siguiente sesión ICA.

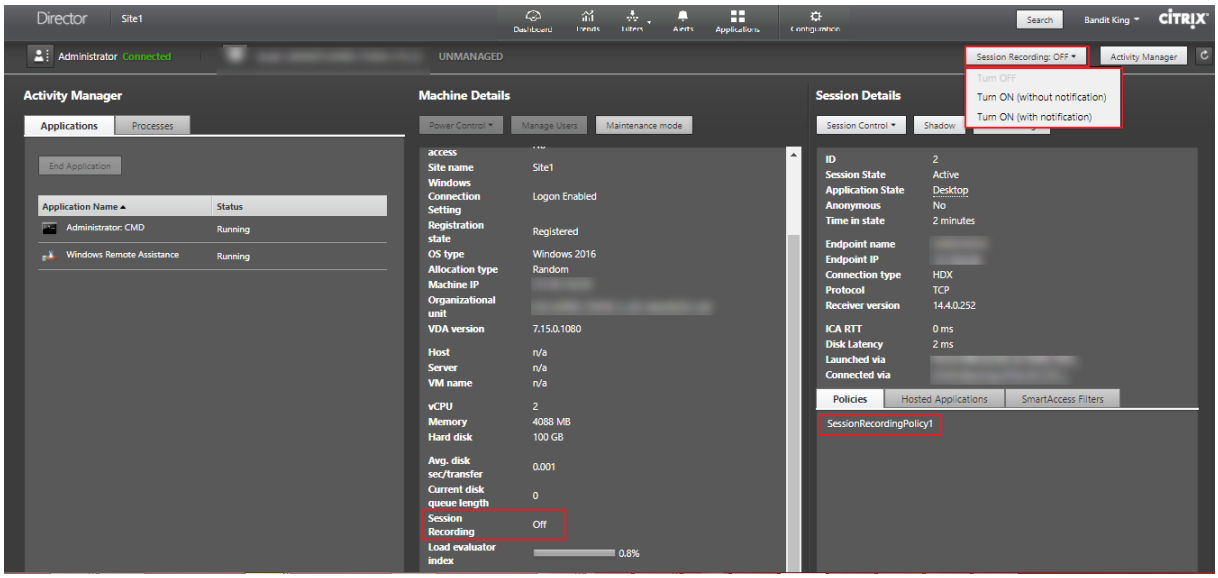
Controles de Grabación de sesiones en Director

Puede habilitar la Grabación de sesiones para un usuario específico desde la pantalla **Administrador de actividades** o **Detalles del usuario**. Las sesiones subsiguientes de ese usuario específico se grabarán en todos los servidores respaldados.

Puede:

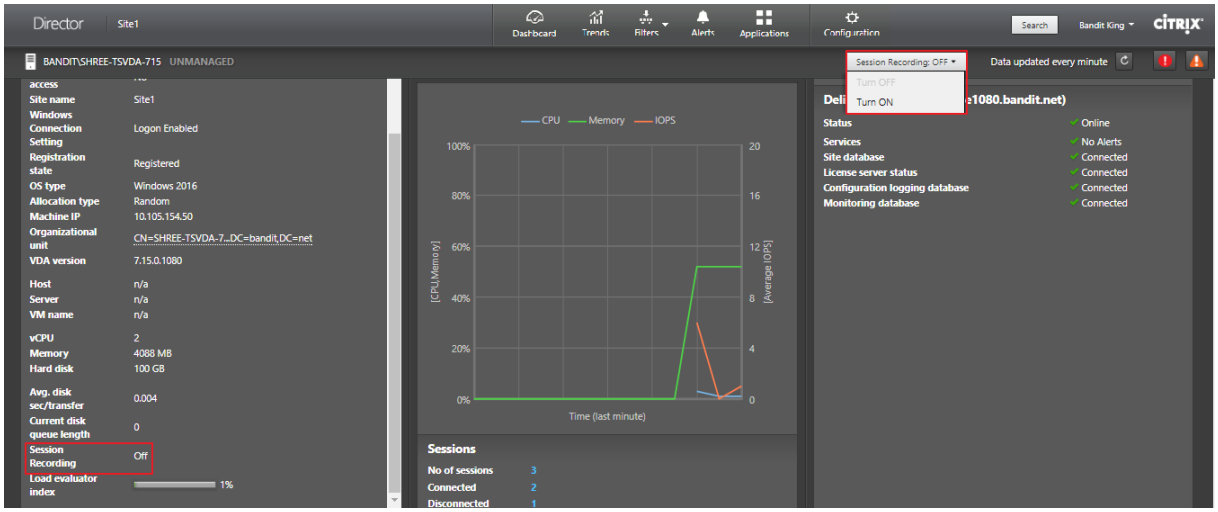
- Activar (con notificación): Se notifica al usuario de que la sesión se está grabando cuando este inicia una sesión ICA.
- Activar (sin notificación): La sesión se graba de forma silenciosa, sin notificar al usuario.
- Desactivar: Inhabilitar la grabación de las sesiones del usuario.

El nombre de la directiva activa de Grabación de sesiones aparece en el panel Directivas.



Puede habilitar la Grabación de sesiones para una máquina específica desde la página Detalles de la máquina. Se grabarán las sesiones subsiguientes de la máquina. El panel Detalles de la máquina muestra el estado de la directiva Grabación de sesiones de la máquina.

© 1999-2019 Citrix Systems, Inc. All rights reserved.



Matriz de compatibilidad de funciones

March 8, 2019

Citrix Director 1811 es compatible con:

- Citrix Virtual Apps and Desktops 7 1808 y versiones posteriores
- XenApp y XenDesktop 7.18 y 7.15 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 un Delivery Controller, se le solicitará que actualice el sitio cuando abra Studio. Para obtener más información, consulte **Secuencia de actualización** en Actualizar una implementación.

La primera vez que inicie sesión después de una actualización de Director, se realiza una comprobación de versión en los sitios configurados. Si un sitio ejecuta una versión de Controller anterior a la de Director, aparece un mensaje en la consola de Director, donde se recomienda actualizar el sitio. Además, mientras la versión del sitio sea anterior a la de Director, aparecerá una nota en el panel de mandos de Director donde se indicará la diferencia de versiones.

A continuación, se presentan las características específicas de Director con la versión mínima de Delivery Controller (DC), VDA y otros componentes dependientes requeridos, junto con la edición de las licencias.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Versión de Director	Función	Dependencias: versión mínima requerida	Edición
1811	Desglose de perfil	DC 7 1811 y VDA 1811	Todas
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 la licencia RDS de Microsoft	DC 7 1811 y VDA 7.16	Todas
1811	Datos clave RTOP	DC 7 1811 y VDA 1808	Premium
1808	Exportar datos de filtros	DC 7 1808	Todas
1808	Desglose de la sesión interactiva	DC 7 1808 y VDA 1808	Todas
1808	Desglose de GPO	DC 7 1808 y VDA 1808	Todas
1808	Datos históricos disponibles de la máquina usando la API de OData	DC 7 1808	Todas
7.18	Sondeo de aplicaciones	DC 7.18	Platinum
7.18	Directivas de alertas inteligentes	DC 7.18	Platinum
7.18	Enlace de Health Assistant	Ninguna	Todas
7.18	Desglose de la sesión interactiva	Ninguna	Todas
7.17	Autenticación con tarjetas inteligentes PIV	Ninguna	Todas
7.16	OData API 4	DC 7.16	Todas
7.16	Remedar usuarios en Linux VDA	VDA 7.16	Todas

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Versión de Director	Función	Dependencias: versión mínima requerida	Edición
7.16	Admitir el grupo local de dominio	Ninguna	Todas
7.16	Acceder a la consola de la máquina	DC 7.16	Todas
7.15	Supervisar fallos de aplicación	DC 7.15 y VDA 7.15	Todas
7.14	Solucionar problemas de aplicación	DC 7.13 y VDA 7.13	Todas
7.14	Supervisar discos	DC 7.14 y VDA 7.14	Todas
7.14	Supervisar GPU	DC 7.14 y VDA 7.14	Todas
7.13	Protocolo de transporte en el panel “Detalles de la sesión”	DC 7.x y VDA 7.13	Todas
7.12	Descripciones claras de los errores de conexión y de máquina	DC 7.12 y VDA 7.x	Todas
7.12	Mayor disponibilidad de datos históricos en la edición Enterprise	DC 7.12 y VDA 7.x	Enterprise
7.12	Informes personalizados	DC 7.12 y VDA 7.x	Platinum
7.12	Automatizar notificaciones de Director con capturas de SNMP	DC 7.12 y VDA 7.x	Platinum
7.11	Informes de utilización de recursos	DC 7.11 y VDA 7.11	Todas

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Versión de Director	Función	Dependencias: versión mínima requerida	Edición
7.11	Alertas extendidas para condiciones de CPU, memoria e ICA RTT	DC 7.11 y VDA 7.11	Platinum
7.11	Mejoras en la exportación de informes	DC 7.11 y VDA 7.x	Todas
7.11	Automatizar notificaciones de Director con Citrix Octoblu	DC 7.11 y VDA 7.x	Platinum
7.11	Integración en Citrix ADM	DC 7.11, VDA 7.x y MAS versión 11.1, compilación 49.16	Platinum
7.9	Desglosar la duración del inicio de sesión	DC 7.9 y VDA 7.x	Todas
7.7	Supervisión y alertas mejoradas	DC 7.7 y VDA 7.x	Platinum
7.7	Integrar en SCOM	DC 7.7, VDA 7.x, SCOM 2012 R2 y PowerShell 3.0	Platinum
7.7	Integrar en Autenticación de Windows	DC 7.x y VDA 7.x	Todas
7.7	Usar SO de escritorio y servidor	DC 7.7 y VDA 7.x	Platinum
7.6.300	Compatibilidad con canal virtual Framehawk	DC 7.6 y VDA 7.6	Todas
7.6.200	Integrar en la Grabación de sesiones	DC 7.6 y VDA 7.x	Platinum

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Versión de Director	Función	Dependencias: versión mínima requerida	Edición
7	Integrar en HDX Insight	DC 7.6, VDA 7.x y Citrix ADM	Platinum

Granularidad y retención de datos

January 29, 2019

Agregar valores de datos

Monitor Service recopila una serie de datos, incluidos el uso de las sesiones de usuario, la información del rendimiento de los inicios de sesión de usuario, la información del equilibrio de carga de las sesiones y la información de fallos de conexión y de las máquinas. Los datos se agregan de forma diferente en función de la categoría. Para interpretar los datos, es fundamental comprender la agregación de los valores de los datos presentados mediante las API de Método de OData. Por ejemplo:

- Los errores de máquinas y sesiones conectadas se producen durante un período de tiempo. Por lo tanto, se exponen como máximos a lo largo de un período de tiempo.
- La duración del inicio de sesión es una medida de tiempo, por lo que se expone como el promedio en las métricas tomadas a lo largo de un período de tiempo.
- Los recuentos de inicio de sesión y los fallos de conexión son el número de casos a lo largo de un período de tiempo, por lo que se exponen como sumas para un período de tiempo.

Evaluar datos simultáneos

Las sesiones deben superponerse para considerarse simultáneas. No obstante, cuando el intervalo de tiempo es de 1 minuto, todas las sesiones en ese minuto (se superpongan o no) se consideran simultáneas; es decir, el tamaño del intervalo es tan pequeño que se considera que el esfuerzo de rendimiento que conlleva un cálculo más preciso no añade mucho valor. Si las sesiones se producen en la misma hora, pero no en el mismo minuto, no se consideran superpuestas.

Correlacionar tablas de resumen con datos sin procesar

El modelo de datos representa las métricas de dos maneras diferentes:

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- Las tablas de resumen representan vistas agregadas de las métricas por minuto, por hora y por día.
- Los datos sin procesar representan eventos individuales o de estado actual de seguimiento de una sesión, conexión, aplicación y otros objetos.

Al intentar establecer una correlación entre las llamadas de la API o en el modelo de datos mismo, es importante comprender los conceptos y las limitaciones siguientes:

- **No hay datos de resumen para intervalos parciales.** Los resúmenes de métricas están diseñados para satisfacer las necesidades de tendencias históricas en períodos de tiempo prolongados. Estas métricas se agregan en la tabla de resumen para intervalos completos. No habrá datos de resumen para un intervalo parcial al comienzo (en los datos más antiguos) de la recopilación de datos ni al final de la misma. Cuando se consultan los datos agregados de un día (Intervalo=1440), esto significa que los días incompletos al principio y los más recientes no tendrán datos. Aunque es posible que existan datos sin formato para esos intervalos parciales, estos datos no se resumirán. Para determinar el intervalo combinado más antiguo y más reciente para una granularidad de datos en particular, se puede usar la fecha de resumen (SummaryDate) máxima y mínima de una tabla de resumen. La columna SummaryDate representa el inicio del intervalo. El valor de la columna Granularity representa la duración del intervalo para los datos agregados.
- **Correlación por tiempo.** Las métricas se agregan en la tabla de resumen para intervalos completos, como se ha descrito antes. Se pueden usar para descubrir tendencias históricas, pero los eventos sin procesar pueden ser más actualizados en los datos de estado que lo que se resumió para el análisis de tendencias. En cualquier comparación basada en el tiempo entre datos de resumen y datos sin procesar, hay que tener en cuenta que no habrá datos de resumen para intervalos parciales que puedan ocurrir ni para el comienzo o el final del periodo de tiempo en cuestión.
- **Eventos latentes y perdidos.** Las métricas agregadas en tablas de resumen pueden ser ligeramente inexactas si hay eventos perdidos o latentes en el periodo de agregación. Aunque Monitor Service intenta mantener un alto nivel de precisión del estado actual, no vuelve atrás en el tiempo para recalcular la agregación en las tablas de resumen para eventos perdidos o latentes.
- **Alta disponibilidad de conexiones.** Durante la alta disponibilidad de conexiones, habrá huecos en los datos de resumen sobre los recuentos de las conexiones actuales, pero las instancias de sesión seguirán ejecutándose en los datos sin procesar.
- **Períodos de retención de datos.** Los datos de las tablas de resumen se conservan siguiendo una programación de limpieza distinta de la programación para datos de eventos sin procesar. Puede que falten datos porque se hayan limpiado las tablas de resumen y de datos sin procesar. Los períodos de retención también pueden diferir según las distintas granularidades de los datos de resumen. Una granularidad de datos menor (minutos) se limpia más rápidamente que una granularidad de datos mayor (días). Si faltan datos de una granularidad debido a una

© 1999-2019 Citrix Systems, Inc. All rights reserved.

limpieza, puede 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 periodo de tiempo.

- **Zonas horarias.** Las métricas se guardan con marcas de hora UTC. Las tablas de resumen se agregan en límites de una hora de la zona horaria. Para las zonas horarias que no caen en límites de una hora, puede haber una discrepancia en cuanto a dónde se agregan los datos.

Granularidad y retención

La granularidad de los datos agregados obtenida por Director es una función del intervalo de tiempo (T) solicitado. Las reglas son las siguientes:

- 0 < T < = 1 hora, se utiliza granularidad de minutos
- 0 < T <= 30 días, se utiliza granularidad de horas
- T > 31 días, se utiliza granularidad de días

Los datos solicitados que no provienen de datos agregados provienen de la información sin procesar sobre sesiones y conexiones. Estos datos tienden a aumentar rápidamente y, por lo tanto, tienen su propia configuración de limpieza. La limpieza de la base de datos garantiza que solo se conserven los datos que sean relevantes a largo plazo. Esto garantiza un mejor rendimiento, al tiempo que se mantiene la granularidad necesaria para crear informes. Los clientes de Premium pueden cambiar la retención de limpieza por la cantidad de días de retención que quieran; si no la cambian, se usa la predeterminada.

Para acceder a los parámetros, ejecute los siguientes comandos de PowerShell en el Delivery Controller:

```
asnp Citrix.*
 Get-MonitorConfiguration
 Set-MonitorConfiguration -<setting name> <value>
```

© 1999-2019 Citrix Systems, Inc. All rights reserved.

	Nombre del parámetro	Limpieza afectada	Valor predeterminado (días) con Premium	Valor predeterminado (días) sin Premium
1	GroomSessionsRe	Retención de registros de conexión y de sesión después de cerrar la sesión	90	7
2	GroomFailuresRetentionDays	Registros de MachineFailureLog y ConnectionFailureLog	90	7
3	GroomLoadIndexe	Registros de LoadIndex	90	7
4	GroomDeletedRetentionDays	Entidades de máquina, catálogo de máquinas, grupo de escritorios e hipervisor cuyo estado de ciclo de vida (LifecycleState) es “Eliminado” (Deleted). Esta acción también elimina los registros de Session, SessionDetail, Summary, Failure o LoadIndex relacionados.	90	7

© 1999-2019 Citrix Systems, Inc. All rights reserved.

	Nombre del parámetro	Limpieza afectada	Valor predeterminado (días) con Premium	Valor predeterminado (días) sin Premium
5	GroomSummaries	Registros de DesktopGroup-Summary, FailureLogSummary y LoadIndexSummary. Datos agregados, de granularidad diaria.	90	7
6	GroomMachineHotfixLogRetentionDays	Registros de hotfix aplicadas a las máquinas de VDA y Controllers	90	90
7	GroomMinuteRete	Datos agregados, de granularidad de minuto	3	3
8	GroomHourlyRetentionDays	Datos agregados: granularidad horaria	32	7
9	GroomApplication	Historial de instancia de aplicación	90	0
10	GroomNotificationLogRetentionDays	Registros del registro de notificaciones	90	
11	GroomResourceUs	Datos de utilización de recursos: datos sin procesar	1	1

© 1999-2019 Citrix Systems, Inc. All rights reserved.

	Nombre del parámetro	Limpieza afectada	Valor predeterminado (días) con Premium	Valor predeterminado (días) sin Premium
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	7
14	GroomResourceUsageDayDataRetentionDays	Datos resumidos de utilización de recursos: granularidad de día	90	7
15	GroomProcessUsageRawDataRetentionDays	Datos de utilización de procesos: datos sin procesar	1	1
16	GroomProcessUsageMinuteDataRetentionDays	Datos de utilización de procesos: granularidad de minuto	3	3
17	GroomProcessUsageHourDataRetentionDays	Datos de utilización de procesos: granularidad de hora	7	7

© 1999-2019 Citrix Systems, Inc. All rights reserved.

	Nombre del parámetro	Limpieza afectada	Valor predeterminado (días) con Premium	Valor predeterminado (días) sin Premium
18	GroomProcessUsageRawDataRetentionDays	Datos de utilización de procesos: granularidad de día	30	7
19	GroomSessionMet	Datos de métricas de sesiones	7	7
20	GroomMachineMetricsDataRetentionDays	Datos de métricas de máquinas	3	3
21	GroomMachineMe	Datos resumidos de métricas de máquinas	90	7
22	GroomApplicationEventsRetentionDays	Datos de eventos de aplicaciones	1	1
23	GroomApplication	Datos de fallos de aplicaciones	1	1

Precaución: La modificación de los valores en la base de datos del servicio de supervisión (Monitor Service) requiere reiniciar el servicio para que los nuevos valores tengan 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.

Notas sobre la retención de limpieza:
GroomProcessUsageRawDataRetentionDays y GroomProcessUsageMinuteDataRetentionDays se limitan a sus valores predeterminados de 1 y 3 días, respectivamente. Los comandos de PowerShell para establecer estos valores se han inhabilitado, ya que los datos de uso del proceso tienden a crecer con rapidez.
Además, los parámetros de la retención basada en licencia son los siguientes:

- **Sitios con licencias Premium:** Se puede actualizar la configuración de retención de limpieza de datos con cualquier cantidad de días.
- **Sitios con licencias Advanced:** La retención de limpieza de datos para todos los parámetros se limita a 31 días.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

- **Todos los demás sitios:** La retención de limpieza de datos para todos los parámetros se limita a 7 días.

Excepciones:

- GroomApplicationInstanceNetentionDays sólo 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 periodos de tiempo tiene las implicaciones siguientes en los tamaños de las tablas:

- **Datos por hora.** Si se conservan datos por hora en la base de datos durante dos años, un sitio con 1000 grupos de entrega puede hacer que la base de datos crezca así:

  1000 grupos de entrega x 24 horas/día x 365 días/año x 2 años = 17 520 000 filas de datos. El impacto que esta gran cantidad de datos tiene en el rendimiento de las tablas agregadas es importante. Puesto que los datos de panel de mandos se sacan de esta tabla, los requisitos del servidor de la base de datos pueden ser altos. Si la cantidad de datos es excesiva, el impacto en el rendimiento puede resultar significativo.

- **Datos de sesiones y eventos.** Estos datos se recopilan cada vez que comienza una sesión y se realiza una conexión o reconexión. En sitios grandes (100 000 usuarios), estos datos pueden crecer muy rápidamente. Por ejemplo, las tablas correspondientes a dos años recopilarían más de un TB de datos, para lo cual se necesitaría una base de datos de nivel empresarial de gama alta.

SDK y API

December 4, 2018

Se ofrecen varios SDK y API en esta versión. Para obtener más información, consulte Developer Documentation. Desde allí, puede acceder a información de programación de:

- Delivery Controller
- OData de Monitor Service
- StoreFront

Citrix Group Policy SDK permite visualizar y configurar los filtros y las configuraciones de directivas de grupo. 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. Consulte la siguiente sección Group Policy SDK para obtener más información.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Delivery Controller SDK

El SDK se compone de una serie de complementos de PowerShell que se instalan automáticamente al instalar el Delivery Controller o Studio.

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.

Para 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 más información acerca de la directiva de ejecución de PowerShell, consulte la documentación de Microsoft.
3. Agregue los complementos que necesite en el entorno de PowerShell con el `Add -PSSnapin` cmdlet Add -PSSnapin en la consola de Windows PowerShell.

   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*`

Después de agregar los complementos, puede acceder a los cmdlets y a la ayuda asociada.

Para ver la ayuda de los cmdlets actuales de PowerShell para Citrix Virtual Apps and Desktops:

1. Desde la consola de PowerShell, agregue los complementos de Citrix: `Add -PSSnapin Citrix.*.Admin.V*`
2. Siga las instrucciones indicadas en Entorno de scripting integrado (ISE) de PowerShell.

Group Policy SDK

Para utilizar Group Policy SDK, es necesario tener instalado Studio o el SDK de Citrix Virtual Apps and Desktops.

Para agregar Group Policy SDK, 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.

cadena de Controller es el nombre de dominio completo de un Controller en el sitio al que quiere conectarse y del que quiere cargar la configuración.

OData de Monitor Service

La API de Monitor permite el acceso a los datos de Monitor Service utilizando la versión 3 o 4 de la OData API. 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

© 1999-2019 Citrix Systems, Inc. All rights reserved.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2019 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).